SCHLESWIG-HOLSTEINISCHER LANDTAG **Drucksache 15/870**
15. Wahlperiode 01.04.24

Bericht

**des Unabhängigen Landeszentrums
für den Datenschutz Schleswig-Holstein**

Tätigkeitsbericht 2001

Tätigkeitsbericht 2001

des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

Berichtszeitraum: 2000, Redaktionsschluss: 16.03.2001
Landtagsdrucksache 15/870

(23. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz)

Dr. Helmut Bäumler
Leiter des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein, Kiel

Inhaltsverzeichnis **Seite**

1 Situation des Datenschutzes in Schleswig-Holstein

1.1 Das neue LDSG auf dem Stand der Technik

Durch das neue Landesdatenschutzgesetz (LDSG), das am 01.07.2000 in Kraft getreten ist, wurde ein „datenschutzpolitisches Signal“ gesetzt, weil es nicht nur die Europäische Datenschutzrichtlinie umsetzt, sondern auch ein zeitgemäßes Datenschutzkonzept verkörpert. Die Kombination von materiellen Verarbeitungsvorschriften, technikoffenen Datensicherheitsbestimmungen, der Gewährleistung einer unabhängigen Datenschutzkontrolle sowie von Beratung, Service und Prävention als integrale Bestandteile eines effizienten Grundrechtsschutzes hat sich schon in den ersten Monaten nach In-Kraft-Treten des Gesetzes bewährt. Auf dieser Grundlage hat der Datenschutz eine reelle Chance, über die Rolle des nachträglich Kritisierenden hinauszuwachsen und an der **Gestaltung der Informationsgesellschaft** im Interesse der Privatsphäre der Bürgerinnen und Bürger aktiv mitzuwirken. Offensichtlich liegt das Gesetz auch mit seinen Bestimmungen zum Systemdatenschutz richtig, die Reaktionen aus den Reihen der Praktiker sind jedenfalls positiv (vgl. Tz. 7.1).

Zu beobachten ist allerdings eine gewisse Zurückhaltung der Behörden bei der Bestellung **behördlicher Datenschutzbeauftragter** nach § 10 LDSG. Lediglich die Polizei in Schleswig-Holstein nimmt hier bislang eine Vorreiterrolle ein. Manche Behördenchefs scheinen dagegen dem Irrtum zu unterliegen, aus der Tatsache, dass das Gesetz die Bestellung behördlicher Datenschutzbeauftragter nicht zwingend vorschreibt, sei zu folgern, auch im Übrigen sei die Beachtung des LDSG mehr oder weniger eine freiwillige Angelegenheit. Dem ist natürlich nicht so. Die Kompetenz zur Erfüllung der datenschutzrechtlichen Anforderungen muss in jedem Falle bei allen öffentlichen Stellen im Lande vorhanden sein. Vieles spricht dafür, dann gleich einen kompetenten, gut ausgebildeten Datenschutzbeauftragten zu bestellen, der der Behördenleitung über den eigentlichen Datenschutz hinaus bei der revisionssicheren Beherrschung der Informationstechnik von großem Nutzen ist (vgl. Tz. 4.1.1). Wird ein behördlicher Datenschutzbeauftragter nicht bestellt, so sind nach den zwingenden Vorgaben der Europäischen Datenschutzrichtlinie alle sensiblen Verarbeitungsverfahren dem Unabhängigen Landeszentrum zur **Vorabkontrolle** nach § 9 LDSG vorzulegen – eine Tatsache, die vielen Behörden bislang offenbar noch gar nicht bewusst ist. Hier ist angesichts der Risiken der elektronischen Datenverarbeitung auf die gelegentlich gestellte Frage, wie viel die Bestellung eines behördlichen Datenschutzbeauftragten kostet, die Gegenfrage zu stellen: Wie viel kann die unterlassene Bestellung eines Datenschutzbeauftragten kosten?

Das Landesdatenschutzgesetz enthält erstmals Bestimmungen zum **Datenschutzaudit** für Behörden und zu **Gütesiegeln** für IT-Produkte. Weil anderswo noch über diese Themen kleinlich gezankt wird, kann sich für die schleswig-holsteinische Wirtschaft und Verwaltung aus Datenschutzaudit und Gütesiegel ein Standortvorteil ergeben.

Das **Datenschutzaudit** kann bei öffentlichen Stellen entweder für die gesamte Datenverarbeitung, für Teile davon oder für einzelne Verfahren durchgeführt werden. Die Behörden haben ihr Datenschutzkonzept zusammen mit weiteren Unterlagen beim Unabhängigen Landeszentrum für Datenschutz zur Prüfung vorzulegen. Ist das Auditverfahren erfolgreich durchlaufen, so erteilt das ULD ein Prüfzeichen, mit dem die Behörde offensiv „werben" kann, z. B. bei den Bürgerinnen und Bürgern oder bei den eigenen Mitarbeitern. Gegenüber den bisherigen Formen der Beratung und Vorabbeteiligung des ULD bei Automationsvorhaben bietet das Datenschutzaudit drei Vorteile:

- Das Votum des ULD bezieht sich auf ein gesamtes Verfahren und nicht nur auf einzelne vorgelegte Teilaspekte.
- Das Audit des ULD ist verbindlich und kann „im Geschäftsverkehr" verwendet werden. Es schafft Rechtssicherheit und wandelt das Datenschutzthema von einer lästigen Obliegenheit zu einem positiven Werbefaktor.
- Ein Datenschutzaudit wird erteilt, wenn ein Konzept vorliegt, das die Einhaltung des Datenschutzes auch über den Zeitpunkt der Auditierung hinaus garantiert.

Nicht zu verwechseln mit dem Audit ist das **IT-Gütesiegel**, das es den Behörden erleichtern soll, solche Produkte zu finden, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit, insbesondere auch mit den Grundsätzen der Datenvermeidung und der Datensparsamkeit in einem förmlichen Verfahren festgestellt wurde. § 4 LDSG macht es den öffentlichen Stellen im Lande zur Pflicht, vorrangig solche Produkte einzusetzen. Die Verordnung der Landesregierung sieht vor, dass beim ULD akkreditierte Gutachter die Zertifizierung von Produkten durchführen. Sie haben ihr Gutachten beim ULD vorzulegen, das eine Nachprüfung unter den Aspekten der Schlüssigkeit und methodischen Korrektheit vornimmt. Verläuft die Nachprüfung positiv, dann verleiht das ULD ein Gütesiegel, das befristet werden kann. Hierdurch haben die öffentlichen Stellen die Gewissheit, dass das Zertifizierungsverfahren korrekt abgelaufen ist. Da auch für die Verbraucher ein von einer unabhängigen staatlichen Stelle verliehenes Gütesiegel einen hohen Vertrauenswert hat, ist zu erwarten, dass die vom ULD verliehenen Gütesiegel nicht nur bei den Behörden, sondern generell auf dem IT-Markt Beachtung finden werden.

Weitere Informationen zum IT-Gütesiegel und zum Datenschutzaudit des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein unter:

www.datenschutzzentrum.de/guetesiegel/ und
www.datenschutzzentrum.de/audit/

Schleswig-Holstein ist das einzige Bundesland, dass die gesetzlichen Regelungen zur Datensicherheit um Ordnungsmäßigkeitskriterien in einer **Datenschutzverordnung** ergänzt hat. Da einige Bestimmungen der seit 1994 gültigen Landesverordnung in das LDSG übernommen worden sind und einige andere Regelungen an die neuen technischen Gegebenheiten anzupassen waren, ist sie einem „Face-

lifting“ unterzogen worden. Sie konnte, wie das LDSG auch, insgesamt verschlankt werden. Nach wie vor gilt der Grundsatz, dass automatisierte Verfahren nur dann als ordnungsgemäß angesehen werden können, wenn die Datenverarbeitung rechtlich zulässig ist, ein Sicherheitskonzept besteht und die Verfahren getestet, freigegeben und dokumentiert sind. Damit behält auch die neue Datenschutzverordnung die bewährte Grundstruktur bei, die bei Praktikern längst Akzeptanz gefunden hat.

Um die Anwendung des neuen Landesdatenschutzgesetzes zu erleichtern, wurden allen Behörden kurz nach In-Kraft-Treten entsprechende Unterlagen zugeleitet. Die Behördenleiter wurden zudem in einem „Chefschreiben“ auf die zehn wichtigsten Neuerungen hingewiesen. Zugleich wurde in der Reihe „Datenschutz leicht gemacht“ eine Broschüre unter dem Titel „**Tipps und Hinweise** zur Anwendung des neuen Landesdatenschutzgesetzes“ herausgegeben. Die DATENSCHUTZAKADEMIE Schleswig-Holstein nahm insgesamt 20 Sonderkurse in ihr Programm auf, in denen die Mitarbeiterinnen und Mitarbeiter der öffentlichen Stellen mit den wesentlichen Neuerungen vertraut gemacht wurden.

www.datenschutzzentrum.de/recht/dsleicht/
www.datenschutzzentrum.de/akademie/

1.2 Datenschutz aus einer Hand

Mit dem In-Kraft-Treten des neuen Landesdatenschutzgesetzes wurden auch die Aufgaben der Datenschutzaufsicht im nichtöffentlichen Bereich vom Innenministerium des Landes Schleswig-Holstein auf das Unabhängige Landeszentrum für Datenschutz übertragen. Durch die **Konzentration der Kräfte** und die **Bündelung der Aufgaben** sollen Synergieeffekte erzielt werden. Dies ist notwendig, denn seit der Schaffung der Datenschutzgesetze haben sich die Gewichte deutlich verschoben: War früher das Hauptaugenmerk auf die Datenverarbeitung staatlicher Stellen gerichtet, so vermuten heute viele Bürgerinnen und Bürger nicht ganz zu Unrecht, dass der „Big Brother“ eine Reihe von Brüdern in der privaten Wirtschaft hat.

Der ganze Umfang der neuen Aufgaben für das ULD wird sich aber erst zeigen, wenn 2001 das **neue Bundesdatenschutzgesetz** in Kraft tritt. Es verändert die Datenschutzaufsicht im nichtöffentlichen Bereich radikal: Während bislang im Wesentlichen nur bei konkreten Beschwerdefällen kontrolliert werden durfte, haben die Aufsichtsbehörden künftig „**anlassfrei**“, d. h. flächendeckend und systematisch die Datenverarbeitung aller nichtöffentlichen Stellen zu kontrollieren.

Tausende von Wirtschaftsunternehmen, Handwerksbetrieben, Arztpraxen, Anwaltskanzleien usw. müssen dann regelmäßig datenschutzrechtlich unter die Lupe genommen werden. Die Bürgerinnen und Bürger haben einen **Anspruch auf** diese **Kontrollen**. Spätestens seit der BSE-Krise dürfte allen klar sein, dass staatlichen Stellen auch hier früher oder später die Frage gestellt wird, ob und in welchem Umfang tatsächlich kontrolliert worden ist. Unter Nutzung aller Synergieeffekte

wird dieses Aufgabenpensum ohne **Personalverstärkungen** nicht zu meistern sein. Bislang hat der Landtag hierfür jedoch noch keine zusätzlichen Stellen bewilligt.

In jedem Fall kommt es darauf an, durch einen möglichst geschickten Einsatz der knappen Kräfte möglichst viel Wirkung zu erzielen. Wir haben deshalb ein **Aktionsprogramm** für den Privatbereich entwickelt, durch das ein effizienter Personal- und Mitteleinsatz erreicht werden soll. Es besteht aus **drei Elementen**: gezielte Kontrollen, Beratung der Verbraucher und Verstärkung marktwirtschaftlicher Anreize (vgl. auch Tz. 6).

Kontrollen sind auch im Bereich der privaten Wirtschaft unverzichtbar. Darauf haben die Bürger einen Anspruch. Anderenfalls hätten im Übrigen diejenigen Firmen und Stellen, die das Datenschutzrecht beachten, einen Nachteil gegenüber denjenigen, die glauben, sich über die Vorschriften hinwegsetzen zu können. Angesichts der knappen Ressourcen müssen sich die Kontrollen auf die Verarbeitung besonders sensibler Daten konzentrieren, z. B. bei Auskunfteien, Versicherungen und im Bereich der ärztlichen Versorgung.

Die **Beratungsaktivitäten** werden sich schwerpunktmäßig an die Verbraucher richten. Ihnen ist vielfach gar nicht bewusst, welche Rechte sie nach den Datenschutzgesetzen haben. Die Beratung von Firmen und anderen privaten Daten verarbeitenden Stellen kann in der Regel nicht mehr kostenlos sein. Das neue LDSG gibt dem ULD die Befugnis zur Gebührenerhebung. Hiervon werden wir besonders dann Gebrauch machen, wenn aus der datenschutzrechtlichen Beratung konkrete wirtschaftliche Vorteile gezogen werden können.

Schließlich gilt es, gezielt **marktwirtschaftliche Anreize** zu schaffen. Da es offensichtlich ein breites Bedürfnis vieler Bürgerinnen und Bürger nach dem Schutz ihrer personenbezogenen Daten gibt, müssten diejenigen Unternehmen Marktvorteile haben, die ihren Kunden ein attraktives Datenschutzangebot machen. Unter dem Motto „**privacy sells**“ wollen wir deshalb die Unternehmen in Schleswig-Holstein ermuntern, sich mit aktiver Werbung um das Vertrauen der Kunden zu bemühen. Ausgangspunkt ist das Datenschutzgütesiegel, das schon in absehbarer Zeit Marketingvorteile bringen dürfte. Es geht aber auch darum, die bislang zumeist in den schwer verständlichen, oft zweideutigen allgemeinen Geschäftsbedingungen „versteckten“ Datenschutzinformationen attraktiv und gut verständlich zusammenzufassen und sie zu einem hervorgehobenen Instrument der Kundeninformation zu machen. Dabei dürfte es wichtiger sein, nach dem Motto „... und ein gutes Datenschutzangebot ist auch dabei“ das Wesentliche prägnant und verständlich auszudrücken, als den Kunden langweilige juristische Texte zuzumuten. Um privaten Stellen die Formulierung eines überzeugenden Datenschutzangebotes zu erleichtern, dürfte es sinnvoll sein, die allgemeinen, generalklauselartigen Bestimmungen des BDSG bereichsspezifisch zu präzisieren. Es ist beabsichtigt, im Zusammenwirken mit berufsständischen Verbänden und Unternehmen **Leitlinien** und **Checklisten** auszuarbeiten. Alles in allem sollte am Ende für möglichst viele Unternehmen die Erkenntnis stehen, dass Datenschutz nicht eine Belastung oder gar ein Standortnachteil ist, sondern im Gegenteil eine legitime Erwartung

der Kunden, die demjenigen Marktvorteile verspricht, der sie fair und offensiv erfüllt. An Grenzen stößt ein solcher Ansatz allerdings bei solchen Firmen, die glauben, den Kunden auch weiterhin mit Tricks und Täuschungen Informationen entlocken zu können, um anschließend detaillierte Kundenprofile zu erstellen, die mit viel Gewinn vermarktet werden. In solchen Fällen hilft auch in Zukunft nur konsequente Kontrolle und rechtzeitige Aufklärung der Verbraucher.

1.3 Das neue Informationsfreiheitsgesetz

Neben dem LDSG ist im Jahre 2000 auch das Informationsfreiheitsgesetz in Kraft getreten. Es gibt allen Bürgerinnen und Bürgern gegenüber den öffentlichen Stellen in Schleswig-Holstein einen **Anspruch auf Zugang** zu den dort **vorhandenen Informationen**, ohne dass sie dafür besondere Gründe darlegen müssten. Schleswig-Holstein ist damit nach Brandenburg und Berlin das dritte Land, in dem ein solches Informationszugangsrecht besteht. In den meisten anderen europäischen Staaten gehören Informationszugangsrechte schon seit einiger Zeit zum Bestandteil des demokratischen Lebens. Auch in Deutschland gibt es weitere Gesetzgebungsvorhaben auf diesem Gebiet (vgl. Tz. 12.1).

Das schleswig-holsteinische Informationsfreiheitsgesetz ist ohne intensive öffentliche Debatte verabschiedet worden. Entsprechend reserviert reagierten zunächst einige Behörden, als sie dem Gesetzblatt entnehmen konnten, dass sie von nun an ohne „Vorwarnzeit“ ihre Akten offen legen müssen. Es spricht für eine gut entwickelte Informationskultur im Lande, dass das Gesetz nur vereinzelt auf regelrechte Ablehnung gestoßen ist. Dazu mag beigetragen haben, dass sich im Rahmen der zweiten Lesung des Gesetzes praktisch alle Fraktionen im Landtag grundsätzlich zu einem Informationszugangsrecht bekannten.

Das Gesetz weist dem **Unabhängigen Landeszentrum** die Aufgabe zu, Beschwerden von Bürgerinnen und Bürgern über unzureichende Informationswährung nachzugehen. Seit In-Kraft-Treten des Gesetzes gab es eine ganze Reihe von förmlichen Eingaben (vgl. Tz. 12.5.2 und 12.6) und von Anfragen von Bürgern und Behörden im Vorfeld konkreter Streitfragen. Fast täglich erkundigen sich Bürger nach dem Umfang und den Modalitäten ihres Informationsrechts, während Behörden Hinweise über ihre Pflichten, insbesondere zur Abgrenzung des Informationszugangs von entgegenstehenden öffentlichen Belangen, Geheimhaltungsinteressen, Betriebs- und Geschäftsgeheimnissen oder Datenschutzrechten Dritter wünschen. Um die Anwendung des Gesetzes zu erleichtern, haben wir eine **Broschüre** mit Tipps und Hinweisen zum Informationsfreiheitsgesetz und ein **Faltblatt** herausgegeben. Die DATENSCHUTZAKADEMIE Schleswig-Holstein hat ihr Angebot um Kurse zum Informationsfreiheitsgesetz erweitert.

Zieht man eine erste Bilanz, so scheint es, dass das Informationsfreiheitsgesetz **in der Praxis gut anwendbar** ist. Die uns vorgelegten Eingaben vermitteln den Eindruck, dass es kaum missbräuchlich in Anspruch genommen wird, sondern dass die Informationsbegehren gut nachvollziehbar sind. Eine förmliche Beanstandung wegen einer unzulässigen Verweigerung einer begehrten Information musste nur ein einziges Mal ausgesprochen werden. In allen anderen Fällen konnte durch

unsere vermittelnde Tätigkeit, insbesondere durch die Präzisierung des Informationswunsches, eine für beide Seiten tragbare Lösung gefunden werden. Es hat sich gezeigt, dass Datenschutz und Informationszugang durchaus miteinander harmonieren können, ja dass sie letztlich zwei Seiten einer Medaille sind: Es geht um eine **faire Informationsverteilung** zwischen dem Einzelnen und dem Staat. Versteht man das Informationsfreiheitsgesetz nicht als ein Kampfinstrument gegen die Verwaltung, sondern als ein im Zeitalter der Informationsgesellschaft selbstverständliches Recht der Bürger, dann ist es nur ein kleiner Schritt, die Erfüllung der Pflichten aus dem Informationsfreiheitsgesetz aufseiten der Behörden als einen neuen Service der Verwaltung für die Bürger zu begreifen.

www.datenschutzzentrum.de/informationsfreiheit/

1.4 Die Errichtung des Unabhängigen Landeszentrums für Datenschutz

Die Zusammenfassung der Aufgaben der Datenschutzkontrolle bei den öffentlichen Stellen, der Datenschutzaufsicht im privaten Bereich und der Vermittlungstätigkeit nach dem Informationsfreiheitsgesetz unter dem Dach des Unabhängigen Landeszentrums für Datenschutz stellt eine grundlegende **Reorganisation des Datenschutzes** in Schleswig-Holstein dar. Die Rechtsform der Anstalt des öffentlichen Rechts hat sich bereits in den ersten Monaten als gut geeignet erwiesen. Sie ist geradezu eine ideale Organisationsform, wenn es darum geht, die Aufgaben nach dem LDSG, BDSG und dem IFG unabhängig, flexibel und effizient zu erfüllen. Das ULD beschäftigt derzeit 25 Mitarbeiterinnen und Mitarbeiter. Hinzu kommen sechs im Rahmen der Projekte zeitlich befristete Beschäftigte sowie Teilzeitkräfte.

Die Dienststelle bezieht im 1. Halbjahr 2001 ein **neues Gebäude** mitten in der Fußgängerzone der Stadt Kiel. Dadurch soll der unmittelbare Kontakt zu den Bürgern und der Wirtschaft noch einfacher werden als bisher. Die technische Ausstattung der Dienststelle und der **IT-Labore** ist als gut zu bezeichnen. In den neuen Diensträumen wird erstmals ein eigener **Schulungsraum** mit Computern ausgestattet werden, sodass die Aufgaben des ULD auf dem Gebiet der Vermittlung von Medienkompetenz adäquat erledigt werden können.

1.5 Schwerpunkte der Tätigkeit im abgelaufenen Jahr

1.5.1 Kontrollen

Im Mittelpunkt unserer Tätigkeit standen erneut die Kontrollen vor Ort. Herausragende Skandale sind dabei nicht zu Tage getreten, wohl aber viele Verhaltensweisen, die nicht akzeptabel sind.

So zeigten die routinemäßigen Kontrollen gravierende Mängel im Kommunalbereich auf, die offenbar auf **Managementfehler** zurückzuführen sind. Bei der Suche nach möglichst billigen Lösungen werden Sicherheitsstandards vernachlässigt, was sich mittel- und langfristig bitter rächen kann (vgl. Tz. 7.5.2). Manche Behördenleiter suchen ihr Heil im vollständigen Outsourcing der EDV und realisieren nicht, dass sie damit Gefahr laufen, die Kontrolle über ihre eigenen Verwaltungsabläufe weitgehend zu verlieren. Die Spätfolgen hastiger Automationsentscheidungen zeigten sich auch bei Kontrollen im Polizeibereich. Aus gutem Grund hat der Gesetzgeber auf diesem sensiblen Feld präzise Regeln für den Umgang mit personenbezogenen Daten aufgestellt. Sie sind im „regulären" Informationssystem COMPAS gut abgebildet. Die daneben in vielen Polizeidienststellen seit einigen Jahren hastig und ohne klare Konzeption nach dem Motto „Die EDV-Ausstattung der Polizei muss dringend und sofort verbessert werden" angeschafften PC erweisen sich jetzt als ein Sicherheitsproblem, dessen Lösung alles andere als einfach ist (vgl. Tz. 7.5.1).

Erfreulich war das Ergebnis der Kontrollen im Bereich der **Sicherheitsüberprüfungen**. Die Akten, die der Verfassungsschutz und die örtlichen Geheimschutzbeauftragten hierzu führen, waren weitgehend in Ordnung (vgl. Tz. 4.4). Ein Grund dafür liegt darin, dass in Schleswig-Holstein die Durchführung von Sicherheitsüberprüfungen beim Geheimschutzbeauftragten des Landes konzentriert ist. Ausgerechnet diese bewährte Konstruktion will der Innenminister in seinem Entwurf eines Sicherheitsüberprüfungsgesetzes wegen angeblicher Kosteneinsparungen beseitigen.

Man wundert sich immer wieder, dass längst bekannte Sicherheitslücken nur schwer auszurotten sind. Obwohl bereits mehrfach angeprangert, fanden wir bei unangekündigten Kontrollen in einem Gericht erneut im **Papierkorb** neben dem Kopiergerät auf dem offen zugänglichen Flur Fehlkopien von **Haftbefehlen** und dergleichen (vgl. Tz. 5).

Im Bereich der **Wirtschaft** konnten wir bislang im Wesentlichen nur aufgrund konkreter Anlässe kontrollieren. Deshalb können allgemeine Aussagen nur bedingt getroffen werden. Besonders unangenehm fiel ein Betrieb auf, in dem eine für jedermann einsehbare „Rennliste" an der Wand hing, aus der man die Verkaufserfolge und den Krankenstand der Mitarbeiterinnen und Mitarbeiter ablesen konnte (vgl. Tz. 6.3.2). Zu Recht beschwerten sich Bankkunden über die fehlende Diskretion an manchen Geldautomaten (vgl. Tz. 6.3.5). In anderen Fällen verlangten Banken von Kunden, die vor Jahren einen Kredit aufgenommen und diesen seither ordentlich bedient hatten, zu Unrecht plötzlich detaillierte Vermögens- und Einkommensangaben (vgl. Tz. 6.6). Bereits jetzt zeigt sich, dass Probleme im Zusammenhang mit der SCHUFA uns künftig besonders beschäftigen werden. Zumeist können sich hier schon kleine Fehler zu gravierenden Problemen für die Betroffenen auswachsen. So brachte eine alte, nicht ordnungsgemäß vernichtete SCHUFA-Auskunft einen Architekten in arge Bedrängnis (vgl. Tz. 6.4.1). In einem anderen Fall musste eine Bankkundin die Erfahrung machen, dass schon eine Eintragung bei der SCHUFA in Höhe von 200 DM (die Betroffene hatte die Monatsrechnung eines Mobilfunkbetreibers zunächst nicht bezahlt, weil familienintern gestritten wurde, wer so viel telefoniert hatte) ihr drei Jahre lang von den

Banken vorgehalten wurde (vgl. Tz. 6.4.2). Problematisch ist auch die Auffassung der SCHUFA, dass die von ihr nach einer geheimen Methode errechneten Score-Werte, die für die Kreditwürdigkeit von Bankkunden von großer Bedeutung sind, keine personenbezogenen Daten der Betroffenen, sondern eine Art „Betriebsgeheimnis“ der SCHUFA seien (vgl. Tz. 6.4).

1.5.2 Beratung

Unsere Beratungstätigkeit konzentrierte sich auf eine Reihe von **Großprojekten**. Nach wie vor gibt es noch kein überzeugendes Konzept für den Schutz des Fernmeldegeheimnisses bei den Telefonaten im gesamten Bereich der Landesregierung und des Parlaments, nachdem die **Telekommunikationsrechner** des Landes **privatisiert** worden sind (vgl. Tz. 7.3). Den Großteil der Arbeitskraft eines Mitarbeiters kosten die umfangreichen Beratungsleistungen, die beim Anschluss von Behörden an das **Internet** zu erbringen sind (vgl. Tz. 4.1.2). Der Aufwand lohnt sich, denn wenn hier geschlampt wird, können die Schäden hinterher immens sein. Bei der Konzeption von **INPOL-neu**, das sich mehr und mehr zum Millionengrab entwickelt, lässt sich die Polizei zwar umfangreich von uns beraten, nimmt unseren Rat aber kaum an (vgl. Tz. 4.2.2).

Ein weiterer Schwerpunkt der Beratungstätigkeit liegt im **Medizinbereich**. Hier gibt es auch in Schleswig-Holstein ehrgeizige Automationsprojekte. Den Ärzten ist leider nicht immer bewusst, dass dabei das Patientengeheimnis auf der Strecke bleiben kann (vgl. Tz. 4.8.3 und 4.8.9). Immer wieder wollten Vereinsvorstände und -mitglieder wissen, wie mit Mitgliederlisten umzugehen ist (vgl. Tz. 6.3.1). Die Häufung von Anfragen über den manchmal heiklen Umgang mit Daten im Betreuungswesen veranlasste uns zur Entwicklung von Leitlinien, die den Betroffenen zur Verfügung gestellt werden. Die meisten Beratungsersuchen kamen erwartungsgemäß zum neuen Informationsfreiheitsgesetz (vgl. Tz. 12).

1.5.3 Die Modellprojekte und das IT-Labor

„Den Datenschutz von Anfang an in die Produkte einbauen und so datenschutzrechtliche Probleme von vornherein vermeiden“, das ist ein Ideal, das wir seit vielen Jahren propagieren. In unseren Modellprojekten konnten wir einiges davon bereits realisieren. Das Projekt **Webzugriff anonym und unbeobachtbar (WAU)** steht kurz vor dem Abschluss. Es hat zur erfolgreichen Installation eines „Anonymisierers“ bei der Lübecker Online-Drogenberatung „Ecstasy“ geführt. Die dabei gewonnenen Erkenntnisse werden jetzt ausgewertet, aufbereitet und in ein neues Projekt größeren Zuschnitts eingebracht, das gemeinsam mit der TU Dresden betrieben und vom Bundeswirtschaftsministerium gefördert wird. **AN.ON** soll schon in absehbarer Zeit dazu beitragen, dass das Recht auf Anonymität, das im Teledienstedatenschutzgesetz jedem Surfer garantiert wird, in der Realität tatsächlich in Anspruch genommen werden kann (vgl. Tz. 9.2).

Schon in wenigen Jahren werden **biometrische Verfahren** unseren Alltag begleiten. Ob wir uns dabei einen weiteren Schritt dem Horrorszenario einer totalen

Überwachung nähern oder die Kontrolle über unsere biometrischen Daten behalten, hängt entscheidend von den Weichenstellungen bei der Technikentwicklung ab. Im Rahmen des Projektes **BioTrusT** bringen wir das Interesse der Verbraucher nach effektivem Schutz ihrer Persönlichkeitsrechte in die Überlegungen der Industrie ein und bemühen uns um eine datenschutzgerechte Technikgestaltung (vgl. Tz. 9.3).

Das **virtuelle Datenschutzbüro** hat am 05.12.2000 seinen Betrieb aufgenommen. Es ist ein Gemeinschaftsprojekt von deutschen und ausländischen Datenschutzinstitutionen. Seit seiner Inbetriebnahme wird es täglich von ca. 4.000 Surfern besucht. Im Schnitt vollziehen sie ca. fünf „Clicks“, woraus man ersehen kann, dass sie offenbar im virtuellen Datenschutzbüro auf interessante Informationen stoßen (vgl. Tz. 9.1).

Im Rahmen eines vom Bundesministerium für Wissenschaft und Forschung geförderten **Projektes** zur Entwicklung einer **CD**, die in **Schulen** im Rahmen des Unterrichts zum Thema „Datenschutz“ eingesetzt werden soll, werden wir einzelne Module entwickeln sowie generell die datenschutzrechtlichen Inhalte überprüfen (vgl. Tz. 9.4).

Das **IT-Labor** erweist sich als wertvolle Hilfe bei der Durchführung von Tests und Simulationen. Damit die dabei gewonnenen Erkenntnisse nicht Theorie bleiben, haben wir in der Reihe der backUP-Magazine Hinweise zur Datensicherheit publiziert (vgl. Tz. 10.1).

1.5.4 Die Vermittlung von Medienkompetenz

Im neuen Landesdatenschutzgesetz wird dem Unabhängigen Landeszentrum erstmals ausdrücklich die Aufgabe zugewiesen, Fortbildungsveranstaltungen zu den Themen Datenschutz und Datensicherheit durchzuführen. Hierbei kann das ULD auf die seit sieben Jahren bewährte Arbeit der **DATENSCHUTZAKADEMIE** Schleswig-Holstein zurückgreifen. Sie hat seit ihrer Gründung insgesamt 230 Kurse mit über 4.700 Teilnehmern durchgeführt. Im Jahresprogramm 2001 werden die neuen Aufgaben des ULD auf dem Gebiet des Datenschutzes in der privaten Wirtschaft sowie beim Informationszugang aufgenommen. Das Angebot der DATENSCHUTZAKADEMIE Schleswig-Holstein wurde auf insgesamt 56 Kurse erweitert. Auch in diesem Bericht finden sich am Rand Hinweise auf Kurse, in denen hier dargestellte Themen behandelt werden.

2 Der Weg in die Informationsgesellschaft

Alles Big Brother, oder was?

Die Aufregung war groß, als RTL II im Frühjahr 2000 seine 100-Tage-Life-Show „Big Brother“ ankündigte. Zehn junge Frauen und Männer wurden in einen Käfig – Container genannt – gesperrt und rund um die Uhr von Kameras in jedem Winkel beobachtet. Die Bilder konnten im Internet und als Zusammenfassung des letzten Tages zur besten Einschaltzeit im Fernsehen verfolgt werden. Viele „Alte“ waren ent- und viele „Junge“ begeistert.

Traumhafte Einschaltquoten wurden zunächst erreicht, und das gerade bei dem idealen Zielpublikum der Werbung, nämlich den 14- bis 25-Jährigen. Die Begeisterung wurde eher bestärkt als getrübt, als Medienwächter einen verzagten Versuch unternahmen, die Sendung zu verbieten. Das Sendeformat verstoße gegen den wichtigsten Artikel unseres Grundgesetzes, in dem es heißt: „Die **Würde des Menschen** ist unantastbar.“ Sie forderten Zensur, obwohl es in einem anderen Grundgesetzartikel heißt: „Eine **Zensur** findet nicht statt.“

Auch wir äußerten uns zu dem den intimitätslüsternen Voyeurismus fördernden Medienexperiment öffentlich. Dabei ging es uns weniger um den Schutz der freiwillig Eingesperrten, die dem **Ausverkauf** ihrer **Intimsphäre** zugestimmt haben, als um eine schleichende Veränderung unseres gesellschaftlichen Bewusstseins: Mit „Big Brother“ werden um eines kurzfristigen Quotenvorteils willen Schamgrenzen beim Eindringen in den sensiblen Bereich der Wohnung beseitigt. Es wird ein gesellschaftliches Bewusstsein suggeriert und propagiert, wonach die Privatsphäre nur noch wenig wert sei.

Vielleicht kann die Sendung aber auch bei den Zuschauern das Gespür dafür wecken, was wir auf jeden Fall verhindern sollten: den **realen „Big Brother“**, so wie ihn George Orwell in seinem berühmten Roman „1984“ beschrieben hat. Anderen Leuten amüsiert dabei zuzusehen, wie sie ihre Privatsphäre verkaufen, ist eine Sache – selbst das unfreiwillige Opfer von Beobachtung und Ausspähung zu sein, ist etwas ganz anderes. Vermutlich wurde manchen bei diesem Sendeformat klar, warum die Datenschutzbeauftragten gegen den Großen Lauschangriff erbitterten Widerstand geleistet haben und weshalb sie sich der Zulassung von staatlichen Videokameras in Privatwohnungen entgegenstemmen. Mag sein, dass die Privatsphäre einigen nicht mehr wert ist als eine TV-Gage; die Mehrzahl der Fernsehzuschauer würde so etwas in ihrer Privatwohnung aber wohl nicht zulassen. Schon gar nicht würden sich die Menschen damit abfinden, wenn ihre Wohnungen heimlich und gegen ihren Willen beobachtet würden.

Die Versuche, mit rechtlichen oder moralischen Argumenten gegen die Abstimmung über die Fernbedienung anzukommen, waren zunächst eher hilflos. Bei allem Respekt vor der Programmautonomie der Fernsehzuschauer: Wenn es nur noch auf die **Quote** ankäme, müssten wir uns demnächst vermutlich auf Liveübertragungen aus den Hinrichtungszellen der amerikanischen Gefängnisse und ähnlich sensationelle, „unterhaltsame“ Bilder gefasst machen.

Big Brother is really watching you

Wichtig bleibt aus der Sicht des Datenschutzes die durch „Big Brother“ u. Ä. angeregte Diskussion zu der Frage, ob es in der Informationsgesellschaft überhaupt noch ein Privatleben gibt. Kurz bevor RTL II mit seiner Reality-Soap auf Sendung ging, wurde der **Große Lauschangriff**, das polizeiliche Eindringen in die private Wohnung zum Zweck der akustischen Überwachung, vom Gesetzgeber freigegeben. Selbst als einige Polizeivertreter zusätzlich den Großen Spähangriff – die heimliche optische Wohnungsüberwachung – forderten, war angesichts dieses massiven Angriffs auf die räumliche Privatsphäre von öffentlicher Empörung der Bevölkerung – in ihrer räumlichen Privatsphäre vor dem Bildschirm sitzend – wenig zu spüren. Viele waren vom Trommelfeuer der ständigen „Rekordmeldungen“ aus dem Bereich der Organisierten Kriminalität mürbe oder glaubten, sie selbst könnten nie betroffen sein.

Die im Herbst 2000 in Essen organisierte Security-Messe zeigte, dass Lausch- und Spähangriffen immer weniger technische Hindernisse im Wege stehen: Mit versteckten **Minikameras** können gestochen scharfe Farbbilder in vielfacher Vergrößerung auf den Bildschirm gezaubert werden; mit **Infrarot** lassen sich selbst den Blick versperrende Kleidungsstücke oder sonstige Hindernisse wegzaubern. Geradezu genial erscheinen elektronische Mustererkennungsverfahren, mit denen so genannte **intelligente Kameras** im Supermarkt oder in der Tiefgarage „reguläres“ von „verdächtigem“ Verhalten unterscheiden. Soeben wurde anlässlich des Football-Endspiels in den USA, dem „Super-Bowl“, ein weiteres faszinierendes Videoexperiment durchgeführt: An den vier Eingängen wurden Kameras installiert, die von jedem der über 70.000 Zuschauer mehrere Bilder aufnahmen, die automatisch mit einem polizeilichen Bildfahndungscomputer abgeglichen wurden. Und tatsächlich hatte man 19 „Treffer“, davon 18 „kleine Fische“, die man laufen ließ. Der Einzige, für den sich die Polizei ernsthaft interessierte, war in der Masse nicht mehr zu finden. Aber das ist bald auch kein technisches Problem mehr: Ein einmal per Kamera identifizierter „Verdächtiger“ kann von Kameras lückenlos automatisch weiterverfolgt werden, vorausgesetzt, es gibt genügend Kameras.

Auch in Deutschland ist die **Videobeobachtung auf dem Vormarsch**. Überall werden Kameras aufgestellt oder als so genannte Dom-Kameras in „Lampenkugeln“ versteckt, sodass das ganze Ausmaß der Beobachtung von den Menschen auf der Straße gar nicht mehr bemerkt werden kann. Für jede dieser Kameras mag es im Einzelfall eine nachvollziehbare Begründung geben, in ihrer Gesamtheit führen sie gleichwohl zu einer Struktur, an der „Big Brother“ tatsächlich seine Freude haben könnte. Die Beobachtung beschränkt sich auch nicht auf den Einsatz von Kamera und Mikrofon. Lange bevor Boris Becker „drin“ war, waren schon Millionen von Menschen im Internet, um sich zu unterhalten und zu informieren. Dass bei dieser Gelegenheit ihr **Surfverhalten** von Webseiten-Betreibern minuziös **beobachtet** wird, ist den meisten heute noch nicht bewusst. Und wer hat sich schon darüber Gedanken gemacht, dass die schicken Kundenkarten, mit denen man Bonuspunkte sammeln und Geld sparen kann, geeignet sind, um detaillierte **Konsumprofile** von ihren Nutzerinnen und Nutzern zu erstellen? Nicht zu reden von den Handys, mit denen es technisch kein Problem ist, den tatsächlichen

Aufenthaltsort des Benutzers recht genau einzugrenzen. Auch das, was per **SMS** ausgetauscht wird, muss nicht ein Geheimnis der Nutzer bleiben. Das Mitlesen und Abfangen dieser Nachrichten ist nicht nur der Polizei möglich.

Was ist heute noch Privatsphäre?

Die Bedrohungen der Privatsphäre kommen von allen Seiten und haben auch im Berichtsjahr keineswegs nachgelassen. Eigentlich hat sich an Schutz und Missachtung der Privatsphäre seit hundert Jahren im Kern nicht viel geändert. Als damals ein Paparazzo sich in das Totenzimmer des früheren Reichskanzlers Otto von Bismarck schlich und Fotos schoss, um diese gegen Bares in der Presse zu veröffentlichen, reagierte der Reichsgesetzgeber sofort und erließ das Kunsturhebergesetz, in dem u. a. das **Recht am eigenen Bild** garantiert wird. Das Gesetz gilt noch heute. Das Recht am eigenen Bild ist immer noch relevant, z. B. wenn heute Schulen Klassenbilder im Internet veröffentlichen, Journalisten versteckte Kameras installieren oder Videoüberwachung in einer öffentlich zugänglichen Einkaufszone stattfindet.

Dennoch hat sich mit der modernen Informations- und Kommunikationstechnik einiges geändert. Sie erlaubt viel **tiefere Eingriffe** in die Privatsphäre als noch vor 5, 10 oder 20 Jahren und zugleich deren **weltweite Verbreitung**, z. B. über das Internet. Das führt zwangsläufig dazu, dass wir tagtäglich mit Intimitäten von Menschen konfrontiert werden, mit denen wir persönlich überhaupt nichts zu tun haben. Dies kann die Familie eines Tennisstars sein, aber auch jemand, dessen Prominenz sich darauf beschränkt, zufällig ins Blickfeld einer Kamera gelaufen zu sein. Solange wir selbst diese betroffene Person nicht sind, ist der Blick in die Privatsphäre des anderen für viele offenbar unterhaltsam bis spannend. Ein bisschen Voyeurismus ist überall.

Neu ist der ausgeprägte **Exhibitionismus**. War es zu Zeiten des Schwarz-Weiß-Fernsehens mit drei Programmen praktisch unmöglich, den eigenen Geltungsdrang über Medien zu befriedigen – Derartiges konnte nur im engen sozialen Umfeld ausgelebt werden –, so eröffnen zig TV-Kanäle, Websites, Chatrooms usw. ganz neue Möglichkeiten der Selbstdarstellung. Damit einher ging eine Enttabuisierung in unserer Gesellschaft: War in den 60er-Jahren ein entblößter Busen im Film ein nationaler Skandal, so muss man sich heute schon kesser präsentieren, um öffentlich wahrgenommen zu werden. Dabei hat das, als was man sich medial darstellt, oft nur noch wenig mit der Wirklichkeit zu tun. Da der Exhibitionismus nicht Halt macht vor dem eigenen sozialen Umfeld, können gelegentlich große Probleme entstehen. Man gibt sich nicht nur selbst – unter Umständen der Lächerlichkeit – preis, betroffen sind dann auch schon mal Freunde, Verwandte oder sonstige nahe stehende Personen. Viele scheinen sich nicht darüber bewusst zu sein, welche persönlichen Folgen ihre Selbstdarstellung für sie selbst und ihr Umfeld hat. Soziale Isolation, Depressionen oder sonstige negative Folgen sind für die Medien regelmäßig nicht mehr berichtenswert, schon gar nicht, wenn sie auf Medienberichte zurückgehen.

Das Bedürfnis nach Privatsphäre ist ein **urmenschliches Bedürfnis**, das in den verschiedensten Ländern und Kulturen – teilweise sehr unterschiedlich – befriedigt wird. Auch die Technik hat insofern den Menschen nicht geändert. So ist es z. B. verblüffend, wie sensibel manchmal gerade solche Politiker reagieren, wenn die eigene Privatsphäre berührt ist, die ansonsten bei Eingriffen in die Privatsphäre anderer nicht gerade zimperlich und äußerst geübt in der medialen Selbstdarstellung sind. Es spricht vieles dafür, dass die Sensibilität für die **Privatsphäre anderer** in unserer Mediengesellschaft nachlässt. Zwar erlebt man die eigene Gefährdung; doch solange es nur andere trifft, gibt es keine Veranlassung, sich Gedanken zu machen. Wenn es einen tatsächlich trifft, ist es zu spät. Solidarität nimmt ab; neugieriges, belustigtes oder teilnahmsloses Zuschauen oder gar das bewusste Wegschauen nimmt zu.

Dabei scheint es keine Grenzen zu geben: So spekulierte z. B. eine im Allgemeinen als seriös angesehene Zeitschrift in scheinbar wissenschaftlicher Weise darüber, ob ein bestimmter Adliger nicht vielleicht ein „Prügel-Gen“ in sich trägt. Nun sind **genetische Veranlagungen** etwas sehr Persönliches, was nicht auf die Titelseiten der Yellow Press gehört. Aber damit nicht genug: Schon heute ist es möglich, anhand eines ausgerissenen Haares eine genetische Analyse für wenige Hundert Mark vornehmen zu lassen. Wann werden wir den ersten Fall erleben, in dem ein gestohlenes Haar einer interessierenden Person analysiert und das Analyseergebnis auf allen Kanälen vermarktet wird?

Ein Blick in andere scheinbar zivilisierte Länder ist wenig ermutigend. So gibt es in den USA offensichtlich keine Scham, **Videobilder aus** einem **Gefängnis** direkt ins Internet zu übertragen. Es gibt Firmen, die offen im Internet damit werben, sie könnten für 50 Dollar detaillierte Informationen auch sensibelster Art über beliebige Mitbürger liefern. In Großbritannien gibt es Stadtteile, in denen inzwischen sämtliche öffentliche Straßen videoüberwacht werden. Dass beim Hobeln an der Privatsphäre auch Späne fallen können, zeigte die Veröffentlichung von Namen und Bildern von verurteilten Sexualtätern im Internet und durch eine englische Tageszeitung. Der dadurch angestachelte Mob demonstrierte vor Häusern von Menschen, die zufällig so aussahen wie die Angeprangerten oder den gleichen Namen hatten. Diese Aktion verhinderte zwar kein Sexualdelikt, provozierte aber zwei Selbsttötungen.

Verletzungen des Datenschutzes und der Privatsphäre hinterlassen zumeist keine direkt sichtbaren, aber dennoch **gravierende Spuren bei den Menschen**. Verfolgungswahn kann die Folge sein oder auch „nur“ Angst, soziale Gehemmtheit und Gleichgültigkeit gegenüber anderen. Neben diesen bei einer Medienfolgenabschätzung festzustellenden individuellen Konsequenzen gibt es auch gesellschaftliche Folgen des Einbruchs in die Privatsphäre. Vor knapp zwanzig Jahren hat das Bundesverfassungsgericht hervorgehoben, dass die technische Beobachtung zu Verunsicherung bei den Betroffenen führt und letztendlich dazu, durch abweichende Verhaltensweisen möglichst nicht auffallen zu wollen. Ein dadurch bedingter Verzicht auf die Ausübung von Grundrechten würde – so das Gericht – das Gemeinwohl beeinträchtigen, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten demokratischen Gemeinwesens ist.

Jetzt erst recht Datenschutz

„Big Brother“ von RTL II kokettierte mit der Assoziation zu George Orwells „Big Brother is watching you“ aus dem Roman „1984“, als wäre es schick oder besser hip, ein bisschen allwissende Diktatur zu spielen und dabei auch noch Geld zu verdienen. Der Informationswert solcher Fernsehformate tendiert gegen null. Wer dies für sich festgestellt hat, sollte bei solchen **Sendungen abschalten**. Dabei kann es aber nicht sein Bewenden haben. Das Unabhängige Landeszentrum für Datenschutz versteht es als eine seiner Aufgaben, sich hierzu in öffentlicher Diskussion zu äußern. Ein **Engagement** für **Datenschutz** ist angesichts der Herausforderungen im Betrieb und in der Freizeit, in der virtuellen und in der realen Welt zugleich ein Engagement für eine **menschlichere Gesellschaft**. Angesichts neuer Techniken müssen wir neu lernen, hierfür einzutreten. In Zeiten von Internet, Gentechnik und „Big-Brother-Formaten“ müssen wir neue Antworten auf die Frage suchen, was uns Privates und Persönliches wert ist. Haben wir die richtigen Antworten gefunden, dann bleibt „Big Brother“ als TV-Format nichts anderes als seichte Unterhaltung und im wirklichen Leben ein beherrschbares Risiko. Deshalb kann „Big Brother“ für alle, denen am Schutz der Privatsphäre trotz größer gewordener Bedrohung gelegen ist, nur ein Ansporn zu einem entschiedenen „**Jetzt erst recht**“ sein. Die Container von Köln können nicht die Modellstadt für eine demokratisch verantwortbare Informationsgesellschaft sein.

3 Landtag

Datenschutzgremium noch nicht gebildet

Unser Bericht des letzten Jahres zum Kapitel Landtag endete mit der Feststellung: „Das Datenschutzgremium muss endlich benannt werden und seine Arbeit beginnen.“ Diesen Appell müssen wir wiederholen.

Nach langwierigen Debatten hat sich der Schleswig-Holsteinische Landtag Anfang 1999 eine eigene **Datenschutzordnung** gegeben (vgl. 22. TB, Tz. 3.1). Wir wiesen die Fraktionen seinerzeit auf das darin vorgesehene Datenschutzgremium des Landtags hin. Nachdem in der 14. Legislaturperiode von den Fraktionen keine Aktivitäten in diese Richtung zu verzeichnen waren, hatten wir die Erwartung, dass der Anfang 2000 neu gewählte Landtag sich dieser Aufgabe mit frischem Elan stellen würde. Da wieder fast ein Jahr ohne erkennbare Fortschritte vergangen ist, sahen wir uns veranlasst, erneut auf die Notwendigkeit der Besetzung des Gremiums hinzuweisen.

Wegen der parlamentarischen Unabhängigkeit hat das ULD gegenüber dem Landtag keine Kompetenzen. Dennoch müssen wir darauf aufmerksam machen, dass nicht davon gesprochen werden kann, im Landtag gäbe es keine **Datenschutzprobleme**: Wie steht es z. B. mit der Abhörsicherheit der Telefone der Abgeordneten? Ist die Datensicherheit beim PC-Einsatz in den Fraktionen gewährleistet? Wird der E-Mail-Verkehr der Fraktionen und der einzelnen Abgeordneten auch dann unverschlüsselt über das Internet abgewickelt, wenn es sich um „sensible“ Nachrichten handelt? Wo wird das Kommunikationsverhalten der Parlamentarier protokolliert?

Wir konnten immer wieder feststellen, dass bei den Fraktionen im Landtag eine hohe Sensibilität in den unterschiedlichsten Datenschutzfragen besteht. Das Datenschutzgremium sollte vorrangig nicht als ein Kontrollorgan verstanden werden, sondern als eine Einrichtung, in der sich die Fraktionen über ihre Probleme bei Datenschutz und Datensicherheit austauschen und verständigen können.

Was ist zu tun?
Die Mitglieder des Datenschutzgremiums sollten benannt werden und mit ihrer Arbeit beginnen.

4 Datenschutz in der Verwaltung

4.1 Kommunalbereich

4.1.1 Behördliche Datenschutzbeauftragte sind kein Kosten-, sondern ein Rationalisierungsfaktor

Manche Behördenleitungen meinen, dass behördliche Datenschutzbeauftragte nur Zeit und Geld kosten sowie Ärger verursachen. Sie übersehen, dass diese Spezialisten ihnen helfen können, den Aufwand für eine korrekte und sichere personenbezogene Datenverarbeitung zu verringern.

Aus guten Gründen hat der Gesetzgeber im **neuen LDSG** den Daten verarbeitenden Stellen im Lande nicht zwingend vorgeschrieben, behördliche Datenschutzbeauftragte zu bestellen. Es gibt sehr kleine Organisationseinheiten bzw. solche, in denen nur in einem ganz geringen Umfang personenbezogene Daten verarbeitet werden. In diesen Fällen hätte man eine Pflicht zur Bestellung eines behördlichen Datenschutzbeauftragten als eine bürokratische Überreaktion ansehen können.

Was als eine sinnvolle Ausnahme gedacht war, wird insbesondere im kommunalen Bereich aber offensichtlich als der Normalfall missverstanden. Da es sich um eine „**Kannbestimmung**“ handelt, werden zurzeit nur relativ wenige förmliche Bestellungen zu behördlichen Datenschutzbeauftragten vorgenommen. Viele Behördenleitungen gehen offenbar von der irrigen Annahme aus, diese Position erfordere – wenn nicht gar eine neue Planstelle – zumindest aber einen zusätzlichen Arbeitsaufwand. Dabei wird übersehen, dass bei richtiger Organisation des behördlichen Datenschutzbeauftragten das Gegenteil der Fall sein kann.

Zunächst muss man sich nämlich darüber klar werden, dass die **datenschutzrechtlichen** und **sicherheitstechnischen Problemstellungen** in einer Behörde die gleichen bleiben, unabhängig davon, wer sich mit ihrer Lösung befasst: In Krankenhäusern ist auf allen Stationen das Patientengeheimnis während und nach der Behandlung zu wahren. Alle Mitarbeiterinnen und Mitarbeiter der Finanzämter haben das Steuergeheimnis zu beachten. Krankenkassen und Sozialämter haben die „Abfertigungsschalter“ (modern: Kundencenter) so zu gestalten, dass über soziale Verhältnisse gesprochen werden kann, ohne dass andere Personen mithören. Polizeibehörden und Staatsanwaltschaften haben Verdachtsmomente, die sich nicht als stichhaltig erwiesen haben, zu löschen. Auskünfte aus behördlichen Datenbeständen dürfen nur erteilt werden, wenn der Empfänger hierauf einen Anspruch hat. Computersysteme dürfen nicht missbräuchlich genutzt werden können. Die Aufzählung dieser Selbstverständlichkeiten könnte um viele Positionen fortgesetzt werden.

Hinzu kommt, dass die Rechtsgrundlagen für die personenbezogene Datenverarbeitung sich nicht nur im Landesdatenschutzgesetz selbst, sondern in einer Vielzahl bereichsspezifischer Regelungen finden (eine einschlägige Publikation weist nicht weniger als 45 Gesetze, Rechtsverordnungen und Satzungen allein auf Landesebene auf). Berücksichtigt man außerdem, dass die Ausgestaltung der techni-

schen und organisatorischen Maßnahmen zur Datensicherheit sehr stark von der Art und dem Hersteller der eingesetzten Hard- und Software abhängt, so wird deutlich, dass bereits Behörden mittlerer Größe besser daran tun, die Bearbeitung dieser Fragestellungen einem **spezialisierten Mitarbeiter** zu übertragen, anstatt von Fall zu Fall immer andere Personen mit der Materie zu befassen. Im letzteren Fall erfindet man nur allzu oft das Rad wieder neu, vergeudet viel Zeit durch das Beschreiten und Korrigieren von Irrwegen und geht das Risiko suboptimaler Lösungen ein.

Bezeichnend ist, dass diejenigen Daten verarbeitenden Stellen, die aufgrund der Regelungen im SGB X **Sozialdatenschutzbeauftragte** zu bestellen haben, und die, die bereits in der Vergangenheit die Zuständigkeit für alle Fragen des Datenschutzes und der Datensicherheit auf einen internen Datenschutzbeauftragten konzentriert haben, sich mit dieser Lösung sehr zufrieden zeigen und nicht bestrebt sind, zu der früheren Zersplitterung zurückzukehren.

Im Wortlaut: § 10 Abs. 4 LDSG

Die oder der behördliche Datenschutzbeauftragte überwacht und unterstützt die Einhaltung der datenschutzrechtlichen Vorschriften bei der Daten verarbeitenden Stelle. Sie oder er hat insbesondere

1. *auf die Einhaltung der Datenschutzvorschriften bei der Einführung von Datenverarbeitungsmaßnahmen hinzuwirken,*
2. *die Beschäftigten der Daten verarbeitenden Stelle mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen,*
3. *die Daten verarbeitende Stelle bei der Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten zu beraten und bei der Einführung neuer Verfahren oder der Änderung bestehender Verfahren auf die Einhaltung der einschlägigen Vorschriften hinzuwirken,*
4. *das Verzeichnis nach § 7 Abs. 1 zu führen und zur Einsicht bereitzuhalten,*
5. *die Vorabkontrolle nach § 9 Abs. 1 durchzuführen.*

In Zweifelsfällen hat sie oder er das Unabhängige Landeszentrum für Datenschutz zu hören.

Befürchtungen, dass durch die gesetzlich vorgeschriebene Anbindung des behördlichen Datenschutzbeauftragten unmittelbar an die **Behördenleitung**, durch die Weisungsfreiheit und das Benachteiligungsverbot eine „Behörde in der Behörde“ aufgebaut wird, sind unbegründet. Falsch ist auch die Annahme, die Überwachung der Einhaltung datenschutzrechtlicher Vorschriften, die Unterrichtung der Beschäftigten über das Datenschutzrecht und die Beratung der Behörden bei der Gestaltung automatisierter Verfahren würden zu mehr behördeninterner Bürokratie führen. Dass das Gegenteil vom Gesetzgeber gewollt ist, zeigt sich daran, dass das Verfahrensverzeichnis und die Unterlagen über besonders sensible automatisierte Verfahren nicht dem Unabhängigen Landeszentrum für Datenschutz übersandt bzw. zur Prüfung vorgelegt werden müssen, wenn ein behördlicher Datenschutzbeauftragter bestellt ist und dieser die entsprechenden Kontrollaufgaben (im Hause) übernimmt. Außerdem ist es auch völlig unschädlich, wenn dem behördlichen Datenschutzbeauftragten neben seiner eigentlichen Aufgabe auch andere Zuständigkeiten übertragen wer-

den. Sehr effektiv lassen sich Organisations-, Revisions- und Controllingfunktionen sowie die Auskunftserteilung und die Öffentlichkeitsarbeit mit dieser Aufgabenstellung kombinieren. Manche Behördenchefs, die verzweifelt fragen, wie sie denn ihrer Leitungsfunktion im Bereich der automatisierten Datenverarbeitung nachkommen sollen, können in der Bestellung eines kompetenten **behördlichen Datenschutzbeauftragten** die **Lösung** ihres Problems finden.

Sicherlich muss einem behördlichen Datenschutzbeauftragten für seine Aufgabe und die Vorbereitung darauf (Schulung) ein angemessenes Zeitkontingent zur Verfügung stehen. Dies ist aber kein zusätzlicher Aufwand, sondern in der Regel weniger, als an anderen Stellen eingespart wird. Per Saldo ergibt sich also ein Zeit- und Qualitätsgewinn. Wo dies nicht der Fall ist, wurden möglicherweise die Datenschutzaufgaben bislang vernachlässigt. Für die Erfüllung der gesetzlichen Aufgaben bedarf es eines behördlichen „Full-Time-Datenschutzbeauftragten“ nur in großen Behörden oder wenn mehrere Behörden ihn gemeinsam bestellt haben.

Schleswig-Holstein DATENSCHUTZAKADEMIE
Kurse DW, DR, DT, BDSB

Was ist zu tun?
Zumindest Kommunalbehörden mit mehr als 20 Mitarbeitern sollten zeitnah behördliche Datenschutzbeauftragte bestellen. Wird hierauf verzichtet, sind die Verfahrensverzeichnisse und die Unterlagen über besonders sensible Verfahren unverzüglich dem ULD zur Dokumentation bzw. Kontrolle zu übersenden.

4.1.2 Unkalkulierbare Risiken bei Internet-Anschlüssen

Für die Verknüpfung der Rechnersysteme von Behörden mit dem Internet gibt es noch keine Standardsicherheitspakete. Der Glaube vieler Verantwortlicher an die „Wunderwirkung“ von Firewalls führt dazu, dass die tatsächlichen Sicherheitsrisiken übersehen werden. Datenschutzgerechte Lösungen führen im Augenblick nur über eine Selbstbeschränkung der Behörden und die Erarbeitung von maßgeschneiderten Sicherheitskonzepten.

Voll Erstaunen und Bewunderung werden immer wieder die großen **Technologiesprünge** im Bereich der Informationsverarbeitung beschrieben. Die Rechnergeschwindigkeiten, die Speicherkapazitäten und die Übertragungsbandbreiten weisen in der Tat nach wie vor eine steil nach oben zeigende Tendenz auf. Ganz anders sieht es in einigen Teilbereichen der Softwareentwicklung aus; hier scheint die Zeit stehen geblieben zu sein. Ein hierfür typisches Segment ist die Verknüpfung lokaler Netzwerke mit anderen Netzen, insbesondere mit dem Internet. Die Probleme sind seit mehreren Jahren bekannt und vielfach beschrieben (vgl. z. B. 20. TB, Tz. 7.5.1; 21. TB, Tz. 7.1.2 und 22. TB, Tz. 7.1.1 sowie die nebenstehenden aktuellen Zitate).

Die Gegebenheiten in der Praxis haben sich gleichwohl nicht entscheidend geändert. Immer mehr Behörden eröffnen den E-Mail-Verkehr mit der „ganzen Welt“ und lassen ihre Mitarbeiterinnen und Mitarbeiter im **Internet** surfen, wo immer es ihnen beliebt, nur Porno und Gewaltverherrlichung sind verboten. Auf die Frage nach den Sicherheitsvorkehrungen kommt die Antwort: „Wir haben eine Firewall.“

Diese Softwareprodukte sind offenbar in den Augen vieler Behördenleiter eine Wunderwaffe in Bezug auf die Datensicherheit. Hat man eine **Firewall**, glaubt man die Welt in Ordnung und das böse Internet gezähmt. Welche Funktionalitäten die eingekaufte Software wirklich hat, welche **Internet-Angriffe** herausgefiltert werden können und welche tatsächlich unerkannt durchgelassen werden, wird meist nicht hinterfragt. Auch die Warnungen einiger Anbieter von Firewalls, wie z. B. der Datenzentrale in ihrer Leistungsbeschreibung („Die Firewall bietet keinen Schutz vor der Übertragung gefährlicher Daten, wie z. B. mit Viren verseuchte Programme oder Dokumente/Dateianlagen bei elektronischer Post. Es liegt in der Verantwortung des Anwenders, selbst geeignete Maßnahmen zur Erkennung und Abwehr derartiger Angriffe zu treffen."), führen nur selten zu maßgeschneiderten Sicherheitskonzepten, mit denen die Risiken auf ein vertretbares Maß reduziert werden.

Spiegel-Online, 20/2000

Das wahre Gefahrenpotenzial liegt nicht in Viren, sondern in unserem Umgang mit E-Mail-Attachments. Word-Dokumente („.doc") können Makroviren enthalten. Man sollte grundsätzlich keine Dokumente öffnen, die man nicht angefordert hat. Für Word-Formatvorlagen („.dot") gilt dasselbe. Rich-Text-Format-Dokumente („.rtf") gelten als sicher, sind es aber nicht, wenn sie Grafiken, Bilder und andere Zusätze enthalten. Man sollte die Annahme solcher Dokumente im Zweifelsfall verweigern. VisualBasicScripts („.vbs") sind gefährlich. Nie öffnen: Eine „vbs"-Datei hat nichts in einer E-Mail zu suchen. Ausführbare Programmdateien („.com" und „.exe") sind potenzielle Killer. Nie öffnen, außer man hat die betreffende Datei bestellt. Ganz primitiv, aber hoch effektiv: Stapelverarbeitungsdateien („.bat") sind die einfachste Form, einen Rechner zu attackieren. Das Anklicken der batch-Datei setzt eine Befehlsfolge in Gang. Immer mehr User verschicken per E-Mail „htm"- und „html"-Dateien. Sie gelten als harmlos, sind aber potenziell gefährlich. Html-Dateien können JavaScripts enthalten, die eine Menge Schaden anrichten können. Ist der User beim Öffnen der Mail online, könnte sich die Html-Datei ActiveX oder Java-Inhalte von Servern im Internet abholen oder „Trojaner" installieren. Wer „nur" E-Mails empfängt und keine Attachments öffnet, ist sicher.

Es fällt vielen Verantwortlichen schwer, die Tatsache zur Kenntnis zu nehmen, dass es in diesem Bereich (noch) keine Sicherheitspakete gibt, die man „**von der Stange**" kaufen kann. Ebenso schwer ist ihnen zu vermitteln, dass die Angreifbarkeit ihrer Behördenrechner aus den externen Netzen nicht mit „ein bisschen Software" behoben werden kann, solange selbst die von ihnen eingesetzten Betriebssysteme strukturelle Sicherheitslücken aufweisen. Fakt ist, dass die IT-Industrie zurzeit zwar die Taktraten der PC im Jahresrhythmus verdoppeln, nicht aber deren Sicherheitsprobleme halbieren kann.

In dieser Situation wird verstärkt nach Lösungen durch den Datenschutzbeauftragten gerufen. Wer die personelle und finanzielle Ausstattung des **Unabhängigen Landeszentrums für Datenschutz** kennt, dem dürfte klar sein, dass es nicht die Rolle des „Trouble-Shooters" für Microsoft, INTEL usw. bzw. für die großen IT-Abteilungen in Wirtschaft und Verwaltung übernehmen kann.

Gleichwohl versuchen wir, im Rahmen von zwei **Projekten** mit unterschiedlichen Ansätzen zu Lösungen zu gelangen, die in der Verwaltungspraxis als Muster dienen können.

Das **Virtual Network Computing** (VNC), das im Rahmen des virtuellen Datenschutzbüros erprobt wird, haben wir bereits im letzten Tätigkeitsbericht (vgl. 22. TB, Tz. 7.1.1) erläutert. Das Konzept, das auf einer spezifischen Kombination von Hard- und Softwarekomponenten aufbaut, befindet sich seit Dezember 2000 im Echtbetrieb (vgl. Tz. 10.4). Aussagefähige Erfahrungen werden etwa Mitte 2001 vorliegen. Wir werden sie dann den Daten verarbeitenden Stellen im Lande zur Verfügung stellen.

Die Welt, 31.10.2000

Was ist zu tun? Die Antwort mag in einer Zeit der Online-Euphorie ketzerisch klingen, aber sie kann nicht anders lauten als: Gehen Sie offline! Trennen Sie Ihr Intranet vom Internet! Websurfing und E-Mail-Versand vom Arbeitsplatzrechner aus sind zwar bequem, aus sicherheitstechnischer Sicht aber unverantwortlich. Firewalls und Content-Scanner für den ankommenden und abgehenden Internet-Verkehr? Vergessen Sie's. Ein hinreichend geschickt programmiertes Trojanisches Pferd ist kaum zu entdecken und kann seine Kommunikation mit der Außenwelt auch über die komplizierteste Firewall abwickeln.

An dem zweiten Projekt ist ganz wesentlich der **Kreis Ostholstein** beteiligt. Hier wird versucht, die Wirkungsweise gängiger Sicherheitsprodukte dadurch zu optimieren, dass durch einen genau definierten „Strauß" von technischen und organisatorischen Maßnahmen zwar die erforderlichen Internet-Funktionalitäten zur Verfügung gestellt, die riskanten aber eliminiert werden. Die Vorgehensweise des Kreises ist in doppelter Hinsicht bemerkenswert: Zunächst wurde bereits während der Planungsphase festgelegt, welche Formen der Internet-Nutzung durch die Mitarbeiterinnen und Mitarbeiter einen Sinn machen und bei welchen die damit verbundenen Risiken in einem unangemessenen Verhältnis zum Nutzen stehen. Auf diese Weise war es z. B. möglich, einen **Katalog** nutzbringender und gleichzeitig **vertrauenswürdiger WWW-Sites** aufzustellen und E-Mails mit Anhängen als so unerwünscht zu klassifizieren, dass sie erst nach einer individuellen Überprüfung durch die IT-Abteilung ausnahmsweise auf dem Arbeitsplatz zur Verfügung gestellt werden. Ein weiterer wesentlicher Punkt des Sicherheitskonzeptes besteht in der Absicht, die realisierte Lösung vor ihrem Echteinsatz von einem versierten externen Internet-Dienstleistungsunternehmen auf ihre Wirksamkeit hin testen zu lassen. Die Finanzmittel hierfür waren von vornherein eingeplant. Dabei gehen die Projektverantwortlichen nicht davon aus, dass sie bereits im ersten Anlauf eine schlechthin „sichere" Lösung gefunden haben. Die Tests sollen vielmehr zu weiteren Optimierungen führen, sodass sich Erfolg versprechende Angriffe aus den fremden Netzen so aufwändig gestalten, dass potenzielle Angreifer hinreichend wirksam abgeschreckt werden. Das Projekt wird Anfang 2001 in die Testphase gehen. Auch über dessen Ergebnisse werden wir berichten.

KES, Dezember 2000

Management verschläft Sicherheit ...

22.000 DM pro Jahr und Mitarbeiter werden derzeit in den Unternehmen im Schnitt für die IT investiert. Nur rund ein Dreißigstel davon, 800 DM, wird für die IT-Sicherheit ausgegeben.

Was ist zu tun?
Wer nicht die Geduld aufbringt, bis zur Entwicklung und Erprobung von Musterlösungen die Internet-Kommunikation über isolierte Rechner zu realisieren, kommt an der Entwicklung eines maßgeschneiderten Sicherheitskonzeptes nicht vorbei. Die derzeit auf dem Markt angebotenen Sicherheitsprodukte sind zwar nützlich, führen aber ohne eine Anpassung an die jeweiligen Gegebenheiten nicht zu dem erforderlichen Sicherheitsgewinn.

4.1.3 Datenschutz bei Mandatsträgern

Die Einhaltung des Datenschutzes ist auch im ehrenamtlichen Bereich der Gemeinden sicherzustellen. Eine Gemeinde hat aus diesem Grund in Zusammenarbeit mit uns vorbildliche Regelungen für die Geschäftsordnung der Gemeindevertretung und die Ausschüsse entworfen.

Auch **kommunale Mandatsträger** dürfen als Funktionsträger der Behörde personenbezogene Daten nur verarbeiten, soweit dies für ihre rechtmäßige Aufgabenerfüllung erforderlich ist. Diese Datenverarbeitung ist sowohl im automatisierten wie im konventionellen Bereich durch ausreichende technische und organisatorische Datensicherheitsmaßnahmen zu schützen. Dazu gehören z. B. auch Regelungen über die Speicherung und Verwendung vertraulicher Sitzungsunterlagen durch Mandatsträger.

Notwendige Detailregelungen für die Daten verarbeitende Stelle können bei einer Gemeinde nicht durch den Bürgermeister getroffen werden, da er insoweit keine Weisungsbefugnisse gegenüber der Gemeindevertretung als Organ der Behörde hat. Selbst bei Kommunen, die bereits über eine allgemeine Datenschutzdienstanweisung für die Verwaltung verfügen, entfaltet diese gegenüber den Mandatsträgern keine Wirkung.

In einem Pilotprojekt haben wir jetzt die Gemeinde **Henstedt-Ulzburg** bei der Aufnahme entsprechender Regelungen in die Geschäftsordnung der Gemeindevertretung beraten. Zunächst wurden die Gemeindevertreter im Rahmen einer Informationsveranstaltung von uns über die rechtlichen Rahmenbedingungen aufgeklärt. Anschließend konnten sie selbst unter Beachtung der gesetzlichen Maßgaben, insbesondere des Landesdatenschutzgesetzes sowie der Gemeindeordnung, in der Geschäftsordnung den Begriff des Erforderlichen für ihre Arbeit konkretisieren sowie einheitliche Datenschutzstandards für alle Mandatsträger in geeigneter Weise verbindlich festlegen.

Die inzwischen beschlossene Geschäftsordnung ist aus unserer Sicht geeignet, einen guten und wichtigen Beitrag zur Regelung der Datenverarbeitung durch kommunale Mandatsträger zu leisten. Die Stadt Kaltenkirchen hat sich dem Beispiel bereits angeschlossen und eine entsprechende Novellierung ihrer Geschäftsordnung verabschiedet. Andere Kommunen befinden sich noch in der Beratungsphase.

Die von der Gemeinde Henstedt-Ulzburg beschlossenen Regelungen können auf unserer Homepage nachgelesen werden unter:

www.datenschutzzentrum.de/material/themen/divers/dsingo.htm

Was ist zu tun?
Jede Kommune sollte für ihren Bereich prüfen, ob sie über ausreichende Regelungen zum Datenschutz für ihren ehrenamtlichen Bereich verfügt. Die Regelungen der Gemeinde Henstedt-Ulzburg können dabei als Messlatte herangezogen werden.

4.1.4 Welche von den Kommunen betriebene Gesellschaften „müssen" das LDSG anwenden?

Viele Kommunen haben GmbHs und andere Gesellschaften gegründet, die die Ver- und Entsorgung oder den Nahverkehr abwickeln. Für die Datenverarbeitung dieser Gesellschaften gilt das LDSG, wenn sie Aufgaben der Daseinsvorsorge erbringen.

Die Stadtwerke, Verkehrs- und Entsorgungsbetriebe vieler größerer Kommunen Schleswig-Holsteins werden neuerdings als **GmbH** organisiert, an der die öffentliche Hand die Mehrheit der Anteile hält. Sie betreiben ihrerseits nicht selten verschiedene privatrechtlich organisierte Tochtergesellschaften, deren Geschäftszwecke im Bereich der Energie- und Wasserversorgung sowie in der Durchführung des öffentlichen Personennahverkehrs angesiedelt sind, teilweise werden Telekommunikationsdienstleistungen und dergleichen erbracht.

Im Rahmen von Beratungen wiesen wir auf Folgendes hin: Das neue LDSG findet auch Anwendung auf Vereinigungen des privaten Rechts, die von juristischen Personen des öffentlichen Rechts beherrscht werden und die **Aufgaben der öffentlichen Verwaltung** wahrnehmen. Der Gesetzgeber hat so einer Verschlechterung des Datenschutzes der Bürgerinnen und Bürger durch Privatisierung entgegengewirkt. Entscheidendes Kriterium für die Anwendung des LDSG ist nämlich die Erfüllung öffentlicher Aufgaben, insbesondere im Bereich der **Daseinsvorsorge**. Die Energie- und Wasserversorgung sowie die Gewährleistung des öffentlichen Personennahverkehrs gehören zur Daseinsvorsorge, was für die Energieversorgung ausdrücklich durch das Bundesverfassungsgericht festgestellt wurde. Dagegen zählt die Erbringung von Telekommunikationsdienstleistungen seit der Liberalisierung dieses Sektors nicht mehr zur Daseinsvorsorge, sondern es handelt sich hierbei um eine privatwirtschaftliche Tätigkeit, sodass das LDSG nicht zwingend anzuwenden ist.

Wir wiesen aber auf Folgendes hin: Auch wenn das Landesdatenschutzgesetz nicht zwingend auf juristische Personen des Privatrechts angewandt werden muss, so ist dies natürlich keineswegs „verboten“. Im Zeitalter der **Service- und Kundenorientierung** steht es Unternehmen der öffentlichen Hand gut an, ihren Kunden den Service des schleswig-holsteinischen Landesdatenschutzgesetzes anzubieten, der besser ist als der des Bundesdatenschutzgesetzes. Viele Kunden wissen es zu schätzen, wenn ihnen ein gutes, einheitliches Datenschutzniveau auch dann geboten wird, wenn die öffentliche Hand private Gesellschaften betreibt.

Was ist zu tun?
Privatrechtliche Vereinigungen, an denen öffentliche Stellen die Mehrheit der Anteile halten, müssen das LDSG anwenden, wenn sie Leistungen der Daseinsvorsorge erbringen. Das ist bei vielen Infrastrukturleistungen der Fall. Es steht ihnen frei, den Datenschutzservice des LDSG auch darüber hinausgehend anzubieten.

4.1.5 Nachweis der Elterndaten bei der melderechtlichen Anmeldung

Bisher mussten „Kinder“ bis zur Vollendung des 27. Lebensjahres bei der melderechtlichen Anmeldung die Daten ihrer Eltern nachweisen. Dieses bürokratische Verfahren wird jetzt abgeschafft.

Nach der Änderung des schleswig-holsteinischen Meldegesetzes und der Meldescheinverordnung wurde auch das im Melderegister zu speichernde Datenprofil geändert. Die Meldeämter sind seitdem verpflichtet, von Meldepflichtigen, die das 27. Lebensjahr noch nicht vollendet haben, **Name**, **Anschrift** und **Geburtsdatum** der **Eltern** zu erheben. Laut amtlicher Begründung zum Meldegesetz sollten durch die Änderung die melderechtlichen Voraussetzungen für die Berücksichtigung der vielfältigen Eltern-Kind-Beziehungen, die auch nach Vollendung des 18. Lebensjahres eines Kindes bestehen, geschaffen werden. Insbesondere sollte damit die Erteilung notwendiger Bescheinigungen für den Bereich der sozialen Sicherung (z. B. an die Zentralstelle für die Vergabe von Studienplätzen) erleichtert werden. Die Altersgrenze von 27 Jahren wurde gewählt, weil sie auch in anderen Rechtsbereichen (z. B. bei der Gewährung von Kindergeld) maßgeblich ist.

Bereits bei der Einführung der neuen Regelung in die Praxis hat sich gezeigt, dass damit ein erheblicher **bürokratischer Mehraufwand** verbunden ist, der in Anbetracht der großen Fallzahlen bei der meldebehördlichen Anmeldung spürbare Auswirkungen auf die gesamte Arbeitsbelastung der Meldebehörden haben musste. Hinzu kam in vielen Fällen der Unmut der Betroffenen, die den Sinn der Datenspeicherung bei volljährigen Personen nicht einzusehen vermochten.

Da die Daten im Einzelfall Grundlage für Bescheinigungen oder für Datenübermittlungen sein sollen, muss natürlich auch deren Richtigkeit von der Meldebehörde in einem Mindestmaß überprüft werden. Bei einer kreisfreien Stadt wurden zu diesem Zweck von den Meldepflichtigen regelmäßig **Kopien der Personalausweise** der Eltern gefordert und gegebenenfalls bei Nichtvorlage ein

Bußgeldverfahren eingeleitet. Aufgrund unseres Hinweises, dass solche Unterlagen nicht der Verfügungsgewalt und damit der Auskunftspflicht der meldepflichtigen Kinder unterliegen, sind die anhängigen Bußgeldverfahren eingestellt worden.

Aus datenschutzrechtlicher Sicht rechtfertigen die in der amtlichen Begründung angegebenen Zwecke nicht eine derart komplizierte Datenerhebung. In Gesprächen mit dem Innenministerium konnte jetzt Einvernehmen darüber erzielt werden, die **Meldescheinverordnung** so abzuändern, dass nur noch von Minderjährigen im Zuge der Anmeldung Angaben zu ihren Eltern erhoben werden. Wir sehen darin einen begrüßenswerten Beitrag zur Entbürokratisierung des Meldewesens.

Was ist zu tun?
Die Meldebehörden können künftig auf die Erhebung der Elterndaten bei der Anmeldung volljähriger Personen verzichten.

4.2 Polizeibereich

4.2.1 Überblick

Die schleswig-holsteinische Polizei hat durch die frühzeitige Bestellung gut ausgebildeter behördlicher Datenschutzbeauftragter die Weichen in die richtige Richtung gestellt. Infolgedessen ist eine wachsende Souveränität der Dienststellen in der Fläche beim Umgang mit personenbezogenen Unterlagen zu beobachten, wobei allerdings im Bereich der elektronischen Datenverarbeitung vor Ort nach wie vor Defizite bestehen (vgl. Tz. 4.2.4, 4.2.6, 4.2.7 und 7.5.1). Die Einführung von **INPOL-neu** ab 2001 wird die gesamte polizeiliche Datenverarbeitungslandschaft verändern und sich auch auf die Vorgangsbearbeitung in allen Dienststellen auswirken. Diese Umstellung sollte vom Innenministerium dazu genutzt werden, noch vorhandene systematische Unstimmigkeiten der landesinternen polizeilichen EDV zu beseitigen (Tz. 4.2.2 und 4.2.5). Die Einführung von INPOL-neu wird von der deutschen Polizei auch als einmalige Gelegenheit zur Realisierung von Wünschen ergriffen, die rechtlich nicht abgedeckt sind. Sie geht dabei bewusst über die Einwände der Datenschutzbeauftragten hinweg.

4.2.2 INPOL-neu

Das in einem der teuersten IT-Projekte der letzten Jahre entwickelte neue INPOL-System der deutschen Polizei befindet sich seit Oktober 2000 im Probebetrieb und soll bis spätestens 2003 flächendeckend eingeführt sein. Mit zunehmendem Realisierungstempo zeigt sich, dass die Polizei viele Anregungen der Datenschutzbeauftragten bewusst übergeht. Wie INPOL-neu in Schleswig-Holstein in die bestehende polizeiliche EDV eingebunden wird, ist derzeit noch mit etlichen Fragezeichen versehen.

Bezüglich der im letzten Tätigkeitsbericht aufgeführten datenschutzrechtlichen Problempunkte des Projekts INPOL-neu (vgl. 22. TB, Tz. 4.2.2) hat sich im Berichtszeitraum bedauerlicherweise nichts zum Positiven bewegt. Die von allen Datenschutzbeauftragten einhellig abgelehnte **Erweiterung des bundesweit verfügbaren Kriminalaktennachweises** um überregional nicht bedeutsame oder erhebliche Straftaten soll tatsächlich erfolgen, ohne dass hierfür eine ausreichende Rechtsgrundlage besteht.

Die **Errichtungsanordnungen** für die so genannten „logischen Dateien", die den einheitlichen Datenpool entscheidend strukturieren, sind trotz intensiver Beratung durch die Datenschutzbeauftragten im vergangenen Jahr nicht wesentlich vorangekommen, obwohl sie für die Frage der Verhältnismäßigkeit und Rechtmäßigkeit der Datenspeicherungen und -übermittlungen von entscheidender Bedeutung sind. Es wäre fatal, wenn die Fragen der Rechtmäßigkeit dieses polizeilichen Data-Warehouses aufgrund des zunehmenden Zeitdrucks, unter dem das Projekt realisiert wird, nicht ausreichend erörtert und die Errichtungsanordnungen in der Schlussphase des Projekts „durchgepaukt" würden.

Angesichts der technisch nahezu unbegrenzten Verfügbarkeit der Informationen im Datenpool sind auch **differenzierte Zugriffsberechtigungen** entsprechend der jeweiligen fachlichen Erforderlichkeit der einzelnen Nutzer unerlässlich. Auch zu dieser in einem Landesberechtigungskonzept zu entscheidenden Frage konnte uns die Polizei noch keine Konzepte vorlegen. Schließlich bleibt als dritte Unbekannte das **Sicherheitskonzept**. Die zuständige Projektgruppe beim BKA hat es den Ländern noch nicht einmal als Entwurf vorgestellt.

Auch wie die **schleswig-holsteinische** polizeiliche **Datenverarbeitung** an INPOL-neu angepasst wird, kann das Innenministerium immer noch nicht beschreiben. Im letzten Jahr hat es einen kompletten Zuständigkeitswechsel innerhalb des Ressorts gegeben. Es wurde ein so genanntes Anwenderforum konstituiert. Die Entwicklung eines landesspezifischen IT-Konzeptes und eines Sicherheitskonzeptes obliegt nicht mehr der Polizei, sondern der Allgemeinen Abteilung. Das Vorgangsbearbeitungssystem COMPAS muss in diesem Zusammenhang ebenfalls umprogrammiert werden (vgl. Tz. 4.2.5).

Das Problem der Anpassung der Landesdatenhaltung an die Vorgaben des Informationsverbundes wurde, wie es sich bereits im Vorjahr andeutete (vgl. 22. TB, Tz. 4.2.2) zwischenzeitlich tatsächlich auf das BKA delegiert. Mittlerweile möchte nämlich die Mehrzahl der Länderpolizeien die **Landesdatenbestände**, die aus verfassungsrechtlichen Gründen nicht bundesweit verfügbar sein dürfen, z. B. Bagatelldelikte, nicht nur übergangsweise, sondern möglichst **auf Dauer** durch das BKA **als Auftragnehmer** verarbeiten lassen. Bislang bestand Konsens in Deutschland, dass derartige Delikte nicht bundesweit abrufbar gespeichert werden dürfen. Eine Beleidigung im Rahmen eines Nachbarschaftsstreits in Husum z. B. muss nicht für die Polizei in Rosenheim abrufbar sein, sondern allenfalls innerhalb Schleswig-Holsteins. Die möglichen „Vorteile" einer Auslagerung solcher Landesdaten hin zum BKA sind aus Polizeisicht evident: Länderübergreifende Zugriffe wären auf einer gemeinsamen technischen Plattform ebenso denkbar wie

Abgleiche quer durch diese Landesbestände. Technisch sollen die im Auftrag zu verarbeitenden Landesdaten nämlich in derselben Datenbank abgelegt und nur durch ein jederzeit **umschaltbares Attribut „Bund Ja/Nein“** von Verbunddaten getrennt werden. Dies wäre eine technische Ausgangslage, die mit Sicherheit **Begehrlichkeiten** wecken würde, sobald die Erinnerung an rechtliche Bedenken bei der Umstrukturierung der Datenlandschaft verblasst ist.

Während das Bundesinnenministerium im vergangenen Jahr noch Zweifel hatte, ob eine Auftragsdatenverarbeitung in diesem Umfang nach dem Bundeskriminalamtsgesetz zulässig sei, vertritt es nun die Auffassung, eine **Entscheidung des Gesetzgebers** müsse selbst für eine dauerhafte Auftragsdatenverarbeitung nicht herbeigeführt werden. Diese Position wurde auch mit der Stimme Schleswig-Holsteins in der Innenministerkonferenz festgeschrieben. Selbst die von allen Datenschutzbeauftragten vertretene Auffassung, dass eine zentralisierte Datenhaltung die verfassungsrechtlich geforderte informationelle Trennung von Landes- und Verbunddaten gefährdet, konnte diese Entwicklung nicht aufhalten. Die Polizei argumentiert, eine zentrale Landesdatenhaltung beim BKA sei **kostengünstiger** als eine landesspezifische Eigenentwicklung. Allerdings bietet das BKA den Ländern nach wie vor die Übernahme einer Version der INPOL-Datenbank an, auf deren Grundlage auch Schleswig-Holstein seine Daten mit vertretbarem Aufwand wieder selbst verarbeiten könnte, sobald das Übergangsproblem des zeitgerechten Anschlusses an INPOL-neu gelöst ist. Nachdem Schleswig-Holstein zunächst immer für eine eigene Verarbeitung der Landesdaten eingetreten war und sich zwischenzeitlich lediglich an einer übergangsweisen Auslagerung der Daten an das BKA beteiligen wollte, kündigte der Innenminister nun eine „Neupositionierung“ zu dieser Frage an. Auf der Innenministerkonferenz hat er zu Protokoll gegeben, Schleswig-Holstein werde eine Entscheidung über eine dauerhafte Landesdatenhaltung erst „nach umfassender rechtlicher Prüfung“ treffen.

Wir haben ihm daraufhin detaillierte Vorstellungen zur datenschutzgerechten Gestaltung eines **Vertrages** über die beabsichtigte **Auftragsdatenverarbeitung** in einer Übergangszeit übermittelt. Dieser muss gewährleisten, dass

- der Umfang der beim BKA verarbeiteten Daten genau festgeschrieben wird,
- die Daten der einzelnen Länder logisch voneinander abgeschottet werden und nur im Einzelfall auf Anordnung des Auftraggebers anderen Ländern oder dem BKA zugänglich sind,
- datenschutzrechtliche Kontrollen nach Landesrecht nach wie vor möglich sind,
- er vom Auftraggeber kündbar ist, sobald eine eigene Landesdatenhaltung aufgebaut ist.

Zudem muss das Sicherheitskonzept des BKA geprüft und als ausreichend bewertet werden, bevor die Landespolizei die Daten schleswig-holsteinischer Bürger an das BKA gibt. Zwischenzeitlich hat sich eine Kooperation zwischen Hamburg und Hessen zur Entwicklung eines gemeinsamen Prototyps für eine eigene INPOL-neu-fähige Landesdatenhaltung gebildet. Damit ist das Argument vom Tisch, man habe praktisch keine andere Wahl, als die Daten vom BKA verarbeiten zu lassen.

Was ist zu tun?
Der Innenminister sollte auf einer datenschutzgerechten Ausgestaltung des Vertrages über die vorübergehende Auftragsdatenverarbeitung beim BKA bestehen und unter Nutzung des Softwareangebotes des BKA baldmöglichst wieder eine eigene Datenhaltung aufbauen.

4.2.3 Trotz Freispruchs im Polizeicomputer

Trotz eines eindeutigen gerichtlichen Freispruchs weigert sich die Polizei in einem Einzelfall, die Daten in der Kriminalakte und im INPOL-System zu löschen, weil sie nach wie vor einen Tatverdacht hegt.

Bei der Überprüfung der Kriminalakte eines Petenten stellte sich heraus, dass diese Daten zu einem Strafverfahren enthielt, das für den Petenten mit einem **Freispruch** geendet hatte. Das **Gericht** hatte in seinen **Urteilsgründen** das tatbestandsmäßige Vorliegen einer Straftat eindeutig verneint. Damit war – auch für die Polizei bindend – der dem Ermittlungsverfahren zugrunde liegende Tatverdacht entfallen. Gemäß **§ 189 Abs. 2 Satz 3 Landesverwaltungsgesetz** (LVwG) waren die entsprechenden Unterlagen auszusondern. Auch die vom Innenministerium erlassenen Richtlinien für die Führung **kriminalpolizeilicher personenbezogener Sammlungen** sind in diesem Punkt eindeutig: Sie sehen für derartige Fälle eine Aussonderung vor, sofern nicht anhand des Urteils festgestellt wird, dass die Voraussetzungen für eine Speicherung weiterhin gegeben sind. Die Polizei glaubt jedoch trotz des eindeutig formulierten Urteils noch an einen „**Resttatverdacht**“ und erhält die Speicherung in der Kriminalakte und im INPOL-System trotz unserer Beanstandung aufrecht.

Im Wortlaut:
§ 189 Abs. 2 Satz 3 LVwG

Entfällt der dem Ermittlungsverfahren zugrunde liegende Verdacht, sind die Daten zu löschen.

Im Wortlaut: Kps-Richtlinie

Im Falle eines rechtskräftigen Freispruchs sind die Unterlagen [...] auszusondern, sofern nicht anhand des Urteils festgestellt wird, dass die Voraussetzungen gem. § 189 Abs. 1 LVwG weiterhin gegeben sind.

Was ist zu tun?
Das Innenministerium sollte die Daten löschen lassen.

4.2.4 Prüfung der Computer bei der Polizeiinspektion Eutin

Die Überprüfung der automatisierten Datenverarbeitung bei einer Polizeiinspektion zeigte gravierende Mängel beim Einsatz von unvernetzten Arbeitsplatzrechnern auf. Auch das Vorgangsbearbeitungssystem COMPAS lässt sich im Detail datenschutzrechtlich verbessern.

Nachdem wir die Entwicklung des Vorgangsbearbeitungssystems COMPAS über mehrere Jahre beratend begleitet hatten (vgl. 19. TB, Tz. 4.2.4), sollte eine Vor-Ort-Prüfung bei der PI Eutin uns eine Bewertung der tatsächlichen Verfahrensweise ermöglichen. Gleichzeitig haben wir die Datenverarbeitung mithilfe der unvernetzten Arbeitsplatzrechner (APC) untersucht. Die technisch-organisatorischen Aspekte werden unter Tz. 7.5.1 dargestellt.

Hinsichtlich der **rechtlichen Anforderungen** an die polizeiliche Datenverarbeitung ergab sich, dass die Erfassung und Speicherung personenbezogener Daten im Rahmen der Fachanwendung COMPAS gut strukturiert und im Großen und Ganzen korrekt war. Als problematisch waren jedoch folgende Sachverhalte anzusehen:

- Die Grundkonzeption des Vorgangsbearbeitungssystems sah bei Recherchen nach Personen bewusst eine Restriktion der Art vor, dass stets angegeben werden musste, in welcher „Rolle/Eigenschaft“ man die betreffende Person suchte. Gespeichert sind nämlich nicht nur Täter, Verdächtige und Beschuldigte, sondern auch Zeugen, Hinweisgeber, Geschädigte, Opfer usw. Die letztgenannten Personengruppen sollten bei Abfragen nicht standardmäßig als „polizeibekannt“ präsentiert und somit mit der eigentlichen polizeilichen Klientel in einen Topf geworfen werden. Diese an sich vernünftige Trennung ist „auf Wunsch der Anwender“ zwischenzeitlich aufgehoben worden. Worin die Erforderlichkeit für diese Erweiterung der Funktionalität der Recherche konkret besteht, hat das Innenministerium aus unserer Sicht bislang noch nicht schlüssig dargelegt.
- Die einzelnen Mitarbeiter konnten den Zugriff der Dienststellenleitung auf von ihnen erstellte Dokumente in der zentralen Ablage ausschließen. Nach der einschlägigen Dienstanweisung war dies zwar nicht zulässig, da Dienst- und Fachaufsichtsbefugnisse erhalten bleiben müssen. Ein derartiger Ausschluss lässt sich nach Aussage des Innenministeriums aber technisch nicht unterbinden. Dieser Zustand kann unseres Erachtens nicht auf Dauer akzeptiert werden. Nach einer technischen Lösung sollte daher weiter gesucht werden.
- Eine Löschung von Vorgangsverwaltungsdaten nach den in Dienstanweisungen vorgesehenen Fristen von fünf Jahren (Strafverfahren) bzw. zwei Jahren (Vorgänge der Gefahrenabwehr) erfolgte nicht programmgesteuert, sondern musste manuell angestoßen werden. Eine wesentliche Vorgabe aus dem COMPAS-Konzept ist somit nicht umgesetzt worden. Dies ist offenbar auch vielen Polizeidienststellen unbekannt, wie unsere Kontrollen in der Form von AUK (vgl. Tz. 4.2.5) gezeigt haben. Die Dienstanweisungen enthalten keinen Hinweis, dass Löschungen manuell initiiert werden müssen. Viele Mitarbeiter und

auch wir waren überrascht, dass hochmoderne Datenverarbeitungstechnik „alles“ kann, nur nicht Daten nach Fristablauf automatisch löschen. Einen Grund hierfür hat das Innenministerium in seiner Stellungnahme zum Prüfbericht nicht nennen können.

- Es bestanden keine Regelungen darüber, ob und wie die Personaldaten der eigenen Mitarbeiter mithilfe der auf die polizeiliche Arbeit ausgerichteten IT-Systeme verarbeitet werden können bzw. dürfen. Es geht z. B. um die Frage, wie lange Beurteilungen oder andere Dokumente mit Personalaktendatenqualität gespeichert werden dürfen und wer Zugriff auf sie haben darf. Wir haben eine landesweit geltende Dienstanweisung hierzu vorgeschlagen. Das Innenministerium hat Schulungen im Bereich der automatisierten Verarbeitung von Personaldaten angekündigt.
- Auf den elektronischen lokalen „Schreibtischen“ der Mitarbeiter stellten wir eine Reihe von personenbezogenen Sachverhalten fest, u. a. einen Observationsbericht, ein Vernehmungsprotokoll, Lageberichte und Alarm- bzw. Einsatzpläne, deren Speicherung nach der Dienstanweisung der PD „grundsätzlich“ untersagt ist. Die Daten waren im Falle eines Systemabsturzes nicht gesichert und bei Abwesenheit des betreffenden Mitarbeiters für Kollegen oder Vorgesetzte nicht verfügbar.
- Auf den unvernetzten Arbeitsplatzrechnern fanden wir eine Vielzahl von personenbezogenen Dokumenten, die ersichtlich keiner geordneten Datenpflege unterlagen und für die eine Erforderlichkeit der Speicherung nicht genannt werden konnte. Es handelte sich um Einsatzberichte, Lagemitteilungen, Beurteilungen und dergleichen, die von mehreren Nutzern über einen längeren Zeitraum erstellt worden waren. Sie waren unsystematisch bezeichnet und geordnet, sodass einzelfallbezogene Entscheidungen über die Löschung äußerst aufwändig gewesen wären. Diesen desolaten Zustand haben wir beanstandet.

Das Innenministerium hat in seiner Stellungnahme zu einigen dieser Probleme Konsequenzen im Bereich der Schulung und Erstellung von Dienstanweisungen angekündigt. Die übrigen datenschutzrechtlichen Verbesserungsmöglichkeiten müssen aus unserer Sicht im Zuge der Weiterentwicklung von COMPAS auf Grundlage des Landessystemkonzepts mit realisiert werden.

Was ist zu tun?
Das Innenministerium sollte unsere Verbesserungsvorschläge bei der Entwicklung des COMPAS-Nachfolgesystems berücksichtigen. Die Datenverarbeitung mithilfe unvernetzter APC sollte in allen Bereichen der Polizei gründlich überprüft und den rechtlichen Anforderungen angepasst werden.

4.2.5 Bürokommunikation muss reorganisiert werden

Angekündigte/unangekündigte Kontrollen wurden in diesem Jahr bei Dienststellen im Bereich der Polizeidirektion Schleswig-Holstein Mitte sowie der Wasserschutzpolizeidirektion durchgeführt. Immer wieder zeigten sich dabei Mängel im Bereich der automatisierten Datenverarbeitung.

Gravierende Mängel in der **konventionellen Datenverarbeitung** konnten im Rahmen dieser Überprüfungen nicht festgestellt werden. Im Bereich der automatisierten Datenverarbeitung war allerdings unübersehbar, dass sowohl beim Einsatz des in COMPAS integrierten Standardtextverarbeitungsprogramms „Siform“ als auch beim Einsatz von **Arbeitsplatzcomputern** (APC) hinsichtlich der Verarbeitung von personenbezogenen Informationen keine ausreichenden Vorgaben gemacht wurden. So wird in der Regel den einzelnen Anwendern die **Organisation der Ablage** überlassen. Auch über die Zugriffsberechtigungen und die Speicherungsdauer von Dokumenten entscheiden sie selbst. Dies führt dazu, dass **effektive Kontrollen** seitens der verantwortlichen Dienstvorgesetzten nahezu **unmöglich** gemacht werden.

Daher sollten die Dienstanweisungen durch konkrete Handlungsanweisungen zur

- Ausgestaltung der Ablagestruktur,
- Speicherung bzw. Löschung von Dokumenten sowie
- zur Festlegung der Verantwortlichkeiten hinsichtlich der Kontrolle auf Einhaltung der Vorgaben

präzisiert werden. Darüber hinaus sollten Regelungen zur Vergabe von Zugriffsrechten, insbesondere bei Ermittlungsverfahren mit besonders sensiblem Inhalt oder Personaldaten, getroffen werden.

Was ist zu tun?
Die Nutzung der Bürokommunikationssoftware im Bereich der Strafverfolgung und der Gefahrenabwehr muss dringend reorganisiert werden.

4.2.6 Multimediarechner bei der Polizei

Im Rahmen des Projektes „Polizei ans Netz“ wurden die Ämter, Direktionen und Inspektionen der Polizei mit Multimediarechnern ausgestattet. Die Polizei präsentiert sich und recherchiert seitdem im Internet.

Seit Mitte des Jahres sind in mehr als 20 Polizeidienststellen Multimediarechner im Einsatz, die – vom übrigen Polizeinetz abgekoppelt – **Internet-Recherchen** ermöglichen und insbesondere zur schnellen Verteilung von Pressemitteilungen an ca. 260 Agenturen genutzt werden. Außerdem kann die Polizei über den E-Mail-Dienst des Internets mit Bürgern in Kontakt treten und von ihnen E-Mails empfangen.

Während die Recherche und die Pressearbeit datenschutzrechtlich nicht problematisch sind, hat sich die Polizei mit der Eröffnung des **E-Mail-Verkehrs** einige Probleme ins Haus geholt, die nicht ganz einfach zu lösen sind. Zunächst ist dafür Sorge zu tragen, dass keine **unverschlüsselten** E-Mails mit sensiblem personenbezogenem Inhalt versandt werden. Dies lässt sich nicht technisch unterbinden, sodass entsprechende Dienstanweisungen erlassen und ein manuelles Kontrollsystem eingerichtet werden muss.

Sodann müssen die potenziellen E-Mail-Absender darauf **hingewiesen** werden, dass auch E-Mails an die Polizei nicht vor Ausspähungen und Verfälschungen geschützt sind. Dies war zum Zeitpunkt des Projektstarts noch nicht erfolgt und wurde erst auf unsere Information hin nachgebessert. Ausreichende technisch-organisatorische Regelungen, insbesondere Dienstanweisungen und Sicherheitskonzepte, liegen noch nicht vor.

Schleswig-Holstein DATENSCHUTZAKADEMIE
Kurs NET

Was ist zu tun?
Die noch fehlenden Regelungen sollten kurzfristig erstellt werden. Außerdem ist wegen der besonderen Risiken des Internets die ordnungsgemäße Nutzung der Multimediarechner regelmäßig zu überwachen.

4.2.7 Evaluierung des Einsatzes besonderer Ermittlungsmaßnahmen

Nach einer Untersuchung des Fachbereichs Polizei der Verwaltungsfachhochschule Altenholz im Auftrag des Innenministeriums wird von den Befugnissen der Strafprozessordnung zum Einsatz technischer Mittel in Schleswig-Holstein relativ moderat Gebrauch gemacht. Die Ermittlungsakten selbst bieten im Nachhinein wenig nachvollziehbare Anhaltspunkte, warum eine bestimmte Maßnahme durchgeführt wurde. Insgesamt hält das Gutachten die rechtlichen Möglichkeiten für verdeckte technische Mittel wie auch deren Umsetzung in der schleswig-holsteinischen Praxis für angemessen.

Hintergrund der Studie war die Forderung der Datenschutzbeauftragten, angesichts der stetigen Ausweitung des Eingriffsinstrumentariums für die Strafverfolgungsbehörden eine wissenschaftliche **Evaluierung** des **Bedarfs** an besonderen Befugnissen und deren **Wirkung auf die Grundrechte** von Betroffenen vorzunehmen. Eine solche Rechtstatsachenuntersuchung soll dem Gesetzgeber eine empirische Grundlage für die Entscheidung darüber liefern, inwieweit das gegenwärtige Instrumentarium aufrechtzuerhalten und wie mit den regelmäßigen Forderungen aus Polizeikreisen nach weiteren Befugnissen umzugehen ist (vgl. 17. TB, Tz. 4.1.2.1).

Die 1995 beim BKA eingerichtete Bund-Länder-**Rechtstatsachensammelstelle** war von uns wie auch vom Innenministerium wegen ihres Ansatzes kritisiert worden, lediglich Einzelfälle zu präsentieren, die ein Bedürfnis der Strafverfolgungsbehörden nach weiterem Ausbau ihrer Eingriffsgrundlagen belegen sollten. Das ursprüngliche Vorhaben des Innenministeriums, in Schleswig-Holstein eine eigene, wissenschaftlich fundierte Sammelstelle für alle Fälle des Einsatzes beson-

ders in Grundrechte eingreifender, verdeckter Ermittlungsmaßnahmen einzurichten (vgl. 18. TB, Tz. 10.1), konnte aus finanziellen Gründen bislang nicht realisiert werden. Das Innenministerium erteilte jedoch 1998 einen **Gutachtenauftrag** an den Fachbereich Polizei der Verwaltungsfachhochschule Altenholz (vgl. 21. TB, Tz. 4.2.8). Dieser beinhaltete die Untersuchung von Ausmaß und Auswirkungen des Einsatzes besonderer Mittel der Datenerhebung nach der StPO aus abgeschlossenen Strafverfahren im Hinblick auf die Anzahl der Betroffenen, den zeitlichen und räumlichen Umfang, die Beweiserheblichkeit der erlangten Erkenntnisse und der denkbaren Alternativen. Ziel der Untersuchung sollte es sein, festzustellen, ob geringer in Grundrechte eingreifende Maßnahmen hätten ergriffen werden können, auf der anderen Seite aber auch, ob das vorhandene gesetzliche Instrumentarium für die Polizei die erforderlichen Möglichkeiten bot.

Inzwischen wurden Zahlen bekannt, die einen erschreckenden Anstieg bundesweit durchgeführter **Telefonüberwachungen** erkennen ließen. Nachdem die Bundesjustizministerin 1999 ihrerseits einen Gutachtenauftrag an das Max-Planck-Institut für internationales Strafrecht zur Evaluierung der „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation“ vergeben hatte, wurden die Telefonüberwachungsmaßnahmen – mit dem zahlenmäßig größten Anteil an besonderen Ermittlungsmaßnahmen – mit Rücksicht auf die Bundesstudie aus dem schleswig-holsteinischen Vorhaben herausgenommen. Auf die Ergebnisse des Max-Planck-Instituts, die für ca. Ende 2001 erwartet werden, darf man gespannt sein.

Ende des letzten Jahres übersandte uns der Innenminister das Gutachten. Es untersucht aus dem Zeitraum von 1995 bis 1998 die Justizermittlungsakten von insgesamt 47 abgeschlossenen Strafverfahren, in denen nach den Aufzeichnungen des LKA **technische Mittel nach § 100c StPO** eingesetzt worden waren, sowie die Akte eines Verfahrens, in dem eine Rasterfahndung durchgeführt worden war. Das Gutachten kommt im Wesentlichen zu folgenden Ergebnissen:

- In einer durchaus erheblichen Anzahl der vom LKA verzeichneten Fälle – 16 von 47 – ließ sich in der Ermittlungsakte der Justiz gar kein Einsatz technischer Mittel (Bild- oder Tonaufnahmen) feststellen. Entweder sind tatsächlich keine besonderen Maßnahmen durchgeführt worden, oder sie sind erfolglos verlaufen und aus diesem Grunde nicht in der Justizakte dokumentiert worden. In den verbleibenden 31 Verfahren kam es zu insgesamt 39 Einzelmaßnahmen verdeckter Bild- oder Tonaufzeichnungen.
- In 23 Fällen ergaben diese Maßnahmen ermittlungsrelevante Erkenntnisse. Diese reichten von der Dokumentation eines Kontakts (häufigstes Ergebnis) über die Dokumentation einer erfolgten Straftat und die Identifizierung von Beschuldigten, Zeugen und Kontaktpersonen bis hin zu „allgemeinen Umfelderkenntnissen“.
- Lediglich ein geringer Anteil der aus dem Einsatz verdeckter technischer Maßnahmen gewonnenen Erkenntnisse wurde unmittelbar in die Hauptverhandlung eingeführt. Meist wurden die aufgrund der gewonnenen Erkenntnisse erzielten Geständnisse der Tatbeteiligten in der Verhandlung als Beweis benannt.

- Abhörmaßnahmen erbrachten weniger brauchbare Erkenntnisse als Bildaufnahmen, nämlich lediglich in insgesamt 7 von 18 Fällen (einem Großen Lauschangriff 1998 und 17 Lauschangriffen außerhalb von Wohnungen).
- Die einzige durchgeführte Rasterfahndung erwies sich bereits in einem sehr frühen Stadium als erfolglos.
- Schwerpunktmäßig wurden die untersuchten besonderen Mittel bei Rauschgiftdelikten, außerdem noch bei Erpressung, Mord und Brandstiftung eingesetzt.
- Zur zeitlichen und räumlichen Ausdehnung der Einsätze ließ das untersuchte Material kaum Aussagen zu. Die relevanten Protokolle waren zumeist bereits vernichtet. Allerdings fiel auf, dass sich die Abhörmaßnahmen zeitlich meist unterhalb der gerichtlich angeordneten Dauer bewegten und nur wenige Tage durchgeführt wurden. Der zeitliche Umfang von Videoaufnahmen wurde allerdings nicht näher untersucht.
- Überlegungen der Strafverfolgungsbehörden und der Gerichte zur Einhaltung der jeweiligen Subsidiaritätsklausel in den Eingriffsgrundlagen ließen sich den Akten nicht entnehmen. Insbesondere beschränkten sich die richterlichen Anordnungen zumeist auf den reinen Gesetzestext und enthielten nur zu einem sehr geringen Teil überhaupt rechtliche Erwägungen, in keinem dieser Fälle jedoch zur Subsidiaritätsklausel. Die Studie bezweifelt jedoch nicht, dass die Voraussetzungen der Subsidiarität im Ergebnis vorlagen.
- Eine Weiterführung der Untersuchung wäre aufgrund der bereits geleisteten Vorarbeiten insbesondere zur Erfassungs- und Auswertungsmethodik aus Sicht der Verwaltungsfachhochschule wünschenswert.

Der Grundstock zu einer **Landesrechtstatsachensammelstelle** ist mit dem vorliegenden Gutachten bereits gelegt. Schlussfolgerungen aus der Studie müssen sicherlich unter den Vorbehalt gestellt werden, dass das ihr zugrunde liegende Mengenaufkommen recht gering ist. Dennoch zeigt das Gutachten, dass jedenfalls in Schleswig-Holstein von den untersuchten Befugnissen **verantwortungsvoll Gebrauch** gemacht wird. Ein Grund dafür, jedoch sicherlich nicht der einzige, sind nach Ansicht des Gutachters auch die begrenzten Kapazitäten der Dienststellen zur Auswertung des erhobenen Datenmaterials.

Eine sich anschließende Untersuchung könnte folgende Fragen zum Gegenstand haben:

- Wie kann sichergestellt werden, dass alle erfolgten besonderen Maßnahmen unabhängig von ihrem Ertrag für das Verfahren in der Akte dokumentiert werden, sodass für die Betroffenen im Nachhinein das Ausmaß der Grundrechtseingriffe transparent wird? Die Dunkelziffer von fast einem Drittel der in Betracht kommenden Verfahren ist aufklärungsbedürftig.
- Welches Gewicht haben die Erkenntnisse im Einzelnen, die durch besondere Maßnahmen gewonnen wurden? Der Ansatz der Studie ließe sich insoweit noch erheblich verfeinern und gewichtend zu dem Ausmaß der Grundrechtsbeeinträchtigung in Beziehung setzen. Genauere Aussagen ließen sich auch dazu herausarbeiten, wie weit die Bild- und Tonaufnahmen in die Privatsphäre der Betroffenen hineinreichten.

- Des Weiteren könnte eine bislang noch nicht durchgeführte Befragung der ermittelnden Polizeibeamten und Staatsanwälte weiteren Aufschluss zur Frage geben, welche Überlegungen beim Einsatz bestimmter Maßnahmen eine Rolle spielen und wie dabei die grundrechtlichen Positionen von Betroffenen berücksichtigt werden. Anregungen werden sich insoweit vermutlich auch aus der für dieses Jahr zu erwartenden Studie des Max-Planck-Instituts ergeben, zumal sich die Ermittlungstätigkeit der Strafverfolgungsbehörden wohl immer mehr auf die Überwachung der Telekommunikation zu verlagern scheint.

Alles in allem belegt die Studie, dass der Einsatz der besonderen Mittel der Datenerhebung im polizeilichen Alltag eine viel geringere Bedeutung hat, als es aufgeregte Debatten um angeblich unverzichtbare neue Eingriffsbefugnisse vermuten lassen. Andererseits besteht jedenfalls in Schleswig-Holstein keine Veranlassung, am verantwortungsvollen Umgang der Polizei mit sensiblen Eingriffsbefugnissen zu zweifeln.

4.3 Justizverwaltung

4.3.1 Strafverfahrensänderungsgesetz verabschiedet

Mit dem Strafverfahrensänderungsgesetz (StVÄG) sind endlich seit langem geforderte bereichsspezifische Datenschutzregelungen in der Strafprozessordnung in Kraft getreten. Leider sind sie allzu pauschal ausgefallen. Das Gesetz erweitert die Datenverarbeitungsbefugnisse statt sie im Interesse des Grundrechtsschutzes einzuschränken.

Der von der Bundesregierung eingebrachte Entwurf des StVÄG 1999 basierte auf dem von den Parteien vereinbarten so genannten „**Flughafenkompromiss**“, mit dem den immer wieder gescheiterten Versuchen zur Schaffung von Datenschutzregelungen in der StPO endlich zum Durchbruch verholfen werden sollte. Bedauerlicherweise gelang es einigen Ländern, über den Bundesrat und das Vermittlungsverfahren eine Reihe von datenschutzrechtlichen Verschlechterungen gegenüber dem Entwurf durchzusetzen.

Die Strafprozessordnung weist nun im Wesentlichen folgende datenschutzrechtlich bedeutsame Neuregelungen auf:

- Internet-Fahndungen oder wiederholte Öffentlichkeitsfahndungen in Presse und Fernsehen müssen richterlich bestätigt werden.
- Längerfristige Observationen sind nur bei „erheblichen“ Taten und wenn kein milderes Mittel zur Verfügung steht zulässig und müssen richterlich angeordnet werden. Die Polizei darf ohne staatsanwaltschaftliche Anordnung nur bis zu drei Tagen observieren.
- Die Einsichtsrechte in Strafverfahrensakten für Justizbehörden, andere öffentliche Stellen sowie für Private sind nun ausdrücklich gesetzlich geregelt. Privatpersonen erhalten allerdings bereits Einsicht, wenn sie ein „berechtigtes Interesse“ darlegen. Die Datenschutzbeauftragten hatten gefordert, diese sensib-

len Daten nur bei Vorliegen eines „rechtlichen Interesses“ zu öffnen, weil Daten über strafbare Handlungen zu den besonders sensiblen Datenkategorien im Sinne der EG-Datenschutzrichtlinie zählen.

- Strafverfahrensdaten können immer dann für die Gefahrenabwehr verwendet werden, wenn nicht besondere Verwendungsregelungen dem entgegenstehen. Die neuen Regelungen gewährleisten also im Ergebnis kaum noch eine Zweckbindung.
- Justiz- und Strafverfolgungsbehörden werden ausdrücklich zur Unterhaltung gemeinsamer Dateien zur Vorgangsbearbeitung, -verwaltung sowie für Zwecke künftiger Strafverfahren ermächtigt. Es sind allerdings vorab Festlegungen über die Art der Daten, über Nutzungsberechtigte und Speicherfristen in Errichtungsanordnungen und Verordnungen zu treffen.

Obwohl die neuen Bestimmungen eigentlich der Umsetzung des Volkszählungsurteils dienen sollten, lassen sie den Strafverfolgungs- und Justizbehörden in wesentlichen Fragen wie der Zweckbindung **unangemessen weite Spielräume**. Allerdings behalten die Regelungen des schleswig-holsteinischen Gesetzes über die staatsanwaltschaftlichen Verfahrensregister (StARegG) ihre Gültigkeit. Wir sind deshalb mit dem Justizministerium darüber im Gespräch, welche Auswirkungen das StVÄG 1999 auf die Praxis der Justizbehörden und auf bereits vorhandene Systeme haben wird.

Was ist zu tun?
Die Strafverfolgungsbehörden sollten die neuen Bestimmungen in der StPO so umsetzen, dass dabei die Regelungen des StARegG immer dann Wirkung entfalten, wenn das Bundesrecht es zulässt.

4.3.2 DNA-Analysen künftig ohne richterlichen Beschluss?

Immer wieder wird versucht, die für DNA-Analysen gesetzlich geforderten richterlichen Anordnungen durch Einholung einer Einwilligung des Betroffenen zu umgehen. Das Landgericht Kiel hat sogar eine telefonisch gegenüber dem Amtsgericht erklärte Einwilligung eines Betroffenen als ausreichend angesehen und den Erlass einer von der Staatsanwaltschaft beantragten richterlichen Anordnung als nicht erforderlich abgelehnt.

An unseren grundsätzlichen rechtlichen Vorbehalten (vgl. 22. TB, Tz. 4.2.7) gegenüber derartigen „Einwilligungslösungen“ hat sich durch das Urteil des Landgerichtes Kiel nichts geändert. Die große Zahl der so genannten „Altfälle“ bereits strafrechtlich verurteilter Personen lässt sich allerdings offenbar nur schwer in dem vom Gesetzgeber vorgeschriebenen Verfahren der richterlichen Anordnung bewältigen. Dieses Problem war bei der Schaffung der Altfallregelung vorherzusehen. Das **Bundesverfassungsgericht** hat bezüglich des Richtervorbehaltes betont, dass eine sorgfältige Einzelfallentscheidung getroffen werden muss; formelhafte Begründungen und bloße Wiederholungen des Gesetzestextes reichen nicht aus.

Es fällt schwer, von einer Freiwilligkeit zu sprechen, wenn Betroffene in die präventive Speicherung ihres DNA-Profils zum Abgleich mit künftigen oder bereits vorhandenen Spuren in der bundesweiten Datei einwilligen und sich damit selbst gleichzeitig eine Neigung zum Wiederholungstäter attestieren. Dies mit dem formalen Verweis auf den Grundsatz des „volenti non fit iniuria“ (keine Rechtsverletzung bei Vorliegen einer Einwilligung) zu beantworten, erscheint **spitzfindig**. Wahrscheinlicher ist, dass die Einwilligungen nur erteilt werden, um sich nicht erneut verdächtig zu machen oder als uneinsichtig zu gelten.

Die Justiz ist mit einem **Lösungsvorschlag** für den Fall an uns herangetreten, dass Gerichte gleichwohl die Anordnung von DNA-Analysen wegen Vorliegens einer Einwilligung verweigern. Es liegt auf der Hand, dass in dieser Situation ein Verfahren gefunden werden muss, um die Erfassung von zweifelsfrei wiederholungsgefährdeten Tätern schwerer Delikte in der Datei zu ermöglichen. In unserer Stellungnahme gegenüber dem Justizministerium haben wir folgende Anforderungen formuliert:

- Derzeit gibt die Rechtsprechung keine Veranlassung, generell auf ein landesweites Modell der „Freiwilligkeitslösung“ umzuschwenken. Abweichungen sind nur dann vertretbar, wenn Gerichte tatsächlich Anordnungen aufgrund bereits vorhandener Einwilligungen ablehnen.
- Die gesetzlich geforderte Prognose der Wiederholungsgefahr muss von der Staatsanwaltschaft selbst gestellt werden. So wird eine gewisse justizielle Kontrolle der Erhebung und Verarbeitung der DNA-Daten gewährleistet. Ein Vetorecht gegenüber polizeilichen Entscheidungen reicht nicht aus.
- Die Einwilligungen dürfen nicht „vorsorglich“ vom Betroffenen eingeholt werden, bevor das Vorliegen eines schweren Delikts und eine Wiederholungsgefahr festgestellt wurden.
- Einwilligungserklärungen müssen nach ausreichender Darstellung der Verarbeitungsschritte sowie nach Aufklärung über die jederzeitige Möglichkeit eines Widerrufs durch den Betroffenen schriftlich erklärt werden.

Derzeit ist der Generalstaatsanwalt damit befasst, in Zusammenarbeit mit dem Landeskriminalamt eine diesen Gesichtspunkten entsprechende Verfahrensweise auszuarbeiten, die dann dem Justizministerium vorgelegt wird.

Was ist zu tun?
Das Justizministerium sollte den vom Gesetzgeber vorgegebenen Richtervorbehalt respektieren. DNA-Analysen auf der Grundlage von Einwilligungen müssen die Ausnahme bleiben.

4.3.3 Unterbliebene Löschung in MESTA

Bei der Umstellung vom automatisierten staatsanwaltschaftlichen Verfahrensregister GAST auf MESTA ist ein Programmierfehler unterlaufen, der Löschungen von Verfahrensdatensätzen nach der gesetzlich vorgegebenen Frist verhindert.

Bei der Bearbeitung einer Eingabe haben wir festgestellt, dass die Daten über ein im Jahre 1994 gegen die Petentin geführtes Strafverfahren noch immer im automatischen Verfahrensregister MESTA gespeichert waren, obwohl die fünfjährige **Speicherfrist** nach dem Gesetz über die Staatsanwaltschaftlichen Verfahrensregister (StARegG) bereits seit über einem Jahr **abgelaufen** war. Die Staatsanwaltschaft teilte uns mit, die Löschung sei infolge von technischen Problemen bei der Umstellung des Vorläufersystems GAST auf MESTA nicht möglich. Eine Lösung werde zurzeit vom Generalstaatsanwalt erarbeitet.

Die ordnungsgemäße Einhaltung der gesetzlichen **Löschfristen** gehört zu den wesentlichen Grundanforderungen, die **vor Inbetriebnahme** eines automatisierten Systems sicherzustellen und zu testen sind, da es andernfalls – wie im vorliegenden Fall – zu unzulässigen Datenspeicherungen kommt. Wir haben die konkrete Fristüberschreitung daher beanstandet. Der Generalstaatsanwalt teilte uns mit, dass tatsächlich alle zur Löschung anstehenden Datensätze betroffen sind. Die Datenzentrale sei mit der technischen Lösung beauftragt.

Was ist zu tun?
Der Generalstaatsanwalt muss die Einhaltung der gesetzlichen Löschverpflichtung sicherstellen. Betreiber automatisierter Systeme haben vor der Freigabe eines Verfahrens zu testen, ob derartige Funktionalitäten ordnungsgemäß ablaufen.

4.3.4 Auch Justitia hat einen Amtsschimmel

Eine spätabendliche Bahnfahrt eines Berufspendlers mit dem erfolglosen Versuch, eine Fahrkarte zu erstehen, wuchs sich zu einem Verwaltungsvorgang von veritablem Ausmaß aus. Obwohl eine Straftat nach Auffassung aller Beteiligter fern lag und die Bahn sich bei dem Betroffenen schriftlich entschuldigt hat, ist der Vorgang inzwischen im staatsanwaltschaftlichen Verfahrensregister eingetragen und somit bundesweit zwei Jahre lang allen Staatsanwaltschaften verfügbar. Eine Löschung des Datensatzes lehnt die Staatsanwaltschaft bislang ab.

Es fing alles so harmlos an. Ein Fahrgast hatte sich vor Abfahrt des Zuges beim Triebwagenführer zwecks Erwerbs einer Fahrkarte gemeldet, da er die vor kurzem im Bahnhof umgestellten **Fahrkartenautomaten** nicht gefunden hatte. Der Triebwagenführer sowie ein weiterer Mitarbeiter der Regionalbahn sahen sich jedoch außerstande, ihm eine Fahrkarte zu verkaufen. Der Fahrgast nahm im Zug Platz und zeigte dem Kontrolleur, der ihm ebenfalls keine Fahrkarte verkaufen konnte,

seine BahnCard mit der Bitte vor, ihm eine Rechnung über das Beförderungsentgelt zuzusenden. So weit, so gut. Bei der Erstellung der Zahlungsaufforderung wurde jedoch die **Adresse** des Petenten **fehlerhaft** abgeschrieben, sodass die Zahlungsaufforderung mit dem Vermerk „Empfänger unbekannt“ zurückkam. Dies löste bei der Bahn automatisch eine Anzeige wegen Leistungserschleichung aus. Nach Aufklärung des Sachverhaltes entschuldigte sich die Bahn zwar bei dem Betroffenen, konnte aber den bürokratischen Zug nicht mehr stoppen.

Die **Staatsanwaltschaft** hatte das Verfahren zwar wegen „mangelnder Tatbestandsmäßigkeit“ eingestellt, eine Löschung der gespeicherten Verfahrensdaten lehnte sie jedoch ab, da die Fünfjahresfrist nach dem Gesetz über staatsanwaltschaftliche Verfahrensregister nicht abgelaufen sei. Außerdem seien die Daten zur Überwachung der ebenfalls fünfjährigen Aufbewahrungsfrist der papierenen Akte erforderlich.

Der Betroffene empfand dies zu Recht als einen Schildbürgerstreich. Es bestand eindeutig ein **Löschungsanspruch**, da dem Verfahren ein offenkundig haltloser Vorwurf zugrunde lag. Auch die Aufbewahrungsfrist für die papierene Akte muss eine Staatsanwaltschaft nicht in jedem Fall automatisch ausschöpfen. Wir haben die Staatsanwaltschaft daher aufgefordert, das leidige Verfahren einfach durch Datenlöschung und Vernichtung des Vorganges zu beenden. Es ist rechtlich untragbar, dass ein solcher Datensatz über das Zentrale Staatsanwaltschaftliche Verfahrensregister sämtlichen Strafverfolgungsbehörden in Deutschland zur Verfügung steht, ohne dass die zum Abruf berechtigten Stellen Hintergrund und Ablauf des ganzen Malheurs erkennen können.

Nach mehreren Monaten Prüfung bot die Staatsanwaltschaft dem Betroffenen eine Löschung oder Sperrung der Daten im Landessystem MESTA an, lehnte dies jedoch für das bundesweite Verfahrensregister ab.

Was ist zu tun?
Die Unterlagen gehören in den Reißwolf, die Daten gelöscht und die Angelegenheit vergessen. Der Schreibfehler eines Bahnbediensteten darf nicht zu solchen Folgen führen.

4.3.5 Kontrollfreier Raum Staatsanwaltschaft?

Obwohl das schleswig-holsteinische Datenschutzgesetz keine Einschränkung unserer Kontrollbefugnisse enthält, möchte der Generalstaatsanwalt uns Informationen über besondere Maßnahmen wie Telefonüberwachungen in laufenden Verfahren vorenthalten.

Wenn wir in der Vergangenheit überprüft haben, ob und wenn ja warum Telefone von Petenten abgehört wurden, erhielten wir von der zuständigen Staatsanwaltschaft ohne Probleme die notwendigen Informationen. Eine Staatsanwaltschaft nahm jedoch nunmehr eine solche Anfrage zum Anlass, unsere **Kontrollkompetenz** in diesem Bereich grundsätzlich infrage zu stellen, und legte den „Fall“ dem

Generalstaatsanwalt vor. Überraschenderweise sieht auch dieser neuerdings „keine Verpflichtung“ der Staatsanwaltschaften, uns aus laufenden Ermittlungsverfahren Auskunft über Telekommunikationsüberwachungsmaßnahmen zu erteilen. Er befürchte, dass Straftäter die Ermittlungsbehörden mittelbar über uns ausforschen könnten. Zudem sei die Kontrolle über Telefonüberwachungsmaßnahmen nach der StPO allein einem Richter zugewiesen. Durch die Einführung von Datenschutznormen in die StPO (vgl. Tz. 4.3.1) sei eine abschließende Regelung getroffen worden, die keine Kontrollbefugnis des Datenschutzbeauftragten vorsehe.

Diese Rechtsauffassung halten wir für unrichtig. Das Landesdatenschutzgesetz ist hinsichtlich unserer Kontrollkompetenz eindeutig. Die neuen Regelungen in der StPO über „Auskunftserteilungen“ tangieren die Kontrollkompetenzen des ULD oder des Rechnungshofes in keiner Weise. Es konnte seitens der Staatsanwaltschaft auch kein Fall genannt werden, in dem etwa ein Verdächtiger aufgrund unserer Prüfung unzulässige Informationen erhalten hätte. Die datenschutzrechtlichen Prüfungen führen selbstverständlich nicht dazu, dass richterliche Anordnungsbeschlüsse für Überwachungen des Fernmeldeverkehrs inhaltlich überprüft oder einzelfallbezogen kommentiert werden. Durch den Datenschutzbeauftragten ist lediglich zu überprüfen, ob eine Anordnung erlassen wurde, ob deren **Grenzen eingehalten** wurden, wie mit dem erhobenen Datenmaterial weiter umgegangen wurde und ob die Benachrichtigungspflichten eingehalten wurden.

In **kritischen Fällen** haben wir uns zudem bisher immer mit der Staatsanwaltschaft in Verbindung gesetzt und mit dem Betroffenen eine Formulierung gefunden, die eine Preisgabe von Ermittlungsinhalten ausschloss. Eine Auskunft an Petenten erfolgt nach dem Datenschutzrecht in Fällen der Gefährdung der behördlichen Aufgaben oder der öffentlichen Sicherheit grundsätzlich nicht.

Auch das **Justizministerium** hat bereits in der Vergangenheit bekundet, es halte unsere Kontrollbefugnis in dem fraglichen Bereich laufender Ermittlungsmaßnahmen für gegeben.

Was ist zu tun?
Das Justizministerium sollte gegenüber den Staatsanwaltschaften im Lande klarstellen, dass wir – so wie bisher auch – zur Kontrolle von Telefonabhörmaßnahmen befugt sind.

4.3.6 Datenschutz im Strafvollzug

Das Strafvollzugsgesetz enthält nunmehr Normen für den Datenschutz im Strafvollzug. In diesem sensiblen Bereich, der durch unterschiedliche Interessenlagen der Gefangenen, des Wachpersonals oder auch das Schutzbedürfnis der Öffentlichkeit gekennzeichnet ist, tauchen trotzdem immer wieder problematische Fallgestaltungen auf.

- **Was muss der behandelnde Arzt über Gefangene wissen?**

Ein Strafgefangener musste in der Justizvollzugsanstalt (JVA) von einem externen Arzt behandelt werden. Dessen Nachfrage nach dem **Inhaftierungsgrund** wollte der Gefangene nicht beantworten, da er zum ersten Mal Kontakt zu dem Arzt hatte. Daraufhin gab der bei der Behandlung anwesende Sanitätsbedienstete der JVA dem Arzt bereitwillig Auskunft über die Tat, wegen derer der Gefangene eine Strafe verbüßte. Die Leitung der JVA hat diesen datenschutzrechtlichen Verstoß eingeräumt und bedauert, da eine medizinische Notwendigkeit für die Weitergabe dieser Information an den behandelnden Arzt nicht bestand.

- **Urlaubsanschrift von Strafgefangenen**

Vor der Gewährung von Hafturlaub für Strafgefangene wird geprüft, ob die Gefahr besteht, dass der Gefangene sich dem Vollzug der Freiheitsstrafe entziehen oder die Lockerung zu Straftaten missbrauchen wird. Dabei werden auch Auskünfte von Sozialämtern, Polizeidienststellen, Einwohnermeldeämtern über den **Urlaubsgastgeber**, allerdings mit dessen **Einwilligung**, eingeholt. Hierfür wurde bislang ein Vordruck verwendet, der die Betroffenen nur unzureichend über die Umstände der beabsichtigten Datenverarbeitung (Von welchen Stellen werden welche Daten erhoben? Wie lange und in welcher Form werden die Daten gespeichert? Welche Folgen hat eine Nichtbeantwortung der Fragen?) unterrichtete. Auf unser Drängen ist landesweit ein neu gestaltetes Formular eingeführt worden, das den datenschutzrechtlichen Anforderungen entspricht, weil es den Betroffenen fair informiert.

- **Übermittlung der Daten eines Verteidigers durch JVA an Dritte**

Innerhalb einer JVA kursierte das Gerücht, ein Gefangener habe seine Verlegung in eine andere JVA durch Bestechung des Anstaltsleiters über seinen Rechtsanwalt abwenden können. Dies brachte ein Mitgefangener dem Justizministerium per Beschwerde zur Kenntnis und nannte darin auch den Namen seines ebenfalls einsitzenden Informanten. Der Anstaltsleiter erhielt die Beschwerde zur Stellungnahme übersandt und teilte daraufhin dem betreffenden Rechtsanwalt auszugsweise den in der Beschwerde enthaltenen Vorwurf der Bestechung bzw. Bestechlichkeit unter Namensnennung des Beschwerde führenden Gefangenen und seines Informanten mit. Darüber hinaus nannte er den Namen des gemeinsamen Rechtsanwaltes beider Gefangener. Hierin sah der Rechtsvertreter der Gefangenen eine unzulässige Datenübermittlung. Nachdem der **Bestechungsvorwurf** auch in die Öffentlichkeit gelangt war, erhielt die Angelegenheit in der Presseberichterstat-

tung Brisanz, da beide Rechtsanwälte in unterschiedlichen politischen Parteien aktiv waren und sich ein Bestechungsvorwurf durchaus in dem damals laufenden Wahlkampf hätte auswirken können.

Wir konnten im Ergebnis **keinen datenschutzrechtlichen Verstoß** des Anstaltsleiters durch die Namensnennung des gemeinsamen Rechtsvertreters der Gefangenen gegenüber dem durch die Anschuldigungen belasteten Rechtsanwalt feststellen. Nach Angaben des Leiters der JVA wollte dieser dem Anwalt eine zügige Wahrnehmung seiner Rechte dadurch ermöglichen, dass er sich mit Unterlassungsverlangen unmittelbar an den Anwalt der Gefangenen wenden konnte. Eine Übermittlung personenbezogener Daten von Strafgefangenen an Dritte ist nach dem neu gefassten Strafvollzugsgesetz zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person zulässig. Es war vertretbar, dass der Anstaltsleiter den Namen des gemeinsamen Rechtsvertreters als Zusatzinformation im Interesse einer effektiven Verfolgung der Rechte des beschuldigten Anwaltes mit übermittelte.

4.3.7 Sensible Telefongesprächsinhalte in Abrechnungsunterlagen

Um gegenüber dem Amtsgericht Aufwendungen für Telefongespräche von Betreuern nachzuweisen, sind Gesprächsinhaltsdaten nur in ganz allgemeiner Form erforderlich. Die Betreuungsvereine müssen ihre Abrechnungspraxis datenschutzgerecht umgestalten.

Eigentlich sollten nur die geführten Telefongespräche gegenüber dem Amtsgericht abgerechnet werden. Die tabellarische Gesprächsaufstellung enthielt aber auch die Inhalte eines Gespräches eines Betreuers mit der **Pastorin** der zu betreuenden Person. Der Rechtspfleger übersandte die Aufstellung an die Betreute selbst, da diese schließlich die Auslagen aus ihrem Vermögen erstatten musste. Auf diese Weise erfuhr der Sohn der Betreuten, was die Pastorin dem Betreuer über seine Mutter mitgeteilt hatte, und beschwerte sich bei ihr. Die Pastorin fiel aus allen Wolken. Sie hatte geglaubt, ihre Angaben würden vom Betreuer vertraulich behandelt, und bat um datenschutzrechtliche Überprüfung.

Aus Sicht des **Amtsgerichts** müssen zu den einzelnen Telefongesprächen der Betreuer zumindest so viel Zusatzinformationen geliefert werden, dass beurteilt werden kann, ob das Telefonat in sachlichem Zusammenhang mit der Betreuung stand. Hierfür reicht eine allgemeine Angabe über den Gesprächspartner sowie den Anlass des Gesprächs (z. B. „Gespräch über den Gesundheitszustand“) aus. Was inhaltlich besprochen wurde, gehört demgegenüber in die Handakte des Betreuers. Eine andere (in erster Linie anhand der Einsichtsfähigkeit zu entscheidende) Frage ist es, inwieweit die betreute Person oder deren Angehörige auf Antrag Einsicht in diese Akte nehmen können, um die sie betreffenden Daten zu erfahren.

Der betroffene Betreuungsverein hat die datenschutzrechtlichen Vorgaben umgesetzt und sämtliche Vereinsbetreuer in seinem Bereich angewiesen, auf den Dokumentationsbögen über Telefongespräche nur noch allgemeine Formulierungen und keine Namen Dritter mehr zu nennen.

Was ist zu tun?
Alle Betreuungsvereine sollten entsprechende Vorgaben machen. Rechtspfleger sollten diese datenschutzrechtlichen Anforderungen an sämtliche – auch die freiberuflichen – Betreuer weitergeben.

4.3.8 Auftragssperre bei Korruptionsverdacht

Bislang gibt es keine Regelungen darüber, an wen Informationen über Auftragssperren gegen Unternehmen des Verdachts der Korruption oder anderen Fehlverhaltens übermittelt werden dürfen. Die Oberfinanzdirektion hatte Daten über einen Unternehmer an eine Vielzahl öffentlicher Stellen gestreut – mit womöglich erheblichen wirtschaftlichen Folgen. Inzwischen hat sich zudem herausgestellt, dass der Korruptionsverdacht nicht aufrechtzuhalten war.

Da gegen einen mittelständischen Unternehmer ein Strafverfahren wegen Verdachts der Bestechung anhängig war, belegte die Oberfinanzdirektion (OFD) das Unternehmen mit einer so genannten **temporären Auftragssperre**. Diese Tatsache wie auch nachfolgende Verfahrensstände wurden von der OFD an einen ziemlich breiten Verteiler von öffentlichen Auftraggebern im norddeutschen Raum übermittelt. Keine der benachrichtigten Stellen hatte signalisiert, dass der Betroffene sich bei ihr um Aufträge beworben hatte bzw. in einem Auftragsverhältnis stand. Auch der **Rechtsanwalt** eines Zweckverbandes in Schleswig-Holstein erhielt auf Nachfrage von der OFD Informationen über die verhängte Auftragssperre und deren Hintergründe. Diese führte er in einem Zivilprozess gegen den Unternehmer als Argument dafür ein, dass das Unternehmen bereits anderweitig durch inkorrekte Abwicklung von Aufträgen aufgefallen sei.

Wie eine Auftragssperre „publik gemacht“ wird, ist von hoher wirtschaftlicher Bedeutung für die Betroffenen. In Hessen etwa besteht eine **zentrale Melde- und Informationsstelle** für Vergabestellen bei der OFD Frankfurt. Die Daten dürfen grundsätzlich nur nach gerichtlicher Verurteilung, also nicht allein aufgrund von Verdachtsmomenten im Ermittlungsverfahren eingestellt und nur in Zusammenhang mit einer geplanten Auftragsvergabe übermittelt werden. In Schleswig-Holstein fehlten bislang dagegen entsprechende Regelungen. Datenschutzrechtlich ist die unaufgeforderte Information anderer öffentlicher Auftraggeber nur zulässig, wenn sie zur rechtmäßigen Aufgabenerfüllung erforderlich ist. Rundschreiben über einen breiten Verteiler können nicht als erforderlich angesehen werden, da der OFD Kiel von keiner der benachrichtigten Stellen Anhaltspunkte für eine bevorstehende Auftragsvergabe mitgeteilt worden waren. Ausschlaggebend war allein die Vermutung, der Betroffene könne sich als Bieter auch anderswo betätigen. Zu berücksichtigen war auch, dass die Anhaltspunkte für Verfehlungen des Betroffenen lediglich Verdachtsstatus besaßen, was angesichts der potenziell weit reichenden wirtschaftlichen Folgen einer derartigen Bekanntmachung zu einer besonders strengen Erforderlichkeitsprüfung hätte veranlassen müssen. Tatsächlich wurde das gegen den Petenten geführte Strafverfahren wegen des Vorwurfs der Korruption von der Staatsanwaltschaft wegen fehlenden Tatverdachts eingestellt.

Die **Gebäudemanagement Schleswig-Holstein** als nunmehr zuständige Stelle hat aus unseren Beanstandungen Konsequenzen gezogen und die Zuständigkeit für diesen sensiblen Bereich beim Justiziariat angesiedelt. Eine Dienstanweisung, in der der Umgang mit Auftragssperren geregelt werden soll, liegt uns im Entwurf vor. Wir werden darauf achten, dass Verdachtsmomente nicht weiterhin nach dem Gießkannenprinzip gestreut werden.

Was ist zu tun?
Es ist die Grundsatzfrage zu klären, ob Auftragssperren nur zur Abfrage bereitgehalten oder aktiv verteilt werden und wie mit den Verdachtsfällen umgegangen wird.

4.4 Verfassungsschutz

Sicherheitsüberprüfungen datenschutzgerecht

Bei den Sicherheitsüberprüfungen der Mitarbeiter der Verwaltung besteht derzeit ein hoher Datenschutzstandard. Bei der anstehenden gesetzlichen Regelung des Sicherheitsüberprüfungsverfahrens sollte deshalb die Funktion eines zentralen Sicherheitsbeauftragten des Landes beibehalten werden.

Die derzeit noch geltenden Richtlinien über Sicherheitsüberprüfungen („Sicherheitsrichtlinien“) sehen einen zentralen **Sicherheitsbeauftragten** des Landes vor. Er führt die Sicherheitsakten, in denen sich die Sicherheitserklärung des Betroffenen mit detaillierten Angaben zu seiner und zu dritten Personen sowie etwaige Hinweise auf Sicherheitsrisiken befinden.

Die **Zentralisierung** gewährleistet zum einen einen landeseinheitlichen Standard und zum anderen die zur Wahrung der Zweckbindung erforderliche Distanz zur Personaldatenverarbeitung in den Beschäftigungsdienststellen. In vielen kleineren Behörden könnte eine wirksame personelle Trennung zwischen Personalsachbearbeitung und Geheimschutz nicht sichergestellt werden. Neben diesen datenschutzrechtlichen Aspekten sprechen aus unserer Sicht auch die Gesichtspunkte der **Verwaltungseffizienz** dafür, eine zentrale Bündelung dieser Spezialaufgaben bei dem Sicherheitsbeauftragten des Landes beizubehalten. Das Innenministerium möchte trotzdem künftig die Verantwortung für geheimschutzrelevante Entscheidungen auf die Dienststellen vor Ort verlagern. Wir werden uns im Gesetzgebungsverfahren (vgl. 21. TB, Tz. 4.3) gegen eine solche Lösung aussprechen.

Anlässlich einer Kontrolle wurde deutlich, dass sich der Sicherheitsbeauftragte und die Verfassungsschutzbehörde bei den Dienststellen im Landes- und Kommunalbereich aktiv darum bemühen, die Anzahl der Personen, die sicherheitsüberprüft werden, **auf das erforderliche Maß** zu begrenzen. So waren zum Prüfungszeitpunkt in ganz Schleswig-Holstein lediglich 15 Personen bis zum Grad „streng geheim“ ermächtigt und hatten daher die eingriffsintensivste Form der so genannten Sicherheitsüberprüfung durchlaufen müssen.

Die Prüfung erbrachte folgende Ergebnisse:

- Akten von Mitarbeitern werden zügig vernichtet, wenn ihr Arbeitsfeld nicht mehr als Sicherheitsbereich eingestuft ist.
- Nach unserer Auffassung besteht eine Verpflichtung zur Aussonderung einzelner nicht mehr erforderlicher Unterlagen aus Sicherheitsakten im Wege der Teilbereinigung, etwa im Zusammenhang mit erforderlichen Wiederholungsüberprüfungen nach jeweils fünf Jahren. Gegenwärtig werden keine Teilbereinigungen durchgeführt, sodass sich bei langer Beschäftigungsdauer in VS-relevanten Bereichen – insbesondere der Stufen „Geheim“ und „Streng geheim“ – ein extrem umfangreiches Persönlichkeitsentwicklungsprofil des Betreffenden ergeben kann. Wenn erneute Befragungen oder eine Herabstufung der Ermächtigung stattgefunden hat, könnten alte Befragungsberichte ausgesondert werden. In einem Fall war sogar noch eine polizeiliche Mitteilung über eine Verurteilung wegen „groben Unfugs“ aus dem Jahre 1961 zu 50 DM Geldstrafe gespeichert. Sie hatte vier Wiederholungsüberprüfungen überstanden.
- Des Weiteren fanden sich in einigen Akten Unterlagen aus Notaufnahmelagern für Flüchtlinge aus der ehemaligen DDR, die Persönlichkeitsbewertungen durch den Lagerleiter enthielten. Soweit eine fachliche Erforderlichkeit heute für die Aufklärung von Spionagefällen nicht mehr gegeben ist, sollten auch hier Teilbereinigungen stattfinden.

Die Verfassungsschutzbehörde und der Sicherheitsbeauftragte stimmten einer Aussonderung derartiger Unterlagen für die Zukunft zu.

Was ist zu tun?
Der gute Datenschutzstandard bei Sicherheitsüberprüfungen sollte beibehalten und endlich durch eine gesetzliche Regelung festgeschrieben werden.

4.5 Ausländerverwaltung

4.5.1 Entwicklung des Ausländerrechts

Die Verwaltungsvorschriften zum Ausländergesetz sind in Kraft getreten. Die Pläne für die Einführung einer AsylCard verfolgt der Bund nach wie vor.

Die Mühlen der Normgebung im Ausländerbereich mahlen langsam: Die bundesweiten **Verwaltungsvorschriften zum Ausländergesetz**, die auch Auslegungshinweise zu den bereichsspezifischen Datenschutzvorschriften enthalten, liegen – zehn Jahre nach Erlass des Gesetzes – endlich vor (vgl. 21. TB, Tz. 4.5.5).

Noch nicht entschieden wurde über einige Verfassungsbeschwerden gegen das Ausländerzentralregistergesetz aus dem Jahr 1995, mit denen Verstöße gegen den Gleichheitsgrundsatz und gegen das Grundrecht auf Datenschutz geltend gemacht werden. Das **Ausländerzentralregister** wurde mit dem Big Brother Award 2000 in der Kategorie „Lebenswerk“ ausgezeichnet. Mit dieser Preisverleihung wird von einer privaten Initiative die nachhaltige und dauerhafte Verletzung von Per-

sönlichkeitsrechten kritisiert. Es wäre zu wünschen, dass der Bundesgesetzgeber diese Kritik zum Anlass nimmt, das Gesetz von seinen verfassungsrechtlich angreifbaren Teilen zu befreien.

Auch die Planungen zur Einführung einer **AsylCard** sind immer noch nicht ad acta gelegt. Ende 1999 wurde eine Bund-Länder-Arbeitsgruppe gebildet, die Modalitäten eines Pilotversuches erarbeiten soll. Nach den Vorstellungen des Bundesinnenministeriums soll in einer ersten Stufe zunächst lediglich eine scheckkartengroße Plastikkarte als bundeseinheitliches Ausweisdokument eingeführt werden. Für die zweite Stufe wird unter Einbeziehung eines Mikroprozessors mit einem abgespeicherten digitalen Daumenabdruck eine eindeutige Identifizierung der Asylbewerber angestrebt. Hierfür müsste eine Rechtsgrundlage geschaffen werden. In einer dritten und vierten Stufe soll ein „Hintergrundsystem“ mit Speicher- und Übermittlungsfunktionen installiert werden. Der Bund favorisiert einen Pilotversuch auf freiwilliger Basis bis zur Stufe zwei, sodass die von uns hinsichtlich der AsylCard geäußerten Datenschutzbedenken noch nicht zum Tragen kommen (vgl. 21. TB, Tz. 4.5.2). Das Land Schleswig-Holstein beteiligt sich nicht an der genannten Arbeitsgruppe.

Unsere Forderung nach einer umfassenden Überarbeitung der Rechtsgrundlage für die geplante europäische Fingerabdruckdatei **EURODAC** wurde inzwischen aufgegriffen (vgl. 21. TB, Tz. 4.5.3). Statt eines völkerrechtlichen Vertrages hat man sich allerdings für eine Regelung in Form einer Verordnung der Europäischen Gemeinschaft entschieden. Wann und mit welchem Inhalt diese Verordnung in Kraft tritt, ist aber noch nicht absehbar.

Im letzten Bericht (vgl. 22. TB, Tz. 4.4.2) äußerten wir die Hoffnung, dass die von der Landeshauptstadt festgelegten Standards bei der Überprüfung von „**Scheinehen**“ landesweit Gültigkeit finden würden. Dem wurde durch die Bekanntgabe der Regelungen durch das Innenministerium entsprochen. Eingaben zeigen aber, dass das Problem in der Praxis weiterhin zu Konflikten führt.

4.5.2 Datenaustausch Sozialamt – Ausländeramt neu geregelt

Im letzten Tätigkeitsbericht wurde unter Tz. 4.4.3 über einen jahrelang schwelenden Konflikt bezüglich der Frage der Meldung des Sozialhilfebezugs durch das Sozialamt an die Ausländerbehörde berichtet. Trotz zunächst scheinbar unvereinbarer Positionen konnten wir jetzt eine datensparsame und praktikable Lösung erreichen.

In einer Dienstanweisung ist vorgesehen, dass die Sozialbehörde von sich aus der Ausländerbehörde vom Umstand des **Sozialhilfebezugs** Mitteilung macht, es sei denn, dieser wird nur kurzfristig (maximal 3 Monate) oder nur darlehensweise gewährt oder der Hilfeempfänger genießt besonderen ausländerrechtlichen Ausweisungsschutz. Dies ist bei Aufenthaltsberechtigten der Fall sowie bei Personen, die einen langjährigen Aufenthalt in Deutschland von Jugend an oder bestimmte familiäre Bindungen aufweisen können. Bei Ausländern, deren Sozialhilfeantrag abgelehnt wurde, weil sie zum Zweck des Hilfebezugs eingereist sind, erfolgt stets eine Mitteilung.

Die jetzt gefundene Regelung kommt Datenschutz und Verwaltung entgegen. Wir bestehen nicht mehr darauf, dass vonseiten der Sozialbehörde vor der Übermittlung eine **eingehende ausländerrechtliche Prüfung** stattfindet. Es wurde uns plausibel gemacht, dass eine solche Prüfung in der Praxis nicht möglich ist. Zugleich wird dadurch vermieden, dass im Sozialamt ausländerrechtlich relevante Daten erhoben werden müssen. Die Ausländerbehörde ihrerseits räumte ein, dass durch die Beschränkung der Mitteilungspflicht auf die vereinbarten Fälle eine Beeinträchtigung der Wahrnehmung ihrer Aufgaben nicht erfolgt. Vielmehr wird sie von bürokratischen Prüfpflichten sowie sich gegebenenfalls anschließenden Löschungspflichten entbunden. Der mit der Landeshauptstadt erzielte Kompromiss hat über die Stadt hinausgehenden Vorbildcharakter.

Was ist zu tun?
Es wird empfohlen, den gefundenen Kompromiss auch bei den anderen Sozialämtern des Landes zu übernehmen.

4.6 Wirtschaft, Technik und Verkehr

4.6.1 Mietwagen contra Taxen

Taxen und Mietwagen stehen in Kiel in starker Konkurrenz zueinander. Dies führt auch zu datenschutzrechtlichen Fragestellungen.

Taxifahrer warten offenbar nicht immer auf den für sie behördlich zugelassenen Taxenständen auf Kundschaft, sondern begeben sich z. B. vor großen Diskotheken **auf Kundenfang**. Das Mietwagengewerbe sah darin einen unlauteren Wettbewerb und verlangte von der Zulassungsbehörde Auskünfte über die Halter dieser Taxen mit der Begründung, dass es sich um einen Rechtsanspruch handele, der im Zusammenhang mit der Teilnahme am Straßenverkehr stehe. Die Zulassungsbehörde lehnte die Auskunft ab, weil sie keinen Zusammenhang im Sinne des Straßenverkehrsgesetzes sah.

Unsere Prüfung aufgrund von Beschwerden des Mietwagengewerbes ergab, dass die Zulassungsbehörde in diesen Fällen sehr wohl Auskunft aus dem Fahrzeugregister erteilen muss. Das Mietwagengewerbe wollte nämlich **Unterlassungs- und Schadensersatzansprüche** nach dem Gesetz gegen den unlauteren Wettbewerb geltend machen. Das Warten der Taxen auf Kundschaft außerhalb eines zugelassenen Taxenstandes stellt auch nach unserer Auffassung eine Verhaltensweise dar, die mit der Teilnahme am Straßenverkehr im Zusammenhang steht. Die Zulassungsbehörde erteilte inzwischen die gewünschten Auskünfte.

4.6.2 Keine Veröffentlichung der Grundstückseigentümer in Planfeststellungsverfahren

Nach den Vorschriften des Landesverwaltungsgesetzes sind in einem Planfeststellungsverfahren auch Pläne öffentlich auszulegen, aus denen sich die betroffenen Grundstücke erkennen lassen. Dies bedeutet jedoch nicht, dass auch die Namen der betroffenen Grundstückseigentümer angegeben werden müssen.

Durch die öffentliche Auslegung der Pläne in einem Planfeststellungsverfahren sollen betroffene Bürger rechtzeitig über beabsichtigte bauliche Maßnahmen informiert werden. Gleichzeitig wird ihnen damit die Möglichkeit eröffnet, Einfluss auf die Planungen zu nehmen und gegebenenfalls auch den Rechtsweg zu beschreiten. Um eine bessere Beurteilung der jeweiligen Baumaßnahme zu ermöglichen, fordert das Landesverwaltungsgesetz zwingend die Angaben der betroffenen Grundstücke in den ausliegenden Plänen. Das Landesamt für Straßenbau und Straßenverkehr Schleswig-Holstein hat darüber hinaus als „besonderen Service" auch die **Namen** der jeweiligen **Grundstückseigentümer** angegeben. Nicht erkannt wurde dabei, dass eine solche Veröffentlichung personenbezogener Daten mangels Befugnisgrundlage nicht zulässig ist.

Die Veröffentlichung der Daten war zudem nicht erforderlich. Schon aus den Flur- und Flurstückbezeichnungen kann jeder Grundstückseigentümer seine Betroffenheit von der jeweiligen Maßnahme selbst erkennen. Zusätzlich kann von der Gemeinde eine Liste der betroffenen Grundstückseigentümer bereitgehalten werden, aus der dann auf **Nachfrage im Einzelfall** Auskunft erteilt werden kann.

Das Landesamt hat sich unserer Auffassung angeschlossen. Künftig werden in den Grunderwerbsplänen und -verzeichnissen statt der Eigentümerdaten nur noch Schlüsselnummern angegeben. In Zweifelsfällen können Betroffene ihre Nummer bei der auslegenden Gemeinde erfragen.

Was ist zu tun?
Bei der öffentlichen Auslegung von Plänen in Planfeststellungsverfahren ist darauf zu achten, dass die personenbezogenen Angaben über Grundstückseigentümer verschlüsselt dargestellt werden.

4.7 Soziales – Schwerpunkt Sozialhilfe

Wie 1999 lag auch im vergangenen Jahr ein Schwerpunkt unserer Tätigkeit im **Sozialhilfebereich**. Erneut wurden Sozialämter „auf Herz und Nieren" geprüft. Ein eigens hierfür entwickeltes Prüfungskonzept ermöglichte es, die Ergebnisse von Querschnittsprüfungen zu vergleichen und strukturelle Defizite sichtbar zu machen. Die Querschnittsprüfungen sowie Kontrollen aufgrund von Eingaben und die neuen Fortbildungsveranstaltungen der DATENSCHUTZAKADEMIE Schleswig-Holstein speziell für die Mitarbeiter von Sozialämtern zeigen Wirkung. Die Beratungsersuchen im Bereich des Sozialdatenschutzes haben sich mehr als verdoppelt.

4.7.1 Querschnittsprüfungen in Sozialämtern

Im Jahr 1999 hatten wir damit begonnen, einzelnen Sozialämtern „auf den Zahn zu fühlen". Mithilfe eines speziellen Prüfungskonzeptes erfolgte vor allem eine Bestandsaufnahme bei der konventionellen Datenverarbeitung. Geprüft wurden im Jahre 2000 kleine und mittlere Sozialämter.

Das Ergebnis der Querschnittsprüfungen hat uns positiv überrascht. Trotz der hier bestehenden starken Arbeitsbelastung begegneten wir durchgängig offenen und engagierten Mitarbeiterinnen und Mitarbeitern. Stets war man bemüht, die von uns festgestellten Mängel und Verstöße schnellstmöglich abzustellen. Insbesondere **Mängel in der Datensicherheit**, z. B. nicht abschließbare Aktenschränke, überfüllte Archive oder veraltete Schließanlagen, waren nicht auf die Sorglosigkeit der Mitarbeiter, sondern auf (bislang) fehlende Mittel im Haushalt der Kommunen zurückzuführen. Es gab aber auch strukturelle Probleme in bestimmten Bereichen. So mussten wir wiederholt feststellen, dass die **Übermittlung von Sozialdaten** an potenzielle Arbeitgeber oder private Arbeitsvermittlungsagenturen recht freizügig erfolgte. Es ließen sich aber im Anschluss an die Prüfungen Verfahren finden, die eine bessere Transparenz für den betroffenen Hilfeempfänger und eine optimale Hilfegewährung ermöglichen.

Schleswig-Holstein DATENSCHUTZAKADEMIE
Kurse SOZ, S

4.7.2 Diskriminierende Bestellscheine abgeschafft

Die Gewährung einmaliger Beihilfen in Form von Bestellscheinen für den Einzelhandel darf nur in begründeten Einzelfällen oder wenn sich hierdurch Steuermittel einsparen lassen erfolgen. Dieser Meinung haben sich sowohl das Sozialministerium als auch der Sozialausschuss des Landtages angeschlossen.

Das Sozialamt der Landeshauptstadt Kiel vertrat als einzige kreisfreie Stadt des Landes zunächst eine andere Auffassung (vgl. 22. TB, Tz. 4.6.5). Sozialhilfeempfängern sei prinzipiell nicht zu trauen. Bestellscheine seien die einzige Möglichkeit, sicherzustellen, dass Beihilfen auch zweckentsprechend verwendet werden. Nach langer Diskussion wird auch das Sozialamt Kiel künftig auf die Verwendung von Bestellscheinen für den Einzelhandel bei der Gewährung von einmaligen Beihilfen, insbesondere bei Elektrogroßgeräten, verzichten. Anfang 2001 wurde außerdem eine **monatliche Beihilfepauschale** eingeführt. Mit ihr erhält der Hilfeempfänger die Möglichkeit, finanzielle Mittel anzusparen, um größere Anschaffungen zu tätigen. Diese Eigenverantwortung beinhaltet auch die Pflicht der zweckgemäßen Verwendung dieser Mittel. Die Landeshauptstadt Kiel hat hiermit eine datenschutzgerechte Lösung gefunden, die zugleich Verwaltungsaufwand reduziert und Steuermittel einspart.

4.7.3 Hausbesuche, der neue Lügendetektor des Sozialamtes?

Vertrauen ist gut, Kontrolle ist besser: Mitarbeiter der Sozialämter fragen sich des Öfteren, wie sie die Angaben von Hilfe Suchenden überprüfen können. In Ermangelung von Lügendetektoren scheinen Hausbesuche ein probates Mittel zu sein. Aber Achtung: Die Würde des Menschen ist ebenso ein Grundrecht wie die Unverletzlichkeit der Wohnung. Nur unter besonderen Voraussetzungen sind Hausbesuche ein geeignetes und angemessenes und damit auch datenschutzrechtlich zulässiges Mittel der Bedarfsfeststellung.

Wiederholt erreichten uns Eingaben, in denen aufgebrachte Petenten ihre Erlebnisse von regelrechten **Hausdurchsuchungen** schildern. Männliche Mitarbeiter durchschnüffelten die Wäsche von allein erziehenden Frauen. Der Presse war gar zu entnehmen, dass in einem Fall die Schmutzwäsche in einer Waschmaschine kontrolliert wurde.

„Dürfen Hausbesuche überhaupt durchgeführt werden?“, lautete deshalb eine häufig gestellte Frage. Die Antwort ist: „Ja, aber nur, wenn diese Form der Datenerhebung wegen der Besonderheiten des Falles erforderlich und verhältnismäßig ist. Regelrechte Hausdurchsuchungen dagegen sind unzulässig.“ Was bei der Durchführung von Hausbesuchen zu beachten ist, sollte vorab in einer Dienstanweisung wie folgt festgelegt werden:

- Vor Durchführung eines Hausbesuches ist stets zu prüfen, ob nicht andere Möglichkeiten der Sachverhaltsklärung bestehen, die weniger tief in die Rechte des Betroffenen eingreifen.
- Der konkrete Grund für die Durchführung eines Hausbesuches, z. B. der Anhaltspunkt für Sozialhilfemissbrauch, ist in der Akte zu vermerken.
- Über die Durchführung von Hausbesuchen sollte der Leiter des Sozialamtes oder eine von ihm besonders ermächtigte Person entscheiden.
- Hausbesuche dürfen nur von Mitarbeiterinnen und Mitarbeitern des Sozialamtes durchgeführt werden.
- Die Mitarbeiter des Sozialamtes müssen sich zu Beginn des Hausbesuches durch die Vorlage ihres Dienstausweises gegenüber den Betroffenen legitimieren.
- Die Gründe für den Hausbesuch sind den Betroffenen zu Beginn des Gespräches offen zu legen. Sie sind darauf hinzuweisen, dass sie den Zutritt zu der Wohnung verweigern können, dass dies jedoch u. U. eine Kürzung der Sozialhilfe zur Folge haben kann.
- Befragungen dritter Personen wie des Hausmeisters oder der Nachbarn ohne Wissen des Betroffenen sowie für die Betroffenen nicht erkennbare Ermittlungen sind nur in Ausnahmefällen zulässig, z. B. wenn ein konkreter Verdacht besteht, dass ein Hilfeempfänger einer Arbeit nachgeht und andere Erkenntnismittel nicht zum Ziel führen.

Kurs SOZ

Als sinnvoll kann sich die Einrichtung eines **zentralen Außendienstes** bei größeren Kreissozialämtern erweisen. So kann ein einheitliches Vorgehen ermöglicht werden. Weitere Hinweise finden sich auf unserer Homepage zum Thema „Prüfbericht über die Kontrolle des Ermittlungsdienstes und der Ausländerbehörde der Landeshauptstadt Kiel“:

http://

www.datenschutzzentrum.de/material/themen/pruefbe/auslbeki.htm

Was ist zu tun?
Diese Grundsätze sollten von allen Sozialämtern umgesetzt werden.

4.7.4 Schweigepflichtsentbindung nicht im „Kleingedruckten“

Die Frage, wie Vordrucke und Formulare datenschutzgerecht gestaltet werden können, stellt sich stets aufs Neue. Insbesondere bei der Formulierung von Einwilligungserklärungen bestehen Unsicherheiten.

Viele Verwaltungen haben im vergangenen Jahr deshalb unsere Beratung in Anspruch genommen (vgl. 22. TB, Tz. 13). In der Regel konnten unbürokratisch datenschutzrechtlich korrekte und praxisgerechte Lösungen gefunden werden. Wegen der Unterschiedlichkeit der Fallkonstellationen kann es bei der Formulierung von Einwilligungen nämlich **kein Patentrezept** geben. Grundsätzlich ist zu beachten, dass eine wirksame Einwilligung voraussetzt, dass der Einwilligende eine Vorstellung davon erhält, worin er einwilligt, und somit die Bedeutung und Tragweite seiner Entscheidung überschauen kann. Er muss wissen, welche Daten zu welchem Zweck von welcher Stelle erhoben werden. Eine Einwilligungserklärung hat grundsätzlich schriftlich zu erfolgen und muss einen Hinweis auf die Freiwilligkeit bzw. die möglichen Folgen bei einer Verweigerung enthalten. Andererseits darf eine Einwilligungserklärung auch nicht mit Informationen derart überladen werden, dass der Betroffene resigniert und das „Kleingedruckte“ gar nicht liest.

Kurs SOZ

Was ist zu tun?
Formulare sollten entsprechend gestaltet werden.

4.7.5 Sind Gemeinden nur Außenstellen der Kreissozialämter?

Im Bundessozialhilfegesetz ist festgelegt, dass die Kreise und kreisfreien Städte als örtliche Träger der Sozialhilfe die Hilfe zum Lebensunterhalt gewähren. Die Kreisverwaltungen bedienen sich hierzu der kreisangehörigen Städte, Gemeinden und Amtsverwaltungen auf der Grundlage von Heranziehungssatzungen. Welche Folgen sich aus dieser Konstellation ergeben, ist strittig.

Die **Bürgernähe der Sozialhilfe** ist sinnvoll. Ein Hilfe Suchender kann in seiner Gemeinde vorsprechen und muss nicht in die Kreisstadt zum Kreissozialamt fahren. Er stellt seine Anträge bei dem Mitarbeiter seiner Gemeinde und erhält von dort die Sozialhilfe. Zieht er in eine andere Gemeinde, kann er in der neuen Gemeinde einen neuen Antrag stellen. Seine „alte" Sozialhilfeakte wird bis zur endgültigen Vernichtung bei der vormals zuständigen Gemeinde aufbewahrt. Die neue zuständige Gemeinde erhält Kenntnis nur von den Daten, die sie für die Sozialhilfeberechnung benötigt (vgl. 20. TB, Tz. 4.7.3; 22. TB, Tz. 4.6.3). Die Daten verarbeitende Stelle ist nicht das (ferne) Kreissozialamt, sondern das Sozialamt der Gemeinde. In Übereinstimmung mit dem Ministerium für Arbeit, Gesundheit und Soziales meinen wir, dass die kreisangehörigen Städte, Gemeinden und die Amtsverwaltungen mit der Aufgabe der Sozialhilfegewährung auch die **Verantwortung** für die Rechtmäßigkeit der Datenverarbeitung übernommen haben.

Nach dem Verständnis einzelner Kreisverwaltungen sind dagegen die Mitarbeiterinnen und Mitarbeiter der Sozialämter in den Gemeinden lediglich ihre „**Außenstellen**". Ein Kreissozialamt dürfe jederzeit und ohne Grund jede Sozialhilfeakte der Gemeinde prüfen, anfordern oder selbst bearbeiten. Andererseits sind die Kreise nicht bereit, die Verantwortung für Fehler bei der Datenverarbeitung zu übernehmen.

Dieser Auffassung können wir uns nicht anschließen. In den teilweise äußerst umfangreichen Sozialhilfeakten sind sensible Angaben über die familiäre, finanzielle oder gesundheitliche Situation der Hilfeempfänger mit besonderem Schutzbedürfnis enthalten. Sie unterliegen aus gutem Grund dem **Sozialgeheimnis**. Sozialdaten dürfen danach nicht unbefugt erhoben, verarbeitet oder genutzt werden. Für den Bürger muss klar ersichtlich sein, wer die Verantwortung für die Rechtmäßigkeit der Verarbeitung seiner Daten trägt. Dies kann nur das Sozialamt vor Ort sein. Alles andere widerspräche der täglichen Verwaltungspraxis, nicht nur in unserem Bundesland. Mit dieser Grundsatzfrage hängt eine Vielzahl weiterer rechtlicher Fragen zu einzelnen Bereichen der Hilfegewährung zusammen, z. B. wer die Aufsicht ausübt (dazu siehe unten), inwieweit im Kreis eine gemeinsame Einrichtung von EDV zulässig ist, aber auch, wer Adressat einer datenschutzrechtlichen Beanstandung ist.

Schleswig-Holstein DATENSCHUTZAKADEMIE
Kurs SOZ

Was ist zu tun?
Die Gespräche mit den Kreisen und der Kommunalaufsicht müssen fortgesetzt werden.

4.7.6 Befreiung von Rundfunkgebühren

Wie das Verfahren zur Befreiung von der Rundfunkgebührenpflicht datenschutzgerecht gestaltet werden kann, ist leider immer noch eine aktuelle Frage. Bis heute ist keine datenschutzgerechte Regelung in Sicht.

Der NDR und die Datenschutzbeauftragten sind sich immer noch nicht einig, ob und in welchem Umfang bei der Beantragung der Gebührenfreiheit Kontrollfragen zulässig sind, mit denen die Glaubwürdigkeit der gemachten Angaben überprüft werden soll. Schon letztes Jahr monierten wir, dass der NDR pauschal jedem Studierenden misstraut und diesem Personenkreis detaillierte Fragen stellt, die nicht einmal ein Sozialamt für erforderlich hält (vgl. 22. TB, Tz. 4.8.3).

Ein erneuter Lösungsvorschlag des NDR verfehlt das Ziel aber ganz und gar. Sahen sich bislang nur Studierende genötigt, detaillierte Angaben z. B. zu ihren Telefon- oder Handygebühren zu machen, so soll diese Pflicht zukünftig **alle Antragsteller** mit geringem Einkommen treffen. Die auch für den NDR bindende Befreiungsverordnung für Rundfunkgebühren grenzt diese Datenerhebung jedoch ein. Kontrollfragen, die über den Datenkatalog der Befreiungsverordnung hinausgehen, sind nur in einzelnen, besonders begründeten Fällen zulässig.

Gleichzeitig zeigt sich der NDR modern und zukunftsorientiert: Papieranträge sind out. Die Angaben der Antragsteller sollen zukünftig **online** von den Mitarbeitern der Sozialämter erhoben und an den NDR bzw. die GEZ übermittelt werden. Dies ist zu begrüßen. Gerade die EDV bietet vielfältige Möglichkeiten für die Wahrung des Datenschutzes. So könnte ein „abgestuftes Verfahren“ eine differenzierte Datenerhebung vorsehen. Dies ließe sich unproblematisch technisch in der neuen Software abbilden. Aufgrund unserer Intervention hat der NDR zugesagt, das Programm zu überarbeiten. Man darf gespannt sein, zu welchem Ergebnis er dabei kommt.

www.datenschutzzentrum.de/material/themen/divers/befrrund.htm

Was ist zu tun?
Der NDR muss ein Verfahren vorlegen, das sich bei der Erhebung von Daten bei Anträgen auf Gebührenfreiheit auf die erforderlichen Daten beschränkt.

4.8 Schutz des Patientengeheimnisses

4.8.1 Überblick

Im letzten Bericht haben wir als die zentralen Probleme mit Datenschutzrelevanz im Gesundheitswesen benannt: Geldknappheit, ungenügende gesetzliche Regelungen und Entwicklungen in der Gentechnik (vgl. 22. TB, Tz. 4.7.1). Mit den gleichen Stichworten lassen sich auch die **wichtigsten Themen** im vergangenen Jahr umreißen. Ergänzt werden muss die Aufzählung allerdings um den Begriff

„Automationsvorhaben“ mit den Unterpunkten „elektronische Krankenakte“ und „Vernetzung“. Die Lösung dieser Probleme wird die Ärzte und Krankenhäuser offenbar noch einige Jahre beschäftigen.

Die Hoffnung auf eine Verbesserung der **Gesetzeslage** im Medizinbereich auf Landesebene hat sich zerschlagen. Überlegungen zu einem umfassenden Gesundheitsdatenschutzgesetz wurden aufgegeben. Allerdings wurden Datenschutzregelungen in einem Gesetz zum öffentlichen Gesundheitsdienst (Gesundheitsämter) auf die Schiene gesetzt. Auf Bundesebene haben sich mit dem Infektionsschutzgesetz, das das Bundesseuchengesetz ablöst, neue medizinische Meldewege ergeben. Die Hoffnungen auf mehr Transparenz der Datenverarbeitung bei der gesetzlichen Krankenversicherung werden auch durch das neue Transparenzgesetz nicht erfüllt werden.

Das **LDSG 2000** enthält auch für die Verarbeitung medizinischer Daten Vorschriften. Sie gelten, soweit spezifische Regelungen fehlen. Medizinische Daten dürfen nur unter klar definierten Voraussetzungen zur Durchführung beratender und begutachtender Tätigkeit im Einzelfall, z. B. an einen Anwalt, herausgegeben und genutzt werden, ebenso für die Durchführung wissenschaftlicher Forschung. Keine Offenbarungsbefugnis besteht gegenüber dem behördlichen Datenschutzbeauftragten. Hierzu bedarf es der Einwilligung der Patientin bzw. des Patienten.

Die beiden Universitätskliniken leisten sich **externe** professionelle **Datenschutzberatung**. Deren Aufgabe ist es, die Bediensteten zu schulen, ein elektronisch verfügbares Datenschutzhandbuch zu entwickeln und zu pflegen, das hausinterne Datenschutzmanagement zu organisieren und für allgemeine Fragen zur Verfügung zu stehen. Dies ist alles andere als Luxus. Es ist nur zu begrüßen, dass die beiden Kliniken den Datenschutz ernst nehmen und sich dies auch etwas kosten lassen. Ob dabei auf externen Sachverstand zurückgegriffen wird, ist zunächst zweitrangig. Auch bei der Beratung durch Externe muss aber der Datenschutz gewahrt bleiben. Die Weitergabe von Personendaten an den externen Berater ist eine Datenübermittlung an Private, die regelmäßig nur nach Vorliegen einer Einwilligung zulässig ist. Außerdem ist darauf zu achten, dass für die Betroffenen erkennbar ist, dass die externe Beratungsstelle kein Teil der Klinik und daher anderen rechtlichen Regeln unterworfen ist. Diese Einsicht wird inzwischen von sämtlichen Beteiligten geteilt und in der Praxis berücksichtigt.

4.8.2 Genomanalyse

Nach der weitgehenden Entzifferung des menschlichen Genoms (DNA) arbeiten viele Wissenschaftler daran, aus bestimmten Genabschnitten medizinische Dispositionen, Krankheiten und körperliche Eigenschaften, aber auch persönliche und charakterliche Anlagen abzuleiten. Die Grenzen der Forschung auf diesem Gebiet sind noch lange nicht erreicht, Konflikte mit dem Recht auf informationelle Selbstbestimmung sind vorgezeichnet.

Mithilfe der **Pränataldiagnostik** kann vor einer Geburt festgestellt werden, welche Eigenschaften ein Mensch künftig haben wird. Soll es zulässig sein, maßgeschneiderte Kinder zu selektieren? Bei Erwachsenen können Ergebnisse von

Genomanalysen bei der Einstellung für bestimmte Berufe, beim Abschluss von Kranken- und Lebensversicherungen und bei der medizinischen Behandlung von Bedeutung sein. Zur Feststellung von verwandtschaftlichen Beziehungen und Abstammungen und zur Identifizierung von Straftätern wird die DNA-Analyse schon in Massenverfahren genutzt. Inzwischen sind Genchips zu erschwinglichen Preisen auf dem Markt erhältlich, über die mit einem relativ einfachen Verfahren das Vorliegen genetischer Dispositionen festgestellt werden kann. Kriminalisten fordern die Untersuchung von Straftätern auf besondere kriminalitätsfördernde Anlagen.

Wir sehen keine Veranlassung, die gesamte Humangenetik zu verteufeln. So mag es möglich sein, mithilfe der **Gendiagnostik** auf den Patienten maßgeschneiderte Medikamente zu „designen". Gegenüber diesen Chancen fallen jedoch erhebliche Risiken ins Gewicht. Solange es keine Behandlungs- oder Vorsorgemöglichkeiten gibt, ist die Feststellung einer Anlage zu einer Krankheit in aller Regel eine kontraproduktiv psychische Belastung für den Patienten. Die Gefahr, dass Menschen je nach genetischer Disposition abgestempelt oder privilegiert werden, ist mit den Händen zu greifen. Gerade Deutschland hat angesichts des Umstandes, dass in seiner jüngeren Geschichte als „minderwertig" eingestuftes Leben diskriminiert und vernichtet worden ist, eine besondere Verantwortung dafür, dass es in der Zukunft keine genetische Diskriminierung gibt.

Der Deutsche Bundestag hat deshalb die Datenschutzbeauftragten des Bundes und der Länder um eine Stellungnahme dazu gebeten, welchen politischen Handlungsbedarf sie zur Absicherung der **genetischen Selbstbestimmung** sehen. Es wird klar zu definieren sein, unter welchen Voraussetzungen Identitäts- und Verwandtschaftsfeststellungen zugelassen werden. Will ein Mensch seine Erbanlagen untersuchen lassen, so muss ihm dies freistehen. Doch darf er nicht gezwungen werden können, dieses Wissen anderen zu offenbaren. Zur genetischen Selbstbestimmung gehört auch, dass jeder Mensch ein „Recht auf Nichtwissen" hat, d. h. niemand darf gegen seinen Willen auf genetische Dispositionen hin untersucht werden. Auch eine „freiwillige" Vorlage gegenüber Versicherungen und Arbeitgebern muss ausgeschlossen werden.

In Sachen humangenetischer Forschung befinden sich die **Ethikkommissionen** der Ärztekammern und der Universitätskliniken an vorderster Front. Wir haben daher mit diesen Gremien den Dialog aufgenommen. In einem Gutachten haben wir für diese Kriterien erarbeitet, die bei solchen wissenschaftlichen Projekten beachtet werden sollten. In der weiteren Diskussion wurden diese Kriterien hinsichtlich der praktischen Umsetzung von der Ärztekammer präzisiert. Dabei geht es insbesondere um die Sicherstellung einer umfassenden Aufklärung der untersuchten Menschen, die Absicherung von deren freier Willensentscheidung und die langfristige Gewährleistung der Anonymität der Untersuchungen.

www.datenschutzzentrum.de/material/themen/gendatei/genanly.htm

Was ist zu tun?
Im Rahmen der Diskussion über eine gesetzliche Regelung muss eine öffentliche Debatte über die ethische, demokratische und rechtsstaatliche Verantwortbarkeit spezieller gentechnischer Anwendungen stattfinden, bei der die kommerziellen Interessen nicht im Vordergrund stehen dürfen.

4.8.3 Digitale medizinische Dokumentationen und ihre Vernetzung

Pilotprojekte zur medizinischen Informationsverarbeitung sprießen an allen Ecken und Enden. Bei Medizinern, Informatikern und EDV-Firmen hat sich eine regelrechte Goldgräberstimmung breit gemacht. Leider haben die Beteiligten oft nicht die Anforderungen des Patientengeheimnisses im Auge.

Gegen eine **digitale medizinische Dokumentation** ist datenschutzrechtlich grundsätzlich nichts einzuwenden. Im Gegenteil: Mithilfe einer differenzierten Zugriffsverwaltung sowie digitalen Signaturen, Verschlüsselungstechniken und elektronischer Protokollierung lässt sich sogar ein **Mehr an Datenschutz** gegenüber der konventionellen Aktenführung erreichen. Problematisch wird es aber dort, wo durch die Nutzung der elektronischen Datenverarbeitung nicht nur die bisherige Dokumentation auf eine effektivere technische Ebene gehoben werden soll, sondern zusätzliche Nutzeffekte angestrebt werden.

Dies ist immer dann der Fall, wenn elektronische Dokumente nicht nur dem behandelnden Arzt bzw. dem Behandlungsteam zur Verfügung gestellt werden sollen, sondern außerdem im Rahmen einer Vernetzung einer größeren, eventuell noch unbestimmten Zahl von Ärztinnen und Ärzten oder gar von fachfremden Personen. Dieses Problem taucht bei so genannten medizinischen **Kompetenznetzwerken**, deren Schwerpunkt in der Forschungsarbeit liegt, ebenso auf wie bei **regionalen Praxisnetzen** und bei **zentralen Archivierungsprojekten**. Dabei gerät nämlich schnell aus dem Blick, dass das Patientengeheimnis eine persönliche ärztliche Pflicht darstellt, die regelmäßig nur durch Erteilung einer wirksamen Einwilligung des Patienten aufgehoben werden kann.

Die an uns herangetragenen **Beratungsersuchen** lassen sich schon fast nicht mehr überblicken. Da hierbei immer wieder die gleichen Fragestellungen auftauchen, haben wir die grundsätzlichen Aussagen zum Patientengeheimnis in medizinischen Netzen wie folgt zusammengefasst:

- Das Patientengeheimnis gilt auch zwischen den Ärzten. Ein Austausch medizinischer Daten ist nur im Rahmen der konkreten Behandlung oder nach Erteilung einer Einwilligung des Patienten zulässig.
- Mitarbeiter von Firmen, die im Rahmen der Systembetreuung, der Wartung oder der Aktenarchivierung tätig sind, können nicht als zugriffsberechtigte „berufsmäßig tätige Gehilfen“ des Arztes angesehen werden, da sie nicht direkt am Behandlungsgeschehen beteiligt und an Weisungen des behandelnden Arztes nicht gebunden sind. Diese Personen dürfen Kontakt zu Daten nur erhalten, wenn sie – z. B. durch Verschlüsselung – für sie nicht lesbar sind.

- Zentrale digitale Patientendatenarchive sind mit dem Patientengeheimnis nur vereinbar, wenn eine Datenverarbeitung im Auftrag der behandelnden Ärzte erfolgt und eine Kenntnisnahme der Daten beim Auftragnehmer ausgeschlossen ist. Eine pauschale Einwilligung der Patienten in die zentrale Datenhaltung wäre wegen der Unbestimmtheit von Datenempfängern, Datenumfang und Zweck unwirksam.
- Die rechtlichen Kriterien für die Wirksamkeit von Einwilligungen (Bestimmtheit von Empfänger, Datenumfang und Zweck) sind sehr streng. Die grundsätzlich in schriftlicher Form zu erteilenden Einwilligungen müssen sich auf einen Behandlungsfall bzw. eine Erkrankung beschränken und so formuliert sein, dass die einwilligende Person eine konkrete Vorstellung von der Art und dem Umfang der bewilligten Offenbarung ihrer Daten erhält. Nur wenn sich die Einwilligung auf – nichtmedizinische – Stammdaten beschränkt, können der Zweck der Weitergabe und der Empfängerkreis der Daten weniger konkret dargestellt werden. Die Hingabe einer Krankenversicherungschipkarte kann als Einwilligung zur Datenübermittlung zwischen Ärzten nicht genügen.
- Sollen digital gespeicherte Daten elektronisch abgerufen werden können, so muss vor jeder Abfrage eine Freischaltung durch den „Datenherrn“, also den behandelnden Arzt erfolgen. Die Einrichtung eines automatisierten Abrufverfahrens ohne Prüfmechanismus ist unzulässig, da mit der Bereitstellung zum Abruf schon eine unbefugte Offenbarung von Patientengeheimnissen erfolgen würde.
- Die Authentifizierung des Arztes bzw. der Ärztin lässt sich zwar mithilfe einer digitalen Signatur, z. B. auf einer Ärztechipkarte (Health Professional Card), nachweisen. Eine solche Chipkarte allein genügt aber nicht zum Nachweis für die Berechtigung zum Empfang übermittelter medizinischer Daten im jeweiligen Einzelfall, wenn nicht die verantwortliche Stelle selbst den Zugriff hierauf autorisiert hat.
- Eine Übertragung der „Datenhoheit“ auf den Betroffenen wäre nur wirksam, wenn dieser die Angaben nach eigenen Vorstellungen verändern und über ihre Verwendung bestimmen könnte. Da dies im Interesse der Integrität und Authentizität medizinischer Daten regelmäßig nicht möglich ist, kommt eine solche Konstruktion in der Regel nicht infrage. Problematisch ist zudem, dass Daten in der Hand des Betroffenen derzeit keinen besonderen rechtlichen Schutz genießen.
- Der Zugriff zu elektronischen medizinischen Datenbeständen durch andere als den behandelnden Arzt ist lückenlos für Kontrollzwecke zu protokollieren.
- Eine Übermittlung von Patientendaten über das Internet ist nur zulässig, wenn der Zugriff für Unbefugte durch eine ausreichende Verschlüsselung ausgeschlossen wird.
- Sollen medizinische Dokumentationen für Zwecke der Forschung, der Qualitätssicherung, der Organisationskontrolle oder zur Herstellung der Behandlungs- bzw. der Kostentransparenz ausgewertet werden, so sind sie zuvor hinreichend zu anonymisieren oder zumindest zu pseudonymisieren.

Wenn diese Voraussetzungen durch die technische Gestaltung des betreffenden Systems tatsächlich erfüllt werden, kann dies, sofern eine Nutzung durch öffentliche Stellen des Landes in Betracht kommt, nach externer Begutachtung über ein im LDSG 2000 erstmals geregeltes Produktaudit zertifiziert werden.

Was ist zu tun?
Bevor eine Vernetzung, bei der Patientendaten ausgetauscht werden sollen, realisiert wird, ist die Beachtung der obigen Kriterien zu gewährleisten.

4.8.4 Wenn die Arztrechnung von einer privaten Firma kommt

Die Übermittlung von medizinischen Daten über Privatpatienten an eine privatärztliche Verrechnungsstelle darf nur erfolgen, wenn der Patient zuvor unterrichtet wurde und seine Einwilligung schriftlich erteilt hat.

Viele Ärzte bedienen sich bei der Erstellung ihrer Rechnungen der professionellen Hilfe von **privatärztlichen Verrechnungsstellen** (PVS). Aber nicht alle Patienten sind damit einverstanden, dass ihre medizinischen Daten an diese Einrichtungen übermittelt werden. So hatte eine Petentin die vorgefertigte Einwilligungserklärung ihres Zahnarztes bewusst nicht unterschrieben und den Arzt gebeten, ihr die Rechnung direkt zuzusenden. Das Erstaunen war groß, als der Arzt daraufhin die Behandlung verweigerte.

Wir haben das Verhalten des Zahnarztes nicht aus standesrechtlicher Sicht zu beurteilen. Hierfür ist die Zahnärztekammer Schleswig-Holstein in Kiel zuständig. Aus datenschutzrechtlicher Sicht konnten wir der Patientin aber nur Recht geben: Zur Rechnungsstellung benötigt die PVS von den Ärzten nicht nur den Namen und die Anschrift der Patienten, sondern auch detaillierte medizinische Angaben zur Behandlung. Das gilt für den allgemeinen Arzt ebenso wie für den Zahnarzt, Psychologen oder Urologen. Eine Befugnis für eine solche Offenbarung findet sich in keinem Gesetz, sodass der Arzt hierfür das **schriftliche Einverständnis** des Patienten benötigt. Selbstverständlich haben Privatpatienten das Recht, ihre Unterschrift zu verweigern. Dies bedeutet, dass der Arzt in diesen Fällen seine Rechnung selbst erstellen muss.

Die Auffassung, dass eine ausreichende Information der Patienten und die vorherige Einholung einer schriftlichen Einwilligungserklärung zwingende gesetzliche Voraussetzung für die rechtliche Zulässigkeit der Übermittlung von Patientendaten an eine PVS ist, wird auch von der Privatärztlichen Verrechnungsstelle Schleswig-Holstein/Hamburg geteilt. Sie sicherte uns zu, ihre Mitglieder durch gesonderte **Rundschreiben** hierüber zu unterrichten. Zudem will man umfangreiche Informationsmaterialien und Mustereinwilligungserklärungen zur Verfügung stellen. Dadurch sollen die Ärzte davor bewahrt werden, gegen die ärztliche Schweigepflicht zu verstoßen und sich strafbar zu machen. In Schleswig-Holstein wurden aus diesem Grund schon einige Strafverfahren eingeleitet.

Was ist zu tun?
Wenn ein Arzt oder Zahnarzt die Rechnung für die Behandlung eines Privatpatienten von einer privatärztlichen Verrechnungsstelle erstellen lassen möchte, muss er den betroffenen Patienten hierüber zuvor unterrichten. Nur wenn der Patient schriftlich sein Einverständnis erteilt, darf der Arzt Patientendaten übermitteln.

4.8.5 Transparenzgesetz

Im Jahr 2000 startete das Bundesgesundheitsministerium einen neuen Anlauf mit einem Transparenzgesetz, durch das im Gesundheitswesen Kosten eingespart werden sollen. Seine datenschutzgerechte Ausgestaltung ist noch nicht sichergestellt.

Während der Entwurf aus dem Jahr 1999 mit der ausschließlich pseudonymen Abrechnung der Krankheitskosten eine elegante Lösung vorsah, wurde das **neue Gesetzeskonzept** nach Intervention der Kassenverbände „**verwässert**". Statt der von uns vorgeschlagenen massiven Vereinfachung des Abrechnungsverfahrens wird es nunmehr noch komplizierter. Das bestehende Verfahren mit seiner Trennung von fallbezogener (anonymer) ambulanter Abrechnung einerseits und personenbezogener Abrechnung von Arzneimittel- und Krankenhauskosten andererseits soll zwar beibehalten werden. Zur Schaffung von mehr Kosten- und weniger Personentransparenz sollen die Angaben bei den Kassenärztlichen Vereinigungen und bei den Kassen zusätzlich pseudonymisiert werden, um sie unter dem Pseudonym an einer dritten Stelle zusammenführen und auswerten zu können.

Allerdings geht der datenschutzrechtliche Gewinn durch die **Pseudonymisierung** teilweise wieder dadurch verloren, dass ein Großteil der Abrechnungen bei den Kassen zumindest mittelfristig personenbezogen erfolgen soll. Es ist für uns nicht nachvollziehbar, dass bei der pseudonymen Abrechnung eine Kostenkontrolle nicht möglich wäre. Wohl stünden die pseudonymisierten Daten nicht so einfach für andere Zwecke, z. B. für Beratung, zur Verfügung. Hierzu müsste in einem geordneten Verfahren eine Reidentifizierung erfolgen. Dieser Gewinn an Datenschutz war aber gerade beabsichtigt: „Es wäre so schön gewesen!" (vgl. 22. TB, Tz. 4.7.2)

Einige andere Teile des Gesetzentwurfes werden dagegen von uns nachhaltig unterstützt. So werden Rechtsregeln für **Werbeaktivitäten** der Kassen geschaffen und der bisherige ungeregelte Zustand beendet. Die Zulässigkeit eines undifferenzierten geschäftsstellenübergreifenden Datenzugriffs – seit Jahren ein Dauerstreitpunkt zwischen Kassen und Datenschützern – soll restriktiv im Sinne des Datenschutzes der Versicherten geregelt werden. Die **Vertraulichkeit der Beratung** durch Krankenkassen wird normativ sichergestellt. Ein kurz vor Redaktionsschluss vorgelegter Referentenentwurf lässt erkennen, dass sich trotz dieser positiven Ansätze eine Vielzahl von Ungereimtheiten und Verschlechterungen „einge-

schlichen“ hat. Dies veranlasste die Konferenz der Datenschutzbeauftragten zu einer kritischen Entschließung.

www.datenschutz-berlin.de/doc/de/konf/61/bmg.htm

Was ist zu tun?
Der Bundesgesetzgeber bleibt aufgerufen, die völlig undurchsichtig gewordenen Regelungen des fünften Sozialgesetzes (SGB V) einer Generalbereinigung zu unterwerfen. Kostentransparenz darf auch in Zukunft nicht zulasten des Patientengeheimnisses gehen.

4.8.6 Kassenweiter Zugriff auf Mitgliederdaten

Ein besonders gewährleisteter Sozialdatenschutz könnte sich als Wettbewerbsvorteil erweisen. Die großen Krankenkassen setzen andere Schwerpunkte und realisieren einen ortsübergreifenden, landesweiten Zugriff auf sensible Patientendaten.

So sachbezogen und ergebnisorientiert im Allgemeinen die Zusammenarbeit mit den regional tätigen Krankenkassen in Schleswig-Holstein ist, so schwierig erweisen sich die Auseinandersetzungen oft mit den bundesweiten Kassen und den Kassenverbänden auf Bundesebene. Leider bestehen unterschiedliche Rechtsanwendungen der in **Konkurrenz** zueinander stehenden Kassen. Symptomatisch ist ein jahrelanger Konflikt wegen des von vielen Kassen zugelassenen **kassenweiten Zugriffs** auf Mitgliederdaten. Der AOK-Bundesverband reihte sich nun definitiv bei den Kassen ein, die allen Geschäftsstellen – teilweise sogar bundesweit – das Abrufen von Mitgliederdaten ermöglichen. Mit der kassenweiten Zugriffsmöglichkeit wird ein großes **Tor zum Missbrauch** von sensiblen Patientendaten geöffnet, denn es ist nicht auszuschließen, dass auf diese für fremde oder gar private Zwecke zugegriffen wird. Selbst unserer Forderung, wenigstens auf solche Kassenmitglieder Rücksicht zu nehmen, die den umfassenden Datenzugriff explizit nicht wollen, wollte man nicht entsprechen. Wer seinen allumfassenden Datenzugriff mit Serviceorientierung begründet, hat nicht verstanden, dass Grundbedingung eines medizinischen Dienstleistungsunternehmens Vertrauen ist. Die Eröffnung des kassenweiten Datenzugriffs gibt keine Grundlage für dieses Vertrauen. Die Kassenmitglieder können nicht überschauen, geschweige denn bestimmen, wer welche sensiblen Krankheits- und Versicherungsdaten über sie zur Kenntnis erhält.

Was ist zu tun?
Der Bundesgesetzgeber sollte den kassenweiten Zugriff auf Krankenkassenmitgliederdaten endlich einschränken.

4.8.7 Outsourcing bei Krankenkassen

Beratungsersuchen in Sachen „Outsourcing“ haben Konjunktur. Krankenkassen beabsichtigten zunehmend die Wahrnehmung der laufenden Verwaltungsaufgaben auf Dritte zu übertragen.

Ein Vertragsentwurf zwischen der Landwirtschaftlichen Krankenkasse und dem Bauernverband sah u. a. die Pflege des Mitgliederverzeichnisses sowie eine **personenbezogene Leistungsabrechnung** zwischen Kasse und dem Verband als Auftragnehmer vor. Da der Auftragnehmer bei der Aufgabenübertragung nicht strengen Weisungen unterworfen werden konnte, waren die Regeln der Datenverarbeitung im Auftrag nicht anwendbar. Für eine regelrechte Übertragung von hoheitlichen Befugnissen – in Form einer Beleihung – fehlte eine hinreichend präzise gesetzliche Grundlage. Da auch die Übermittlungsregelungen des Sozialgesetzbuches die Übertragung eines Gesamtdatenbestandes nicht rechtfertigen konnten, mussten wir der Kasse mitteilen, dass die geplante Aufgabenübertragung nur zulässig sein kann, wenn die betroffenen Mitglieder zuvor ihre **Einwilligung** erteilt haben.

Von der AOK Schleswig-Holstein wurde uns die Frage gestellt, ob und wie es möglich sei, Mitarbeiterinnen und Mitarbeiter anderer Krankenkassen für die eigene Sachbearbeitung einzuspannen. Das SGB eröffnet insofern zwei Wege: Bei einer **Auftragsdatenverarbeitung** können Daten zwischen Auftraggeber und Auftragnehmer ausgetauscht werden. Die Einrichtung von Online-Verfahren ist möglich. Doch darf sich der Auftrag nur auf Hilfsdienste bei der Datenverarbeitung beziehen, wobei die Ausführung streng nach Weisung erfolgen muss. Eine Sachbearbeitung mit eigenen Entscheidungsbefugnissen lässt sich über diesen Weg nicht rechtfertigen.

Hier bietet sich eine andere Regelung im Sozialgesetzbuch an, die die Wahrnehmung der Aufgaben eines Leistungsträgers durch einen anderen Leistungsträger erlaubt. Dies bedeutet, dass nicht nur die Datenverarbeitung, sondern in abgegrenzten Bereichen die **Verantwortung der Aufgabenerfüllung** auf den Auftragnehmer übergeht, der damit zur Daten verarbeitenden Stelle wird. Dies muss im Interesse datenschutzrechtlicher Transparenz den Betroffenen gegenüber offen gelegt werden. Der Datenaustausch zwischen Auftraggeber und Auftragnehmer ist – im Rahmen der Erforderlichkeit – eine zulässige Datenübermittlung. Bei Einrichtung eines automatisierten Abrufverfahrens sind aber Restriktionen zu beachten: Materiell wird die Eilbedürftigkeit der Bearbeitung oder eine große Anzahl von Übermittlungen verlangt, schutzwürdige Betroffenenbelange müssen gewahrt werden. Ein Kontrollverfahren muss eingerichtet werden. Schließlich sind die zuständigen Datenschutzkontrollbehörden zu unterrichten.

Das äußerst problematische Outsourcing-Projekt der AOK, die Mitgliederbetreuung auf private Versicherungsmakler zu übertragen, wurde gestoppt, weil es sich als nicht effizient erwies (vgl. 22. TB, Tz. 4.7.4).

Datenschutzrechtlich keine Probleme scheint eine dritte Lösung zu verursachen: die förmliche **Einstellung der Bediensteten der anderen Kasse**. Bei einer solchen Lösung würden aber vor allem praktische Probleme auftauchen: Die Abschottung der neuen Bediensteten zur ursprünglich Arbeit gebenden Krankenkasse muss wirksam vollzogen werden. Die Verantwortung hierfür trägt ganz allein die „Auftrag“ gebende Kasse.

Was ist zu tun?
Bevor Krankenkassen Teile ihrer Aufgabenerfüllung outsourcen, haben sie eine eingehende Datenschutzprüfung durchzuführen. Es geht nicht an, dass über primär finanziell motivierte, manchmal gewagte Beauftragungen das Sozialgeheimnis ausgehöhlt wird.

4.8.8 Zulassungsverfahren für Psychotherapeuten

Nach der Änderung des Psychotherapeutengesetzes sehen sich viele praktizierende Psychotherapeuten gezwungen, bei dem Zulassungsausschuss für Ärzte einen Antrag auf Zulassung zur vertragsärztlichen Versorgung zu stellen, um die Behandlungskosten über die gesetzlichen Krankenkassen abrechnen zu können. Der dafür nötige Nachweis ihrer Fachkunde ist durch die Vorlage von Falldokumentationen zu erbringen. Nur durch Pseudonymisierung ist es möglich, einen Verstoß gegen die berufliche Schweigepflicht zu vermeiden.

Wie uns ein Psychotherapeut berichtete, sollte er zum **Nachweis seiner Fachkunde** dem Zulassungsausschuss schriftliche Dokumentationen von einigen Fällen, die er in der Vergangenheit behandelt hatte, vorlegen. Der Vordruck hierfür sah eine leicht identifizierbare Chiffre vor. Dies war dem besorgten Therapeuten zum Schutz seiner Patienten zu wenig, er wandte sich an uns.

Ein Psychotherapeut unterliegt der beruflichen Schweigepflicht. Die Übermittlung der Patientennamen an den Zulassungsausschuss ohne deren Einwilligung wäre ein Verstoß gegen das Patientengeheimnis. Der Vordruck zur Erstellung der Dokumentation erfragte zwar weder Name noch Anschrift des Patienten, wohl aber eine **Patientenchiffre**. Diese Patientenchiffre setzte sich aus den ersten Buchstaben des Nachnamens des Patienten sowie seinem Geburtsdatum als sechsstellige Zahl zusammen. Mit guten Gründen bezweifelte der Therapeut, dass diese Patientenchiffre eine ausreichende Pseudonymisierung wäre. Mit nur wenig Zusatzwissen wäre es für den Zulassungsausschuss oft möglich gewesen zu erkennen, welcher Patient sich hinter der Chiffre verbirgt.

Der Zulassungsausschuss für Ärzte in Schleswig-Holstein erklärte zunächst, die Patientenchiffre sei entweder aus den Anfangsbuchstaben des Vor- und Nachnamens oder dem Geburtsdatum oder einer **laufenden Nummer** zu bilden. In diesem Fall hätte man, vorausgesetzt dass weitere identifizierende Merkmale wie Anschrift usw. fehlen, von einer ausreichenden Pseudonymisierung ausgehen können. Es bestand jedoch das begründete Risiko, dass Antragsteller eine Patien-

tenchiffre aus einer Kombination der drei Möglichkeiten bildeten. Erst nach längerem Schriftwechsel sagte der Zulassungsausschuss zu, in einem gesonderten Rundschreiben alle psychologischen Psychotherapeuten und Kinder- und Jugendpsychotherapeuten darüber zu unterrichten, dass die Patientenchiffre nur durch eine vom Antragsteller zu vergebende **fortlaufende Nummer** erstellt werden soll.

Was ist zu tun?
Die ärztliche Schweigepflicht ist von Psychotherapeuten auch im Verfahren der Zulassung bzw. Ermächtigung zur vertragsärztlichen Versorgung zu beachten. Eine Falldokumentation darf hierfür nur in ausreichend pseudonymisierter Form vorgelegt werden.

4.8.9 Datensicherheit im Bereich der Gesundheitsämter

Mit den Sicherheitsanforderungen für ihre Aktenbestände sind die Amtsärzte in der Regel gut vertraut. Mit der Durchsetzung entsprechender Sicherheitsmaßnahmen für ihre automatisierten Dateien tun sie sich schwerer. Bei einer vollständigen Vernetzung der Arbeitsplätze in den Kreisen und kreisfreien Städten stellt sich den Gesundheitsämtern die Frage, ob die Administration der Server durch Mitarbeiter der zentralen IT-Stellen zulässig ist.

Der überwiegende Teil der Datenbestände in Gesundheitsämtern unterliegt der **ärztlichen Schweigepflicht**. Die Ärzte sind danach zur Offenbarung von Informationen, die ihnen in dieser Eigenschaft anvertraut oder bekannt geworden sind, nur befugt, soweit

- sie von der Schweigepflicht entbunden worden sind,
- die Offenbarung zum Schutz eines höherwertigen Rechtsgutes erforderlich ist oder
- gesetzliche Aussage- und Anzeigepflichten oder Befugnisse bestehen.

Dies hat dazu geführt, dass die papierenen Datenbestände der Gesundheitsämter durchweg in speziellen Behältnissen oder Räumen unter Verschluss verwahrt werden. Die Inhalte der Akten gelangen nur den jeweils zuständigen Amtsärzten und den von ihnen beaufsichtigten „berufsmäßig tätigen Gehilfen“ zur Kenntnis. An das Gesundheitsamt gerichtete Post wird erst dort geöffnet, ausgehende Post verlässt das Gesundheitsamt verschlossen. Müssen im Einzelfall der Schweigepflicht unterliegende Daten mit anderen Stellen der gleichen Behörde ausgetauscht werden, erfolgt auch dies in verschlossener Form. Dies haben jedenfalls unsere bisherigen Stichproben bei Prüfungen vor Ort ergeben.

Ein entsprechendes Sicherheitsniveau ist auch bei der **automatisierten Verarbeitung** der betreffenden Daten zu gewährleisten. Die Bundesärztekammer hat den Ärzten hierzu folgende Empfehlungen gegeben:

- Der Einsatz von EDV-Technik erfordert nicht nur die Beachtung der rechtlichen Rahmenbedingungen, sondern macht es auch erforderlich, dass der organisatorische Ablauf den Besonderheiten des Einsatzes dieses Mediums Rechnung trägt.
- Der Arzt muss während der vorgeschriebenen Aufbewahrungsfristen in der Lage sein, auch nach einem Wechsel des EDV-Systems oder der Programme innerhalb angemessener Zeit die elektronisch dokumentierten Informationen lesbar und verfügbar zu machen.
- Die Wartung einer EDV-Anlage oder jegliche Fehlerbeseitigung vor Ort darf grundsätzlich nur mit Testdaten erfolgen. Auch im Notfall, z. B. bei Systemstillstand, muss der Einblick Dritter in Originaldaten auf besondere Ausnahmefälle beschränkt bleiben. Das Wartungspersonal ist in diesen Fällen zu beaufsichtigen und schriftlich zur Verschwiegenheit zu verpflichten. Die durchgeführten Maßnahmen sowie der Name der Wartungsperson sind zu protokollieren.
- Die Fernwartung von EDV-Systemen ist unzulässig, wenn nicht auszuschließen ist, dass dabei auf patientenbezogene Daten zugegriffen werden kann.
- Beim Datenträgeraustausch mit befugten Dritten ist ein sicherer Transport zu gewährleisten.
- Die Datenfernübertragung personenbezogener Daten per Leitung muss chiffriert erfolgen.
- Auszumusternde Datenträger müssen unter Aufsicht des Arztes (z. B. durch mehrfaches Überschreiben mittels geeigneter Software) unbrauchbar gemacht werden.
- Der Arzt sollte in jedem einzelnen Wartungs- oder Reparaturfall darauf achten, dass die genannten Vorschriften eingehalten werden.

Diese Anforderungen sind recht einfach zu erfüllen, solange die EDV-Systeme (in der Regel PC) sich in der **unmittelbaren Verfügungsgewalt** des ärztlichen Personals eines Gesundheitsamtes befinden. Ihre Administration und Nutzung können durch die bzw. unter der Aufsicht derjenigen erfolgen, die der Schweigepflicht unterliegen. Durch eine entsprechende Organisation der Datenbestände kann zudem erreicht werden, dass die Zugriffsmöglichkeiten den jeweiligen Zuständigkeiten entsprechen. Dies ist besonders wichtig, weil eine Offenbarung der der Schweigepflicht unterliegenden Daten nicht allein damit gerechtfertigt werden kann, dass der Empfänger der Informationen selbst auch der Schweigepflicht unterliegt.

Werden die Arbeitsplatzsysteme eines Gesundheitsamtes jedoch mit einem Server **vernetzt** und die Datenbestände **zentral** abgelegt, stellt sich die Frage, wer dessen Administration und die Zuweisung von Zugriffsbefugnissen abwickeln darf. Soll dies durch Mitarbeiter einer zentralen EDV-Arbeitsgruppe geschehen, dürften die von der Bundesärztekammer definierten Kriterien nicht erfüllt sein. Im Hinblick auf die ärztliche Schweigepflicht macht es nämlich keinen Unterschied, ob die Administration/Wartung durch Mitarbeiter externer Dienstleister (Fernwartung)

oder anderer Verwaltungsbereiche erfolgt. Es kommt entscheidend darauf an, ob eine unbeaufsichtigte, tatsächliche Kenntnisnahme der Daten durch Unbefugte möglich ist oder nicht. Das Arztrecht und die dazu ergangene Rechtsprechung des Bundesgerichtshofes kennen, anders als das Sozialdatenschutzrecht, keine Auftragsdatenverarbeitung.

Deshalb bleiben faktisch nur zwei Möglichkeiten für eine „**Fremdadministration**“: Entweder werden die Datenbestände so verschlüsselt, dass sie durch die Administratoren inhaltlich nicht zur Kenntnis genommen werden können, oder ihre Tätigkeit wird durch die Schweigepflichtigen überwacht. Die erste Alternative führt regelmäßig zu technischen Schwierigkeiten beim Einsatz von Datenbanken (z. B. Wegfall der Selektionsmöglichkeiten). Die zweite Lösungsmöglichkeit ist praktikabler. Im Ergebnis ist entscheidend, dass das zur Administratorenkennung gehörende Passwort nur im Gesundheitsamt bekannt ist, sodass jeder Administrationsvorgang durch Verantwortliche aus diesem Bereich freigeschaltet werden muss. Wo der Server installiert wird, ist mithin von sekundärer Bedeutung. Die Schweigepflichtigen entscheiden selbst, ob und wie intensiv sie die Administrationstätigkeiten überwachen und unbefugte Kenntnisnahmen von Dateninhalten unterbinden. Im Zweifel brechen sie den Administrationsvorgang ab.

Was ist zu tun?
Wegen der besonderen rechtlichen Gegebenheiten sollten sich die Amtsärzte zumindest insoweit als „Herren“ ihrer automatisierten Verfahren fühlen, wie es um die Vertraulichkeit der Gesundheitsdaten geht. Die Pflicht zur Garantie der ärztlichen Verschwiegenheit kann ihnen durch keine EDV-Abteilung abgenommen werden.

4.9 Steuerverwaltung

4.9.1 Steuergeheimnis und Outsourcing – kein Dammbruch, aber Schleusen werden eingebaut

Outsourcing ist in der Steuerverwaltung des Landes kein Tabu mehr. Das Steuergeheimnis wird rechtlich neu interpretiert, um durch die Einbeziehung externer Dienstleister in das Besteuerungsverfahren Kosteneinsparungen realisieren zu können. Jetzt ist der Zeitpunkt gekommen, um diese Absichten durch konkrete gesetzliche Regelungen auf ein vertretbares Maß zu begrenzen.

Im Zusammenhang mit der früheren Kooperation zwischen der Oberfinanzdirektion (OFD) und der Datenzentrale (DZ-SH) und der seit 1999 bestehenden Dreierzusammenarbeit zwischen der OFD, der DZ-SH und dem Landesamt für Informationstechnik in Hamburg haben wir bereits einige Male (vgl. zuletzt 22. TB, Tz. 4.9.3) berichtet. Die Diskussion ist über die Frage entbrannt, ob die Vorschriften über das Steuergeheimnis eine Beauftragung **externer Dienstleister** mit Rechenzentrums- und Versandarbeiten zulassen, wenn dabei eine Offenbarung steuerlicher Verhältnisse nicht zu vermeiden ist. Bis vor kurzem bestanden in

Schleswig-Holstein klare Verhältnisse: Ein solches Outsourcing wurde von der Steuerverwaltung schlechthin als unzulässig angesehen. Obwohl es organisatorisch durchaus aufwändig war, wurde den Mitarbeitern im Rechenzentrum der DZ-SH der Blick auf ausgedruckte Steuerbescheide unmöglich gemacht.

Im letzten Jahr hat das Finanzministerium jedoch aus Kostengründen diese **Rechtsauffassung** geändert. Von der Zusammenlegung der so genannten Nachverarbeitungsbereiche (Druck, Kuvertierung und Versand von Steuererklärungen, Mahnungen und Steuerbescheiden) der DZ-SH, des Landesamtes für Informationstechnik und der OFD wurde zwar entgegen der ursprünglichen Absicht „vorerst" Abstand genommen. Es bleibt also bis auf weiteres bei der bisherigen, datenschutzrechtlich nicht zu beanstandenden Abschottung. Ausschlaggebend für diese Entscheidung waren jedoch keine rechtlichen, sondern personalwirtschaftliche Gründe. Es ließen sich nämlich die unterschiedlichen Arbeits-/Schichtdienstzeiten der OFD und der DZ-SH nicht vereinheitlichen.

Zu den rechtlichen Aspekten hat das Ministerium für Finanzen und Energie uns jedoch mitgeteilt, dass es eine Zusammenführung der Nachbearbeitungsbereiche unter Beachtung der Vorgaben des Steuergeheimnisses nunmehr grundsätzlich für zulässig erachtet. Dies ist im Ergebnis eine klassische Kehrtwendung in der Rechtsauffassung bei unveränderter Gesetzes- und Rechtsprechungslage. Ganz wohl scheint sich das Ministerium bei diesem „Einbau einer Schleuse für alle Fälle" nicht zu fühlen. Es kündigte nämlich gleichzeitig an, im Rahmen der derzeit vorbereiteten Überarbeitung des **Finanzverwaltungsgesetzes** eine entsprechende gesetzliche Klarstellung einzubringen. So klar wie behauptet ist die Rechtslage wohl dann doch nicht. Warum erscheint es sonst zweckmäßig, zusammen mit den anderen Bundesländern, die ihre Meinung zu diesem Thema gleichfalls geändert haben, den Gesetzgeber davon zu überzeugen, dass nach dem Sozialgeheimnis (vgl. § 80 SGB X) ein weiteres „besonderes Amtsgeheimnis" aus ökonomischen Gründen ausgehöhlt werden muss?

Die Folgen dieser Entwicklung liegen auf der Hand. Wer der Steuerverwaltung das preiswerteste Angebot macht, wird künftig bundesweit das Geschäft mit dem Druck und dem Versand der jährlich Millionen von Steuerbescheiden machen. Firmen wie die DATEV oder die Post-AG stehen sicher schon „Gewehr bei Fuß".

Was ist zu tun?
Wenn der aus dem Grundgesetz abgeleitete Begriff der „Steuerverwaltungshoheit" auch in Zukunft eine herausgehobene Bedeutung haben soll, bedarf es der Zurückhaltung bei der Einschaltung von externen Dienstleistern. Bei den Beratungen auf Bund-Länder-Ebene sollte das Ministerium für Finanzen und Energie sich der Tatsache bewusst sein, dass es auch künftig „oberster Hüter des Steuergeheimnisses" ist.

4.9.2 FISCUS – Der Fortschritt ist eine Schnecke

Die Steuerverwaltungen des Bundes und der Länder tun sich schwer, eine einheitliche Steuerfestsetzungs- und Erhebungssoftware zu entwickeln. Datenschutzrechtliche Bewertungen der bisherigen Konzepte konnten mangels Masse noch nicht vorgenommen werden.

Das Vorhaben der Datenschutzbeauftragten, die Planungen der Steuerverwaltungen des Bundes und der Länder im Zusammenhang mit der Entwicklung des „**Föderalen Integrierten Standardisierten Computer-Unterstützten Steuersystems**“ datenschutzrechtlich zu durchleuchten, musste verschoben werden, da das Projekt zunächst ins Stocken geraten ist und dann auf eine völlig neue organisatorische (möglicherweise auch inhaltliche) Grundlage gestellt wurde.

FISCUS war bisher nach dem Prinzip einer verteilten dezentralen Aufgabenwahrnehmung durch die Länder auf der Grundlage einer zentralen Gesamtprojektleitung durch den Bund und durch föderale Entscheidungsgremien organisiert. Die bisherige arbeitsteilige Organisation des Projektes und die dezentrale Entwicklung der Software waren nach Ansicht der Beteiligten nicht erfolgreich. Das zeigte sich daran, dass das Projekt um mehr als zwei Jahre in Verzug geraten ist. Die Finanzministerkonferenz hat daher im Oktober 2000 beschlossen, eine **FISCUS-GmbH** als zentrale Entwicklungsstelle für den Softwarebedarf der Steuerverwaltungen zu gründen. Sie soll zudem ein geeignetes Unternehmen aus dem Bereich der Informationsverarbeitung auswählen, mit dem das Projekt zusammen entwickelt und das in die Geschäftsführung integriert wird.

Ziel der Zentralisierung der Softwareentwicklung ist es, den Kommunikations- und Reiseaufwand drastisch zu vermindern, die Personalführung zu straffen, das Projektcontrolling zu verbessern und die softwaretechnische Vorgehensweise besser zu unterstützen. Letzteres kann weit reichende Auswirkungen auf die sicherheitstechnischen Aspekte haben. Deshalb erschien es nicht angezeigt, die bisher verfügbaren Konzepte einer vertieften datenschutzrechtlichen und sicherheitstechnischen Analyse zu unterziehen. Sobald sich jedoch das neue Softwarehaus etabliert hat, werden intensive Kontakte erforderlich sein, um die bereits jetzt sichtbaren Fragestellungen im Zusammenhang mit elektronischen Aktenführungen, personenbezogenen Verknüpfungsmöglichkeiten und Zugriffsberechtigungskonzepten zu erörtern. Die Dimension des Projektes zeigt sich daran, dass als Leistungsentgelte an die GmbH für die nächsten vier Jahre ca. **330 Millionen DM** eingeplant sind.

Was ist zu tun?
Das Ministerium für Finanzen und Energie sollte in den Bund-Länder-Gremien seinen Einfluss dahingehend geltend machen, dass die von den Datenschutzbeauftragten eingesetzte Arbeitsgruppe, deren Geschäftsführung beim Unabhängigen Landeszentrum für Datenschutz liegt, umfassend über die Planungen und Konzepte des neuen FISCUS-Projektes informiert wird.

4.9.3 Reorganisation der PC-Welt in den Finanzämtern

In dem Maße, wie sich die IT-Systeme von Schreib- und Rechenmaschinen zu Organisationsmitteln entwickeln, wird es schwieriger, sie sicherheitstechnisch im Griff zu behalten. Selbst der Steuerverwaltung mit ihrer 30-jährigen Automationserfahrung bereitet die Bewältigung dieser Aufgabe Probleme.

Es ist bereits drei Jahre her, dass wir im Rahmen einer Prüfungsmaßnahme festgestellt haben, dass die Datenverarbeitungsprozesse in der Steuerverwaltung sich faktisch mehr und mehr aus dem Verantwortungsbereich der Automationsabteilung der OFD herauslösen und von den Finanzämtern eigenständig entwickelt und durchgeführt werden. Wegen unklarer Zuständigkeitsregelungen haben wir eine Reihe von **sicherheitstechnischen Defiziten** aufgedeckt (vgl. 21. TB, Tz. 6.7.2). Mit der OFD konnte daraufhin ein Einvernehmen dahin gehend erzielt werden, dass die Dezentralisierung der Verarbeitungsprozesse durch eine Neugestaltung der aufbau- und ablauforganisatorischen Regelungen begleitet werden muss, um die Sicherheit und Ordnungsmäßigkeit der automatisierten Datenverarbeitung zu gewährleisten und die jeweils Verantwortlichen transparent zu machen. Die Zusage, die bestehenden Defizite zügig abzubauen, konnte die OFD nicht einhalten, da das Jahr-2000-Problem nach eigener Aussage alle verfügbaren personellen Kapazitäten gebunden hatte.

Nunmehr scheint die Sache jedoch voranzukommen. Es haben erste **Beratungsgespräche** darüber stattgefunden, ob zunächst die grundlegenden strukturellen Änderungen in Angriff genommen werden sollten oder ob es möglich ist, durch die Festschreibung punktuell wirkender Sicherheitsmaßnahmen (z. B. durch neue Dienstanweisungen zum Gebrauch von Bürokommunikationssoftware) eine landesweit einheitliche Vorgehensweise in den Finanzämtern zu erreichen.

Eine übereinstimmende Sicht der Dinge konnte bisher noch nicht erreicht werden. Wenn die notwendigen strukturellen Änderungen „**auf die lange Bank**“ geschoben werden, sehen wir auf die Steuerverwaltung ähnliche Schwierigkeiten zukommen, wie sie derzeit in der Polizeiverwaltung zu verzeichnen sind (vgl. Tz. 7.5.1). Es dürfte einerseits nicht möglich sein, die Datenverarbeitung in 20 Finanzämtern mit über 4.000 Arbeitsplätzen ausschließlich zentral zu managen, andererseits darf sich in den einzelnen Finanzämtern wegen der Sensibilität der dort verarbeiteten Daten auch kein „Wildwuchs“ an Datenbeständen und Verfahrensweisen entwickeln. Wo der „goldene Schnitt“ zwischen diesen beiden Polen liegt, wird nicht ganz einfach zu ermitteln sein. Durch Ad-hoc-Entscheidungen und Einzelregelungen wird er aber wahrscheinlich nicht gefunden werden können.

Was ist zu tun?
Die Steuerverwaltung wird ein Gesamtkonzept für die künftige IT-Unterstützung der derzeit 4.000 Arbeitsplätze in den Finanzämtern entwickeln müssen. Darin wird auch festzulegen sein, welche technischen und organisatorischen Entscheidungsspielräume den einzelnen Finanzamtsvorstehern eingeräumt und welche sicherheitstechnischen Entscheidungs- und Eingriffsbefugnisse in der OFD zentralisiert werden.

5 Datenschutz bei Gerichten

Haftbefehl im Papierkorb des Gerichtsflurs

Offene Registraturschränke und sensible Daten im Papierkorb sind im Bereich der Justizverwaltung noch nicht ganz „ausgerottet".

Bei den angekündigten/unangekündigten Kontrollen von Amtsgerichten stellten wir folgende datenschutzrechtliche Mängel fest:

In einem Amtsgericht waren auf den Fluren neben den Kopiergeräten für Gerichtsmitarbeiter **Papierkörbe** aufgestellt, in denen wir interessante, jedem Gerichtsbesucher zugängliche Funde machten: Als Fehlkopien lagen dort ein **Haftbefehl** sowie ein **Kostenfestsetzungsbeschluss** mit den personenbezogenen Daten der Betroffenen. Wir haben unsere Beanstandung mit dem Vorschlag verbunden, entweder Schredder für solche Fehlkopien neben dem Kopierapparat aufzustellen oder die Mitarbeiter zu verpflichten, derartige Papiere in den Büros datenschutzgerecht zu entsorgen und die Papierkörbe auf den Fluren zu entfernen.

Darüber hinaus wurden immer noch Hängeregistraturschränke für die Gerichtsakten vorgefunden, die nicht abschließbar waren. An die Zusage der Justiz, im Rahmen der jährlichen Haushaltsmittel auf eine Anschaffung verschließbarer Behältnisse für personenbezogene Unterlagen hinzuwirken (vgl. 21. TB, Tz. 10.3), mussten wir daher erinnern. In einem Fall waren sogar erst vor wenigen Jahren neue Büromöbel angeschafft worden, ohne auf die Verschließbarkeit zu achten. Wir haben eine Nachrüstung dieses Mobiliars empfohlen, da zumindest Reinigungskräfte faktischen Zugang zu den darin enthaltenen Akten haben. Allerdings stellten wir bei unseren Prüfrundgängen in keinem Fall unabgeschlossene, unbesetzte Geschäftsstellen fest.

Was ist zu tun?
Die Justiz sollte sich weiterhin um die flächendeckende Ausstattung mit verschließbaren Schränken für Gerichtsakten bemühen. Sensible personenbezogene Unterlagen haben in Papierkörben auf Gerichtsfluren nichts zu suchen.

6 Datenschutz in der Wirtschaft

6.1 Übernahme der Aufsichtstätigkeit vom Innenminister

Entsprechend den neuen Zuständigkeitsregelungen im LDSG 2000 übernahm das ULD zum 01.07.2000 die Aufgaben der Aufsichtsbehörde nach § 38 BDSG vom Innenminister. Nach gründlicher Vorbereitung gestaltete sich der Vorgang nahezu reibungslos. Der Innenminister übergab ein „**wohl bestelltes Haus**“, sodass wir seine erfolgreiche Aufsichtstätigkeit nahtlos fortsetzen konnten. Die noch vom Innenminister geplanten Prüfungsvorhaben wurden durchgeführt. Es hat sich als vorteilhaft erwiesen, dass die Neuorganisation des Datenschutzes in Schleswig-Holstein von Anfang an im Einvernehmen zwischen dem Innenminister und dem Unabhängigen Landeszentrum für Datenschutz konzipiert und in die Gesetzgebung eingebracht worden ist.

Es besteht Einvernehmen mit dem Innenministerium, dass das ULD damit die Funktion der obersten Datenschutzaufsichtsbehörde Schleswig-Holsteins wahrnimmt. Daher repräsentiert das ULD das Land seit dem 01.07.2000 auch in dem so genannten **Düsseldorfer Kreis**, einem Koordinierungsgremium der obersten Aufsichtsbehörden für den nichtöffentlichen Bereich. Der Düsseldorfer Kreis trifft sich etwa halbjährlich, um ein einheitliches Auftreten der Datenschutzbehörden gegenüber der Wirtschaft zu erleichtern. Daneben hat er mehrere Arbeitsgruppen eingerichtet, die datenschutzrechtliche Fragen im Zusammenhang mit der Privatwirtschaft aufgreifen und einer Beschlussfassung zuführen bzw. für die Beschlussfassung des Düsseldorfer Kreises vorbereiten.

Die unterschiedliche organisatorische Ausgestaltung der Datenschutzaufsicht in den einzelnen Ländern hat während des Berichtszeitraums zu Erörterungen im Düsseldorfer Kreis hinsichtlich der Frage geführt, wer an diesem Gremium teilnehmen und in ihm den Vorsitz führen kann. Um die gemeinsame Willensbildung der obersten Aufsichtsbehörden im nichtöffentlichen Bereich effektiver zu gestalten, werden derzeit im Düsseldorfer Kreis außerdem Vorschläge diskutiert, die kurzfristigere und verbindlichere Beschlussfassungen ermöglichen.

6.2 Was wird neu?

Die Übertragung der Datenschutzaufsicht auf das Unabhängige Landeszentrum für Datenschutz bietet auch die Chance, methodisch und inhaltlich **neue Schwerpunkte** für den Datenschutz in der Wirtschaft zu setzen. Dabei zeichnet sich schon jetzt eine zweigleisige Vorgehensweise ab:

Da die Datenverarbeitung in den Wirtschaftsunternehmen für deren Kunden weitgehend undurchsichtig ist, kommt der **Kontrolltätigkeit** eine besondere Bedeutung zu. Die Erfahrungen, die wir mit unseren Kontrollen bei den Behörden gemacht haben, lassen sich bis zu einem gewissen Grad durchaus auf die Wirtschaft übertragen. Wer unsere bisherige Vorgehensweise verfolgt hat, kann abschätzen, wie wir die Kontrollen im Wirtschaftsbereich durchführen werden: Fair,

aber konsequent. Die Bürgerinnen und Bürger können sich darauf verlassen, dass wir auch gegenüber Firmen und sonstigen Organisationen als loyaler Anwalt ihrer Interessen auftreten werden. Angesichts der begrenzten Personalausstattung kommen allerdings nur Schwerpunktkontrollen in Betracht. Diese werden sich naturgemäß auf die neuralgischen Bereiche konzentrieren, also auf Rechtsverhältnisse und Verfahrensweisen, bei denen in besonderem Maße mit Interessenkonflikten zwischen Wirtschaft und Verbrauchern zu rechnen ist.

Aber der Datenschutz ist weit mehr als nur ein mit ordnungsbehördlichen Mitteln durchzusetzendes Recht. Die Bürgerinnen und Bürger und damit die Kunden der Wirtschaft fragen immer häufiger danach, welchen **Datenschutzkundendienst** ein Unternehmen anbieten kann. Welche Nachteile es haben kann, wenn kein überzeugendes Datenschutzangebot gemacht wird, müssen zurzeit gerade einige Unternehmen der New Economy erfahren. Sie haben schwer darunter zu leiden, dass der E-Commerce bislang weit hinter den Erwartungen zurückbleibt. Einer der Gründe dafür liegt nach übereinstimmenden Umfrageergebnissen aus den USA, Europa und Deutschland an dem fehlenden Vertrauen der Nutzer in die Möglichkeit, ihre Daten im Internet wirksam zu schützen. Nicht zu viel Datenschutz, sondern fehlender Datenschutz als Wettbewerbsnachteil ist eine Sichtweise, die längst noch nicht alle Unternehmensleitungen verinnerlicht haben.

Hat man ein gutes Datenschutzangebot erst einmal als ein zeitgemäßes Mittel zur Werbung und Überzeugung von Kunden erkannt, dann ergeben sich plötzlich ganz **neue Perspektiven**. Denn wenn der Datenschutz nicht die auferlegte Last, sondern eine Chance ist, um Kundenvertrauen zu werben, kann das Bestreben nicht mehr darauf beschränkt sein, möglichst nicht von der Aufsichtsbehörde für datenschutzrechtliche Mängel kritisiert zu werden, sondern die Anstrengungen gehen in die Richtung, auf dem Gebiet des Datenschutzes möglichst besser zu sein als die Mitbewerber. Es deutet sich an, dass durchaus in einigen Wirtschaftsbranchen darüber nachgedacht wird, wie man sich auf den Wettbewerb um den bestmöglichen Datenschutz einstellen soll.

Wir möchten unsere Arbeitsweise von vornherein auf diese geänderten Rahmenbedingungen einstellen. Dafür bieten sich gerade in Schleswig-Holstein günstige Möglichkeiten. Die im schleswig-holsteinischen Landesdatenschutzgesetz enthaltenen Instrumente Datenschutzaudit und Gütesiegel bieten einen guten Ansatz für einen **marktwirtschaftlich orientierten Datenschutz**. Die Kunden werden es begrüßen, wenn sie Produkte und Dienstleistungen auf dem Markt finden, die von einer unabhängigen Stelle auf ihre Vereinbarkeit mit dem Datenschutz hin geprüft und gegebenenfalls mit einem entsprechenden Siegel ausgezeichnet sind. Sinnvoll dürfte es auch sein, auf einzelne Wirtschaftsbranchen zugeschnittene Leitlinien und Checklisten zu erarbeiten, in denen die Generalklauseln des BDSG konkretisiert werden, sodass die Kunden besser abschätzen können, mit welcher Datenverarbeitung sie rechnen können. Die bisherige Information der Kunden mittels nichts sagender Allgemeinplätze („Ihre Daten werden gemäß Datenschutzgesetz verarbeitet“) oder umfangreichen, aber kaum verständlichen Detailinformationen („Kleingedrucktes“) genügt nicht mehr den Ansprüchen.

Wir freuen uns auf die Zusammenarbeit mit allen Unternehmen, die erkannt haben, dass man den Datenschutz nicht nur stereotyp als lästiges Übel, sondern als Gelegenheit zur positiven Profilierung begreifen kann. Wir sind offen für eine Kooperation mit berufsständischen Organisationen und Verbänden. Ein besonderes Augenmerk wird auf die Kontakte mit den **betrieblichen Datenschutzbeauftragten** zu richten sein. Ihre Bedeutung wird sich bei zunehmender Durchsetzung des marktwirtschaftlichen Ansatzes spürbar steigern, denn sie können bei diesem Konzept ihre Rolle als lästige Mahner und Bedenkenträger gegen die des gesuchten Ratgebers eintauschen. Wenn „Privacy“ tatsächlich „sells“, sind bei den Unternehmensleitungen Fach- und Sachkenntnisse im Datenschutz gefragt. Die betrieblichen Datenschutzbeauftragten würden sich bei dieser Sichtweise von „Belastungsfaktoren“ geradezu zu Konkurrenzvorteilen für die Unternehmen wandeln. Wir suchen bevorzugt die Zusammenarbeit mit betrieblichen Datenschutzbeauftragten, die an einer Fortentwicklung ihrer Rolle in dieser Richtung interessiert sind.

Unsere **Beratungskapazitäten** stehen in erster Linie den Kundinnen und Kunden der Wirtschaft zur Verfügung. Denn von ihrer Nachfrage wird es letztlich abhängen, ob der marktwirtschaftliche Datenschutz tatsächlich eine Zukunft hat. Sie haben derzeit angesichts der Undurchsichtigkeit der Zusammenhänge der Datenverarbeitung nur sehr begrenzt die Möglichkeit, über die Verwendung ihrer Daten selbst zu bestimmen. Deshalb werden wir uns verstärkt bemühen, geeignete **Verbraucherinformationen** zur Verfügung zu stellen. Dabei bietet sich ein Ausbau der Zusammenarbeit mit Verbraucherschutzorganisationen an.

6.3 Aktuelle datenschutzrechtliche Fragestellungen

6.3.1 Mitgliederlisten im Internet?

Die Veröffentlichung von Mitgliederlisten im Internet oder am schwarzen Brett ist Vereinen nicht ohne weiteres gestattet. In der Regel muss die Einwilligung der Betroffenen vorliegen.

Die Veröffentlichung von Mitgliederdaten darf ohne Einwilligung der Betroffenen ausschließlich zur Wahrung berechtigter Interessen des Vereins erfolgen und nur, wenn ihr keine überwiegenden schutzwürdigen Interessen seiner Mitglieder entgegenstehen. Wenn Vereine Namen, Bilder oder sonstige Daten ihrer Mitglieder im **Internet** veröffentlichen, geben sie diese Informationen an potenziell jeden Internet-Nutzer weiter, und dies zu keinem bestimmten Zweck. Damit wird einer Auswertung der Mitgliederdaten beispielsweise zu wirtschaftlichen Zwecken Tür und Tor geöffnet. Viele Vereinsmitglieder sind damit nicht einverstanden.

Vereine sind verpflichtet, den Wunsch derjenigen Mitglieder zu respektieren, die ihre personenbezogenen Daten nicht veröffentlichen lassen wollen. Die rechtliche Zulässigkeit der Veröffentlichung hängt von der **vorherigen Zustimmung** eines jeden Mitgliedes ab. Eine solche Einwilligung kann auch vorab für mehrere Internet-Veröffentlichungen gegeben werden, wenn dem Betroffenen bewusst ist, dass sie jederzeit widerruflich ist.

Das Aushängen von **Mitgliederlisten** in **Vereinslokalen** ist unzulässig, wenn sie neben den Namen der Mitglieder auch deren Adressen, Geburtsdaten und dergleichen enthalten. Vereinslokale stehen nämlich in der Regel auch anderen Vereinen und damit der Öffentlichkeit zur Verfügung. Auch in diesen Fällen ist die Einwilligung der betroffenen Vereinsmitglieder notwendig.

Was ist zu tun?
Vereine müssen vor der Veröffentlichung von personenbezogenen Mitgliederdaten grundsätzlich die Zustimmung der betroffenen Mitglieder einholen.

6.3.2 Arbeitnehmer sind keine Renntiere

Noch immer findet man Unternehmen, die modernes Personalmanagement über „Rennlisten" und dergleichen realisieren wollen und damit Arbeitnehmerrechte verletzen.

Ein Mitarbeiter empörte sich über die Veröffentlichung von „**Rennlisten**" in einem mittelständischen Unternehmen: Im Büro des Prokuristen hing eine sich über eine drei Viertel Wand erstreckende, jedermann gut einsehbare Statistik, die über die Häufigkeit und Dauer von **krankheitsbedingten Arbeitsabwesenheiten** der einzelnen Mitarbeiter und Mitarbeiterinnen informierte. Außerdem wurde eine Liste geführt, die Auskunft über die **Verkaufserfolge** der Mitarbeiter gab und die von jedem Mitarbeiter eingesehen werden konnte. Auf diese Weise sollten die Mitarbeiter motiviert werden, ihre Leistungen zu steigern. Die Veröffentlichung der Krankheitszeiten und von Erfolgslisten (Rennlisten) verstößt gegen das Persönlichkeitsrecht der betroffenen Arbeitnehmer, weil sie so einer permanenten Kontrolle durch ihre Kollegen ausgesetzt sind. Wir konnten das Unternehmen davon überzeugen, beide Listen nicht mehr zu veröffentlichen.

Was ist zu tun?
Listen, in denen die jeweiligen Krankheitszeiten der Mitarbeiter veröffentlicht werden, sollten der Vergangenheit angehören. „Erfolgslisten" dürfen nur mit dem schriftlichen Einverständnis der Mitarbeiter oder auf der Grundlage von Betriebsvereinbarungen veröffentlicht werden.

6.3.3 Ungebetene Faxwerbung führt zu schlaflosen Nächten

Nicht alle Firmen halten sich an das Verbot ungebetener Faxwerbung. Oft hilft nur, das Faxgerät nachts auszuschalten.

Immer wieder werden Bürger „aus dem Schlaf gerissen", weil ihr Faxgerät nachts anspringt und haufenweise **unerwünschte Werbung** – überwiegend aus dem europäischen Ausland – ausspuckt. Ihre gegenüber den jeweiligen Firmen eingelegten Widersprüche gegen die Nutzung ihrer Faxnummer zu Werbezwecken werden häufig ignoriert. Leider können auch wir nur begrenzt helfen, da die Unternehmen zumeist ihren Sitz außerhalb Schleswig-Holsteins haben. Soweit

sich aus den jeweiligen Werbefaxen überhaupt eine Adresse der werbenden Firma ergibt, können wir die Eingabe lediglich an die jeweils zuständigen Datenschutzkontrollbehörden weiterleiten.

Hierbei werden die Grenzen des länderspezifischen Datenschutzes sichtbar. Leider haben noch immer nicht alle europäischen Staaten Datenschutzkontrollinstitutionen eingerichtet. So können die Betroffenen bei Faxwerbungen aus einigen Staaten nur auf den zivilen Rechtsweg verwiesen werden. Schließlich bleibt manchmal nichts anderes übrig, als sich selbst zu helfen: Künftig wird das Faxgerät abends von „Stand-by“ auf „Aus“ umgeschaltet, um so wenigstens die nächtliche Ruhe zu sichern.

Was ist zu tun?
Bei der Preisgabe seiner Faxnummer sollte jeder Vorsicht walten lassen, um unerwünschte Faxwerbung zu vermeiden.

6.3.4 Anforderungen an betriebliche Datenschutzbeauftragte

Fachkunde und Zuverlässigkeit sind die beiden Schlüsselbegriffe, welche die Eignung eines betrieblichen Datenschutzbeauftragten beschreiben. Daneben spielt die Frage möglicher Interessenkollisionen eine wichtige Rolle.

Wir wurden gefragt, ob der Arbeitnehmervertreter im Aufsichtsrat einer GmbH zugleich betrieblicher Datenschutzbeauftragter sein könne. Es ist rechtlich unbestritten, dass nur diejenigen Mitarbeiter zum betrieblichen Datenschutzbeauftragten bestellt werden dürfen, die in dieser Funktion nicht in **Interessenkonflikte** mit ihren übrigen Aufgaben geraten würden, die über das unvermeidliche Maß hinausgehen. Die Praxis zeigt aber, dass immer wieder Personen berufen werden, bei denen solche Konflikte vorprogrammiert sind. Häufig handelt es sich dabei um Leiter der EDV und der Personalabteilung. Probleme kann es z. B. auch geben, wenn der Datenschutzbeauftragte zugleich die Funktion des Arbeitnehmervertreters im **Aufsichtsrat** des Unternehmens hat.

Im Wortlaut:
§ 77 Abs. 1 Betriebsverfassungsgesetz 1952

Bei Gesellschaften mit beschränkter Haftung ... mit mehr als fünfhundert Arbeitnehmern ist ein Aufsichtsrat zu bilden. Seine Zusammensetzung sowie seine Rechte und Pflichten bestimmen sich nach ... §§ 95 bis 114, ... § 171 ... des Aktiengesetzes ...

§ 111 Abs. 1 Aktiengesetz

Der Aufsichtsrat hat die Geschäftsführung zu überwachen.

§ 171 Abs. 1 Satz 1 Aktiengesetz

Der Aufsichtsrat hat den Jahresabschluss, den Lagebericht und den Vorschlag für die Verwendung des Bilanzgewinns zu prüfen ...

Der Aufsichtsrat einer GmbH nimmt nicht Aufgaben der Geschäftsführung wahr, sondern ist ein Kontrollorgan: Seine Rolle besteht vor allem in der Überwachung der Geschäftsführung. Des Weiteren hat der Aufsichtsrat zwar auch

Zustimmungsrechte bezüglich wichtiger Unternehmensentscheidungen, anders als bei einer Aktiengesellschaft kann jedoch seine Entscheidung jederzeit durch einen anders lautenden Beschluss der Gesellschafterversammlung überspielt werden. Arbeitnehmervertreter erfüllen die Funktion, die Tätigkeit des Aufsichtsrates im Ganzen im Sinne der Arbeitnehmerinteressen zu beeinflussen. Derartige Interessenkonflikte sind somit geradezu gesetzlich vorprogrammiert.

Konflikte sind bezüglich der Tätigkeit als betrieblicher Datenschutzbeauftragter bei der GmbH dagegen eher selten und beschränken sich im Wesentlichen auf die datenschutzrechtliche Kontrolle der Arbeitnehmervertreter im Aufsichtsrat. Da in dem betroffenen Unternehmen solche problematischen Fragen nicht ersichtlich waren, konnte der betriebliche Datenschutzbeauftragte einstweilen im Amt belassen werden.

Was ist zu tun?
Bei der Bestellung eines betrieblichen Datenschutzbeauftragten ist darauf zu achten, dass er nicht unauflöslichen Interessenkonflikten ausgesetzt wird. Dies ist bei einem Arbeitnehmervertreter in einem GmbH-Aufsichtsrat nicht zwangsläufig der Fall.

6.3.5 Diskretion am EC-Automaten

Immer mehr Banken und Sparkassen gehen dazu über, die Kunden weg vom personalintensiven Beratungstresen hin zu automatisierten Selbstbedienungsterminals zu locken. Dabei bleiben Diskretion und Datenschutz leicht auf der Strecke.

Wer lässt sich beim Eingeben einer Banküberweisung schon gerne über die Schulter schauen? Jedenfalls nicht die Bankkunden, die sich bei uns über die mangelhafte Einhaltung der **Diskretion** an den Selbstbedienungsterminals diverser Banken und Sparkassen beschwerten. Unsere Überprüfungen bei Kreditinstituten ergaben, dass zwar die neue Generation von Terminals datenschutzrechtlich nicht zu beanstanden ist. Diese Geräte verfügen nämlich über so genannte „**Sichtschutzfilter**“, die eine Einsichtnahme nur dann zulassen, wenn der Kunde unmittelbar vor dem Bildschirm bzw. dem Display steht. Bereits in einiger Entfernung oder bei seitlichem Blickwinkel sind keine Einzelheiten mehr zu erkennen.

Aber es gibt noch Kreditinstitute, die **ältere Terminals** ohne Sichtschutzfilter verwenden. Zumindest in diesen Fällen sollte die Situation bis zum Austausch der Geräte durch zusätzliche Maßnahmen verbessert werden. Hier kommen beispielsweise die Anbringung geeigneter Hinweisschilder („Achtung: Bitte Diskretionsabstand einhalten!“), Diskretionslinien oder das Aufstellen von Absperrbändern in Betracht. Kleine Räume, die den erforderlichen Abstand nicht zulassen, sind für die Aufstellung der Automaten überhaupt nicht geeignet. Wir haben die betroffenen Kreditinstitute zu entsprechenden Maßnahmen aufgefordert und werden die Praxis weiter beobachten.

Was ist zu tun?
Die Kreditinstitute sollten bei der Installation neuer Eingabeterminals darauf achten, dass ausschließlich solche Geräte angeschafft werden, die den Anforderungen der Kunden an Diskretion und Datenschutz gerecht werden.

6.3.6 Unzulässige Aufbewahrung von Schuldnerlisten

Schuldnerlisten, die von den Amtsgerichten an private Unternehmen herausgegeben worden sind, werden nicht immer zeitgerecht gelöscht. Für die Betroffenen kann dies unangenehme Folgen haben.

Die Vergangenheit holte einen Kunden ein, der bei seiner Sparkasse ein Darlehen aufnehmen wollte. Statt mit dem begehrten Geldsegen beglückt zu werden, sah er sich mit einer **eidesstattlichen Versicherung** konfrontiert, die er eineinhalb Jahre zuvor abgegeben hatte.

Es stellte sich heraus, dass der Sachbearbeiter der Sparkasse diese Tatsache aus dem monatlich erscheinenden listenmäßigen Abdruck eines **amtsgerichtlichen Schuldnerverzeichnisses**, der über ein Jahr alt war, entnommen hatte. In solchen Verzeichnissen führen die Amtsgerichte diejenigen Personen auf, die eine eidesstattliche Versicherung abgegeben haben oder gegen die ein Schuldhaftbefehl verhängt worden ist. Die seiner eidesstattlichen Erklärung zugrunde liegende Forderung hatte der Petent längst beglichen, die eidesstattliche Versicherung selbst war bei dem zuständigen Amtsgericht schon lange gelöscht. Die Sparkasse wäre nach der Zivilprozessordnung verpflichtet gewesen, mit der Mitteilung über die Löschung aus dem Schuldnerverzeichnis den Namen des Petenten unverzüglich zu löschen.

Was ist zu tun?
Listen über Eintragungen im Schuldnerverzeichnis müssen regelmäßig und zuverlässig aktualisiert werden.

6.4 Das Informationssystem der Kreditwirtschaft „SCHUFA“

Die SCHUFA entwickelt sich von einer Clearingstelle, die objektiv richtige Informationen weitergibt, zu einem Unternehmen, das auch „Schätzwerte“ verkauft.

Das **Scoring-Verfahren** der SCHUFA war Gegenstand einer Vielzahl von Anfragen. Das Kredit-Scoring greift auf Krediterfahrungen aus der Vergangenheit zurück, um die Chancen eines ordnungsgemäßen Vertragsablaufes für den Antragsteller eines Kredits zu prognostizieren. Es basiert auf einem angeblich „objektiv mathematisch-statistischen“ Verfahren, in dem bestimmte statistische Angaben mit Krediterfahrungen verknüpft werden. Je nach Grad der positiven Erfahrungen erhält die betreffende Person einen Wert zugeordnet. Je höher dieser „Score-Wert“

liegt, umso höher soll die statistische Wahrscheinlichkeit liegen, dass der Antragsteller seinen Kreditvertrag ordnungsgemäß erfüllt.

Die SCHUFA bestreitet vehement, dass der Scorewert personenbezogene Daten enthält. Nach ihrer Auffassung ist das Scoring ein Wahrscheinlichkeitswert, der eine objektive statistische Aussage beinhaltet. Über den Scorewert werde deshalb keine Auskunft an den Betroffenen erteilt. Diese Auffassung vernachlässigt, dass der Scorewert zwar mit einer statistischen Methode ermittelt, zugleich aber auch einer konkreten Person zugeordnet wird. Er enthält ein **Wahrscheinlichkeitsurteil** darüber, wie kreditwürdig eine **bestimmte Person** ist, und stellt damit ein personenbezogenes Datum dar.

Personenbezogene Daten dürfen nur zu einem Scorewert verarbeitet werden, wenn der Kunde zuvor wirksam in die Übermittlung an die SCHUFA eingewilligt hat oder es sich um so genannte Negativdaten (z. B. Abgabe einer eidesstattlichen Versicherung) handelt. Die Weitergabe eines Scorewertes an die Vertragspartner der SCHUFA ist eine geschäftsmäßige Datenübermittlung. Eine solche Weitergabe von personenbezogenen Daten ist nur zulässig, wenn der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und kein Grund zu der Annahme besteht, dass der Betroffene ein **schutzwürdiges Interesse** an dem Ausschluss der Übermittlung hat. Die betroffenen Kunden haben ein schutzwürdiges Interesse, das der Übermittlung des Scorewertes an die SCHUFA-Vertragspartner entgegenstehen kann, denn es wird aus einer Summe von statistischen Daten die personenbezogene Information abgeleitet: „Der Kunde erfüllt seinen Kredit mit überwiegender Wahrscheinlichkeit nicht." Diese Aussage mag in vielen Fällen zutreffen, in vielen anderen Fällen ist sie aber falsch, weil sie eben nur eine nicht überprüfbare statistische Wahrscheinlichkeit widerspiegelt. Die Übermittlung eines Scorewertes kann außerordentlich beeinträchtigend für die betroffenen Kunden sein, weil Kreditinstitute sich bei der Kreditvergabe in der Praxis am Scorewert orientieren. Nach unserer Auffassung hat der Kunde außerdem einen Anspruch auf Auskunft über seinen Scorewert.

Was ist zu tun?
Das Scoring ist unseres Erachtens rechtswidrig, sofern der Betroffene zuvor nicht eingewilligt hat. Für eine wirksame Einwilligung ist es erforderlich, dass der Betroffene die Tragweite seiner Entscheidung überblicken kann. Das ist bei der aktuellen SCHUFA-Klausel nicht gegeben, weil sie die Kriterien nicht offen legt, nach denen der Scorewert ermittelt wird.

6.4.1 Die Folgen alter SCHUFA-Auskünfte

Überholte SCHUFA-Auskünfte können große wirtschaftliche Schäden anrichten.

Was ist davon zu halten, wenn eine Bank trotz der Bestätigung der SCHUFA, ein bestimmtes Negativmerkmal gelöscht zu haben, kein Girokonto eröffnen will? Der Informationsfluss von der SCHUFA zu ihren Vertragspartnern funktioniert

offensichtlich nicht immer reibungslos. Einem Architekten wurde immer wieder die Neueröffnung eines **Girokontos** mit dem Hinweis auf eine schlechte SCHUFA-Auskunft **verweigert**. Dabei hatte ihm die SCHUFA doch schriftlich bestätigt, ein bestimmtes Negativmerkmal gesperrt und später sogar gelöscht zu haben. Im vorliegenden Fall handelte es sich um einen dubiosen Mahnbescheid, dessen Existenz der angebliche Gläubiger nicht nachweisen konnte. Sogar eine Personenverwechslung war nicht auszuschließen. Der Architekt vermutete daraufhin, dass die SCHUFA zwei unterschiedliche Datenbestände bereithalte, einen „**guten**" für die Selbstauskünfte an die Betroffenen und einen „**schlechten**" für die Vertragspartner.

Unsere Nachforschungen konnten diese Vermutung nicht bestätigen. Bei der SCHUFA gibt es **nur einen** zentralen Datenbestand, in welchem der Hinweis auf einen Mahnbescheid auch tatsächlich gelöscht war. Der Fehler lag jedoch aufseiten der Bank. Deren Mitarbeiterin hatte, statt eine aktuelle SCHUFA-Auskunft einzuholen, auf einen **veralteten** hausinternen **Datenbestand** der Bank zugegriffen, der die Information über den bestrittenen Mahnbescheid noch enthielt. Hätte sie, wie es die vertraglichen Regeln der SCHUFA vorsehen, eine neue SCHUFA-Anfrage gestartet, wäre das Problem gar nicht erst entstanden.

Nachdem die Mitarbeiterin auf ihren Fehler hingewiesen worden war und eine neue SCHUFA-Anfrage die Löschung des dubiosen Mahnbescheides sofort bestätigt hatte, stand der Eröffnung des Girokontos nichts mehr im Wege.

Was ist zu tun?
Die SCHUFA sollte ihre Vertragspartner durch geeignete Schulungsmaßnahmen darauf hinweisen, dass vor Kreditentscheidungen stets aktuelle SCHUFA-Auskünfte einzuholen sind.

6.4.2 Kleine Ursache – große Wirkung!

Peanuts dürfen die Kreditwürdigkeit nicht beeinträchtigen. Für die Speicherung von Negativmerkmalen müssen Geringfügigkeitsgrenzen eingeführt werden.

Der Kreditantrag einer Bankkundin wurde bei mehreren Banken immer wieder unter Hinweis auf eine negative SCHUFA-Auskunft abgelehnt, obwohl die betreffende Forderung längst bezahlt war. Die Betroffene hatte die Monatsrechnung eines Mobilfunkbetreibers **in Höhe von ca. 200 DM** erst mit Verspätung bezahlt. Vorher sollte nämlich erst einmal familienintern geklärt werden, wer überhaupt mit Mutters Handy so viel telefoniert hatte. Inzwischen hatte der Netzbetreiber das Vertragsverhältnis gekündigt und diese Tatsache der SCHUFA mitgeteilt. Auch die später erfolgte Bezahlung wurde bei der SCHUFA per so genanntem Erledigungsvermerk erfasst. Nach den SCHUFA-Regelungen bleibt ein solcher Datensatz aber für drei Jahre gespeichert. So hatte die verspätete Zahlung eines geringen Betrages für die Dauer von drei Jahren den Verlust der Kreditwürdigkeit dieser Person zur Folge.

Dieser Fall wirft die Frage auf, ob es hinnehmbar ist, dass derartige Peanuts über den Umweg der SCHUFA den Verlust der Kreditwürdigkeit eines Menschen für drei Jahre zur Konsequenz haben dürfen. Insofern bedarf das Verfahren einer Korrektur, z. B. durch frühzeitige **Löschung von Kleinbeträgen**.

Was ist zu tun?
Die SCHUFA muss angehalten werden, für die Speicherung von Negativdaten Geringfügigkeitsgrenzen einzuführen.

6.5 Videokameras an der Arbeitsstelle und auf dem Marktplatz

Videokameras, z. B. am Arbeitsplatz und auf öffentlichen Plätzen, kommen immer mehr in Mode. Obwohl das Bundesdatenschutzgesetz noch keine einschlägigen Regelungen enthält, sind gleichwohl rechtliche Grenzen zu beachten.

Die Videoüberwachung durch öffentliche Stellen ist bereits seit geraumer Zeit Gegenstand datenschutzrechtlicher Diskussionen (vgl. 22. TB, Tz. 4.2.3) und gesetzgeberischer Maßnahmen. Aber auch im nichtöffentlichen Bereich ist der Einsatz von Überwachungskameras zu unterschiedlichen Zwecken längst in Mode, häufig ohne dass sich die Betreiber der rechtlichen Auswirkungen ihres Tuns bewusst sind.

Immer wieder werden Anfragen zu den Voraussetzungen für die Einrichtung von Videoüberwachungsanlagen am **Arbeitsplatz** gestellt. Installiert der Arbeitgeber eine Videoüberwachungskamera, löst bereits deren abstrakte Eignung zur Kontrolle des Arbeitnehmerverhaltens ein Mitbestimmungsrecht des Betriebsrates aus. Eine solche Überwachung steht daneben unter dem strikten Vorbehalt der Verhältnismäßigkeit. Sie ist nach der Rechtsprechung nur in Ausnahmefällen zulässig, etwa um vom Arbeitgeber oder den Arbeitnehmern erhebliche Schäden abzuwenden.

Bei der Einrichtung von **Webcams** auf öffentlichen Plätzen kommt es auf die Umstände des Einzelfalles an. Ein Petent hatte auf dem Alten Lübecker Markt eine Kamera entdeckt und sich an uns gewandt. Es stellte sich heraus, dass eine Firma zu Werbezwecken jede volle Stunde zwei Bilder des Marktplatzes und des Bahnhofes im Internet veröffentlichte. Personen waren auf den Bildern nicht zu individualisieren. Eine Vergrößerung der Bilder führte zu einer Verzerrung der Gesichtszüge, sodass auch in diesem Fall kein Personenbezug herstellbar war.

www.datenschutzzentrum.de/material/themen/video/

Was ist zu tun?
Der Bundesgesetzgeber muss endlich Rechtsklarheit schaffen und den Einsatz von Videokameras im nichtöffentlichen Bereich in einer Weise regeln, die dem Persönlichkeitsrecht entspricht.

6.6 Der Bankkunde als König ohne Kleider

Ein übersteigertes Sicherheitsbedürfnis und bürokratisches Denken verleitet manche Banken dazu, von ihren Kunden einen regelmäßigen „Vermögensstriptease“ zu verlangen.

Kein märchenhaftes Vergnügen bereitete einem Petenten das Verhalten seiner Bank: Er hatte einen Kredit aufgenommen, um sein Eigenheim zu finanzieren. Wie üblich hatte er dabei seine Vermögens- und Einkommensverhältnisse offen legen müssen, darüber hinaus war das Darlehen dinglich durch eine Hypothek solide abgesichert. Nach dem Vertragsabschluss hatte er es über fünf Jahre lang ordnungsgemäß bedient. Dann flatterte ihm plötzlich die Aufforderung seiner Bank auf den Schreibtisch, er möge doch für die letzten Jahre eine **detaillierte Vermögensaufstellung** inklusive **Einkommensteuerbescheid** und Einkommensteuererklärung mit Anlagen nachreichen. Auf unsere Initiative hin teilte die Bank zunächst mit, diese Informationen seien erforderlich, weil das Kreditwesengesetz dies verlange.

Eine solche Aufforderung zum „**Vermögensstriptease**“ ist jedoch in keiner Weise gerechtfertigt: Denn das Kreditwesengesetz sieht eine laufende Offenlegung der wirtschaftlichen Verhältnisse nicht einmal dann zwingend vor, wenn ein Darlehensnehmer Kredite von insgesamt über 500.000 DM in Anspruch nimmt. Unterhalb dieser Grenze kann die Bank solche Informationen nur im Rahmen der Grundsätze ordnungsgemäßer Geschäftsführung verlangen. Für den Eigenheimbauer, dessen Kredit hinreichend durch Hypothek oder Grundschuld abgesichert ist und der seinen Kredit unter 500.000 DM vertragsgemäß bedient, genügt in der Regel eine so genannte Erst-Offenlegung bei Vertragsabschluss. Erst nach einigem Hin und Her konnten wir die Bank schließlich überzeugen, ihrem König Kunde die Kleider zu belassen.

Was ist zu tun?
Banken dürfen sich die Vermögensverhältnisse ihrer Kunden grundsätzlich nur bei Vorliegen eines berechtigten Interesses offen legen lassen. Hinreichend abgesicherte Kredite unterhalb eines Gesamtbetrages von 500.000 DM dürfen nicht zu regelmäßigen Vermögenskontrollen führen.

6.7 Ergebnisse von Kontrollen

Überprüfungen von Amts wegen bei Unternehmen, die Datenverarbeitung als Dienstleistung betreiben (Servicerechenzentren, Datenerfassungsbüros, Büroservicefirmen, Akten- und Datenträgervernichtungsbetriebe und sonstige Auftragsdatenverarbeiter), führen in vielen Fällen zu Beanstandungen und stets auch zu Empfehlungen und Verbesserungsvorschlägen.

Folgende **Mängel** wurden bei den Prüfungen am häufigsten festgestellt:

- Nicht oder nur unzureichend durchgeführte Verpflichtungen der Mitarbeiter auf das **Datengeheimnis**.
- Unzulängliche **technische** und **organisatorische Sicherungsmaßnahmen**.

  Bei einer Behindertenwerkstatt z. B. war der EDV-Raum, in dem eine Datenarchivierung für Dritte durchgeführt wurde, scheinbar hervorragend abgeschottet. Tatsächlich verfügte die Hauptzugangstür über eine Sicherung mit elektronischer Schließanlage und Zahlencode. Der Zahlencode war nur den direkt zuständigen Mitarbeitern bekannt. Der EDV-Raum hatte jedoch noch eine **Hintertür** zum unmittelbar daneben liegenden und frei zugänglichen Besprechungszimmer. Diese Hintertür war unverschlossen. Jeder Werkstattangehörige konnte unbemerkt in den EDV-Raum gelangen. Die Reaktion der Werkstatt: „Daran haben wir gar nicht gedacht!“

  Im Rechenzentrum eines bundesweit tätigen Einrichtungshauses hatten Mitarbeiter der Personalabteilung freien Zutritt zum zentralen **Serverraum** in der **EDV-Abteilung**. Begründung des Unternehmens: Dort stehe ein Drucker, und die Personalsachbearbeiter müssten sich ihren Output zeitnah abholen können. Auf die Idee, den Drucker außerhalb des Serverraums aufzustellen und die Zahl der zugangsberechtigten Mitarbeiter auf das unbedingt erforderliche Minimum zu reduzieren, war die Firma bis zum Besuch der Aufsichtsbehörde von sich aus nicht gekommen.
- Fehlende oder unzulängliche schriftliche Verträge zur **Auftragsdatenverarbeitung.**

  In diesem Punkt haben die in den Unternehmen geführten Kontrollbesuche sehr starken Beratungscharakter und finden nicht selten auf ausdrücklichen Wunsch der Firmen statt.

- Fehlende oder verspätete Meldungen zum **Datenschutzregister.**
- Fehlende **betriebliche Datenschutzbeauftragte**; nicht ausreichende Qualifikation der betrieblichen Datenschutzbeauftragten.

Was ist zu tun?
Nachkontrollen werden zeigen, ob die Mängel behoben worden sind.

7 Systemdatenschutz

7.1 Sicherheits- und Ordnungsmäßigkeitsregelungen im neuen Datenschutzrecht

Die über 20 Jahre alten Datensicherheitsvorschriften sind durch die Neuregelungen im LDSG 2000 und in der Datenschutzverordnung (DSVO) „ad acta" gelegt worden. Das neue Datensicherheitsrecht schafft für die Daten verarbeitenden Stellen konkretere und der aktuellen technischen Situation angepasste Rahmenbedingungen. Das Echo der Datenverarbeiter hierauf ist durchweg positiv.

Die Bestimmungen zu den „technischen und organisatorischen Maßnahmen" des bis 2000 geltenden Landesdatenschutzgesetzes sind in ihrer Grundstruktur bereits Anfang der 70er-Jahre entwickelt worden. Die damaligen Überlegungen wurden als die „**10 Gebote zur Datensicherheit**" erstmals im Bundesdatenschutzgesetz von 1977 als Rechtsnormen formuliert und sind 1978 nahezu unverändert in das schleswig-holsteinische Datenschutzrecht übernommen worden. Sie reflektierten die Sicherheitsprobleme bei der automatisierten Datenverarbeitung in zentralisierten Großrechenzentren und waren recht abstrakt formuliert. Zudem gab es zwischen den einzelnen „Sicherheitsgeboten" Abgrenzungs- und Überschneidungsprobleme, sodass ihre Zielrichtung vielfach nur durch umfangreiche Kommentierungen und anhand von Beispielen deutlich gemacht werden konnte. Dabei zeigte sich zunehmend das Problem, dass die heutigen informationstechnischen Systeme und automatisierten Verfahrensabläufe ganz andere Sicherheitsanforderungen stellen als die vor 30 Jahren.

Eine Reorganisation des Datensicherheitsrechts war mithin seit langem überfällig und ist in den §§ 5 bis 7 LDSG 2000 und den §§ 3 bis 8 der DSVO vollzogen worden. Aus diesen neuen Regelungen zum **Systemdatenschutz** lassen sich die folgenden konkreten Grundforderungen ableiten:

- Für jedes automatisierte Verfahren sind seine **Zweckbestimmung** und die **Rechtsgrundlagen** für Datenverarbeitung festzulegen, damit zweckwidrige und rechtlich bedenkliche Nutzungen erkennbar werden.
- In **Sicherheitskonzepten** ist unter Berücksichtigung der tatsächlichen personellen und organisatorischen Gegebenheiten für jedes Verfahren zu beschreiben, wie Unbefugten der Zugang zu Datenträgern, auf denen personenbezogene Daten gespeichert sind, verwehrt werden soll, wie verhindert werden soll, dass personenbezogene Daten unbefugt verarbeitet oder Unbefugten zur Kenntnis gelangen können, und wie gewährleistet wird, dass die Daten verarbeitenden Personen, der Zeitpunkt und der Umfang der Datenverarbeitung festgestellt werden können.
- Die Nutzung von informationstechnischen Systemen darf erst ermöglicht werden, nachdem die betreffenden Benutzer ihre Berechtigung hierzu nachgewiesen haben (in der Regel erfolgt die Authentifizierung durch ein **Passwort**).

- Das Recht, Veränderungen auf der Betriebssystemebene der informationstechnischen Systeme vorzunehmen (**Systemadministration**), darf nur wenigen Personen eingeräumt werden. Ihre Aktivitäten sind zu protokollieren und zu kontrollieren.
- Datenbestände, die auf Datenträgern von informationstechnischen Systemen gespeichert sind, die außerhalb des gesicherten Bereiches einer Daten verarbeitenden Stelle, z. B. im Rahmen von Telearbeit oder beim Außendienst, eingesetzt werden, müssen **verschlüsselt** werden (Schadensbegrenzung bei Diebstahl).
- Werden Datenbestände ausschließlich in automatisierten Dateien gespeichert, so sind die Bestandsveränderungen und die veranlassenden Personen/Stellen (in Ermangelung papierener Unterlagen) in den Dateien selbst umfassend zu **protokollieren**.
- Die in einer Daten verarbeitenden Stelle eingesetzten automatisierten Verfahren sowie die Hard- und Softwarekomponenten sind in **Verfahrens**-, **Geräte**- und **Softwareverzeichnissen** zu registrieren, damit „illegale" Komponenten erkannt werden können (was nicht registriert ist, muss deaktiviert werden).
- Es ist zu **protokollieren**, welchen Personen von wann bis wann welche **Nutzungsrechte** an welchen Hard- und Softwarekomponenten tatsächlich gewährt worden sind, um einen nachträglichen Abgleich mit den entsprechenden Vorgaben der Verantwortlichen zu ermöglichen.
- Die automatisierten Verfahren sind vor ihrem „Echteinsatz" zu testen und von der Leitung der Daten verarbeitenden Stelle zum Einsatz **freizugeben**. Um dies zu ermöglichen, sind sie so zu dokumentieren, dass ihre Funktionsweise für sachkundige Personen in angemessener Zeit nachvollziehbar ist.
- Während des „Echteinsatzes" der automatisierten Verfahren ist laufend zu **überwachen**, ob die mit der Freigabe verbundenen Weisungen der Leitung der Daten verarbeitenden Stelle zur ordnungsgemäßen Anwendung der Verfahren eingehalten werden; unzulässige Abweichungen sind zu korrigieren.

Interessant waren die **Reaktionen der Datenverarbeiter** im Lande (Softwareentwickler, Administratoren, EDV-Leiter, Benutzer von IT-Systemen) nach dem In-Kraft-Treten der einschlägigen Regelungen. Die überwiegend positiven Beurteilungen gipfelten in der Aussage: „Endlich hat auch der Gesetzgeber erkannt, wodurch Datensicherheit tatsächlich erreicht werden kann." Geäußert wurden allerdings auch völlig ablehnende Auffassungen.

Die Gründe für derartig divergierende Ansichten sind in folgendem Phänomen zu finden: Soweit die öffentliche Verwaltung ihre Datenbestände in Papierform (also in Akten) führt, wird es als eine Selbstverständlichkeit betrachtet, dass alles, was zu einem „Fall" vorliegt, in die betreffende Akte gehört, dass es keine „privaten" Zweit- und Drittakten geben darf und dass nur die jeweils Zuständigen die Akten führen dürfen. Diese althergebrachten Grundsätze werden auch eingehalten, wenn ganze Akteninhalte oder Teilmengen in Datenbanken übertragen werden, um die Verarbeitungsprozesse zu beschleunigen. Man weiß genau, wo die Daten gespeichert sind und wer den Zugriff auf sie hat. Eine völlig neue Situation entsteht,

wenn man den Mitarbeiterinnen und Mitarbeitern an ihren computergestützten Arbeitsplätzen **Softwarewerkzeuge** an die Hand gibt, mit denen sie große Datenbestände kopieren, zusammenführen, selektieren, umspeichern, auf andere Systeme übertragen, Zugriffsberechtigungen verändern oder gar ganze Datenbanken neu anlegen können. Derartige Aktionen kosten weder viel Zeit noch erzeugen sie Kosten. Werden die von den technischen Systemen (Client-Server-Systeme, Netzwerke, mobile Systeme) und den Softwarepaketen (Bürokommunikationssysteme, Datenbankgeneratoren, Falltransfer- und Mail-Systeme) angebotenen Optionen nicht durch technische und organisatorische Maßnahmen kanalisiert, entsteht – wie wir bei vielen unserer Prüfungen feststellen mussten – nach kurzer Zeit ein Wildwuchs an Datenbeständen, der sich jedem Sicherheitskonzept und jeder Kontrolle entzieht (vgl. 21. TB, Tz. 4.1.2, Tz. 6.7.1; 22. TB, Tz. 4.12; Tz. 7.5 dieses Berichtes).

> ***Im Wortlaut: § 44 LDSG***
>
> *Ordnungswidrig handelt, wer entgegen den Vorschriften dieses Gesetzes personenbezogene Daten, die nicht offenkundig sind, erhebt, speichert, zweckwidrig verarbeitet, verändert, übermittelt, zum Abruf bereit hält oder löscht ...*
>
> *Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 50.000 Euro geahndet werden.*

Die neuen Regelungen im LDSG 2000 und in der Datenschutzverordnung fangen zum Vergnügen der meisten **IT-Verantwortlichen** die „vergessenen", „vagabundierenden" und „privat-dienstlichen" Datenbestände und Rechnersysteme wieder ein und unterwerfen sie dem gleichen Sicherheitsreglement, das für alle Akten und die „offiziellen" Dateien gilt. Mancher PC-Freak in der Verwaltung, dem dies nicht passt, übersieht, dass die Verarbeitung von personenbezogenen Daten von Bürgerinnen und Bürgern, aber auch von Personalaktendaten der eigenen Kollegen bereits aus Rechtsgründen nicht der Dispositionsfreiheit einzelner Mitarbeiter unterliegt, sondern dass für den Umgang mit ihnen die Behörde die Verantwortung trägt. Wenn eine Mitarbeiterin oder ein Mitarbeiter einer Behörde ohne eine Freigabe durch eine hierzu befugte Person personenbezogene Datenbestände anlegt, begeht sie oder er unter Umständen eine Ordnungswidrigkeit im Sinne des LDSG. Sollte das den Kritikern der neuen Sicherheitsregelungen noch nicht aufgefallen sein?

Was ist zu tun?
Die Verantwortlichen in den Behörden sollten die neuen Bestimmungen über die Datensicherheit und Ordnungsmäßigkeit der Datenverarbeitung auch als einen Leitfaden zur Rückgewinnung ihrer Datenherrschaft erkennen. Wer nicht einmal weiß, wo welche personenbezogenen Daten in „seiner" Behörde zu welchen Zwecken gespeichert werden, wird schwerlich in der Lage sein, rechtlich fragwürdige Verfahrensweisen oder Sicherheitslücken zu entdecken und abzustellen.

7.2 Outsourcing der Systemadministration

Einige Dienstleistungsunternehmen suggerieren ihren Kunden, sie könnten die Kosten für die Ausbildung und die Tätigkeit eigener Systemadministratoren sparen, wenn sie diese Arbeiten outsourcen. Sie verschweigen, dass damit die Fremdadministration unkontrollierbar wird und dass die Behörden mangels eigenen Wissens auf Dauer jedwede Entscheidungskompetenz auf dem Gebiet der Informationstechnik verlieren.

Die Kosten für die Einrichtung und den laufenden Betrieb von computergestützten Arbeitsplätzen sind nach wie vor sehr hoch. Der Löwenanteil entfällt dabei auf die **Personalkosten** für die Administration der Hardware, der Software und der Datenbestände, für die Schulung und Betreuung der Benutzer sowie für das Trouble-Management bei fehlerhaften Nutzungen oder Ausfällen der technischen Systeme.

Zwei neue Begriffe haben deshalb im letzten Jahr in der IT-Szene für Aufsehen und Euphorie gesorgt. Sie lauten „**Terminal-Server-Systeme**“ und „**Application-Service-Providing**“. Die Begeisterung für die diesen Begriffen zugrunde liegenden Konzepte resultiert aus folgenden Überlegungen: Wenn die Kosten für die Ausbildung und die laufende Bezahlung von Systemadministratoren so hoch sind und wenn ein unverhoffter Weggang dieser besonders qualifizierten Mitarbeiter die betreffenden Behörden in größte Nöte stürzt, warum versucht man nicht, dieses Wissen und die Arbeitskraft bei externen Dienstleistern einzukaufen? Den ersten Schritt in diese Richtung ging man folgerichtig bereits vor einigen Jahren mit der so genannten **Fernadministration** (vgl. 20. TB, Tz. 6.7.5; 22. TB, Tz. 6.2 und 6.3). Die eigenen Administratoren müssen bei dieser Verfahrensweise nur über Grundfähigkeiten verfügen. Reichen ihre Kenntnisse für die Durchführung bestimmter Konfigurationsmaßnahmen bzw. für Fehlerbereinigungen nicht aus, wird der externe Dienstleister auf das System „aufgeschaltet“ und führt die Arbeiten unter Aufsicht durch. Anschließend wird die Verbindung wieder gekappt. Diese Methode hat aber den Nachteil, dass die Experten meistens erst dann mit ihrer segensreichen Tätigkeit beginnen, wenn „das Kind bereits in den Brunnen gefallen ist“. Ein solches „Trouble-Shooting“ ist natürlich aufwändiger, als wenn die Fehler gar nicht erst gemacht worden wären.

Deshalb verfolgt man mit den **Terminal-Server-Systemen** und dem **Application-Service-Providing** das Ziel, die Rechnersysteme in den Daten verarbeitenden Stellen nur mit einfach strukturierten Betriebssystemen auszurüsten und alle wesentlichen Teile der Software sowie alle Datenbestände auf zentralen Servern (möglichst noch in den Räumlichkeiten des Dienstleisters) zu platzieren. Dort findet dann die gesamte Administration statt, die Programme und Daten kommen aus dem Netz. Die Rechner der Behörde müssen faktisch nicht mehr administriert werden, denn wenn sie nicht funktionieren, werden sie ausgetauscht. Die Leistungsentgelte für diesen Service sind so kalkuliert, dass sie unter den Personalkosten eigener Systemadministratoren liegen.

Ist damit das Problem der Ausbildung und Bezahlung eigener Systemadministratoren gelöst und trotzdem die **Sicherheit und Ordnungsmäßigkeit** der Datenverarbeitung auf Dauer gewährleistet? Keineswegs, da ein totales Outsourcing der Systemadministration dazu führt, dass der sicherheitskritischste Bereich der automatisierten Datenverarbeitung von der Daten verarbeitenden Stelle nicht mehr überwacht werden kann (vgl. Tz. 7.4).

Die modernen informationstechnischen Systeme sind nämlich schon lange mehr als nur schnelle Schreib- und Rechenmaschinen, in die man Daten hineinwirft und die Ergebnisse (Ausdrucke) in die Verwaltungsverfahren übernimmt, wenn sie für richtig befunden worden sind. Heute werden informationstechnische Systeme als **Organisations-** und **Steuerungsinstrumente** eingesetzt, deren entscheidende Elemente die Benutzer- und Zugriffsverwaltung, das Softwareversionsmanagement, die Arbeitsprozesssteuerung sowie das Datenmanagement sind. Dabei geht es um die Entscheidung, wer z. B. auf Textdokumente mit ärztlichen Gutachten aus dem Bereich eines Gesundheitsamtes oder auf Personaldaten zugreifen darf, wie mit E-Mail-Attachments verfahren wird, wer überwacht, dass nur vorübergehend erforderliche Datenbestände auch tatsächlich zeitnah gelöscht werden und nicht ein Eigenleben entfalten, wer den termingerechten Einsatz neuer Softwareversionen steuert, wer überprüft, dass rechtlich erforderliche Zugriffsrestriktionen auch tatsächlich technisch umgesetzt worden sind usw.

Wenn die hierfür erforderlichen Revisionskriterien bzw. Sicherheitsmaßnahmen ausschließlich von den externen Dienstleistern gemanagt werden und die Daten verarbeitenden Stellen keine technischen Möglichkeiten haben, ihnen „in die Karten“ (d. h. nichts anderes als in ihr eigenes System) zu schauen, und wenn ihr eigenes Personal zudem nicht einmal über das Fachwissen verfügt, kritische Fragen zu stellen, dann haben sie faktisch die **Verfügungsgewalt** über ihre

Im Wortlaut:

§ 5 LDSG

... Automatisierte Verfahren sind vor ihrem erstmaligen Einsatz und nach Änderungen durch die Leiterin oder den Leiter der Daten verarbeitenden Stelle oder eine befugte Person freizugeben.

§ 6 LDSG

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

... Die Daten verarbeitenden Stellen haben die ordnungsgemäße Anwendung der automatisierten Verfahren zu überwachen.

§ 17 LDSG

(1) Lässt eine Daten verarbeitende Stelle personenbezogene Daten in ihrem Auftrag verarbeiten, bleibt sie für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich.

(2) Die Daten verarbeitende Stelle hat dafür Sorge zu tragen, dass personenbezogene Daten nur im Rahmen ihrer Weisungen verarbeitet werden.

(3) Bei der Erbringung von Wartungsarbeiten oder von vergleichbaren Unterstützungstätigkeiten bei der Datenverarbeitung durch Stellen oder Personen außerhalb der Daten verarbeitenden Stelle gelten die Abs. 1 bis 3 entsprechend.

automatisierten Verfahren **verloren**. Hinzu kommt, dass in diesen Fällen auch gegen die Bestimmungen des Landesdatenschutzgesetzes zur Auftragsdatenverarbeitung und zu den Sicherheitsmaßnahmen für automatisierte Verfahren verstoßen wird.

Der Traum vieler Behördenleiter von dem Computer, der alles macht und der ohne eigenes Zutun alles „mit Sicherheit“ auch richtig macht, weil man monatlich einen bestimmten Geldbetrag an ein Dienstleistungsunternehmen überweist, wird ein Traum bleiben. Terminal-Server-Systeme und das Application-Service-Providing werden gleichwohl die Datenverarbeitungsmethoden der Zukunft sein. Sie werden, wenn sie durch qualifiziertes Personal auf der Basis von **ausgereiften IT-Konzepten** eingesetzt werden, wesentlich effektivere und sicherere automatisierte Verfahren als bisher ermöglichen. Sie sind aber trotz gegenteiliger Versprechungen einiger Dienstleistungsunternehmen kein Wundermittel, das ein Maximum an Produktivität und Sicherheit bei einem Minimum von Investitionen in Personal und Wissen erzeugt.

Was ist zu tun?
Wer sich dafür entscheidet, auf jegliche eigene Administrationskompetenz zu verzichten und den Zusicherungen externer Dienstleister vertraut, begibt sich in fremde Hände. Verantwortungsbewusste Behördenleitungen sorgen dafür, dass in ihrem Haus zumindest so viel IT-Know-how vorhanden ist, dass die eingesetzten technischen Systeme und automatisierten Verfahren durch sie beherrschbar bleiben und die Arbeit externer Dienstleister überwacht werden kann.

7.3 Datensicherheit beim Betrieb der privatisierten Telekommunikationsrechner des Landes

Das Land hat mehr als 250 Telekommunikationsrechner privatisiert und lässt sie von externen Dienstleistern administrieren. Die dadurch entstehenden Sicherheits- und Revisionsprobleme sind immer noch nicht abschließend analysiert. Das Sprachnetz läuft zurzeit noch ohne ein verbindliches Sicherheitskonzept. Die Teilnehmer sind über die Konsequenzen der Nutzung sicherheitskritischer Leistungsmerkmale nicht informiert.

Der Austausch der alten Telekommunikationsrechner der Behörden im Lande gegen neue Rechner der Telekom und die Übernahme der **Gesamtadministration** aller Rechner durch das Firmenkonsortium Telekom/Siemens im Rahmen des integrierten Sprach- und Datennetzes (vgl. 22. TB, Tz. 6.3) bleibt ein **schwieriges Geschäft**. Nicht dass die neuen Rechner nicht funktionieren und die externen Administratoren nicht kompetent wären, das Telefonieren in der schleswig-holsteinischen Landesverwaltung funktioniert nach wie vor prächtig, und billiger als früher ist es wohl obendrein.

Trotzdem kann noch immer **keine** datenschutzrechtliche und sicherheitstechnische **Entwarnung** gegeben werden. Auf zu viele offene Fragen können das Ministerium für Finanzen und Energie und ihre externen Dienstleister Telekom und Siemens

auch 18 Monate nach dem Start des Echtbetriebes noch keine abschließenden Antworten geben bzw. fertige Lösungen präsentieren. Untätig ist man in der Zwischenzeit nicht gewesen, aber andere Probleme hatten offensichtlich eine höhere Priorität. So liegen zurzeit die „baulichen und technischen Sicherheitsanforderungen an die Betriebsräume und die Kabelnetze“ sowie die „Verfahrensanweisungen für die TK-Anlagenverantwortlichen“ erst als Entwürfe vor. Die darin enthaltenen Regelungen definieren allerdings durchweg einen recht hohen Sicherheitsstandard. Werden diese Konzepte nach der Klärung einiger Detailfragen für verbindlich erklärt und wird ihre Einhaltung konsequent überwacht, dürften die in den Behörden installierten Hardwarekomponenten vor Manipulationen und sonstigen missbräuchlichen Aktivitäten hinreichend geschützt sein.

Die entscheidenden Defizite bestehen nach wie vor darin, dass das Ministerium für Finanzen und Energie die **Administration** der Telekommunikationsrechner **aus der Hand gegeben** hat, bevor in einem nachvollziehbaren Sicherheitskonzept festgelegt war, welche Sicherheitsprozeduren von den externen Dienstleistern Telekom und Siemens erwartet werden und wie man die konkrete Arbeit der Dienstleister zu überwachen gedenkt. Dabei sind zwei Fragenkomplexe von besonderer Bedeutung:

- Wie wird mit den Leistungsmerkmalen umgegangen, die die **Vertraulichkeit der Kommunikation** beeinträchtigen können? Hierzu gehören z. B. „Aufschalten“, „Raumhören“ und „Konferenz“. An welchen Stellen in dem Gesamtsystem entstehen Datenbestände, die das Kommunikationsverhalten der Teilnehmer sichtbar werden lassen? Wer außer den betreffenden Teilnehmern hat Zugriff auf diese Bestände? Wo und wie lange werden z. B. Voicemail- und Faxmail-Inhalte gespeichert? Wer kann sie löschen? Erfolgt eine „rückstandsfreie“ oder nur eine „logische“ Löschung? Können (vorher) Sicherungskopien angefertigt werden? Ähnliche Fragen stellen sich auch in Bezug auf die Anruferlisten und die sonstigen Kommunikationsprotokolle. Umfassende Antworten erwarten insbesondere die Teilnehmer, deren Telekommunikationsverhalten unter bestimmten Konstellationen von „öffentlichem“ Interesse sein könnte.
- Wie will das Ministerium für Finanzen und Energie seine **Betreiberfunktion** wahrnehmen? Es ist zwar avisiert, dass im Gebäude der Telekom eine Revisionsschnittstelle eingerichtet wird, von der aus ein Zugriff auf alle Protokolldaten aller Telekommunikationsrechner möglich sein soll, und es ist auch die personelle Besetzung geregelt. Unklar ist aber nach wie vor, mit welchem Aufwand welche Revisionsfragen mithilfe welcher Softwarekomponenten beantwortet werden können. Konsequent wäre es, den gesamten Protokolldatenbestand nach Data-Warehouse-Prinzipien aufzubereiten, um auch Ad-hoc-Anfragen beantworten zu können. Dabei geht es nicht nur um den Nachweis, dass alle Administrationsaufträge korrekt ausgeführt wurden, sondern auch darum, dass keine Aktivitäten erfolgten, für die kein Auftrag vorlag.

Zurzeit findet eine systematische Kontrolle der Arbeiten der externen Administratoren noch nicht statt. Wie wichtig es ist, dass sich das Ministerium für Finanzen und Energie seiner Betreiberfunktion bewusst ist, zeigte sich bei der Übermittlung der PIN an die einzelnen Teilnehmer. Nicht nur dass wohl nur Insider etwas mit

dem Absender „**Customer-Service-Center Kommunikationsnetz Schleswig-Holstein**“ anfangen konnten. Entgegen allen Sicherheitsregeln war die PIN auf einem Merkblatt abgedruckt, das eine „Zusatzinformation zur Bedienung der Endgeräte“ enthält, eine Unterlage also, die ständig gebraucht wird. Die Aufforderung, die PIN vertraulich zu behandeln, erscheint unter diesen Bedingungen kurios. Alle sicherheitsbewussten Teilnehmer werden sie mühsam geschwärzt haben, um das Merkblatt für den täglichen Gebrauch nutzbar zu machen. Bei den weniger sicherheitsbewussten Teilnehmern liegt die PIN wahrscheinlich entweder unter dem Apparat oder im Fernsprechverzeichnis.

Im Rahmen der parlamentarischen Beratungen des 22. Tätigkeitsberichtes waren die entsprechenden Sicherheitskonzepte für November 2000 angekündigt worden. Dieser Termin wurde vom Ministerium für Finanzen und Energie um ca. drei Monate verschoben. Die dann vorgelegten Entwürfe konnten noch nicht akzeptiert werden, weil sie in vielen Punkten noch zu überarbeiten sind.

Was ist zu tun?
Der von allen Beteiligten bedauerte Zustand, dass die Telekommunikationsrechner im Land ohne definierte Sicherheitsmaßnahmen betrieben werden, muss kurzfristig abgestellt werden. Von Woche zu Woche fällt es schwerer, eine Rechtfertigung für die Nichtbeachtung klarer datenschutzrechtlicher Regelungen zu finden. Das Ministerium für Finanzen und Energie sollte seinen externen Dienstleistern feste Fristen für die Entwicklung von Sicherheitskonzepten setzen.

7.4 Startschuss für das Landesnetz vor der Klärung aller Sicherheitsfragen?

Das Grundkonzept des Landesnetzes sorgt erfreulicherweise für eine klare Trennung zwischen den Verantwortungsbereichen des Innenministeriums als dessen Betreiber und den einzelnen Teilnehmergruppen. Es besteht allerdings die Gefahr, dass mit dem Betrieb des Netzes bereits begonnen wird, bevor die Sicherheitsfragen im Detail geklärt sind. Die Methode „Pilotprojekt“ wird möglicherweise aus Termingründen wieder einmal dazu herhalten müssen, die Verlagerung der Testphase in den Echtbetrieb zu rechtfertigen.

Als wir im Jahr 1996 den Vorläufer des Landesnetzes, das so genannte CAMPUS-Netz, einer datenschutzrechtlichen Überprüfung unterzogen (vgl. 19. TB, Tz. 7.9; 20. TB, Tz. 6.7.6), war insbesondere zu beanstanden, dass selbst die dem Netz angeschlossenen Behörden nicht im Einzelnen wussten, welche Dienstleistungen das Innenministerium als Netzbetreiber ihnen gegenüber erbrachte und welche Netzsicherheit gewährleistet wurde. Bis heute sind die schriftlichen Unterlagen hierüber fragmentarisch geblieben, konkrete Vereinbarungen zwischen den beteiligten Behörden gibt es noch immer nicht. Da sich etwa zwei Jahre nach der Prüfung abzeichnete, dass das **CAMPUS-Netz** durch das leistungsfähigere **Landesnetz** ersetzt werden würde, haben wir unsere Bemühungen eingestellt, das Innenministerium zu einer „Generalüberholung“ des CAMPUS-Netzes zu bewegen, und sind der Bitte gefolgt, die Arbeiten an der Grundkonzeption des Landesnetzes beratend zu begleiten (vgl. 21. TB, Tz. 6.4). Diese Arbeiten sind im letzten Jahr

einen großen Schritt vorangekommen und haben ihren Niederschlag in den „**Landesnetz-Rahmenbedingungen (Organisation, Technik und Betrieb)**“ – **Version 17** – und „**Landesnetz-Anschlussbedingungen“ – Version 14** –, beide vom 20.12.2000, gefunden. Die recht hohen Versionsnummern der unmittelbar vor der Testphase geltenden Fassungen der Papiere weisen darauf hin, wie aufwändig der Entwicklungsprozess dieses Projektes bis jetzt war. Unser „Investment“ an Personal und Zeit war jedenfalls beträchtlich.

Aus datenschutzrechtlicher und sicherheitstechnischer Sicht sind die folgenden bislang getroffenen **konzeptionellen Festlegungen** von besonderer Bedeutung:

- Verantwortlicher Betreiber des Landesnetzes ist das **Innenministerium**. Es bedient sich für die technische Realisierung der Deutschen Telekom AG und der Datenzentrale Schleswig-Holstein als externe Dienstleister. Das ursprünglich zuständige Ministerium für Finanzen und Energie ist „nur“ noch für die das Landesnetz nutzenden Telekommunikationsrechner verantwortlich, nicht mehr für das Netz an sich (vgl. Tz. 7.3 dieses Berichtes).
- Die **Standarddienstleistung** des Landesnetzes besteht in dem „transparenten Transport von Voice- und Non-Voice-Daten mittels Standard-IP-Datenpaketen zwischen festgelegten Endpunkten“. Welche Daten die angeschlossenen Behörden in welcher Form (verschlüsselt oder unverschlüsselt) übertragen, liegt also nach wie vor in deren Verantwortung.
- Der Anschluss einer Behörde an das Landesnetz setzt eine **schriftliche Vereinbarung** mit dem Innenministerium voraus, in der die Rahmen- und Anschlussbedingungen akzeptiert und die ergänzenden Vereinbarungen festgelegt werden.
- Möchten Behörden **optionale Dienste** (z. B. Übergänge in das Internet, Firewall-Funktionen, Verschlüsselungs-, Zwischenspeicherungs- und Weiterverarbeitungsfunktionen) in Anspruch nehmen, so haben sie hierüber Vereinbarungen unmittelbar mit der Datenzentrale zu treffen. Das Innenministerium hat diese Vereinbarungen zu prüfen und darf sie nur zulassen, wenn eine Beeinträchtigung der Kommunikation der anderen Benutzer des Netzes nicht zu befürchten ist.
- Alle Teilnehmer sind bestimmten „**geschlossenen Benutzergruppen**“ zugeordnet. Das Innenministerium gewährleistet durch softwaretechnische Maßnahmen, dass die über das Landesnetz übertragenen Datenpakete die jeweilige geschlossene Benutzergruppe nicht verlassen können. Geschlossene Benutzergruppen sind z. B. die Finanzämter einschließlich der OFD, die Polizeidienststellen, die Staatsanwaltschaften, die Gerichte und die anderen nachgeordneten Bereiche der Ministerien.
- Sollen Datenpakete eine geschlossene Benutzergruppe verlassen und in eine andere „eingespeist“ werden, ist hierüber eine Vereinbarung zwischen den beiden betroffenen Gruppen abzuschließen, die der Genehmigung durch das Innenministerium bedarf, um **Schnittstellenprobleme** auszuschließen. Die Verknüpfung der geschlossenen Benutzergruppen erfolgt ausschließlich in einer „Service-Area“, die durch die Datenzentrale betrieben wird.

- Den Abschluss des Landesnetzes zur Teilnehmerseite hin bilden so genannte **Zugangsrouter**. Auf deren Funktionalität haben die Teilnehmer keinen Einfluss. In ihnen werden die „Telefoniepakete“ von den „Datenpaketen“ getrennt. Erstere gelangen über ein so genanntes Voice-Over-IP-Gateway in die Telekommunikationsrechner (vgl. Tz. 7.3). Die Datenpakete werden über einen Übergaberouter in das lokale Netzwerk des Teilnehmers eingespeist. Die Funktionalität der Übergaberouter kann durch die Teilnehmer nur im Rahmen der (genehmigungspflichtigen) optionalen Dienste beeinflusst werden. Das Landesnetz hat keinen Einfluss auf das lokale Netzwerk des Teilnehmers.

- Die Risiken, die entstehen, wenn Teilnehmer einer geschlossenen Benutzergruppe untereinander Datenpakete austauschen, deren Inhalt „schädliche“ Wirkungen in den Rechnersystemen der lokalen Netze entfalten können (**Computerviren**, „**Trojanische Pferde**“, „**Würmer**“ und sonstiger **ausführbarer Code**), werden durch die Funktionen des Landesnetzes nicht wesentlich reduziert. Das Gleiche gilt auch für die Kommunikation **zwischen** den geschlossenen Benutzergruppen und für die **Anbindung** ganzer Benutzergruppen oder einzelner Teilnehmer an das **Internet**. Da sich die geschlossenen Benutzergruppen bzw. die einzelnen Teilnehmer nach dem Konzept gegenseitig nicht vertrauen können, sind sie verpflichtet, selbst „Vorsorge“ zu treffen. In einem Sicherheitshinweis in den „Anschlussbedingungen“ wird seitens des Innenministeriums ausdrücklich hierauf hingewiesen (vgl. nebenstehendes Zitat).

Im Wortlaut:
Sicherheitshinweise des Innenministeriums für Landesnetz-Teilnehmer

„Es wird hiermit ausdrücklich darauf hingewiesen, dass der Betreiber des Landesnetzes keinerlei Verantwortung für die Datensicherheit im Bereich der angeschlossenen Organisationen übernehmen kann. Die im Landesnetz getroffenen Sicherheitsmaßnahmen für das Netz und die zu transportierenden Daten wirken im Landesnetz bis zu den Übergabeschnittstellen und stellen natürlich auch einen bewertbaren Schutzfaktor für die hinter der Übergabeschnittstelle befindlichen Netze und Systeme dar. Gleichwohl sind die Bereiche der Organisation eigenverantwortlich zu schützen. Dies trifft insbesondere auf dortige Zugänge in oder aus anderen Netzen zu. Bei unsachgemäßer Behandlung solcher Zugänge besteht die Gefahr, dass sich Fremde vorhandene gültige IP-Adressen aneignen können, welche vom Landesnetz nicht als „falsch oder ungültig“ erkannt, sondern wie gültige Adressen behandelt werden. Es wird daher empfohlen, bei der Notwendigkeit derartiger Zugänge einen strengen Maßstab anzulegen und die Herstellung mit hohem Sicherheitsniveau zu versehen.“

Diese durchaus positive Zwischenbilanz der bisherigen Entwicklung des Landesnetzes wird allerdings dadurch getrübt, dass zu befürchten ist, dass mit dem **Pilotbetrieb** des Netzes bereits begonnen wird, **bevor** die entsprechenden Sicherheitskonzepte erarbeitet und beschlossen worden sind. Pikant erscheint, dass gerade das Innenministerium, unter dessen Federführung die Ordnungsmäßigkeitskriterien für automatisierte Verfahren im letzten Jahr neu gefasst wurden (vgl. Tz. 7.1), sie damit möglicherweise selbst nicht uneingeschränkt beachten wird.

Die noch **offenen Sicherheitsfragen** beziehen sich im Wesentlichen auf die Abschottungsmechanismen, mit denen die Deutsche Telekom AG gewährleistet, dass die Grenzen der geschlossenen Benutzergruppe nicht unbefugt durchbrochen werden können. Weiterhin ist noch im Detail zu klären, welche „Beeinflussungsmöglichkeiten" sich im Bereich der Service-Area der Datenzentrale Schleswig-Holstein ergeben und wer die Administrationsaktivitäten dieses Dienstleisters aufgrund welcher Protokolle überwachen wird (vergleichbares Problem wie bei den Telekommunikationsrechnern; vgl. Tz. 7.3). Es scheint, dass befriedigende Antworten gefunden werden können, dies erfordert aber noch viel Kärrnerarbeit.

Was ist zu tun?
Ein Projekt dieser finanziellen Größenordnung und dieser sicherheitstechnischen Tragweite sollte bis ins Detail durchgeplant und eingehend getestet sein, bevor ein (Pilot)betrieb mit Echtdaten gestartet wird. Das Innenministerium sollte seine Terminplanung daher noch einmal überdenken. Die Teilnehmer am Landesnetz sollten erkennen, dass die Verantwortung für die Sicherheit der Rechnersysteme in den lokalen Netzen bei ihnen verbleibt. Deshalb sind für diesen Bereich nach wie vor eigene Sicherheitskonzepte erforderlich.

7.5 Prüfung automatisierter Verfahren

7.5.1 Polizeiliche Datenverarbeitung ist dringend reformbedürftig

Die sicherheitstechnische Überprüfung einer Polizeiinspektion zeigte auf, dass die gesamte polizeiliche Datenverarbeitung dringend reformbedürftig ist. Das Sicherheitsniveau ist in der Praxis unterschiedlich hoch, je nachdem welche informationstechnischen Systeme eingesetzt werden. Die durch das LDSG 2000 vorgeschriebenen Vorabkontrollen im Polizeibereich sind derzeit nicht realisierbar.

Im Rahmen der umfassenden rechtlichen und sicherheitstechnischen Überprüfung in der Polizeiinspektion Eutin (vgl. auch Tz. 4.2.4) trafen wir im Bereich der automatisierten Verarbeitung personenbezogener Daten auf **drei** „**Welten**": auf eine recht straff organisierte „COMPAS-Welt", eine kaum reglementierte „Arbeitsplatz-PC-Welt" und eine zwar genehmigte, aber faktisch nicht kontrollierte „Welt der privaten IT-Systeme".

Während der Teilkomplex „Vorgangsbearbeitung" im Bereich der vernetzten COMPAS-Systeme weitgehend den **Ordnungsmäßigkeitskriterien** der Datenschutzverordnung entsprach, galt dieses bereits für den Teilkomplex „Bürokommunikation" nicht uneingeschränkt. Die diesbezüglichen Nutzungsmöglichkeiten der Software sind so vielfältig, dass auf Dauer ein ordnungsgemäßer Betrieb nur auf der Basis konkreter Anweisungen erreichbar ist. Die Aufgaben- und Verfahrensbeschreibungen waren allerdings nicht so formuliert, dass die Grenze zwischen einer zulässigen und einer unzulässigen Nutzung dieser Standardprogramme erkennbar wurde.

Bezüglich der isolierten **Arbeitsplatzrechner** mangelte es durchweg an verfahrensbezogenen Sicherheitskonzepten, an Aufgaben- und Verfahrensbeschreibungen sowie an formellen Verfahrensfreigaben. Für Dritte war lediglich die tatsächliche Nutzung der Systeme nachvollziehbar, die gewollte Nutzung war nicht dokumentiert. Wegen der faktisch nicht nachvollziehbaren Nutzung der **privat beschafften Systeme** durch die sie bereitstellenden Mitarbeiter fehlten bereits die Grundlagen für ihren ordnungsgemäßen Einsatz.

Bezeichnend ist der hohe Detaillierungsgrad der Anweisungen und Dokumentationsunterlagen für den Bereich COMPAS im Verhältnis zu dem minimalen Umfang der entsprechenden Papiere für die **PC-Welt**. Inhalt und Zweck der personenbezogenen Datenverarbeitung rechtfertigen diese Unterschiede nicht. Auch bezüglich der Überwachung der ordnungsgemäßen Anwendung der DV-Programme bestand zwischen den einzelnen Organisationsformen der automatisierten Verfahren ein nicht unerhebliches Gefälle.

Die festgestellten **technischen** und **organisatorischen Mängel** waren **vielfältig**. Maßnahmen, die bei den vernetzten COMPAS-Systemen als Selbstverständlichkeit galten (z. B. zentral gesteuertes Datenmanagement und deaktivierte Diskettenlaufwerke), waren bei den Arbeitsplatz-PC nur teilweise realisiert und bei den privaten Systemen nicht einmal angedacht. Dass die als „Schreibmaschinenersatz“ angeschafften Arbeitsplatz-PC schon lange über diese Funktion hinausgewachsen sind, zeigte sich daran, dass auf einem Rechner sogar ein datenbankgestütztes Spurendokumentationssystem vorgefunden wurde, das nie offiziell zum Einsatz freigegeben war und dessen Inhalte nur von einem einzigen Polizeibeamten sichtbar gemacht werden konnten. Bei der Brisanz der gespeicherten Daten war dies ein klarer Verstoß gegen die polizeirechtlichen Vorschriften im Landesverwaltungsgesetz.

Es kann davon ausgegangen werden, dass vergleichbar **problematische Sachverhalte landesweit** anzutreffen sind. Die Behebung der Mängel insgesamt und eine grundsätzliche Verbesserung des Datenschutzes dürfte nur erreichbar sein, wenn sich neben der geprüften Stelle auch die Polizeidirektionen, das Polizeiverwaltungsamt und das Innenministerium zur Änderung der bisherigen Verfahrensweisen aufgefordert fühlen. Über unsere Beanstandungen haben wir daher auch die vorgesetzten Behörden unterrichtet.

Das **Innenministerium** teilte uns als oberste Polizeibehörde zu den grundsätzlichen Problemstellungen kurz und bündig mit, dass die vorhandene IT-Struktur der Landespolizei in das „Konzept für den Einsatz der Informations- und Kommunikationstechnik in der Landesverwaltung“ integriert werde. Die Regularien dieses **Landessystemkonzeptes** würden ab sofort auch für den Umgang mit Datenverarbeitungsanlagen durch die Polizei gelten. Die Polizeiabteilung des Innenministeriums werde sich vordringlich auf die Formulierung der fachlichen Anforderungen und auf die Gewährleistung der Systemsicherheit im praktischen Betrieb der automatisierten Verfahren konzentrieren. Vorabkontrollen, die Einführung aussagefähiger Test- und Freigabeprozeduren und die Revision sollten künftig Schwerpunkte ihrer Arbeit sein. Weiteren grundsätzlichen konzeptionellen Überlegungen

seitens der Polizeiabteilung bedürfe es nicht. Im Übrigen seien im konkreten Fall die Verfahrensdokumentation für die Arbeitsplatzrechner ergänzt und die Privat-PC durch dienstliche Systeme ersetzt worden. Bezüglich der unterschiedlichen Regelungslage in den einzelnen Systemwelten vertrat das Innenministerium die Auffassung, dass es durchaus abweichende technische und organisatorische Regelungen geben könne. „Weil von übergeordneter Stelle abschließende Regelungen aufgrund der unterschiedlichen Gegebenheiten in den einzelnen Dienststellen nicht getroffen werden können, sind die Leiter der jeweiligen Dienststellen angewiesen, diese Regelungen zu ergänzen, wenn Angelegenheiten nur vor Ort geregelt werden können." Diese Argumentation widerspricht natürlich ganz erheblich dem Prinzip der Vorabkontrolle für sensible Datenbestände, wie sie im LDSG 2000 festgeschrieben ist.

Wir haben dem Innenministerium **detaillierte Vorschläge** zur Behebung der Mängel und zur Verbesserung der Datensicherheit unterbreitet. In sicherheitstechnischer Hinsicht sind drei Teilbereiche differenziert zu betrachten:

- Strafverfolgung und Aufrechterhaltung der öffentlichen Sicherheit,
- Personaldatenverarbeitung und Datenverarbeitung des ärztlichen Dienstes,
- Verarbeitung sonstiger Verwaltungsdaten.

Während an die beiden erstgenannten Komplexe sehr hohe Sicherheitsanforderungen zu stellen sind, dürfte für den dritten Bereich nur ein mittlerer Schutzbedarf erforderlich sein. Wir haben daher empfohlen, die Aufbau- und Ablauforganisation bezüglich der Planung und Realisierung automatisierter Verfahren so umzugestalten, dass die Verantwortungsabgrenzungen und die Regelungsinhalte den **unterschiedlichen Sicherheitsanforderungen** entsprechen.

Mit hoher Priorität sollte ein **grundlegendes IT-Konzept** erstellt werden, das technikunabhängig beschreibt, welche Ziele durch welche Software in welchen Stellen erreicht werden sollen. Ihm sollte durch eine Genehmigung und Prioritätensetzung durch das Innenministerium der Charakter einer verbindlichen Sollregelung gegeben werden. Dabei wird zwangsläufig auch die Frage zu klären sein, ob die Polizeidirektionen auch weiterhin in eigener Verantwortung automatisierte Verfahren für ihren Zuständigkeitsbereich „kreieren" dürfen. Tendenziell sollte von einer solchen Verfahrensweise Abstand genommen werden. Gerade die Überlegungen zu INPOL-neu legen den Ansatz nahe, dass die Gleichartigkeit der Aufgabenstellungen der Polizeidienststellen auch **gleichartige** hard- und softwaretechnische **Lösungsansätze** erfordert. Die Folgen des nicht zu übersehenden bisherigen „PC-Nutzungwildwuchses" zeigen, dass die Gestaltung effizienter automatisierter Verfahren eine professionelle Systemanalyse und eine landesweite Koordination voraussetzt. Auch spezielle Anwendungen einzelner Dienststellen (z. B. Wirtschaftskriminalität) sollten ihren Niederschlag in dem IT-Konzept finden. Im Ergebnis sollten automatisierte Verfahren, die nicht im IT-Konzept verzeichnet sind, als „nicht gewollt" und damit als unzulässig gelten.

Im Ergebnis haben sich bislang **mehrere „IT-Welten“** entwickelt, die nur bedingt miteinander synchronisiert worden sind. Die entstandenen Defizite dürften nur behoben werden können, wenn die Planung, Entwicklung und Administration aller automatisierten Verfahren und technischen Systeme aufbau- und ablauforganisatorisch einer einheitlichen Struktur unterworfen werden. Dies schließt **dezentrale Entscheidungsbefugnisse** (z. B. welche Softwarekomponenten welchen Mitarbeitern zur Verfügung gestellt werden) nicht aus, zwingt aber zu **einheitlichen konzeptionellen** und **technischen Standards**. Wir haben außerdem dringend empfohlen, unabhängig von den Aktivitäten im Zusammenhang mit der Übernahme des Landessystemkonzeptes eine Bestandsaufnahme sämtlicher Geräte, mit denen zulässigerweise personenbezogene Daten verarbeitet werden dürfen, durchzuführen. Weiterhin sollte festgestellt werden, welche Softwarekomponenten auf welchen Systemen eingesetzt werden dürfen.

Im Wortlaut:
§ 197 Landesverwaltungsgesetz

(1) Die Errichtung von Dateien und anderer Datensammlungen ist auf das erforderliche Maß zu beschränken. In angemessenen Abständen ist die Notwendigkeit ihrer Weiterführung oder Änderung zu prüfen.

(2) Für jede Datei und andere Datensammlungen sind in einer Errichtungsanordnung mindestens festzulegen:

1. *Bezeichnung,*
2. *Rechtsgrundlage und Zweck,*
3. *Personenkreis, über den Daten gespeichert werden,*
4. *Arten der zu speichernden Daten,*
5. *Arten der Daten, die der Erschließung des Datenbestandes dienen,*
6. *Anlieferung oder Eingabe der Daten,*
7. *Voraussetzungen (Anlass und Zweck), unter denen in der Datei gespeicherte Daten an welche Empfänger und in welchen Verfahren übermittelt werden,*
8. *Prüffristen nach Absatz 1 Satz 2 und § 196 Abs. 3 und*
9. *technische und organisatorische Maßnahmen nach dem Landesdatenschutzgesetz.*

Vor dem Hintergrund der Regelungen des § 197 Landesverwaltungsgesetz und der weitgehenden Gestaltungsmöglichkeiten bei der Nutzung von Standardsoftwareprodukten kommt einer regelmäßigen Kontrolle der tatsächlich gespeicherten Datenbestände eine erhebliche Bedeutung zu. Auch im Hinblick auf die Anforderungen des Landesdatenschutzgesetzes handelt es sich hierbei um eine „**Pflichtaufgabe**“ der weisungsbefugten Mitarbeiter. Ihre diesbezüglichen Aktivitäten sollten künftig protokolliert werden. Als nicht akzeptabel sollten Datenbestände angesehen werden, auf die Vorgesetzte keine Zugriffsmöglichkeiten haben. Die Zugriffs- und Löschungsberechtigungen sollten die sich aus der Geschäftsverteilung ergebenden Befugnisse widerspiegeln. Der Aufwand hierfür wird sich auf ein Minimum reduzieren, wenn ausschließlich vernetzte Systeme eingesetzt werden.

Was ist zu tun?
Da das Innenministerium ohnehin eine Reihe von automatisierten Verfahren im Bereich der Polizei an die INPOL-neu-Konventionen anpassen muss, dürfte der richtige Zeitpunkt für eine grundlegende aufbau- und ablauforganisatorische sowie sicherheitstechnische Reform der automatisierten personenbezogenen Datenverarbeitung im Bereich der Strafverfolgung und Gefahrenabwehr gekommen sein. Der erste Schritt in diese Richtung sollte in einer konstruktiven Erörterung unserer Vorschläge bestehen.

7.5.2 Das Behördenmanagement als Risikofaktor?

Bei Routineprüfungen „in der Fläche" werden relativ selten Sicherheitslücken entdeckt, die auf menschliches Versagen einzelner Mitarbeiter zurückzuführen sind. In den meisten Fällen werden strukturelle Sicherheitsmängel erkennbar, die von den Behördenleitungen zu verantworten sind. Nicht selten mangelt es auf dieser Ebene an Wissen und Engagement. Aspekte der Kostenvermeidung werden zumeist über alles andere gestellt.

Neben den umfassenden Schwerpunktprüfungen, wie z. B. im Polizeibereich oder zuvor bei der AOK Schleswig-Holstein, führen wir so viele Nachschauen „in der Fläche" durch, wie personell irgendwie realisierbar sind. Je mehr Daten verarbeitende Stellen wir besuchen und deren Datenverarbeitungsorganisation und Sicherheitsmaßnahmen begutachten, desto genauer ist unser Überblick über die **aktuelle sicherheitstechnische Situation** im Lande.

Wenn man am Ende des Jahres 2000 ein Fazit aus diesen Aktivitäten zieht, drängen sich zwei **grundlegende Feststellungen** auf:

- Es gibt derzeit nur **zwei Bereiche**, in denen die Hard- und Softwareindustrie für die Anforderungen der Praktiker in den Daten verarbeitenden Stellen keine zufrieden stellenden Lösungen bereithält. Es sind dies die Komplexe „revisionsfeste Protokollierung verändernder Zugriffe auf die Betriebssystemebene" und „sichere Verknüpfung lokaler Netzwerke mit anderen Netzen auf der Basis der Internet-Protokolle". Für alle anderen verwaltungsspezifischen Problemstellungen sind Musterlösungen entwickelt, erprobt und in Form von Produkten oder Konzepten auf dem Markt verfügbar.
- Die Gründe, dass die vorhandenen Lösungen nach wie vor nicht allgemein eingesetzt werden, liegen in dem Versuch vieler **Behördenmanager**, sich mit einem Minimum an personellem und finanziellem Investment **durchzulavieren**.

Unisono klagen z. B. die Anbieter hochwertiger (und damit etwas teurerer) Hard- und Softwarekonzepte, dass sie gegen die billigeren Anbieter von „**Schmalspurlösungen**" ausgespielt werden. Zitat: „Es reicht den Behörden, dass die Software Firewall heißt, ob sie wie eine Firewall funktioniert, ist denen doch völlig egal." Dieser Eindruck deckt sich mit unseren Prüfungserfahrungen. Die Fälle des menschlichen Versagens als Ursache für das Entstehen von Schwachstellen sind

nicht besonders häufig, meist liegen die Ursachen im Desinteresse oder in **Fehlentscheidungen der Behördenleitungen**. Wie anders sind die folgenden, immer wieder auftauchenden Fragestellungen aus der Prüfungspraxis zu erklären:

- Warum werden **Systemadministratoren** nur **unzureichend ausgebildet**? Allen Beteiligten müsste doch klar sein, dass ein „Einführungskurs“ nicht ausreicht, wenn das Ausbildungspaket mehrere Aufbaukurse umfasst.
- Warum werden sie verpflichtet, die Administrationsaufgaben neben ihrer normalen Tätigkeit zu erledigen, wenn das zur Verfügung stehende **Zeitkontingent** völlig **unzureichend** ist und die Hauptaufgabe die betreffenden Mitarbeiter praktisch voll auslastet?
- Warum werden sie mit ihrer **Verantwortung** für die Auswahl der richtigen sicherheitstechnischen Komponenten allein gelassen? Warum setzt eine Behördenleitung Dienstanweisungen in Kraft, an die sie sich selbst nicht hält, und warum lässt sie damit allen Mitarbeitern deutlich werden, dass Abweichungen von Sicherheitsvorschriften billigend in Kauf genommen werden? Warum fehlt eine kritisch-konstruktive Unterstützung ihrer Arbeit? Wer erklärt z. B. einem Systemadministrator, dass Personaldaten gegenüber den übrigen Datenbeständen besonders abzuschotten sind, wenn nicht der „Personalchef“?
- Was nutzt es, wenn für den **Internet-Zugang** ein Quarantäne-PC angeschafft wird, wenn auf ihm, um der besseren Ausnutzung willen, dann doch „sensible“ Verwaltungsdaten gespeichert werden?
- Warum erklärt eine Behörde, aus Sicherheitsgründen auf einen Internet-Anschluss verzichtet zu haben, wenn sie weiß bzw. wissen müsste, dass ausgerechnet die **Systemadministratoren** über einen solchen Zugang verfügen?
- Warum muss ausgerechnet der Systemadministrator zum **behördlichen Datenschutzbeauftragten** ernannt werden, der sich damit selbst kontrollieren muss?

In diesem Zusammenhang treffen wir auf ein offenbar weit verbreitetes Missverständnis: Die Behebung der festgestellten Mängel wird als eine Obliegenheit zur „Befriedung“ der Datenschutzkontrollinstanz und nicht zur **Reduzierung von Risiken im eigenen Interesse** angesehen. Allzu oft müssen wir der Behauptung widersprechen, „die Datenschützer“ hätten ein Problem. Es gilt dann deutlich zu machen, dass das Problem aufseiten der Behörden(leitungen) liegt. Das ULD weist bei seinen Prüfungen nur auf technische und organisatorische Sicherheitslücken hin, die dadurch nicht zu unserem Problem werden.

Schleswig-Holstein DATENSCHUTZAKADEMIE
Kurs ITR

Was ist zu tun?
Prüfungsmaßnahmen sind auch in der Zukunft unverzichtbar. Da ein flächendeckendes Aufspüren von Sicherheitsrisiken durch das ULD aber wohl in absehbarer Zeit nicht zu erreichen sein wird, müssen die Verantwortlichen in den Behörden Eigeninitiative entwickeln. Den Vorwurf, sie seien selbst ein Risikofaktor, sollten sie nicht auf sich sitzen lassen.

8 Recht und Technik der neuen Medien

8.1 Mobilfunkprovider werden zu Außenstellen der Sicherheitsbehörden

Beim Kauf von Handys mit Prepaid-Karten müssen die Kunden ihren Personalausweis von Mobilfunkprovidern kopieren lassen. Dies dient ausschließlich dem Interesse der Strafverfolgungsbehörden, die in der Lage sein wollen, jeden Benutzer eines mobilen Telefons abzuhören. Das Verwaltungsgericht Köln hat diese Praxis nun für rechtswidrig erklärt.

Wer ein „normales“ Handy erwirbt, wird vom Mobilfunkprovider aufgefordert, seine persönlichen Daten zu offenbaren. Dies ist nachvollziehbar, da es um ein **Dauerschuldverhältnis** geht, bei dem der Anbieter in Vorleistung tritt. Er ermöglicht dem Kunden Telefonate, die einen erheblichen Gegenwert haben können, und rechnet diese erst am Ende des Monats ab. Im Endeffekt wird dem Kunden damit ein nicht unerheblicher Kreditrahmen eröffnet.

Allerdings stößt es auf das Unverständnis der Kunden, dass die Identifizierung durch Vorlage des Ausweises auch dann gefordert wird, wenn es um den Erwerb eines Handys mit **Prepaid-Karte** geht. Dem Vernehmen nach werden inzwischen mehr Handys mit Prepaid-Karte gekauft als andere. In diesem Fall ist die Sachlage genau umgekehrt. Durch den Erwerb der Karte tritt der Kunde in Vorleistung. Er bezahlt zunächst und kann die Dienste des Anbieters danach nur bis zu dem entrichteten Betrag in Anspruch nehmen. Wozu also dient in diesen Fällen die genaue Identifizierung der Kunden?

Diese erfolgt jedenfalls nicht im Interesse der Telekommunikationsunternehmen. Sie würden es vielmehr vorziehen, ihre vorbezahlten Produkte z. B. im Warenhausregal oder an der Tankstelle ohne weitere Formalitäten anbieten zu können. Ein solches kundenfreundliches Vorgehen ist ihnen durch so genannte „**Leitlinien**“ verwehrt, die die **Regulierungsbehörde** für Telekommunikation und Post (RegTP) herausgegeben hat.

> ***? RegTP***
>
> *Die Regulierungsbehörde hat u. a. die Aufgabe, die Telekommunikationsunternehmen zuzulassen (zu lizensieren) und deren Tätigkeit zu überwachen. Aus diesem Grund kommen offenbar viele Unternehmen den Hinweisen der Behörde nach, auch wenn diese nicht als formaler Bescheid erlassen, sondern lediglich informell ausgesprochen werden.*

Die RegTP ist der Auffassung, dass sich die Verpflichtung, die Identitätsdaten auch beim Verkauf von Prepaid-Produkten zu erheben, aus dem Telekommunikationsgesetz (TKG) ergibt. Danach haben die Anbieter die Rufnummern sowie Namen und Anschrift in eine so genannte **Kundendatei** aufzunehmen. Diese Datei muss der Regulierungsbehörde in elektronischer Form so zur Verfügung stehen, dass sie von ihr automatisiert abgefragt werden kann, ohne dass diese Abfragen dem jeweiligen Unternehmen zur Kenntnis kommen (vgl. 19. TB, Tz. 7.3.1). Dieses Verfahren soll den Staatsanwaltschaften und der Polizei, aber auch den Geheim-

diensten über die Regulierungsbehörde einen Online-Zugriff auf sämtliche Kundendateien ermöglichen. Angeblich wird dies benötigt, um zu ermitteln, unter welcher Rufnummer eine bestimmte Person in den Telekommunikationsnetzen agiert.

Da Erwerber und Nutzer von Handys häufig nicht identisch sind, kann man hier aber Zweifel am Sinn der Maßnahme haben. Es ist umstritten, wie weit die Pflicht zur Führung von Kundendateien geht. Klar ist, dass in diese Kundendateien solche Daten aufzunehmen sind, die ohnehin aus Gründen der betrieblichen Abwicklung bei den Telekommunikationsunternehmen gespeichert werden.

Mehrere Provider haben deshalb Klage erhoben. Das **Verwaltungsgericht Köln** entschied, dass § 90 TKG keine ausreichende Rechtsgrundlage für eine so weitgehende Verarbeitung personenbezogener Daten ist. Die Vorschrift müsse im Lichte ihrer Entstehungsgeschichte so gelesen werden, dass sie lediglich die Daten erfasst, die die Provider ohnehin aufgrund ihrer betrieblichen Erfordernisse bereits erhoben und gespeichert haben. Eine extensivere Auslegung der Vorschrift scheide aus, da die Grundrechte der Telekommunikationskunden tangiert würden. Auch das Grundrecht der Provider auf freie Berufsausübung werde bei dieser Auslegung eingeschränkt, da sie aufgrund der Vorgaben der Regulierungsbehörde gehindert seien, Prepaid-Karten in einem kundenfreundlicheren Verfahren anzubieten. Die Regulierungsbehörde hat das Oberverwaltungsgericht Münster als Berufungsinstanz angerufen. Da die Entscheidung keine aufschiebende Wirkung hat, bleiben die Leitlinien der Regulierungsbehörde zunächst in Kraft.

Im Wortlaut: § 90 TKG

(1) Wer geschäftsmäßig Telekommunikationsdienste anbietet, ist verpflichtet, Kundendateien zu führen, in die unverzüglich die Rufnummern und Rufnummernkontingente, die zur weiteren Vermarktung oder sonstigen Nutzung an andere vergeben werden, sowie Name und Anschrift der Inhaber von Rufnummern und Rufnummernkontingenten aufzunehmen sind, auch soweit diese nicht in öffentliche Verzeichnisse eingetragen sind.

Was ist zu tun?
Die Käufer von Handys mit Prepaid-Karten sollten gegenüber den Verkäufern gegen ihre Registrierung protestieren, damit die Provider ihrerseits die Wünsche ihrer Kunden gegenüber der Regulierungsbehörde geltend machen können.

8.2 Schleswig-Holstein im Internet

Das Land hat sich entschieden, seine Internet-Präsentation unter der Adresse *www.schleswig-holstein.de* nicht selbst zu organisieren, sondern sich dafür einer privaten Firma zu bedienen. Inzwischen scheint es dort mit dem Datenschutz zu klappen.

Die Firma S-Netline, ein Unternehmen der Sparkassenorganisation, hat vom Land den Auftrag erhalten, die **Präsentation des Landes Schleswig-Holstein** unter der Internet-Adresse „www.schleswig-holstein.de“ zusammenzufassen. Das Land stellt

den attraktiven Domain-Namen zur Verfügung. Die Firma S-Netline hat sich verpflichtet, die Inhalte, die öffentliche Stellen anliefern, aufzubereiten und der Öffentlichkeit in einem so genannten „Portal“ zu präsentieren. Eine ähnliche Vereinbarung gibt es zwischen dem Unternehmen und Hamburg.

Es sollen nicht nur die Inhalte der öffentlichen Verwaltung, sondern auch die Privater, vor allem regionaler und lokaler Kaufleute, präsentiert werden. So findet man unter „schleswig-holstein.de“ bereits erste Online-Shops, weitere sollen folgen. Das System soll weiter ausgebaut werden. Gedacht ist z. B. an ein so genanntes **Lebenslagenkonzept**, das es dem Bürger ermöglichen soll, zu bestimmten Ereignissen (z. B. Hochzeit) einen schnellen Überblick über die erforderlichen Behördengänge, die benötigten Unterlagen und die passenden Waren- und Dienstleistungsangebote der örtlichen Unternehmen zu gewinnen. Eine weitere Entwicklung ist das Bürgerinformationssystem „Dibis“, das dazu dienen soll, die Nutzer mit wenigen Klicks darüber in Kenntnis zu setzen, welche Unterlagen sie für bestimmte Behördengänge benötigen, wo sie diese absolvieren können, welche Öffnungszeiten die Ämter haben usw.

Wie bei allen Angeboten im WWW werden auch bei „schleswig-holstein.de“ **IP-Nummern** verarbeitet, die unter bestimmten Umständen personenbezogen sein können (vgl. 22. TB, Tz. 7.1.2). Im Einzelfall können noch weitere personenbezogene Daten anfallen. So ist es z. B. möglich, eine E-Mail-Adresse nach dem Muster Bürgername@schleswig-holstein.de zu erwerben. Dafür müssen bestimmte personenbezogene Angaben gemacht werden. Auch für die Nutzung der Online-Shops und des Bürgerinformationssystems sind personenbezogene Daten erforderlich.

Bezüglich der weiteren Entwicklungsstufen des Systems hat das Unternehmen S-Netline das ULD frühzeitig über die Konzeptionen informiert. In Zusammenarbeit mit dem Hamburgischen Datenschutzbeauftragten sind für alle Beteiligten brauchbare Lösungen gefunden worden. Einzelne Fehlentwicklungen konnten noch korrigiert werden. So wurden z. B. die ersten Online-Shops mithilfe von **Cookies** betrieben, die nicht datenschutzgerecht programmiert waren. Bei Bestellungen war gesetzeswidrig „voreingestellt“, dass die Kunden von den einzelnen Anbietern zukünftig **Werbung** erhalten „wollten“. Von einer echten Einwilligung konnte so keine Rede sein. Wir haben S-Netline auf die Defizite hingewiesen, die sofort beseitigt wurden.

Was ist zu tun?
Das Land Schleswig-Holstein sollte darauf achten, dass www.schleswig-holstein.de auch weiterhin datenschutzgerecht betrieben wird.

8.3 Fotoalbum ins Internet?

Ein Internet-Auftritt muss farbig sein mit möglichst vielen bunten Bildern. Das glauben viele Behörden und stellen die verschiedensten Fotos ins Netz. Doch Vorsicht: Wer Abbildungen von Personen veröffentlicht, benötigt im Regelfall deren Einwilligung. Wird dies nicht beachtet, drohen sogar strafrechtliche Konsequenzen.

Viele öffentliche Stelle treten an uns heran und bitten um Beratung bei der Gestaltung ihrer Homepage, weil sie **Fotos** von Mitarbeitern, Kunden oder sonstigen Personen integrieren wollen (vgl. 20. TB, Tz. 7.1.3). Wir weisen in diesen Fällen darauf hin, dass nach **§ 22 Kunsturheberrechtsgesetz** Bildnisse nur mit der Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden dürfen. Es genügt nicht, die Möglichkeit zum Widerspruch zu gewähren, vielmehr muss vor der Veröffentlichung eine eindeutige zustimmende Erklärung der Betroffenen vorliegen. Die Einwilligung muss sich auf die näheren Umstände der Veröffentlichung beziehen (z. B. welche Bilder des Betroffenen auf welcher Seite der Homepage). Bei Minderjährigen haben die Erziehungsberechtigten die Befugnis, die Einwilligung abzugeben. Um im Nachhinein Missverständnisse zu vermeiden, sollte die Einwilligung schriftlich erteilt werden.

Im Wortlaut:
§ 22 Kunsturheberrechtsgesetz

Recht am eigenen Bilde
Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Die Einwilligung gilt im Zweifel als erteilt, wenn der Abgebildete dafür, dass er sich abbilden ließ, eine Entlohnung erhielt. Nach dem Tode des Abgebildeten bedarf es bis zum Ablaufe von 10 Jahren der Einwilligung der Angehörigen des Abgebildeten. Angehörige im Sinne dieses Gesetzes sind der überlebende Ehegatte und die Kinder des Abgebildeten und, wenn weder ein Ehegatte noch Kinder vorhanden sind, die Eltern des Abgebildeten.

Ausnahmen von dem Erfordernis der Einwilligung bestehen nur dann, wenn die Abgebildeten **Personen** der **Zeitgeschichte** sind oder es sich um **künstlerische Bildnisse** handelt. Ohne Einwilligung können auch solche Bildnisse veröffentlicht werden, die Versammlungen, Aufzüge oder ähnliche Vorgänge darstellen, sofern es sich um eine größere Menschenmenge handelt. Entscheidend ist, ob der Einzelne als Bestandteil der Menge in dieser optisch untergeht. Dies ist etwa der Fall bei dem Bild eines belebten Großstadtplatzes mit einer unübersehbaren Menge von Fußgängern. Auch wenn ein einzelner Passant hier noch erkennbar sein mag, geht er doch in der Menge der Menschen unter. Das OLG München hat entschieden, dass bei der Abbildung einer zufällig zusammengekommenen, sonnenbadenden Gruppe von sieben Personen keine ausreichend große Menge vorlag.

Fehlt es an der Einwilligung, und werden die Bilder gleichwohl veröffentlicht, so liegt nicht nur ein Rechtsverstoß vor, der vor einem Zivilgericht mit einer Unterlassungsklage bekämpft werden kann. Das Kunsturheberrechtsgesetz erklärt den Verstoß gegen diese Vorschriften für **strafbar**; es droht eine Freiheitsstrafe von bis zu einem Jahr oder eine Geldstrafe.

Das Gesagte gilt auch, wenn eine **Webcam** so installiert wird, dass natürliche Personen (z. B. Passanten) erkannt werden können, ohne dass sie nur Bestandteile der Menge sind und in dieser untergehen. Besonders zu beachten ist dabei, dass Webcams häufig Weitwinkelobjektive verwenden. Weiter entfernte Personen sind zwar kaum noch identifizierbar; die unmittelbar vor dem Objektiv Stehenden werden jedoch in der Regel gut erkannt.

Was ist zu tun?
Sollen Abbildungen von Personen auf der Homepage veröffentlicht werden, so ist zuvor deren Einwilligung einzuholen.

8.4 Berufliche Internet-Nutzung – Der Arbeitgeber als Provider oder als Big Brother?

Immer mehr Beschäftigte haben am Arbeitsplatz Zugang zum Internet. Nicht immer surfen sie nur Seiten an, die im Interesse ihres Arbeitgebers liegen. Wie viel Kontrolle ist notwendig und wie viel ist erlaubt? Darf der E-Mail-Verkehr vollständig überwacht werden?

Leider wird mit der Internet-Nutzung durch Mitarbeiter oft begonnen, bevor die entsprechenden Regelungen festgelegt sind. Dann kommt es häufig zu Problemen, wenn die Geschäfts- oder Behördenleitung im Nachhinein die Nutzung des World Wide Web durch die Mitarbeiter überprüfen will. Denn es liegen zwar Protokolle über die Nutzung vor, diese wurden jedoch lediglich für Zwecke der Datensicherheit erstellt, nicht für **Verhaltens- und Leistungskontrollen** (vgl. 21. TB, Tz. 7.1.2). Eine nachträgliche Zweckänderung dieser Daten ist sowohl nach dem LDSG als auch nach dem BDSG ausgeschlossen.

Ein weiterer Problembereich bezieht sich auf die Kontrollbefugnisse des Arbeitgebers im Bereich der **E-Mail-Kommunikation** der Mitarbeiter. Ist den Mitarbeitern die private Kommunikation über die dienstliche Anlage gestattet, so gilt für diese privaten E-Mails, unabhängig davon, ob sie ankommen oder abgesendet werden, das Fernmeldegeheimnis. Das heißt, dass hier eine inhaltliche Kontrolle durch den Vorgesetzten nur in ganz wenigen, vom Telekommunikationsgesetz abschließend definierten Ausnahmefällen zulässig ist (vgl. 21. TB, Tz. 7.1.2; 22. TB, Tz. 7.1.4). Doch selbst bei rein dienstlicher Kommunikation bestehen bei vielen Experten Bedenken, ob eine umfassende und lückenlose Inhaltskontrolle der E-Mail-Kommunikation zulässig ist oder einen übermäßigen Eingriff in die Persönlichkeitsrechte der Beschäftigten darstellt. In diese Richtung deutet ein Urteil des Bundesverfassungsgerichts, das sich allerdings auf Sprachtelefonie bezog. Das Gericht sah die Überwachung dienstlicher Telefonate als unzulässig an, da in diese erfahrungsgemäß ein größerer Anteil der Arbeitnehmerpersönlichkeit einfließt. Entscheidend ist demnach, ob E-Mail-Verkehr eher mit herkömmlichen dienstlichen Schreiben oder mit dienstlichen Telefonaten vergleichbar ist. Im ersten Fall dürften keine Bedenken gegen die vollständige Offenbarung der Schreiben bestehen; im zweiten Fall wäre dies durchaus der Fall.

Nach unserer Beobachtung lassen sich **zwei Typen** von dienstlichen E-Mails unterscheiden. Zum einen wird das Kommunikationsmittel E-Mail als Ersatz für einen **förmlichen Brief** verwendet. In diesen Fällen kann auch für E-Mails nichts anderes als für Briefe gelten, d. h. der Vorgesetzte hat selbstverständlich das Recht, die für die Organisation relevante Kommunikation einzusehen. Der zweite Typ ist eine eher **informelle Kommunikation**. Hier wird häufig statt des Mediums Telefon das Medium E-Mail gewählt, da die asynchrone Kommunikation Vorteile insbesondere dann bietet, wenn der Kommunikationspartner nicht sofort erreicht werden kann. Zu diesem Typus dürften informelle Absprachen über Termine oder sonstige Arbeitsverabredungen und vergleichbare Kommunikation zählen. Sie sind häufig weniger förmlich; das bedeutet auch, dass das Persönlichkeitsrecht der Arbeitnehmer durch eine Kontrolle hier stärker beeinträchtigt wäre.

Als Lösung bietet es sich z. B. an, für die dienstliche Kommunikation der Mitarbeiter zwei **unterschiedliche E-Mail-Accounts** einzurichten. Während über den einen die formale Kommunikation abgewickelt wird, die praktisch den herkömmlichen Schriftverkehr ersetzt, dient der zweite Account der eher informellen Kommunikation. Dem wird durch unterschiedliche Kontrollbefugnisse und Vertretungsregelungen Rechnung getragen. Für den dienstlichen Account besteht eine vollständige Kontrolle der Vorgesetzten; weiterhin muss dafür gesorgt werden, dass eingehende Mails im Abwesenheitsfall automatisch an andere Mitarbeiter weitergeleitet werden, damit keine relevanten Vorgänge über längere Zeit liegen bleiben. Anders beim zweiten Account. Hier könnten Parallelen zum Telefon gezogen werden. Die Kontrollintensität könnte reduziert werden. So ließe sich z. B. in einer Betriebsvereinbarung festhalten, dass lediglich eine stichprobenartige Kontrolle und darüber hinaus eventuell eine auf konkrete Anlässe bezogene Nachschau stattfindet. Außerdem ist für diesen Account eine Vertretungsregelung verzichtbar, wenn sichergestellt wird, dass unmittelbar dienstlich relevante Mails über den ersten Account eingehen. Dies kann z. B. durch entsprechende Hinweise im Abspann oder durch Voreinstellungen bei der „Reply-to-Adresse“ im Mailprogramm erfolgen.

Die Bundesregierung plant den Erlass eines **Arbeitnehmerdatenschutzgesetzes**, das auch den Bereich „dienstliche Nutzung des Internets und verwandte datenschutzrechtliche Probleme“ behandeln soll. Dabei wird darauf zu achten sein, dass es zu einem ausgewogenen Kompromiss zwischen den Interessen der Arbeitgeberseite und dem Persönlichkeitsrecht der Arbeitnehmer kommt.

Was ist zu tun?
Sobald ein dienstlicher Internet-Zugang für eine Organisation geschaffen wird, sollte in einer internen Regelung festgelegt werden, nach welchen Mechanismen beim Verdacht auf missbräuchliche Nutzung die Kontrolle erfolgen darf. Im geplanten Arbeitnehmerdatenschutzgesetz sollten die Datenschutzrechte der Beschäftigten angemessen berücksichtigt werden.

8.5 Neue Telekommunikations-Datenschutzverordnung verdoppelt Speicherfrist

Die Ende des Jahres 2000 verabschiedete Telekommunikations-Datenschutzverordnung (TDSV) bringt neben datenschutzrechtlichen Verbesserungen auch eine deutliche Ausweitung der Speicherfristen.

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

Im Dezember 2000 beschloss die Bundesregierung die endgültige Fassung der TDSV. Im Vergleich zur vorherigen enthält sie einige Verbesserungen für den Datenschutz. Bedenklich ist jedoch die neue Regelung zur Speicherung von Verbindungsdaten. Entgegen der Forderung von Datenschutzbeauftragten des Bundes und der Länder sowie abweichend von den Empfehlungen des Wirtschaftsausschusses des Bundesrates können nämlich Verbindungsdaten nun statt bisher 80 Tage nach Rechnungsversand **sechs Monate lang** vorgehalten werden. Bezeichnenderweise wurde die längere Speicherungsdauer nicht von den Telekommunikationsunternehmen, sondern von den Sicherheitsbehörden gefordert. Damit wird die Menge der gespeicherten Daten deutlich vergrößert, was auf eine verfassungsrechtlich angreifbare **Vorratsdatenspeicherung** hinausläuft. Dabei ist die Eignung der Regelung für die anvisierten Zwecke der Strafverfolgung und der Geheimdienste fraglich. Kundinnen und Kunden können im Einzelfall eine kürzere Speicherungsdauer vertraglich vereinbaren. Vielen ist diese Möglichkeit gar nicht bekannt, während Kunden mit unlauteren Absichten sie sich gezielt zu Nutze machen können.

Die Verlängerung der Speicherfristen reiht sich ein in die seit einiger Zeit zu beobachtende Tendenz, die tatsächlichen und rechtlichen Möglichkeiten bei der **Überwachung der Telekommunikation** auszuweiten (vgl. 21. TB, Tz. 7.7; 22. TB, Tz. 7.2 sowie Tz. 11.2). Es ist zu hoffen, dass das Fernmeldegeheimnis als wichtiges Grundrecht in der Informationsgesellschaft in Zukunft nicht weiter beeinträchtigt wird.

Was ist zu tun?
Kunden, die mit der Verlängerung der Speicherfristen für ihre Verbindungsdaten nicht einverstanden sind, sollten mit ihren Telekommunikationsunternehmen eine kürzere Speicherfrist vereinbaren.

8.6 P3P – Neuer Standard für Online-Privacy

Immer mehr Surfer wollen wissen, welche Daten die Webserver über sie beim Internet-Surfen speichern. Neuerdings geben viele Anbieter eine Datenschutzerklärung (Privacy Policy) auf ihren Webseiten ab, in der sie beschreiben, welche Daten ihrer Kunden sie zu welchen Zwecken speichern. P3P könnte den Surfern das Verständnis von Privacy Policies erleichtern.

In den USA, wo es (noch) keine grundlegenden Datenschutzgesetze gibt, gehören Datenschutzerklärungen zur Tagesordnung. Aber auch in Deutschland klären immer mehr Anbieter ihre Kunden über ihre Datenspeicherungen und -nutzungen auf. Das virtuelle Datenschutzbüro nimmt insoweit selbstverständlich eine Vorreiterrolle ein (vgl. Tz. 9.1). Seine datenschutzgerechte Privacy Policy betont ausdrücklich, dass **keine personenbezogenen Nutzerdaten** gespeichert werden.

> **? *P3P***
>
> *P3P steht für „Platform for Privacy Preferences Project". Damit können Websites auf einfache Weise ihre Privacy Policy nach einem einheitlichen Schema ausdrücken, sodass sie von dem Nutzerrechner ausgewertet werden kann. Die Nutzerin oder der Nutzer entscheidet dann, ob sie oder er die Website unter den gegebenen Bedingungen besuchen möchte oder nicht.*

Ziel muss es aber sein, dass man sich nicht nur auf Versprechungen in solchen Datenschutzerklärungen verlassen können muss, sondern dass bereits technisch sichergestellt ist, dass tatsächlich nur die genannten Daten zum Anbieter übertragen werden. Ein erster Ansatz besteht darin, mit möglichst wenigen Datenspuren auf die Webseiten zu kommen (wie beim Anonymitätsprojekt, vgl. Tz. 9.2). Doch was ist, wenn man doch Daten hergeben muss oder will, z. B. beim Online-Einkauf? Ein Teil dessen, was in Privacy Policies steht, kann technisch implementiert oder zumindest dem Nutzer so angezeigt werden, dass er nicht in jedem Einzelfall die Datenschutzerklärungen eines Anbieters durcharbeiten muss. Der neue **weltweite Standard** dafür heißt **P3P** – Platform for Privacy Preferences Project (vgl. 22. TB, Tz. 9.3, und 21. TB, Tz. 7.1.4).

Damit ist es möglich, sich anzeigen zu lassen, welche Kundendaten der Anbieter zu welchem Zweck benötigt. Das könnte beim **Online-Einkauf** so aussehen: „Der Anbieter X benötigt von Ihnen den Namen und die Lieferadresse, um Ihnen die Ware zustellen zu können. Ihre personenbezogenen Informationen werden nur zur Abwicklung dieser Transaktion verwendet und keinem Dritten übermittelt. Bitte geben Sie die Daten in das Formular ein." Sofern der Kunde damit einverstanden ist, bestätigt er und weist per Mausklick seinen Computer an, die erforderlichen Daten bereitzustellen.

P3P als universeller technischer Standard erlaubt es, weltweit im ganzen Internet **Datenschutz-Policies** für die Nutzer **transparent** zu machen, sofern auch die Anbieter P3P verwenden. Die Nutzer haben damit eine größere Kontrolle darüber, was mit ihren persönlichen Daten geschieht. P3P kann sich den verschiedenen

lokalen Bedingungen anpassen und damit einen Wettbewerb der Anbieter um den besten Datenschutz ermöglichen.

Der internationale Standardisierungsprozess der ersten Version von P3P, der vom World Wide Web Consortium (W3C) betrieben wird, steht kurz vor dem Abschluss. An der Standardisierung beteiligt sich neben Firmen und Organisationen auch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein. Im Rahmen der **Sommerakademie 2000** wurde P3P durch das W3C erstmals der deutschen Öffentlichkeit vorgestellt. In Kürze werden die ersten Software-Tools für P3P allgemein verfügbar sein.

www.datenschutzzentrum.de/somak/somak00/somak00.htm

P3P löst nicht alle Datenschutzprobleme im Internet, sondern stellt lediglich einen technischen Standard zur Transparenz der Datenverarbeitung dar. Allerdings kann technisch nicht garantiert werden, dass die Anbieter die erhobenen Daten tatsächlich nur zu den angegebenen Zwecken verwenden. **Unverzichtbar** bleiben auch in Zukunft eine ergänzende, wirksame **Datenschutzkontrolle** und **präzise Rechtsnormen** zum Schutz der Internet-Nutzerinnen und -Nutzer. Außerdem hängt es massiv von der Gestaltung der P3P-Software ab, welche Datenschutzfunktionalität integriert ist und wie datenschutzgerecht die Standardeinstellungen sind. Zum Beispiel ist es wichtig, dass sich die Software merkt, welche Informationen man unter welchen Bedingungen herausgegeben hat. Dies wäre ein wesentlicher Schritt in Richtung informationelle Selbstbestimmung, denn wer hat heutzutage schon den Überblick darüber, wo er welche Daten gelassen hat? Sobald der Standardisierungsprozess abgeschlossen ist, ist zu erwarten, dass P3P von den Marktführern in den gängigen Browsern integriert wird.

Was ist zu tun?
P3P sollte zusammen mit weiteren Datenschutz-Tools in Deutschland schnell implementiert werden, um das Teledienstedatenschutzgesetz technisch umzusetzen. Mit einer Weiterentwicklung von P3P müssen weitere Datenschutz-Features abgedeckt werden.

8.7 Bringt Open Source mehr Datenschutz?

Mit der Sicherheit heutiger Software steht es nicht zum Besten. Derzeit wird diskutiert, ob Open Source eine bessere Softwarequalität und angemessenere Datenschutz- und Datensicherheitsfunktionalität bringt.

Wie bereits im letzten Tätigkeitsbericht vorgestellt, bedeutet Open Source eine erhöhte Transparenz und die Möglichkeit der Prüfung und Revision durch unabhängige Experten (vgl. 22. TB, Tz. 7.5). Dadurch kann die Vertrauenswürdigkeit der Software gesteigert werden.

Wenn jeder in den Quellcode der Programme Einblick nehmen kann, wird kaum ein Programmierer absichtlich Hintertüren einbauen. Die **Qualität** von Open-Source-Software ist damit aber **nicht automatisch besser**. Auch dort werden – genauso wie bei anderer Software – des Öfteren Fehler entdeckt, die möglicherweise schon jahrelang Sicherheitsrisiken verursacht haben. Dies liegt zum einen daran, dass heutzutage häufig der Code bei Software so komplex ist, dass er kaum mehr zu durchschauen ist, geschweige denn die möglichen Wechselwirkungen mit anderen Systemkomponenten. Zum anderen kann es recht zufällig sein, ob überhaupt und wie gründlich die Software evaluiert wird.

? Open Source

Open Source bedeutet „offene Quelle". In Open-Source-Projekten werden im Gegensatz zur Closed-Source-Softwareentwicklung, bei der der Programmquellcode als zu verbergendes Geschäftsgeheimnis verstanden wird, die Programminterna frühzeitig allen Interessierten offen gelegt. Diese sind gleichzeitig zur Mitarbeit an der Entwicklung aufgerufen. In einigen Bereichen, gerade im Internet, haben die kostenlosen Open-Source-Produkte schon weite Verbreitung gefunden und sich zu De-facto-Standards entwickelt.

Ein Unterschied zum herkömmlichen Closed-Source-Modell liegt darin, dass erkannte Schwachstellen in Open-Source-Software meist wesentlich schneller behoben werden: Es ist nicht untypisch, dass der „**Patch**" („Flicken", Fehlerkorrektur) gleich zusammen mit der Meldung des Fehlers verteilt wird. Auch können solche Fehler oft selbst zeitnah behoben werden, sofern das nötige Know-how vorhanden ist. Aus diesem Grund empfiehlt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Einsatz von Open-Source-Produkten.

Aus Datenschutzsicht bestehen generell folgende **Erwartungen** an Software:

- Der Quellcode, aus dem das lauffähige Programm erzeugt wird, muss tatsächlich von vertrauenswürdigen Stellen überprüft (gegebenenfalls zertifiziert) werden.
- Die fertige Software muss bei ihrer Verteilung gegen unerkannte Manipulationen geschützt sein. Daher sollten Quellcode und lauffähiges Programm mit einer digitalen Signatur versiegelt sein.
- Betreuung, Fehlerbearbeitung und Weiterentwicklung müssen sichergestellt sein.

Die zweite Anforderung wird traditionell in den meisten Open-Source-Projekten erfüllt. Für den ersten und dritten Punkt treten im Open-Source-Bereich mittlerweile meist herstellerunabhängige Dienstleister auf, die diesen Service anbieten. Wir sehen in Open Source eine interessante Chance auch für die Entwicklung und Verbreitung von **Privacy Enhancing Technologies**, bei denen die Vertrauenswürdigkeit eine besonders wichtige Rolle spielt. Daher setzen wir in unseren Projekten „Virtuelles Datenschutzbüro" (vgl. Tz. 9.1) und „WAU – Webzugriff anonym und unbeobachtbar" sowie AN.ON (vgl. Tz. 9.2) Open-Source-Produkte ein. Die dort entwickelten Ergebnisse wollen wir ebenfalls als Open Source der Internet-Öffentlichkeit zur Verfügung stellen.

Inwieweit man bestehende Systeme auf Open-Source-Produkte umstellen sollte, hängt von vielen Faktoren ab (siehe z. B. die Open-Source-Broschüre des Bundeswirtschaftsministeriums). Egal ob Open Source oder nicht: Ohne angemessenes **IT-Know-how** bei Nutzern und Administratoren ist der Einsatz von Informationstechnik ein Risiko.

Was ist zu tun?
Die Bundes- und die Landesregierung sollten den Einsatz von Open-Source-Systemen zumindest parallel zu Standardprodukten in ihren Bereichen fördern.

8.8 Von der „digitalen" zur „elektronischen" Signatur

Der europäische Gesetzgeber hat grünes Licht für die Einführung interoperabler digitaler Signaturen gegeben. Nun müssen die europäischen Vorgaben in das deutsche Recht umgesetzt werden.

Grundansatz der europäischen Signaturrichtlinie (vgl. 21. TB, Tz. 7.5 und Tz. 8) ist es, die Bereitstellung von Zertifizierungsdiensten nicht von einer vorherigen Genehmigung abhängig zu machen. Auf Betreiben der deutschen Seite findet sich jedoch ein Passus, wonach das nationale Recht Verfahren der „**freiwilligen Akkreditierung**" vorsehen kann, bei denen Anbieter sich freiwillig einer technisch-organisatorischen Prüfung unterziehen. Neben der „einfachen elektronischen Signatur" sieht die Richtlinie eine so genannte „**fortgeschrittene elektronische Signatur**" vor. Diese muss ausschließlich dem Unterzeichner, einer natürlichen Person, zugeordnet sein, dessen Identifizierung ermöglichen, mit Mitteln erstellt sein, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann (gemeint sind z. B. Chipkarten), und in einer Weise mit den zu signierenden Daten verknüpft sein, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Diese fortgeschrittene elektronische Signatur ist nach den Vorgaben der Richtlinie dann der **Schriftform gleichzustellen**, wenn sie auf einem **qualifizierten Zertifikat** beruht und von einer sicheren Signaturerstellungseinheit erstellt worden ist. Wann Signaturerstellungseinheiten als sicher anzusehen sind, regelt die Richtlinie in einem Anhang. Der Inhalt eines qualifizierten Zertifikats entspricht etwa dem eines Zertifikats nach dem deutschen Signaturgesetz von 1997. Weitere Voraussetzung für die Erstellung eines qualifizierten Zertifikats ist, dass der Zertifizierungsdiensteanbieter eine Reihe technischer und rechtlicher Anforderungen in Bezug auf seine Zuverlässigkeit und den Einsatz bestimmter Technologien erfüllt. Im Ergebnis entspricht das Maß an technischer Sicherheit dem, was bereits in der ersten Fassung des deutschen Signaturgesetzes gefordert wurde. Die Richtlinie verlangt von den Mitgliedstaaten auch, dass durch ein Kontrollsystem die Einhaltung dieser Anforderungen bei den Anbietern überwacht werden muss, deren Zertifikate zur Erzeugung „fortgeschrittener elektronischer Signaturen" verwendet werden können.

Wegen der von der Richtlinie geforderten grundsätzlichen Zulassungsfreiheit muss die Einhaltung der Vorgaben nicht geprüft werden, bevor der Anbieter seinen Betrieb aufnimmt. Damit enthält die Richtlinie ein **Element der Unsicher-**

heit: Signaturen müssen der Schriftform gleichgestellt werden, ohne dass vorab tatsächlich geprüft wurde, ob die zur Erzeugung der Schlüssel verwendeten Verfahren und technischen Komponenten hinreichend sicher sind. Zum Ausgleich für dieses Risiko ordnet die Richtlinie eine **gesetzliche Haftung** der Zertifizierungsdiensteanbieter gegenüber Dritten an, die auf ein Zertifikat dieses Anbieters vertraut haben. Zur Abdeckung dieses Risikos haben die Anbieter entsprechende Haftpflichtversicherungen abzuschließen.

Das novellierte deutsche Signaturgesetz berücksichtigt die Vorgaben der Richtlinie. Es spricht nicht mehr von digitalen, sondern von elektronischen Signaturen. Den Anforderungen der EU zur Zulassungsfreiheit kommt das Gesetz dadurch nach, dass es lediglich vorschreibt, der zuständigen Behörde die Aufnahme des Betriebes eines Zertifizierungsdienstes anzuzeigen. Mit der Anzeige muss dargelegt werden, dass die materiellen Anforderungen an Fachkunde, Zuverlässigkeit und technische Sicherheit eingehalten werden. Die Regulierungsbehörde nimmt die Aufsicht über die Anbieter wahr und kann mit unterschiedlichen Maßnahmen für die Einhaltung der Vorgaben sorgen.

Das deutsche Recht bietet darüber hinaus aber die Möglichkeit einer **freiwilligen Akkreditierung** des Anbieters. In diesen Fällen wird vor der Aufnahme des Betriebes nachgeprüft, ob der Anbieter die hohen technischen Sicherheitsstandards tatsächlich einhält. Ist dies der Fall, kann er mit der Akkreditierung als dem Nachweis für umfassend geprüfte technische und administrative Sicherheit werben. Nur für akkreditierte Anbieter stellt die Regulierungsbehörde als Wurzelinstanz die benötigten Zertifikate aus, mit denen die Anbieter die an die Kunden ausgegebenen Zertifikate signieren. Insoweit wird auf der Basis der freiwilligen Akkreditierung das Verfahren beibehalten, das vom bisher geltenden Signaturgesetz vorgeschrieben war. Die Bundesregierung geht davon aus, dass sich das Vertrauen der Kunden auf die akkreditierten Anbieter konzentrieren wird. Damit könnte die durch die Richtlinie aufgezwungene Verfahrensunsicherheit behoben werden.

Zurzeit liegt dem Bundestag ein Gesetzentwurf zur Änderung der **Formvorschriften** im **bürgerlichen Recht** vor. Ziel ist eine jedenfalls partielle Gleichstellung der elektronischen Signatur mit der herkömmlichen Schriftform.

Zu den Grundanliegen des Datenschutzes gehört es, personenbezogene Daten vor Verfälschungen und Missbrauch zu schützen. Hier liegt die Stärke elektronischer Signaturen. Sie verhindern, dass Informationen auf dem Weg durch das Datennetz verfälscht werden, und ermöglichen es zu prüfen, ob Nachrichten tatsächlich von der Person stammen, die als Aussteller angegeben ist. So gesehen können elektronische Signaturen ein wichtiges Hilfsmittel zur technischen Absicherung des Rechts auf informationelle Selbstbestimmung sein. Problematisch wäre es allerdings, wenn der Gebrauch elektronischer Signaturen dazu zwingen würde, stets mit voller Identität aufzutreten. Viele Geschäfte könnten genauso gut unter einem Pseudonym abgeschlossen werden, das nur dann aufgedeckt wird, wenn es Probleme mit der Abwicklung oder der Zahlung gibt. Das Signaturgesetz kommt diesem Anliegen entgegen, indem es auch die Ausstellung **pseudonymer Signaturen** ermöglicht. Auf diesem Wege kann die Verwendung personenbezogener Daten

eingeschränkt werden, ohne dass die geschäftliche Sicherheit gefährdet wird. Es steht zu hoffen, dass sich pseudonyme elektronische Signaturen schnell am Markt durchsetzen. Eine wichtige Voraussetzung dafür ist, dass ihre Nutzung ohne Nachteil und diskriminierungsfrei möglich ist.

Was ist zu tun?
Die Anbieter von Internet-Diensten sollten die Möglichkeit schaffen, Geschäfte auch mit pseudonymen Signaturen abzuschließen. Die Zertifizierungsstellen sollten pseudonyme Zertifikate ohne diskriminierende Bedingungen bereithalten.

8.9 Carnivore – Der gierige „Fleischfresser“ vom FBI

Das amerikanische Federal Bureau of Investigation (FBI) hat Mitte des letzten Jahres ein neues „Lauschsystem“ vorgestellt. Durch dieses System mit dem Namen „Carnivore“ (Fleischfresser) soll es möglich sein, einen gezielten „Lauschangriff“ auf E-Mail und Datenkommunikation einer bestimmten Person durchzuführen. Auch E-Mails aus Deutschland können betroffen sein.

Das Computersystem Carnivore ermöglicht es, das „Fleisch“ aus einer unüberschaubaren Datenmenge herauszufiltern. Berichten zufolge soll das Programm Millionen von E-Mails pro Sekunde untersuchen und abfangen können. Naturgemäß werden dabei auch die **E-Mails von Unverdächtigen** belauscht.

Es ist allerdings nicht klar, wie Carnivore genau funktioniert. Es ist wahrscheinlich, dass auch **deutsche Kunden** amerikanischer Provider in Mitleidenschaft gezogen werden. Die amerikanischen Internet-Provider befürchten, dass ihre Datensicherheitsmaßnahmen durch Carnivore beeinträchtigt werden, da das Lauschsystem direkt an das Netzwerk des Providers angeschlossen wird. Kontrollverfahren sind offensichtlich nicht vorgesehen.

Nach Protesten von Bürgerrechtsgruppen und Politikern wurde das FBI im Wege eines Gerichtsverfahrens verpflichtet, Informationen über Carnivore offen zu legen. Zudem wurde auf Anregung des US-Justizministeriums eine Expertengruppe eingesetzt, die die „**Schnüffelsoftware**“ untersuchen soll. Ein erster Bericht dieser Gruppe wurde Ende des Jahres 2000 veröffentlicht und scheint mit heißer Nadel gestrickt worden zu sein. Wesentliche Punkte wie z. B. die Vereinbarkeit der Überwachungsroutinen mit der amerikanischen Verfassung sind nicht untersucht worden. Auch den Sicherheitslücken im Programm ist nicht genauer nachgegangen worden. Die ersten vom FBI veröffentlichten Informationen zu Carnivore lassen den Schluss zu, dass das Schnüffelsystem noch erheblich leistungsfähiger ist als erwartet. Bleibt zu hoffen, dass die amerikanische Öffentlichkeit weiterhin Druck gegen das unkontrollierte Belauschen ihrer elektronischen Kommunikation ausübt. Davon würde dann auch der deutsche E-Mail-Verkehr in die USA profitieren.

Was ist zu tun?
Wer E-Mails in die USA verschickt oder sich amerikanischer Provider bedient, sollte sich vorsehen.

9 Modellprojekte zur Weiterentwicklung des Datenschutzes

Seit Mitte 1999 laufen beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein Modellprojekte für einen besseren Datenschutz. Hier werden aktuelle Datenschutzthemen mit juristischem und informationstechnischem Know-how im Detail untersucht und geeignete Lösungen entwickelt. Ergebnisse können sein: Gutachten und Stellungnahmen zu einzelnen Aspekten, Beratung für Technikgestaltung, **Musterlösungen** für bestimmte Verfahren, Privacy-Tools oder auch Informationsmedien wie Faltblätter oder eine CD-ROM.

Von besonderer Bedeutung ist die enge **Verzahnung der Projekte** mit der Dienststelle. Nur so lassen sich notwendiges Spezialistenwissen und jahrelange Erfahrungen in die Projekte einbringen, sodass für gute und praxistaugliche Resultate gesorgt ist. Gleichzeitig profitiert die Dienststelle von den neuen Impulsen, die von den Projekten und ihren engagierten Mitarbeitern ausgehen. Einige Modellprojekte werden hier vorgestellt.

www.datenschutzzentrum.de/projekte/

9.1 Jetzt online: das virtuelle Datenschutzbüro

Interessiert Sie Datenschutz? Haben Sie Fragen? Wollen Sie mitreden? Mit dem virtuellen Datenschutzbüro steht jetzt ein geeignetes Internet-Portal zur Verfügung.

Zu einer ganzen Reihe von Themen haben die **Datenschutzinstitutionen**, die gemeinsam diesen **Service** (vgl. 22. TB, Tz. 8.4) aufbauen, bereits interessante Informationen bereitgestellt. Datenschutzthemen werden von „Moderatoren" betreut, Antworten auf häufig gestellte Fragen in internettypischen FAQs (Frequently Asked Questions) zusammengefasst. Das virtuelle Datenschutzbüro dient außerdem als Wegweiser, wer für Ihre individuellen Anliegen zuständig ist.

> ***? Virtuelles Datenschutzbüro***
>
> *Das virtuelle Datenschutzbüro ist ein gemeinsamer Service von Datenschutzinstitutionen aus aller Welt. Auf der Website findet man alle möglichen Informationen rund um den Datenschutz und kann sich an Diskussionsforen beteiligen.*
>
> ***http://www.datenschutz.de***

Als **Plattform** für alles, was mit Datenschutz zu tun hat, enthält es neben vielen wichtigen Informationen Diskussionsforen, in denen sich die Nutzer zu Datenschutzfragen austauschen oder zu spannenden Projekten zusammenfinden können. Nicht nur professionelle Datenschützer, sondern auch alle anderen Experten, interessierte „Freaks" und „Privacy-Aktivisten" sollen mit ihren Kenntnissen das virtuelle Datenschutzbüro mitgestalten.

Als **Projektpartner** sind zurzeit die Datenschutzbeauftragten des Bundes sowie der meisten Länder in Deutschland, der norddeutschen Bistümer der katholischen Kirche, der Evangelischen Kirche Deutschlands, aus der Schweiz, den Niederlanden, der Slowakei und Kanadas beteiligt. Über die technischen Methoden des virtuellen Datenschutzbüros können sie einfacher als bisher kooperieren und durch Arbeitsteilung, Spezialisierung und systematische Bündelung ihrer Ressourcen ihre Effizienz steigern. Alle Datenschutzbeauftragten sind zur Mitarbeit eingeladen.

Die Konzepte für das virtuelle Datenschutzbüro sind vom **Unabhängigen Landeszentrum für Datenschutz** entwickelt worden, das auch für die nächsten zwei Jahre die **Geschäftsführung** im Projekt innehaben wird. Von hier aus wird das technische Rückgrat mit Schwerpunkt auf Privacy Enhancing Technologies bereitgestellt. Außerdem werden diverse Themenbereiche betreut. Das Projekt wird im Rahmen der **Initiative Informationsgesellschaft Schleswig-Holstein** seit Juli 1999 gefördert; die Unterstützung der Technologiestiftung Schleswig-Holstein hat zur Entwicklung des Prototyps beigetragen.

In der nächsten Zeit wird das virtuelle Datenschutzbüro sukzessive inhaltlich und technisch ausgebaut. Nicht nur die schleswig-holsteinischen **Bürger**, sondern auch die **Verwaltung** und die hier ansässige **Wirtschaft** werden vom Datenschutzbüro profitieren: sei es durch das Informationsangebot, die vielfältigen Foren zum Mitmachen oder die Ergebnisse der Projekte, von denen einige bereits beim Unabhängigen Landeszentrum für Datenschutz laufen (vgl. Tz. 9.2 und 9.3).

Kontakt:
Das virtuelle Datenschutzbüro im Web

deutsche Sektion:	http://www.datenschutz.de
Schweizer Sektion:	http://www.datenschutz.ch
international:	http://www.privacyservice.org

9.2 Prototyp für Webanonymisierungsdienst in Betrieb

Der Nutzer hinterlässt beim Surfen im Internet permanent Datenspuren. Längst haben Firmen das Potenzial erkannt, das sich in den darin verborgenen Interessen und Nutzungsprofilen der Netzteilnehmer widerspiegelt, und sammeln diese personenbezogenen Informationen zielbewusst für kommerzielle Zwecke. Aktuelle Umfragen zeigen, dass die Internet-Teilnehmer um ihre Daten im Netz besorgt sind: Mit dem E-Commerce geht es deshalb nicht so recht voran.

Für ein „Safer Surfen“ im Internet kann man im eigenen Browser konfigurieren, keine Cookies und keine Verwendung von aktiven Inhalten wie ActiveX, JavaScript oder Java zuzulassen (vgl. 21. TB, Tz. 7.1.2). Außerdem kann man die Kommunikation verschlüsseln. Dies alles hilft aber noch nicht gegen die Datenspuren, die automatisch hinterlassen werden: Kennungen, die den Surfer identifizieren können. Abhilfe sollen unsere Anonymitätsprojekte schaffen.

- Im Projekt „**WAU – Webzugriff anonym und unbeobachtbar**“, das bis Mitte 2001 durch die Initiative Informationsgesellschaft Schleswig-Holstein gefördert wird, geht es um Anonymität bei „Ecstasy Online“, einer Drogenberatung im Web, die an der Medizinischen Universität Lübeck angebunden ist (vgl. 22. TB, Tz. 8.2).
- „**AN.ON – Anonymität online**“, seit Anfang 2001 gefördert durch das Bundesministerium für Wirtschaft und Technologie, baut auf den Ergebnissen von WAU auf. Dieses Projekt hat das Ziel, einen Anonymitätsdienst anzubieten, der anwendungsunabhängig auch gegenüber dem Betreiber des Dienstes bzw. dem eigenen Serviceprovider Anonymität und Unbeobachtbarkeit garantiert und jedem Nutzer frei zur Verfügung steht. Nach der dreijährigen Projektlaufzeit soll nicht nur das anonyme Surfen, sondern ebenso die anonyme Nutzung weiterer Internet-Dienste möglich sein. Auch die noch offenen Rechtsfragen, die sich im Zusammenhang mit einer solchen anonymen Nutzung stellen, sollen dann geklärt sein.

> ***? Anonymisierung durch Mixe***
>
> *Mixe sind Netzknoten, die bei der Kommunikation zwischengeschaltet werden. Sie sammeln eingehende Nachrichten, kodieren sie um und leiten diese anschließend verschlüsselt weiter. Sofern mindestens ein Mix in einer Kette aus mehreren Mixen vertrauenswürdig arbeitet, sind die darüber versandten Nachrichten anonym.*

Ein erstes Tool, das von der Technischen Universität (TU) Dresden in Zusammenarbeit mit uns realisiert wird, ist der **Java Anon Proxy** (JAP), der als Open-Source-Projekt (vgl. Tz. 8.7) entsteht. Installiert auf dem heimischen Rechner, kann der Nutzer mithilfe so genannter Mix-Proxys, die sein eigentliches Surfziel für alle Dritten unkenntlich machen, über die Strecke seines Datenstroms selbst entscheiden. So sind derzeit als Mix-Stationen die Medizinische Universität Lübeck, die Rheinisch-Westfälische Technische Hochschule Aachen und die TU Dresden in verschiedenen Kombinationen wählbar. Einige Firmen haben zugesagt, ebenfalls Mixe zu betreiben. Auch das Unabhängige Landeszentrum für Datenschutz wird einen eigenen Mix zur Verfügung stellen.

Beratungsdienste im Internet wie Drogenberatung oder Telefonseelsorge, bei denen es um besonders sensible Daten der Nutzer geht, beginnen mittlerweile, ihre traditionellen Angebote nicht nur um eine Verschlüsselung der Daten, sondern auch um die Funktion eines anonymen Zugangs, z. B. mit dem JAP, zu erweitern. Auch für Wahlen oder andere E-Government-Anwendungen ist eine starke Anonymität im Netz vonnöten.

Neben den technischen Arbeiten für die Realisierung von Anonymitätsdiensten sind Untersuchungen zu den notwendigen bzw. hinreichenden Randbedingungen einer möglichen Deanonymisierung gegenüber Ansprüchen verschiedener Bedarfsträger erforderlich. Dies bedeutet ein Abwägen, wie weit das Recht auf Anonymität für jeden Internet-Nutzer geht und wo Beschränkungen, etwa im Interesse der Strafverfolgung, akzeptabel sind. Die Ergebnisse unserer Überlegungen sollen in die **internationale Standardisierung** zu Anonymität in Netzen einfließen. Mitarbeiter der TU Dresden und des Unabhängigen Landeszentrums für Daten-

schutz sind Mitglieder der zu diesem Zweck gegründeten transatlantischen Forschungsgruppe „NymIP“. Auf diese Weise können die in Deutschland gesammelten Erfahrungen und Ideen über die Grenzen hinweg Einfluss haben.

Die ersten Ergebnisse des Anonymitätsprojektes und das Anonymitäts-Tool JAP befinden sich im Internet unter:

www.datenschutzzentrum.de/anon/
anon.inf.tu-dresden.de/

9.3 Biometrische Verfahren im Feldversuch: das Pilotprojekt BioTrusT

Mussten wir in den letzten Jahren noch auf Agentenfilme verweisen, um biometrische Verfahren wie Zutrittskontrollen per Fingerabdruck oder Iriserkennung, Stimmprobe oder Gesichtserkennung zu erklären, so haben wir es jetzt einfacher: Immer häufiger berichten Medien über automatisierte Erkennungsverfahren, die den menschlichen Körper vermessen; die einschlägigen Computerzeitschriften stellen neue Produkte vor und vergleichen diese in Produkttests. Auch die Passworteingabe am PC oder die PIN bei Mobiltelefonen kann durch einen Daumenabdruck ersetzt werden.

> ***? Biometrie***
>
> *Durch biometrische Geräte können ganz unterschiedliche Merkmale von Menschen wie Gesicht, Fingerabdruck, Sprachprofil oder Muster der Iris, aber auch die Dynamik der Unterschrift oder des Tastaturanschlags erfasst werden, um eine automatisierte Erkennung vorzunehmen. Zur Erhöhung der (Ausfall-)Sicherheit können auch verschiedene Merkmale kombiniert werden.*

Bereits in den letzten Tätigkeitsberichten (vgl. 21. TB, Tz. 7.2, und 22. TB, Tz. 8.3) wurde über **biometrische Verfahren** berichtet, die eine Legitimation einer Person nicht wie bisher durch *Besitz* (z. B. mittels einer Scheck- oder Chipkarte) oder *Wissen* (z. B. mittels einer PIN oder eines Passworts), sondern durch körperliche Charakteristika vornehmen. Diese Merkmale werden durch Sensoren (z. B. Kameras, Mikrofone oder Spezialsensoren für Fingerabdrücke) erfasst. Danach werden sie anhand eines mathematischen Modells umgerechnet und mit bereits früher erfassten und gespeicherten **Referenzdaten** verglichen. Stimmen sie mit diesen Daten im Rahmen einer gewissen Schwankungsbreite überein, wird eine Aktion ausgelöst: Das Mobiltelefon schaltet sich ein, eine Tür öffnet sich, eine Computerfestplatte wird ver- oder entschlüsselt. Es sind viele Anwendungen denkbar oder schon in Planung, so z. B. die Autorisierung von elektronischen Signaturen (vgl. 22. TB, Tz. 8.3; 21. TB, Tz. 7.5, und 20. TB, Tz. 7.2) oder die Ergänzung von Personalausweisen mit biometrischen Daten.

Wie hängen nun **Datenschutz** und biometrische Verfahren zusammen? Bei biometrischen Merkmalen handelt es sich nicht nur um personenbezogene, sondern um **dauerhaft personengebundene Merkmale** – diese Bindung ist ja gerade der Vorteil gegenüber Passwörtern, die leicht vergessen, weitergegeben oder ausge-

späht werden können. Biometrische Daten können sensibel und daher besonders schützenswert sein, denn es ist möglich, dass sich noch **zusätzliche Informationen**, etwa über Krankheiten, Stimmungslagen oder Drogenkonsum, jetzt oder in Zukunft aus den biometrischen „Rohdaten" (d. h. den Bildern von Personen oder Körperteilen wie den Augen, Stimmaufnahmen usw.) herauslesen lassen. Meistens werden aber die biometrischen Daten für einen ganz anderen Zweck (z. B. zur Zutrittskontrolle) erhoben und müssen daher vor einer unbefugten zweckentfremdeten Auswertung geschützt werden. Eine datenschutzgerechte Gestaltung erfordert, dass die Referenzdaten allein in der **Verfügungsgewalt des Betroffenen** verbleiben (z. B. verschlüsselt auf einer Chipkarte).

Das Pilotprojekt **BioTrusT**, das von der Arbeitsgruppe „Biometrische Identifikationssysteme" von TeleTrusT e. V. ins Leben gerufen wurde, untersucht seit April 1999 die Einsatzmöglichkeiten von biometrischen Verfahren bei Banken und im Bereich E-Commerce. In der ersten von vier Phasen wurden zunächst Geräte getestet, die den Zutritt der Mitarbeiter zu ihrem Arbeitsgebäude bzw. ihren Arbeitsräumen regeln. In den weiteren Phasen werden Computerzugangsverfahren, Geldausgabeautomaten und Homebanking-Anwendungen untersucht. Neben dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, dem Verbraucherschutz und einer sozioökonomischen Begleitforschung durch die FH Gießen-Friedberg sind dabei etliche Hersteller und verschiedene Bankinstitutionen beteiligt. Da viele Hersteller international agieren und Standards und Normen wie etwa zur Speicherung biometrischer Daten auf Prozessorchipkarten (so genannten SmartCards), aber auch Sicherheitsprofile (so genannte Protection Profiles) für Sicherheitsevaluationen nach den Common Criteria (vgl. 21. TB, Tz. 7.6) international abgestimmt werden, ist das Projekt BioTrusT auch in solchen (nationalen und internationalen) Normungsgremien wie **ISO** oder **DIN** oder bei Industriestandards wie **BioAPI** beteiligt, die über kurz oder lang die Gestaltung aller biometrischen Systeme beeinflussen.

Für eine datenschutzgerechte Gestaltung der Biometrie ist es notwendig, dass schon in einer frühen Phase die technische Gestaltung der Geräte und der organisatorische Ablauf exakt ermittelt und festgestellte Probleme behoben werden. Auf einem so sensiblen Gebiet wie der Biometrie muss der Datenschutz schon in der **Konzeptionsphase** von Geräten und bei Entwürfen von Normen mit eingebunden werden. Nur bei transparenter und vertrauenswürdiger Gestaltung lässt sich die Akzeptanz der Benutzer erreichen und obendrein die Datensicherheit erhöhen.

Weitergehende Informationen:

www.datenschutzzentrum.de/biometrie/
www.biotrust.de

9.4 Sichere IT-Nutzung in Aus- und Weiterbildung

Die Vermittlung von Medienkompetenz an den Schulen muss verbessert werden. Eine neu entwickelte CD soll dabei helfen.

Die allgemein bildenden und die Berufsschulen werden zunehmend mit PC ausgestattet und an das World Wide Web angeschlossen. Die Schulen kreieren ihre eigenen Homepages und stellen Berichte, aber auch Fotos von Schülern, Lehrern oder dem Schulgebäude ins Netz. Daneben wird mit personenbezogenen Daten im täglichen Umgang größtenteils locker umgegangen. Zumeist wird auf die Vermittlung von **Medienkompetenz** zu wenig geachtet. Kaum einer der Schüler, gleich welchen Bildungsstandes und Alters, kennt z. B. das Recht auf informationelle Selbstbestimmung und die sich für ihn hieraus ergebenden Rechte und Pflichten. Viele lernen in der Schule zwar, wie man ins Internet kommt, aber sie wissen nicht, wie man sich dort schützt.

Das Projekt „**Sichere IT-Nutzung in Aus- und Weiterbildung**“ wurde im August 2000 ins Leben gerufen und hat zum Ziel, bei Schülern die Medienkompetenz zu verbessern. Die Schüler sollen spielerisch und möglichst effizient in die Thematik eingewiesen werden, eigene Einsichten gewinnen und Wertvorstellungen entwickeln.

Zu diesem Zweck soll in Zusammenarbeit mit dem Bundesministerium für Bildung, Wissenschaft, Forschung und Kultur sowie der Unternehmens- und Informations-Management-Consulting Wuppertal in den nächsten zwei Jahren eine interaktive, multimediale **CD-ROM** entwickelt werden, wobei das Unabhängige Landeszentrum für Datenschutz die Beratung bei Sicherheitsfragen, bei allgemeinen datenschutzrechtlichen Belangen und beim Thema Verschlüsselung übernommen hat. Gegenstand der CD ist es, die Probleme des Datenschutzrechts in gesamtgesellschaftlichen Zusammenhängen in einer für die Zielgruppe verständlichen Form aufzuzeigen, die Gefahren des Datenmissbrauchs in der Privatsphäre darzustellen sowie den Schülern Möglichkeiten zu vermitteln, einen möglichst effektiven Schutz ihrer Privatsphäre auch im Zusammenhang mit der IT-Nutzung zu erreichen.

10 Aus dem IT-Labor

10.1 BackUP-Magazine entwickeln sich zu Bestsellern

Die backUP-Magazine, die als Hilfsmittel für schleswig-holsteinische Behörden gedacht waren, haben bundesweit Aufmerksamkeit gefunden. Die Nachfrage übersteigt alle Erwartungen.

Die im letzten Tätigkeitsbericht vorgestellte Neugestaltung unserer sicherheitstechnischen Hilfestellungen für die Praktiker (vgl. 22. TB, Tz. 11.2) ist unerwartet positiv aufgenommen worden. Bisher haben wir **zwei backUP-Magazine** herausgegeben: eines zum Thema „Planung, Erstellung und Umsetzung von IT-Sicherheitskonzepten“, das andere befasst sich mit dem Komplex „MS-Windows NT – Sicherheitsmaßnahmen und Restrisiken“. Obwohl wir sie grundsätzlich nur für die Bedürfnisse der Daten verarbeitenden Stellen im Lande entwickelt und keine gezielte Werbung betrieben haben, kommen täglich neue Bitten um Überlassung von Exemplaren aus ganz Deutschland auf unseren Schreibtisch. Hier zeigen sich die Auswirkungen der Präsentation unserer Arbeit auf der Homepage im Internet (seit kurzem auch im virtuellen Datenschutzbüro) und des Erfahrungsaustausches in Kreisen der behördlichen und betrieblichen Datenschutzbeauftragten. Die Auflage der Magazine liegt derzeit bei 4.000. Ein Rückgang der Nachfrage ist nicht absehbar.

Schleswig-Holstein DATENSCHUTZAKADEMIE
Kurse NT-I, NT-II

Leider lässt die personelle Ausstattung unseres IT-Labors und die notwendige Priorität der Prüfungs- und Beratungstätigkeiten eine zügige Bearbeitung der vielen von den Praktikern vorgeschlagenen zusätzlichen Themenbereichen nicht zu. Wir streben gleichwohl an, jährlich ein bis zwei backUP-Magazine herauszugeben.

http://

www.datenschutzzentrum.de/material/themen/edv/backup/

10.2 Windows 2000 erfordert erhebliche Investitionen

Die Ausgestaltung des IT-Labors und die Ausbildung der Prüfer und Berater des Unabhängigen Landeszentrums für Datenschutz richten sich nach der IT-Landschaft in den schleswig-holsteinischen Behörden. Weil demnächst viele Betriebssysteme von Windows NT auf Windows 2000 umgestellt werden, muss das ULD nicht unerhebliche Investitionen tätigen.

Das **informationstechnische Know-how** unserer Mitarbeiterinnen und Mitarbeiter und die Hard- und Softwareausstattung unseres **IT-Labors** orientieren sich in erster Linie an den Produkten und Verfahrensweisen, die konkret in der schleswig-holsteinischen Verwaltung eingesetzt werden. Obwohl eine Vielzahl von Betriebssystemen, Datenbankgeneratoren, Bürokommunikationspaketen und Standardapplikationen auf dem Markt angeboten werden, kommt in Schleswig-Hol-

stein nur ein begrenzter Ausschnitt aus diesem breiten Spektrum zum Einsatz. Auf der Betriebssystemebene und im Bereich der Bürokommunikationssoftware sind dies im Wesentlichen Produkte der Firma Microsoft.

Dies hat zur Folge, dass wir in unserem IT-Labor für Zwecke der Beratung der Behörden, der Aus- und Fortbildung unserer Mitarbeiter und zu Testzwecken mehrere Konfigurationen auf der Basis des Betriebssystems Windows NT vorhalten. Es handelt sich dabei um ein **Referenzsystem**, das wir der in den meisten kleineren Behörden (z. B. Gemeinden und Ämtern) eingesetzten Hard- und Software möglichst genau nachgebildet haben, um typische Schwachstellen und deren Behebung zu analysieren bzw. zu erproben. Ein weiteres System dient vorwiegend für „Experimente". Es unterliegt ständigen Veränderungen, um Lösungsansätze für die Behebung von grundsätzlichen Sicherheitsschwächen in den marktgängigen Produkten zu entwickeln und um uns besonders interessierende Softwareprodukte unter sicherheitstechnischen Aspekten testen zu können (Beispiele: Wie effektiv sind allgemein verfügbare Passwort-Crack-Programme tatsächlich? Wie leicht bzw. wie schwierig ist es für einen „normalen" Benutzer, die Grenze zur Administrationsebene zu durchbrechen? Steckt tatsächlich eine Firewall drin, wo „Firewall" draufsteht?). Ein drittes System dient primär zu Demonstrations- und Schulungszwecken. An ihm wird den Mitarbeiterinnen und Mitarbeitern der geprüften bzw. beratenen Behörden dargestellt, welche tatsächlichen Auswirkungen die von uns vorgeschlagenen Maßnahmen und Verfahrensweisen zur Verbesserung der Datensicherheit haben (Vorher-nachher-Effekt).

Diese fein aufeinander abgestimmte Systemlandschaft ist in den letzten drei Jahren mit nicht unerheblichen Kosten aufgebaut worden (vgl. 22. TB, Tz. 9.3 bis 9.5). Sie wird so lange genutzt werden können, wie das Betriebssystem **Windows NT** in der schleswig-holsteinischen Verwaltung zum Einsatz kommt.

Da dieses Betriebssystem aber in nächster Zeit in vielen Daten verarbeitenden Stellen durch das Betriebssystem **Windows 2000** abgelöst wird, bedarf es auch in unserem IT-Labor entsprechender Hardware-, Software- und Schulungsinvestitionen. Es ist praktisch nicht möglich, die unterschiedlichen Softwareprodukte wechselweise auf der gleichen Hardware ablaufen zu lassen. Der dadurch entstehende Umrüstaufwand lässt einen effektiven Testbetrieb nicht zu. Deshalb haben wir im abgelaufenen Jahr damit begonnen, unser IT-Labor um eine Sektion „Windows 2000" zu ergänzen. Das bedeutet im Ergebnis eine Verdoppelung des Hardwarebestandes und der Softwarelizenzen. Wenn im Jahr 2001 entsprechende Räumlichkeiten zur Verfügung stehen, kann die Maßnahme abgeschlossen werden.

Daneben hat die Ausbildung und das Training unserer Prüfer und Berater begonnen. Da nur wenige Schulungsanbieter in Deutschland Kurse auf dem für uns erforderlichen Niveau (es macht einen Unterschied, ob Administratoren oder die Kontrolleure der Administratoren ausgebildet werden) anbieten, müssen wir die in der Wirtschaft üblichen hohen „**Consulting-Tarife**" akzeptieren. Hinzu kommt, dass die Funktionalität des Betriebssystems Windows 2000 gerade im Bereich der Sicherheitseinstellungen so umfangreich ist, dass eine Schmalspurausbildung mehr Probleme brächte, als sie löst. Wir gehen davon aus, dass die Gesamtkosten für

eine umfassende Ausbildung pro Prüfer/Berater über mehrere Jahre verteilt ungefähr 25.000 DM betragen werden.

Bei der Bereitstellung der entsprechenden Finanzmittel ist zu bedenken, dass es sich weder bei den Hard- und Softwareinvestitionen noch bei der Aus- und Fortbildung der Mitarbeiter um optionale Maßnahmen handelt, sondern um eine „**Conditio sine qua non**“, um der Prüfungs- und Beratungsaufgabe gemäß dem LDSG auch künftig gerecht werden zu können.

10.3 Datenspione aus dem Internet – was hilft?

Stets wird vor den Risiken aus dem Internet gewarnt – doch wie groß ist die Gefahr tatsächlich, dass die eigenen Daten ausspioniert werden? In unserem IT-Labor sind wir der Frage nachgegangen, welche Angriffsmethoden bei welchen Systemkonfigurationen Erfolg versprechend sind. Aus den Ergebnissen dieser Untersuchungen leiten wir dann die notwendigen Sicherheitsmechanismen ab.

Um zu verstehen, wo überall ein Internet-Angriff ansetzen kann, muss man sich die **Technik** bei der **Internet-Anbindung** verdeutlichen:

- Der Nutzer arbeitet an seinem Computer, auf dem meist zumindest ein Browser zur WWW-Nutzung und ein E-Mailprogramm installiert sind.
- Sein Computer ist über eine Netzwerkkarte oder ein Modem mit dem Gateway ins Internet verbunden, das der Provider zur Verfügung stellt.
- Die Kommunikation im Internet läuft über eine Vielzahl von Rechnern unterschiedlicher Betreiber ab. Diese Rechner leiten beispielsweise E-Mails und Webanfragen in Form von Datenpaketen weiter. Webserver, die die Angebote enthalten, antworten auf Webanfragen.

An all diesen Punkten können Angreifer aktiv werden. Die **Angriffe** unterscheiden sich im Vorgehen:

- **Angriffe von außen**

Die Angreifer können versuchen, eine unmittelbare Verbindung über das Internet zu dem Zielobjekt herzustellen. Bei den Rechnern des Nutzers geht dies nur, wenn dieser online, also mit **angeschaltetem Modem**, arbeitet und so konfiguriert ist, dass er eingehende Verbindungen gestattet. Nur wenige Nutzerrechner müssen eingehende Verbindungen erlauben. Anders ist dies dort, wo fernadministriert wird, Telearbeit realisiert ist oder bestimmte Dienste, wie etwa auf einem Webserver, angeboten werden.

Für das direkte Aufbauen von Verbindungen muss dem Angreifer die Rechneradresse bekannt sein. Wird eine dynamische IP-Adresse aus einem größeren Pool verwendet – wie bei den meisten Nutzern, die sich über Provider einwählen –, wechselt die Zuordnung zwischen Rechner und Adresse bei jeder Einwahl. Dies

erschwert einen spezifischen Angriff auf einen Nutzercomputer. Einige Nutzer und alle Diensteanbieter haben statische, d. h. nicht ständig wechselnde IP-Adressen, sodass in diesen Fällen ein spezifischer Angriff leichter möglich ist.

Häufig werden bei der Internet-Nutzung **Proxys** (Stellvertreter) eingesetzt, deren Adresse nach außen bei allen Anfragen sichtbar wird. In vielen Fällen sind die dahinter liegenden Rechner gar nicht aus dem Internet adressierbar; eine direkte Verbindung kann also nicht von außen hergestellt werden.

- **Infektionen aus dem Netz**

Der Nutzer kann sich selbst versehentlich bösartige Inhalte auf den Rechner holen: Die **Infektionswege** für Viren und Trojanische Pferde sind vielfältig. Jeder Datenaustausch kann Gefahren bergen, ob über Diskette, CD-ROM oder Internet, ob per E-Mail, Dateiendownload oder aktive Inhalte auf Webseiten. Die bösartigen Programme schleichen sich über denselben Zugang ein, den auch die nützlichen Inhalte nehmen. Auf dem Zielrechner angekommen, können sie eine beliebige Funktionalität, meist lediglich eingeschränkt durch die Zugriffsrechte des Nutzers, entfalten, z. B. die Daten manipulieren oder löschen, E-Mails verschicken, selbst Verbindungen im Internet aufbauen und Daten von der Festplatte übertragen.

Viele **Viren** und **Trojaner** erlangen weite Verbreitung. Sind sie erst einmal den Virenjägern aufgefallen, werden die Antivirenprogramme um neue Abwehrstrategien erweitert und aktualisiert. Es ist aber auch denkbar, dass Trojanische Pferde individuell zugeschnitten werden, um ein einzelnes Rechnersystem spezifisch anzugreifen. Ein solches gezieltes Ausspionieren kann jahrelang unentdeckt bleiben und sehr viel mehr Schaden anrichten als beispielsweise der I-LOVE-YOU-Wurm.

Die **Schadensfunktion** kann in einem E-Mail-Anhang (Attachment) versteckt sein, unter bestimmten Bedingungen reicht sogar der **E-Mail-Text**, der von einigen Windows-Mailprogrammen als Code interpretiert wird. Auch angehängte Visitenkarten können bösartige Funktionen auslösen. Wir haben in unserem IT-Labor unter Ausnutzung bekannter Softwarefehler einen Angriff entwickelt und untersucht, bei dem der Angreifer eine E-Mail an das Opfer schickt. Diese E-Mail hat nach dem Anzeigen dafür gesorgt, dass eine Verbindung, analog zum Surfen im Web, zu einem vom Angreifer kontrollierten Rechner aufgebaut wurde und darüber dann Daten von der Festplatte – unbemerkt vom Betroffenen – übertragen wurden.

- **Missbrauch von Knotenrechnern**

Auch wenn der Rechner selbst nicht aus dem Internet heraus angegriffen werden kann, sind die Daten nicht sicher: Eine Methode besteht darin, die **Zwischenrechner** im Internet zu attackieren und dann ihre Kommunikation mitzulesen oder zu verändern.

Welche Schutzmechanismen gibt es? Was hilft wo?

Korrekt installierte und gewartete **Firewalls** (vgl. 22. TB, Tz. 7.1.1) helfen gegen Zugriffe, die gegen vorab definierte Regeln verstoßen. Damit kann man also beispielsweise recht gut einen unerwünschten Verbindungsaufbau aus dem Internet heraus unterbinden. Zur Absicherung von lokalen Netzen setzt man hier in der Regel eigene Firewall-Rechner ein, für den Hausgebrauch bei einem Privatnutzer tut es oft auch eine PC-Firewall-Software auf dem Computer.

Firewalls helfen aber nicht gegen Viren und Trojanische Pferde. Zusätzliche **Inhaltsfilter** können immerhin bekannten bösartigen Code herausfiltern. Dies funktioniert aber nur dann auf den Firewalls, wenn dort die Kommunikation unverschlüsselt abläuft. Zusätzlich sollte man also auf allen Nutzerrechnern selbst ebenfalls aktuelle Antivirussoftware bereithalten.

Sind die Trojaner noch nicht bekannt oder individuell vom Angreifer zugeschnitten, helfen Virenscanner oder verwandte Tools nicht. Man kann versuchen, das Übel dadurch in den Griff zu bekommen, dass besonders anfällige Mechanismen deaktiviert oder solche Programme ersetzt werden. Dies bedeutet meist gleichzeitig einen Verzicht auf eine gewisse Funktionalität – hier muss man also abwägen. Auf jeden Fall sollte man unbekannte aktive Komponenten wie **ActiveX**, **Active-Scripting** oder **VisualBasicScripting** deaktivieren, da sich damit quasi beliebige (bösartige) Funktionen ausführen lassen. Auch **Java** und **JavaScript** können Risiken bergen. Inwieweit man sich einschränkt, was akzeptierte Dateiformate (Makrovirenrisiko), eingesetzte Browser, Mailprogramme und Betriebssysteme (bei Häufung von sicherheitsrelevanten Fehlern) oder den Zugriff auf unbekannte Webseiten angeht, muss von Fall zu Fall festgelegt werden.

Bei der Anbindung eines lokalen Netzes an das Internet wird man häufig eine sehr restriktive Policy allerdings nur schwer durchsetzen können. Jede Freischaltung weiterer Funktionen – z. B. durch neue Anforderungen nach einiger Zeit – kann riskant sein. Aus diesem Grund haben wir für das **virtuelle Datenschutzbüro** (vgl. Tz. 9.1) eine Konfiguration realisiert, die zusätzlich zur herkömmlichen Absicherung mit einem Firewall-System eine weitere Schutzzone vorsieht. In dieser dem internen Netz vorgelagerten Zone wird die Internet-Nutzung von den Arbeitsplätzen aus ferngesteuert, d. h. Tastatur- und Mauseingaben werden weitergeleitet, die Grafikausgabe gelangt zurück auf die Monitore der Mitarbeiter. Die Methode für diese Fernsteuerung heißt **VNC – Virtual Network Computing** und wurde als Open-Source-Programm von AT&T entwickelt. In unserer Konfiguration läuft die Software auf Linux-Rechnern, die gegen die weit verbreiteten auf Microsoft-Produkte zugeschnittenen Angriffe immun sind. Sollte es zu einem Angriff kommen, können wegen des Fernsteuerungsmechanismus im internen Netz prinzipiell keine Daten von außen eingesehen oder Programme ausgeführt werden.

Eine **goldene Regel** gibt es im Bereich der Datensicherheit, speziell für die Nutzung des Internets: Es werden ständig neue Sicherheitsrisiken entdeckt, auf die man umgehend durch „Patchen“ des Systems reagieren muss. Denn: „Sicherheit ist kein Produkt, sondern ein Prozess.“ (Bruce Schneier)

10.4 PGP-Server als „Big SmartCard“

Eine sichere Einbindung von Kryptosoftware wie „PGP – Pretty Good Privacy“ könnte konzeptionell am besten über eine SmartCard realisiert werden, die die jeweiligen (geheimen) Schlüssel enthält. Da eine solche SmartCard-Lösung nicht zur Verfügung stand, haben wir in unserem IT-Labor für das virtuelle Datenschutzbüro eine Art Nachbau einer solchen Funktionseinheit in Form eines speziellen PGP-Servers entwickelt.

Dieser PGP-Server arbeitet über ein definiertes Protokoll mit **OpenSSL** (Secure Socket Layer) auf TCP/IP-Basis. Die Clients tauschen die PGP-Befehle und Daten mit dem Server über ein Skript aus. Der PGP-Server hat die Aufgabe, das PGP-Verschlüsselungsprogramm sowie die dazugehörigen öffentlichen und geheimen Schlüssel vorzuhalten und die kryptographischen Operationen auf diesem gesonderten Rechner ablaufen zu lassen. Die Handhabung verschlüsselter E-Mails soll für die Nutzer einfach und transparent sein.

? SSL

SSL (Secure Socket Layer) ist ein Verschlüsselungsprotokoll, das in gängigen Internet-Browsern eingebaut ist. Damit können die übertragenen Daten auf dem Weg nicht von Unbefugten im Klartext mitgelesen werden. OpenSSL ist eine frei verfügbare Implementierung von SSL und weiteren kryptographischen Routinen. Als Spezifikation wird OpenSSL von einer unabhängigen Gruppe weiterentwickelt.

Im Rahmen des virtuellen Datenschutzbüros schalten wir für den Internet-Zugriff der Dienststelle einen **Virtual-Network-Computing**-Server (VNC) zwischen (vgl. Tz. 10.3). Verschlüsselte Dateien direkt in das interne Netz zu übertragen ist unpraktikabel und stellt obendrein ein Sicherheitsrisiko dar, weil der Inhalt vor dem Entschlüsseln nicht auf Viren und Trojanische Pferde geprüft werden kann. Auf der anderen Seite ist das Risiko unbefugter Zugriffe auf die geheimen Schlüssel vorhanden, wenn sie auf einer Festplatte gespeichert sind (z. B. Zugriff bei Diebstahl des Rechners). Ferner besteht das Risiko, dass auf dem VNC-Server andere Programme bzw. Benutzer Manipulationen vornehmen. Aus diesen Gründen ist eine physikalische Trennung der Verarbeitungslogik zwingend erforderlich. Als weitere Schutzmaßnahme lässt sich das Dateisystem des PGP-Servers von außen nicht ansprechen, die Konsole ist gesperrt, und die PGP-Schlüssel befinden sich nur im Arbeitsspeicher.

? VNC

Mit dem Prinzip des VNC (Virtual Network Computing) kann ein Server ferngesteuert werden: Die Tastatur- und Mauseingaben von angeschlossenen Rechnern werden an den VNC-Server übertragen, wo die eigentlichen Programme ablaufen. Die Grafikausgabe wird dabei auf diejenigen Rechner umgelenkt, von denen die Anfragen gestartet wurden. Das VNC-Programm wurde von AT&T entwickelt und liegt als Open-Source-Software vor.

Die Methode, die PGP-Schlüssel auszulagern, ist in einer Dienststelle zum Zweck der Ver- und Entschlüsselung dienstlich relevanter Daten unproblematisch. Eine

Auslagerung eines **mitarbeiterbezogenen, geheimen Signierschlüssels** außerhalb des jeweiligen Mitarbeiterbereichs kommt jedoch nicht infrage, da eine Nutzung durch Unberechtigte und damit ein unberechtigtes Auftreten unter der Identität eines anderen Mitarbeiters nicht ausgeschlossen werden kann: Möchte man also über die Verschlüsselung hinaus den Mitarbeitern individuelle digitale Signaturen ermöglichen, die ihnen zurechenbar sein sollen (z. B. für Willenserklärungen oder Mitzeichnungszwecke), müssen die Signierschlüssel im persönlichen Bereich des Mitarbeiters verbleiben (vgl. Tz. 8.8).

10.5 Versteckt und doch entdeckt – verborgene Daten in Dateien

Textdateien, die mit weit verbreiteten Bürokommunikationsprodukten erstellt werden, enthalten mehr Informationen, als im Ausdruck schwarz auf weiß zu sehen ist. Diese Informationen verraten dabei einiges über den Autoren und die Entstehungsgeschichte einer Datei. Dies kann dann zu einem Problem werden, wenn solche Dateien nicht ausgedruckt, sondern im Web publiziert oder per E-Mail weitergegeben werden.

Wird bei der Installation des Textverarbeitungsprogramms WinWord beispielsweise ein Autorenname eingegeben, so wird dieser automatisch mit jedem neu erstellten Dokument verknüpft. Die Weitergabe des Autorennamens kann bei Firmen oder Behörden unerwünscht sein. Außerdem ist der Empfänger einer solchen Datei in der Lage abzurufen, wann der Autor die Datei erstellt, zuletzt geändert, geöffnet, gedruckt und gespeichert hat und wie lange sie für Bearbeitungen geöffnet war. Daten wie diese lassen sich zur Arbeitsplatzüberwachung benutzen oder können in strategisch relevanten Situationen Rückschlüsse auf die Schwierigkeiten der Texterstellung zulassen. In dieser Hinsicht noch schwerer wiegt allerdings, dass der Empfänger sogar die vollständige **Entstehungsgeschichte eines Textes** nachvollziehen kann, sofern der Autor die „Änderungsfunktion“ benutzt hat. Diese wird insbesondere dann gern verwendet, wenn mehrere Autoren nacheinander an einem Text arbeiten. Öffnet man eine solche Textdatei mit einem ASCII-Editor, der sämtliche Zeichen einer Datei anzeigt, lassen sich weitere unter der Oberfläche schlummernde Informationen zutage fördern: Man findet die Namen der Rechner und der Verzeichnisse, in denen der Text zwischenzeitlich gespeichert war, was Rückschlüsse auf die interne Organisation und ein etwaiges „Konfliktmanagement“ ermöglicht. Weitaus gravierender aber ist, dass man auch gelöschte Textpassagen in der Datei gespeichert wiederfindet: Das verständlicherweise häufig genutzte „Schnellspeichern“ löscht in der Datei keine Texte, sondern markiert sie nur als gelöscht.

Möchte man sichergehen, dass solche Daten in elektronischen Publikationen oder bei der Weitergabe per E-Mail nicht mehr enthalten sind, dann empfiehlt es sich generell, beim endgültigen Abspeichern ein **anderes Format** zu wählen. Soll die Datei weiterverarbeitbar sein, so bietet sich dafür das von Microsoft standardisierte Rich Text Format (RTF) an. Hierbei ist zu beachten, dass die mittels der Änderungsfunktion erstellten und nacheinander verworfenen Textbestandteile nicht verschwinden. Zusätzlich in Kauf genommen werden muss, dass Feinheiten des Layouts nicht erhalten bleiben, etwaig genutzte Formatvorlagen verloren gehen

können und nicht gewährleistet ist, dass ein anderes Textverarbeitungsprogramm dieses Format fehlerfrei einlesen kann.

Unser IT-Labor hat die Tücken von Office-Programmen, wenn sie in einen elektronisch gestützten Workflow eingebunden sind, systematisch untersucht und **Gegenmaßnahmen** oder **Alternativen** für einige Fälle entwickelt. Es zeigt sich, dass in erschreckend vielen Fällen der Empfänger einer solchen Datei heikle und vor allem auch falsche Informationen erhält, weil dem Autoren seitens der Programme keine hinreichende Kontrolle über den Inhalt seines Dokuments eingeräumt wird.

Tipps zu diesem Problem werden veröffentlicht unter:

www.datenschutzzentrum.de/it-labor/

10.6 Privacy-Tools für souveräne Bürger

Das Recht auf informationelle Selbstbestimmung bedarf nicht nur der gesetzlichen, sondern auch der technischen Unterstützung. Effektives Identitätsmanagement könnte genau der richtige Ansatz sein.

Nutzerprofile überall im Internet – die Datenschützer schlagen Alarm! Was wäre aber mit der Möglichkeit, dass die Nutzer selbst Profile mit ihren Daten anlegen und bestimmen, unter welchen Umständen sie wem welche Daten geben? Dies ist die Grundidee von **Identitätsmanagement**, der technischen Umsetzung des Rechts auf informationelle Selbstbestimmung.

Manche **Privacy-Tools** (vgl. 22. TB, Tz. 9.3) schmücken sich bereits mit dem Etikett „Identitätsmanagement“. Wir haben einige davon in unserem IT-Labor unter die Lupe genommen. Ergebnis: Nichts davon realisiert wirklich den erhofften Datenschutz.

Die Nutzer haben zwar bei einigen Produkten die Möglichkeit, mehrere Profile mit eigenen Daten anzulegen und zu verwalten, doch bei fast allen Produkten (z. B. Digitalme, Persona oder Microsoft Passport) lagern die **Nutzerinformationen auf den Servern der Anbieter**. Selbst wenn die Nutzer auswählen können, unter welchen Umständen sie wem welche Daten offenbaren, erfährt der Anbieter über seinen Server alles: die gesamten Daten und sogar Teile über den Anwendungskontext, in dem sie genutzt werden (z. B. ein Online-Einkauf) – der Wolf im Schafspelz.

Die Auswahl zwischen verschiedenen Profilen erfolgt in der Regel rein manuell. So gut dies für die Transparenz ist – der Nutzer, der explizit sein Profil freischaltet, ist sich dessen bewusst –, so leicht kann man die Auswahl des Profils vergessen oder dabei einen Fehler machen: Schon hat man ungewollt seine Daten hergegeben. Stattdessen sollte der Nutzer hier besser unterstützt werden, z. B. mit einer **Protokollierung**, wann man welche Profile genutzt hat – selbstverständlich auf der eigenen Festplatte und nicht wieder auf dem Anbieterserver.

Die Dienste laufen im Internet ab – mit all seinen Schwächen, was Datenschutz angeht. Nur wenige Anbieter nutzen **standardmäßig Verschlüsselung**, Anonymität ist selbstverständlich nicht gegeben. Hier ist also eine Ergänzung mit Anonymitäts- und anderen Datensicherheits-Tools (vgl. Tz. 9.2) notwendig.

Alle Dienste sind speziell auf bestimmte Anwendungen zugeschnitten, noch fehlt ein Standard, der eine **universellere Nutzung** möglich macht.

Alles in allem zeigt sich, dass es zurzeit keineswegs umfassende Identitätsmanager für mehr Selbstdatenschutz im Netz gibt. Allerdings existieren einige **hoffnungsvolle Ansätze**: Erste Tools belassen die Daten beim Nutzer und sehen automatisch eine Verschlüsselung vor. Für mehr Universalität ist der Online-Privacy-Standard P3P (vgl. Tz. 8.6) prädestiniert: Seine Implementierungen könnten verschiedene eigene Profile im Nutzerbereich unterstützen. Dies kann ein Weg sein, um wirkliches Identitätsmanagement für alle Aktionen im Netz auf die Schiene zu setzen und damit den Nutzern einen selbstbestimmten Datenschutz zu ermöglichen.

11 Europa

11.1 Europäische Grundrechtecharta

In der vom Europäischen Rat in Nizza in einer Erklärung proklamierten Charta der Grundrechte der Europäischen Union ist auch das Grundrecht auf Schutz personenbezogener Daten verankert. Die Union setzt damit einen in den letzten Jahren deutlich erkennbaren Akzent auf die Verbesserung des Datenschutzes.

Das Ergebnis von Nizza mag insofern unbefriedigend erscheinen, als eine rechtsverbindliche Verabschiedung der Grundrechtecharta als Teil der Unionsverträge nicht erfolgte und die Charta vom Europäischen Rat lediglich im Wege eines **feierlichen Bekenntnisses** beschlossen wurde. Allerdings verweist Art. 6 Abs. 2 EUV bereits auf die Achtung der Grundrechte, wie sie in der Europäischen Menschenrechtskonvention (EMRK) und in den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten gewährleistet sind. Solange kein Konsens über die rechtsverbindliche Verabschiedung der Grundrechtecharta als Teil einer europäischen Verfassung erzielt ist, wird das gemeinsame Bekenntnis zu den Formulierungen der Europäischen Grundrechtecharta auch hierüber Eingang in die Rechtsanwendung der Union, insbesondere in die Rechtsprechung des EuGH, finden können.

In Art. 8 der Charta wurde explizit ein **Datenschutzgrundrecht** festgeschrieben und mit den grundlegenden Maßgaben für seine Ausgestaltung und Durchsetzung versehen. Die Charta verlangt eine Einhaltung der Zweckbindung, des Gesetzes- oder Einwilligungsvorbehalts sowie des Auskunfts- und Berichtigungsanspruchs der betroffenen Person und gibt damit die tragenden Grundsätze des Datenschutzrechts, wie sie auch in der Datenschutzrichtlinie der EU enthalten sind, in knapper Form vor. Auch die Garantie einer institutionalisierten, unabhängigen Datenschutzkontrolle als wesentliche Voraussetzung dafür, dass dieses Grundrecht mit Leben gefüllt wird, ist bereits in Art. 8 der Charta niedergelegt.

Unabhängig von der formellen primärrechtlichen Einordnung der Grundrechtecharta stellt die Aufnahme des Datenschutzgrundrechts einen weiteren Meilenstein in dem Bemühen der EU dar, auf europäischer Ebene **Schrittmacher in Sachen Datenschutz** zu sein (vgl. auch die nachfolgenden Tzn.).

Was ist zu tun?
Die Grundrechtecharta sollte rechtsverbindlich gemacht werden.

11.2 Cyber-Crime Convention

Vom Europarat wird gegenwärtig der Entwurf einer Konvention, einer so genannten Cyber-Crime Convention, ausgearbeitet. Darin soll ein weit reichender internationaler Mindeststandard der Strafbarkeit sowie der prozessualen Eingriffsbefugnisse und internationalen Rechtshilfenormen für die Bekämpfung von Computerkriminalität festgeschrieben werden. Bislang ist der Entwurf einseitig auf die Strafverfolgung ausgerichtet und berücksichtigt weder rechtsstaatliche Anforderungen noch datenschutzrechtliche Belange. Die EU-Kommission ist inzwischen mit einer ausgewogeneren Initiative mit präventiver Schwerpunktsetzung an die Öffentlichkeit getreten.

Der Entwurf einer Cyber-Crime Convention des Europarats soll bereits in diesem Jahr unterschriftsreif und potenziell weltweit anwendbar sein. Anders als es der Titel suggeriert, geht es in dem Entwurf nicht nur um Internet-Kriminalität, sondern auch um die **Verfolgung sonstiger Computerdelikte**. Darüber hinaus sollen ganz allgemein Befugnisse der Strafverfolgungsbehörden zum Zugriff auf elektronisch gespeicherte Daten geschaffen bzw. international vereinheitlicht werden. Die Verpflichtungen der Staaten aus der Konvention sollen – abgesehen von besonderen Rechtshilferegelungen – unabhängig von der grenzüberschreitenden Natur der Straftaten und Ermittlungsmaßnahmen gelten.

Der Europaratsentwurf greift tief in entscheidende aktuelle Fragestellungen der nationalen Rechtspolitik ein. Wie weitgehend das Recht von Nutzern auf Anonymität in der Informationsgesellschaft im Verhältnis zur Strafverfolgung sein kann, welche Datenspuren in Netzen vorgeschrieben werden sollen, inwieweit Selbstschutzmaßnahmen gegen fremde Datenzugriffe zugunsten staatlicher Behörden beschränkt werden dürfen, welche Kommunikation für eigene Zwecke oder für fremde Staaten durch Strafverfolger belauscht werden darf, all dieses haben **demokratisch legitimierte Gesetzgebungsorgane** zu entscheiden. Auch wenn es auf der Hand liegt, dass zur Bekämpfung von Computerkriminalität oder zur Gewinnung elektronischer Beweise für sonstige Strafverfolgung eine internationale Zusammenarbeit unerlässlich ist, dürfen Regierungen die Parlamente in diesem hochbrisanten Bereich nicht im Wege der Begründung völkerrechtlicher Bindungen vor vollendete Tatsachen stellen. Vielmehr muss im Vorwege ausreichender demokratischer Konsens hergestellt werden. Eine Vielzahl der im Entwurf vorgesehenen Regelungen betreffen Eingriffsbefugnisse, die in Deutschland auch gegenwärtig eine ausgeprägte rechtspolitische Debatte zum Hintergrund haben.

Eine im europäischen Rahmen zustande kommende internationale Vereinbarung über Strafverfolgung im Bereich von elektronischen Netzen darf nicht **einseitig Eingriffsbefugnisse** der sensibelsten Art wie Abhörbefugnisse und Aufzeichnung von Verbindungsdaten zum Inhalt haben, sondern muss gleichermaßen im Sinne eines internationalen **Mindeststandards an Rechtsstaatlichkeit** einen angemessenen Schutz der Grundrechte von Nutzern und unbeteiligten Dritten gewährleisten. Die rechtsstaatliche Ausgestaltung von Straftatbeständen und prozessualen Ermittlungsmaßnahmen überlässt der Entwurf jedoch der Disposition der Unterzeichnerstaaten. Der Konventionsentwurf lässt eine immerhin in seiner Präambel

beschworene Balance zwischen Strafverfolgungsinteressen und Grundrechtsschutz im Text vollkommen vermissen.

Dieses grundsätzliche Defizit ist auch im Bereich der **Rechtshilfevorschriften** festzustellen. Wenn sich die Staaten zur Übermittlung hochsensibler personenbezogener Informationen verpflichten sollen, so muss die Konvention selbst bereits für einen **angemessenen Datenschutzstandard** im Empfängerland sorgen.

Besonders schwieriges Terrain wird mit der Einführung einer **Strafbarkeit so genannter „Hacking-Tools“** beschritten. Es bedarf einer sorgfältigen Diskussion unter Einbeziehung von Experten der Datensicherheit, um zu klären, ob mit einer solchen Strafnorm nicht gleichzeitig Selbstschutzmaßnahmen gefährdet werden, die angesichts der Unmöglichkeit staatlicher Sicherheitsgewährleistungen für die Integrität von Datennetzen anerkanntermaßen immer unverzichtbarer werden.

Ebenso sensibel ist die geplante Einführung von **aktiven Mitwirkungspflichten Privater** bei Strafermittlungen über bestehende Pflichten zum Bereitstellen von Überwachungsschnittstellen hinaus. Sollen – anders als bisher im deutschen Strafprozess – etwa Systemadministratoren im Einzelfall zur Preisgabe von Schlüsseln oder Kennwörtern gezwungen werden können? Was soll für Zeugnisverweigerungsberechtigte gelten? Auch diese Frage hat derart weit reichende Implikationen, dass sie nicht originär auf der Ebene einer exekutiv dominierten internationalen Vereinbarung beantwortet werden darf.

Aus Sicht des deutschen Datenschutzrechts erscheinen auch Verpflichtungen zur Aufzeichnung und Sicherstellung von **Inhalts- und Verbindungsdaten** untragbar, die tatbestandlich völlig unklar bleiben. Die in der deutschen Multimediagesetzgebung verankerten Grundsätze der Datenvermeidung und -sparsamkeit dürfen nicht auf internationalem Wege untergraben werden. Darüber hinaus darf es auch in anderen Staaten nicht zur Einführung einer Vorratshaltung von Datenbeständen kommen, sofern ihre Speicherung nicht im Einzelfall durch einen konkreten Straftatenverdacht veranlasst wird.

Bei der Durchführung von Abhör- und anderen Ermittlungsmaßnahmen in **Rechtshilfe** für andere Staaten muss nicht nur – wie im Entwurf bereits vorgesehen – die Einhaltung der Rechtsvorschriften des ersuchten Staates, sondern auch das Vorliegen einer entsprechenden justiziellen Anordnung im ersuchenden Staat gewährleistet werden. Nur wenn der Zugriff auf personenbezogene Daten in beiden Rechtsordnungen rechtlich zulässig ist, kann verhindert werden, dass Rechtshilfe zu einem Instrument der Umgehung eigener rechtsstaatlicher Anforderungen missbraucht werden kann.

Im Januar 2001 veröffentlichte nun die **EU-Kommission** einen eigenen Vorschlag zur international koordinierten Bekämpfung von Computerkriminalität, in dem sie sich auch kritisch mit der Europaratsinitiative auseinandersetzt. Bemerkenswert erscheint an dem Vorschlag, der in einem transparenten Verfahren öffentlich diskutiert werden soll, dass die EU-Kommission **technische Sicherheitsmaßnahmen** wie starke Verschlüsselung – und damit den **Selbstschutz der Nutzer** – an

erste Stelle setzt. So könne auch das dringend erforderliche Vertrauen der breiten Bevölkerung in die Datensicherheit beim E-Commerce gestärkt werden.

Die Kommission dringt auf die Berücksichtigung des nach den geltenden EU-Richtlinien im Bereich Datenschutz und Telekommunikation bereits erreichten **Schutzes der Privatsphäre** gegenüber Abhörmaßnahmen und anderen Befugnissen der Strafverfolgungsbehörden. Insbesondere gegenüber einer generellen Mindestspeicherung von **Verbindungsdaten** erhebt die Kommission Bedenken und verweist auf das **Recht auf anonyme Nutzung** von Datennetzen, welches lediglich in begrenzten und begründeten Einzelfällen zu durchbrechen sei. Die Kommission möchte eine Koordinierungsrolle bei der Meinungsbildung der EU-Mitgliedstaaten im Rahmen der Europaratsinitiative übernehmen.

Damit sind die auch aus unserer Sicht zentralen Belange in die Diskussion eingebracht, die im Rahmen der internationalen Zusammenarbeit zur Computerstraftatenbekämpfung sorgfältig zu berücksichtigen sind. Nunmehr ist zu hoffen, dass die durch den Cyber-Crime-Konventionsentwurf berührten rechtspolitischen Fragestellungen aus dem Hinterstübchen internationaler Expertengremien dorthin gebracht werden, wo sie in einer Demokratie hingehören, nämlich in die **öffentliche Diskussion** und in die **Parlamente**. Wir werden uns an dem Diskussionsprozess beteiligen, um auch für die Zukunft eine freie Teilnahme der Mehrheit der rechtstreuen Nutzer des Internets an der Informationsgesellschaft zu sichern. Eine Stellungnahme zum Konventionsentwurf des Europarats haben wir dem Justizministerium zugeleitet.

www.datenschutzzentrum.de/material/themen/cybercri/

Was ist zu tun?
Die Justizministerin des Landes sollte sich auf Bundes- wie Europaebene aktiv für eine bürgerrechtsfreundliche Gestaltung einer Cyber-Crime Convention einsetzen.

11.3 Safe-Harbor-Principles

Mit der EU-Datenschutzrichtlinie verlangt die Europäische Gemeinschaft innerhalb des gesamten Bereichs der Europäischen Union ein einheitliches Mindestniveau an Datenschutz. Der Datenexport in Drittländer ist nur zulässig, wenn dort ein angemessenes Datenschutzniveau herrscht. In den USA soll dies mit den Safe-Harbor-Principles gewährleistet werden.

Die EU-Datenschutzrichtlinie hat die Einrichtung einer „**Datenschutzgruppe**“ vorgesehen, welche für die Kommission Stellungnahmen zum Datenschutzstandard des jeweiligen Empfängerlandes verfasst. Im Zusammenhang mit den USA hat die Datenschutzgruppe festgestellt, dass die Rechtsordnung dieses Staates nicht generell einen angemessenen Datenschutz gewährleistet.

Eine generelle Einstufung der USA als Drittland ohne hinreichenden Datenschutz hätte allerdings zur Folge gehabt, dass eine Weitergabe von personenbezogenen Daten – von einigen Ausnahmefällen abgesehen – nur mit Einwilligung der Betroffenen erfolgen dürfte.

Um diese Konsequenz zu vermeiden, haben sich die Europäische Union und die Vereinigten Staaten auf die so genannte „**Safe-Harbor**"-Regelung geeinigt. Diese Vereinbarung soll privaten Unternehmen mit Sitz in der Europäischen Union ermöglichen, denjenigen Stellen in den USA personenbezogene Daten zu übermitteln, die aufgrund ihrer Geschäftsbedingungen zum Datenschutz („Privacy Policy") auch nach unionsrechtlichen Bewertungsmaßstäben einen hinreichenden Datenschutz gewährleisten. Um im Bild des Begriffs „Safe Harbor" zu bleiben: Man soll diese Unternehmen wie einen sicheren Hafen im Meer der Daten verarbeitenden Stellen getrost ansteuern können.

Im Wortlaut: Art. 25 Absätze 2 und 6 EU- Datenschutzrichtlinie

(2) Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen, insbesondere werden die Art der Daten, die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort geltenden Staatsregeln und Sicherheitsmaßnahmen berücksichtigt.

(6) Die Kommission kann ... feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen ... hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet.

Wie sieht nun diese Vereinbarung inhaltlich aus? Die EU-Kommission und das US-amerikanische Handelsministerium haben im Zusammenwirken mit anderen Stellen **Leitlinien zum Datenschutz** ausgearbeitet. Diese Leitlinien sind teils in Grundsätze zum Datenschutz, teils in Antworten auf häufig gestellte Fragen (Frequently Asked Questions – FAQ) gefasst. Beispiele für zu beachtende Grundsätze sind etwa, dass die Datenempfänger angemessene Sicherheitsvorkehrungen zu treffen haben, um einen Verlust, Missbrauch und unbefugten Zugriff usw. zu verhindern, oder dass betroffenen Privatpersonen Auskunft über die über sie gespeicherten personenbezogenen Daten zu erteilen ist.

Das US-Handelsunternehmen veröffentlicht die Dokumente, welche den zu erfüllenden Datenschutzstandard beschreiben. Will nun eine Organisation in den Genuss der Vorteile der Safe-Harbor-Regelung kommen, muss sie sich öffentlich und eindeutig verpflichten, die in den Grundsätzen und FAQ geforderten Datenschutzstandards einzuhalten. Darüber hinaus muss sie den gesetzlichen Überwachungsbefugnissen der **Federal Trade Commission (FTC)** unterliegen, einer Institution, die für die Ahndung von Wettbewerbsverstößen zuständig ist. Wenn das beteiligte Unternehmen der FTC gegenüber seinen Beitritt zu den genannten Datenschutzstandards erklärt, nimmt das US-amerikanische Handelsministerium das betreffende Unternehmen in die Liste aller Safe-Harbor-Stellen auf. Danach gilt das Unternehmen als eine Stelle mit angemessenem Datenschutzniveau mit

der Folge, dass an sie personenbezogene Daten grundsätzlich ebenso übermittelt werden kann wie an eine Stelle mit Sitz in der Europäischen Union.

Eine datenschutzrechtliche Bewertung der Safe-Harbor-Regelung muss verschiedene Gesichtspunkte berücksichtigen. Das amerikanische System gründet stärker auf den Selbstschutz des Verbrauchers und ist damit schwerlich mit dem europäischen Datenschutzsystem vergleichbar. Einerseits fehlt es in den Vereinigten Staaten an einer umfassenden datenschutzrechtlichen Gesetzgebung, andererseits verfügt die FTC letztlich über wesentlich weiter reichende Befugnisse als die deutschen Aufsichtsbehörden. Die Werthaltigkeit der Vereinbarung, die offenbar von den US-amerikanischen Unternehmen nur zögerlich angenommen wird, wird sich erst in der Zukunft herausstellen.

Was ist zu tun?
Auch schleswig-holsteinische Unternehmen dürfen personenbezogene Daten an amerikanische Firmen nur dann übermitteln, wenn diese sich zur Einhaltung der Safe-Harbor-Principles verpflichtet haben.

12 Informationsfreiheit

12.1 Informationsfreiheitsgesetz in Kraft

Zeitgleich mit der Novelle des LDSG verabschiedete der Landtag das „Gesetz über die Freiheit des Zugangs zu Informationen für das Land Schleswig-Holstein" – das Informationsfreiheitsgesetz Schleswig-Holstein (IFG).

Schon im Rahmen der Verfassungsreform 1997 hatten wir die Aufnahme eines Grundrechts auf „**Teilhabe an der Informationsgesellschaft**" in die Landesverfassung vorgeschlagen. Damit sollte den gesellschaftlichen Auswirkungen der Entwicklung der Informations- und Kommunikationstechnik Rechnung getragen werden. Der neu aufzunehmende Artikel sollte u. a. bewirken, dass die Informationen aus dem öffentlichen Bereich allen zugänglich sind, soweit nicht schützenswerte Interessen Dritter oder das Wohl der Allgemeinheit dem entgegenstehen. Zwar hatte der Sonderausschuss „Verfassungsreform" die Aufnahme eines solchen Artikels empfohlen, doch die für eine Verfassungsänderung erforderliche Mehrheit kam im Landtag nicht zustande (vgl. 20. TB, Tz. 3.1).

Nachdem Brandenburg und Berlin mit Akteneinsichts- und Informationszugangsgesetzen vorangegangen sind, war die Zeit für einen allgemeinen Anspruch auf Informationszugang offenbar auch hier reif. Nicht zuletzt mit Blick auf die in Skandinavien schon seit Jahrzehnten geltenden vergleichbaren Gesetze legte der **SSW** im Frühjahr 1999 einen entsprechenden Entwurf für Schleswig-Holstein vor. Im November 1999 präsentierte dann auch das Innenministerium einen Gesetzentwurf, der das allgemeine Recht auf Informationszugang im Landesverwaltungsgesetz unterbringen wollte. Im Rahmen der schriftlichen Anhörung haben wir eine vergleichende Stellungnahme, die sich im Ergebnis für ein eigenständiges Informationsfreiheitsgesetz aussprach, gefertigt. So sah es auch der Innen- und Rechtsausschuss und empfahl dem Landtag die Verabschiedung des SSW-Entwurfs mit leichten Modifikationen. Das IFG wurde verabschiedet und trat am 25.02.2000 in Kraft.

Schleswig-Holstein befindet sich mit seinem Informationsfreiheitsgesetz in Übereinstimmung mit der europäischen Rechtsentwicklung. Auch der **Bund** und **andere Länder** haben angekündigt, den Zugang zu den Verwaltungsinformationen zu eröffnen. Art. 255 der **EU-Verträge** enthält bereits ein allgemeines Zugangsrecht zu den Dokumenten des Europäischen Parlaments, des Rates und der Kommission. Die EU hat angekündigt, bis Mai 2001 den Zugang zu den Informationen ihrer Organe zu eröffnen.

12.2 Worum geht es beim Informationsfreiheitsgesetz?

Mit der Verabschiedung des Informationsfreiheitsgesetzes hat der Landtag die öffentliche Verwaltung in Schleswig-Holstein vor völlig neue Aufgaben gestellt. Das darin enthaltene allgemeine Informationszugangsrecht bricht mit der Tradition der beschränkten Aktenöffentlichkeit.

Die Informationszugangsgesetze führen eine bislang nicht gekannte Öffentlichkeit der Verwaltung ein, indem sie einen verfahrensunabhängigen und **voraussetzungslosen Informationszugangsanspruch** für alle Bürgerinnen und Bürger gegenüber den Verwaltungen schaffen. In Zukunft muss nicht mehr das Akteneinsichtsgesuch begründet werden, sondern dessen Ablehnung. Dahinter steht die Absicht, die Arbeit der Behörden transparenter zu machen und die individuellen Möglichkeiten der Partizipation am politischen Prozess zu verbessern. Die Zeiten, in denen sich der Beitrag der Bürgerinnen und Bürger zur Gestaltung ihrer Gesellschaft auf die Wahlen beschränkte, sollen der Vergangenheit angehören.

So gegensätzlich die Anliegen der Informationsfreiheit und des Datenschutzes auf den ersten Blick sind, so eng sind sie miteinander verknüpft und voneinander abhängig. Letztlich basiert die Informationsfreiheit ebenso wie der Datenschutz auf dem **Recht auf informationelle Selbstbestimmung**. Das Abwehrrecht zum Erhalt der eigenen Verfügungsbefugnis über die persönlichen Daten setzt ein Recht auf Teilhabe an der Informationsgesellschaft voraus, denn nur wer hinreichend informiert ist, kann von seinen Rechten auch sinnvoll Gebrauch machen und an der politischen Mitgestaltung mündig teilnehmen. Das Gemeinwesen muss seine Bürgerinnen und Bürger daher in die Lage versetzen, sich über relevante Vorgänge ausreichend informieren zu können.

Selbstverständlich müssen die Zielsetzungen eines umfassenden Informationszugangs mit den Schutzzwecken des Datenschutzrechts harmonisieren. Die Behörden müssen die Gewissheit haben, dass sie sich bei einer informationsfreundlichen Gesetzesanwendung nicht in Widerspruch zu den **Grundsätzen des Datenschutzes** stellen. Das Informationsfreiheitsgesetz berücksichtigt dies, indem es den Zugang zu Informationen restriktiv regelt, sobald personenbezogene Daten Dritter betroffen sind. Daneben schützt es auch die privaten Belange von Unternehmen. Vor einer Offenbarung von Betriebs- und Geschäftsgeheimnissen muss genau geprüft werden, inwieweit ein Zugang gewährt werden kann, ohne die wirtschaftlichen Interessen des betroffenen Unternehmens zu beeinträchtigen.

Schließlich schafft das Gesetz auch einen Ausgleich zu etwaigen entgegenstehenden **öffentlichen Belangen**. Neben der Rechtsdurchsetzung in laufenden Justizverfahren sind hier insbesondere die Beziehungen zu anderen Staaten und Ländern, die Landesverteidigung und die innere Sicherheit zu nennen. Ferner bleiben auch solche Informationen vorenthalten, deren Bekanntgabe die Eigenverantwortlichkeit und Funktionsfähigkeit der Regierung oder den Erfolg behördlicher Entscheidungen gefährden kann.

12.3 Die Rolle des Unabhängigen Landeszentrums für Datenschutz

Ähnlich wie in Kanada, Brandenburg und Berlin ist auch in Schleswig-Holstein das Unabhängige Landeszentrum für Datenschutz für die Klärung von Streitfragen in dem Bereich des Informationszuganges zuständig.

Das Gesetz sieht vor, dass sich die Bürgerinnen und Bürger an den Landesbeauftragten für den Datenschutz – seit dem 01.07.2000 an das **Unabhängige Landeszentrum für Datenschutz** – wenden können, wenn sie der Meinung sind, dass ihr Informationsersuchen nicht rechtmäßig oder sonst wie unzureichend behandelt worden ist.

- Die **Bürgerinnen** und **Bürger** können sich mit Eingaben an uns wenden und sich von uns beraten lassen, wenn sich der Zugang zu den bei den Behörden vorhandenen Informationen schwierig gestaltet.
- Die dem Informationsfreiheitsgesetz unterliegenden **Behörden** sind verpflichtet, uns bei der Wahrnehmung der Aufgaben zu unterstützen, uns Auskunft zu erteilen und gegebenenfalls auch Zugang zu ihren Diensträumen und Informationen zu gewähren.
- Sind im Rahmen von Eingaben oder Prüfungen Mängel festzustellen, weil gegen die Vorschriften des Informationsfreiheitsgesetzes verstoßen oder aus sonstigen Gründen ein Informationszugang zu Unrecht verwehrt wird, kann dies **beanstandet** werden.

Neben diesen Aufgaben und Befugnissen steht für uns auch hier der **Servicegedanke** im Vordergrund:

- Die **Behörden** werden im Rahmen unserer Möglichkeiten beraten und informiert.
- Neben verschiedenen Veröffentlichungen in der Tagespresse und in der Fachliteratur wurde den Behörden in der Reihe *„Datenschutz leicht gemacht“* „**Tipps und Hinweise zum neuen Informationsfreiheitsgesetz**“ als eine erste Arbeitshilfe an die Hand gegeben.
- Gemeinsam mit den Projektpartnern in Brandenburg und Berlin wird über das **virtuelle Datenschutzbüro** sowohl für die Bürgerinnen und Bürger als auch für Behörden und sonstige an der Informationsfreiheit Interessierte ein vielfältiges Angebot zu diesem Thema erarbeitet und bereitgestellt.

Informationen zum Thema Informationsfreiheit:

auf der Homepage des ULD: www.datenschutzzentrum.de/informationsfreiheit/
im virtuellen Datenschutzbüro: www.datenschutz.de/recht/informationsfreiheit/

Schließlich bietet die DATENSCHUTZAKADEMIE Schleswig-Holstein eigenständige Kurse zum Informationsfreiheitsgesetz an, um den mit dieser Thematik befassten Behördenmitarbeiterinnen und -mitarbeitern eine Fortbildungsmöglichkeit zu bieten.

12.4 Zusammenarbeit mit anderen Informationsbeauftragten

Die bislang gesetzlich bestellten Beauftragten für Akteneinsicht und Informationszugang der Länder Brandenburg, Berlin und Schleswig-Holstein haben Ende August 2000 in Kiel die „Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland“ (AGID) gegründet und in diesem Rahmen eine regelmäßige Zusammenarbeit vereinbart.

Die Arbeitsgemeinschaft soll selbstständig neben der Konferenz der Datenschutzbeauftragten des Bundes und der Länder bestehen und sich über die datenschutzrechtlichen Bezüge hinaus mit allgemeinen und speziellen Fragen des Informationszugangs befassen. Die Mitglieder der **AGID** stehen den mit der Informationsfreiheit verbundenen Prinzipien der Verwaltungsöffentlichkeit und -transparenz positiv gegenüber. Auf dieser Basis wurde vereinbart, nicht nur zu Anwendungsproblemen der Akteneinsichts- und Informationsfreiheitsgesetze Stellung zu nehmen, sondern sich bei Bedarf auch zu „artverwandten“ Regelungen wie denen des Umweltinformationsgesetzes oder auch speziellen Akteneinsichtsrechten zu äußern. Eine weitere Sitzung der AGID hat im Dezember vergangenen Jahres in Potsdam stattgefunden und sich mit dem Entwurf eines Informationsfreiheitsgesetzes des Bundes befasst.

Neben der Arbeitsgemeinschaft wurde ein **Arbeitskreis** eingesetzt, in welchem Detailfragen behandelt werden. Der Arbeitskreis tagte erstmalig im September 2000 in Kiel. Er unterzog dabei die bestehenden Landesgesetze einem Rechtsvergleich. Die Teilnehmer hatten Gelegenheit, von ihren ersten Erfahrungen, Erfolgen und Schwierigkeiten zu berichten. Trotz der zum Teil recht großen Unterschiede zeichnet sich hier auf der Grundlage der übereinstimmenden Gesetzesanliegen eine fruchtbare Zusammenarbeit ab.

12.5 Beratung von Bürgerinnen, Bürgern und Behörden

12.5.1 Zusammenarbeit mit Behörden

Das Informationsfreiheitsgesetz stellt ein Novum für die schleswig-holsteinischen Behörden dar. Entsprechend intensiv ist der Beratungsbedarf. Behörden und Bürger möchten in Erfahrung bringen, welche konkreten Pflichten und Rechte das Informationsfreiheitsgesetz für sie bringt.

Die kommunalen Spitzenverbände der Gemeinden, Ämter und Städte unterstützen ihre Mitgliedskörperschaften bei der Umsetzung des Informationsfreiheitsgesetzes und haben uns dabei in die Diskussion und den Erfahrungsaustausch eingebunden. Der **Städteverband** gab uns sowohl das Ergebnis einer von ihm durchgeführten

Umfrage bei seinen Mitgliedern als auch eine bei der Hansestadt Lübeck erarbeitete Handreichung zum Informationsfreiheitsgesetz zur Kenntnis. Auf Bitte des **Schleswig-Holsteinischen Gemeindetages** (SHGT) wurde von uns sowohl auf der Herbsttagung der Bürgermeisterfachkonferenz als auch auf einer Sitzung des Rechts- und Verfassungsausschusses das Gesetz vorgestellt und anschließend mit den Teilnehmern diskutiert. Schließlich haben wir auf Bitte des SHGT aus unserer Sicht die ersten Erfahrungen in dessen Zeitschrift „**Die Gemeinde**" zusammengefasst. Alles in allem stellen sich die von den Behörden festgestellten Probleme aus unserer Sicht als **typische Anlaufschwierigkeiten** dar, die sich bei der Befassung mit einer neuen Rechtsmaterie regelmäßig einstellen und mit zunehmender Erfahrung bewältigen lassen.

www.datenschutzzentrum.de/material/recht/infofrei/erfaifg.htm

Das **Landesamt für Denkmalpflege** bat uns darum, bei der Erstellung eines Arbeitspapiers behilflich zu sein, welches das Informationsfreiheitsgesetz für die Denkmalschutzbehörden umsetzt. Die daraufhin erstellten „Hinweise zum Umgang mit Bürgeranträgen auf Akteneinsicht" befassen sich u. a. mit dem Verhältnis des Informationsfreiheitsgesetzes zu den Datenschutzvorschriften und Einsichtsregelungen im Denkmalschutzgesetz sowie zur Akteneinsicht im Verwaltungsverfahren.

Das Ministerium für Bildung, Wissenschaft, Forschung und Kultur bat uns um Stellungnahme zu der Frage, ob bzw. inwieweit auch **öffentliche Schulen** dem Informationsfreiheitsgesetz unterliegen. Diese Frage stellte sich, weil das Informationsfreiheitsgesetz in seiner Anwendung auf die Behörden im Sinne des allgemeinen Verwaltungsverfahrensrechts beschränkt ist, während das LDSG daneben auch „sonstige öffentliche Stellen" erfasst. Nach dem Wortlaut des Schulgesetzes sind Schulen nur teilweise Behörden und im Übrigen als nicht rechtsfähige Anstalten des öffentlichen Rechts dem jeweiligen Schulträger zuzurechnen. Dies hätte mit Blick auf das Informationsfreiheitsgesetz zu einer wenig plausiblen und unpraktischen Aufspaltung der schulischen Zuständigkeiten geführt. In Übereinstimmung mit einer Entscheidung des OVG Schleswig aus dem Jahre 1992 gehen wir davon aus, dass die öffentlichen Schulen insgesamt als Behörden anzusehen sind, sobald sie im Bereich der so genannten „**inneren Schulangelegenheiten**" selbstständig ihre Aufgaben wahrnehmen.

Im Zusammenhang mit dem gebotenen **Schutz personenbezogener Daten** erreichten uns u. a. folgende Anfragen:

- Ein Mieter wollte die Baugenehmigungsakte des von ihm bewohnten Hauses einsehen, um zu prüfen, ob der in seinem Mietvertrag zugrunde gelegte Quadratmeterpreis zutrifft.
- Die Besucherin eines Restaurants wollte gegenüber den Betreibern einen Schmerzensgeldanspruch geltend machen, weil sie in dem Restaurant verdorbenes Essen zu sich genommen hatte. Sie fragte deshalb beim Kreisgesundheitsamt nach den Ergebnissen der dort angestellten Ermittlungen.

- Neu hinzugezogene Bürger einer Gemeinde wollten sich darüber informieren, wie die für sie zuständige Amtsverwaltung die gemeindliche Baumschutzsatzung umsetzte, und beantragten Einsicht in sämtliche diesbezüglichen Genehmigungsakten aus dem vorangegangenen Jahr.

In Anlehnung an die Regelungen des LDSG über die Übermittlung von Daten an Private sieht auch das Informationsfreiheitsgesetz vor, dass personenbezogene Daten unter bestimmten Voraussetzungen offenbart werden dürfen. Eine dieser Ausnahmen liegt vor, wenn der Antragsteller ein **rechtliches Interesse** geltend machen kann, weil er etwa gegen den datenschutzrechtlich Betroffenen einen Anspruch verfolgt, der sich aus einer konkreten Rechtsbeziehung ergibt. Dies konnte in den beiden ersten hier geschilderten Fällen angenommen werden, weil konkrete vertragliche Beziehungen bestanden. Ob die Offenbarung trotz des bestehenden rechtlichen Interesses an etwaigen überwiegenden Belangen des Betroffenen scheitern musste, war von den Behörden noch zu prüfen. Im dritten Fall fehlte es an einem solchen konkreten Rechtsverhältnis; die Antragsteller wollten sich nur allgemein über die Rechtspraxis informieren. Der Behörde musste deshalb geraten werden, die erbetenen Informationen nur in anonymisierter Form herauszugeben oder – falls dies wegen der verbleibenden Grundstücksbezogenheit der Informationen nicht möglich war – ersatzweise nur eine statistikähnliche Auskunft über die Genehmigungspraxis zu erteilen.

Kurs IFG

12.5.2 Bürgeranfragen

Das Informationsfreiheitsgesetz hat keineswegs zu einem Massenansturm auf die Amtsstuben geführt. Allerdings ist es bei vielen Bürgerinnen und Bürgern auf breites Interesse gestoßen. Sie lassen sich auch schon im Vorfeld konkreter Informationsbegehren von uns beraten.

Folgende Beispiele erscheinen berichtenswert:

Darf ein Gemeindevertreter unter Verweis auf seine mit diesem Amt verbundene Verschwiegenheitspflicht bei einem allgemeinen Informationsgesuch anders behandelt werden als andere Bürgerinnen und Bürger? Natürlich nicht. Als **Gemeindevertreter** steht ihm nach der Gemeindeordnung ein amtsbezogenes Akteneinsichtsrecht zu, soweit dies für seine Aufgabenwahrnehmung erforderlich ist. Dabei gelten andere Voraussetzungen und Grenzen als beim allgemeinen Informationszugangsrecht. Ein Konkurrenzverhältnis in dem Sinne, dass eine Regelung die andere verdrängt, kann nicht angenommen werden. Ist eine Erforderlichkeit für die Akteneinsicht nach dem speziellen Recht nicht gegeben oder beruft sich der Gemeindevertreter von vornherein nur auf das allgemeine Informationszugangsrecht, wird ihm die Akteneinsicht nicht in seiner Funktion und nach dem speziellen Recht, wohl aber als „Jedermann“ nach dem Informationsfreiheitsgesetz gewährt – allerdings auch nur in dem Umfang und unter den Bedingungen, die das Informationsfreiheitsgesetz vorsieht. Es besteht damit auch keine Notwendigkeit, einen Auskunftssuchenden an seine – aus ganz anderen Gründen bestehende – Verschwiegenheitspflicht zu erinnern. Zur Vermeidung von Missverständnissen empfiehlt es sich für die Inhaber solcher besonderen Zugangsrechte allerdings,

von vornherein klarzustellen, in welcher Funktion die Informationen nachgefragt werden.

Kann ein Bürger Einsicht in **Sitzungsprotokolle** eines Naturschutzbeirates verlangen, obwohl die Sitzungen nach der geltenden Naturschutzbeiratsverordnung grundsätzlich nichtöffentlich sind und eine Teilnahme von Dritten nur auf Antrag und bei Vorliegen bestimmter Voraussetzungen zugelassen werden kann? Nähere Regelungen über den Zweck des Ausschlusses der Öffentlichkeit und des Umgangs mit Einsichtsbegehren hinsichtlich der Sitzungsprotokolle existieren im Naturschutzrecht des Landes nicht. Bei einem so pauschal formulierten Ausschluss der Öffentlichkeit kann unseres Erachtens nicht darauf geschlossen werden, dass auch der Zugang zu den in den Protokollen enthaltenen Informationen grundsätzlich zu verwehren ist. Eine Ablehnung des Zugangsantrags kommt nur infrage, wenn die protokollierte Beratung des Beirats **vertraulich** war. Dies muss im Einzelfall geprüft werden.

12.6 Konfliktfälle

Schon bei der Bearbeitung der ersten Eingaben zeigte sich die ganze Bandbreite der Fragestellungen zum Informationsfreiheitsgesetz. So aufgeschlossen und kooperativ sich manche Behörden verhielten, so ablehnend zeigten sich manch andere.

- **Scientology**

Eine der ersten Eingaben betraf den Antrag des „Menschenrechtsbüros der Scientology Kirche e. V." auf Informationszugang beim **Sektenbeauftragten** des Landes. Dessen Aufgabe ist es, die Betätigungen von Sekten oder sektenähnlichen Vereinigungen zu dokumentieren und darüber zu informieren, sobald der Verdacht besteht, dass von deren Aktivitäten Gefahren für Dritte ausgehen. Allein zum Thema „Scientology" werden dort insgesamt 34 Ordner geführt.

Über den Antrag hatte der Sektenbeauftragte innerhalb der gesetzlich vorgesehenen Fristen entschieden, jedoch die begehrte Einsicht nur zum Teil gewährt. Soweit Unterlagen aus den Ordnern nicht zugänglich gemacht werden sollten, wurden diese aussortiert und in einem neuen **Ordner „V" (vertraulich)** abgelegt. Im Bereich der öffentlichen Belange wurde die Ablehnung des Zugangs im Wesentlichen auf den Schutz der Beziehungen zu anderen Ländern und zum Bund, auf den Schutz vertraulicher Beratungsprotokolle sowie auf die Beeinträchtigung der Funktionsfähigkeit und Eigenverantwortung der Landesregierung gestützt. Daneben sind in den Unterlagen auch personenbezogene Daten von Betroffenen und Rat Suchenden enthalten, die ebenfalls ausgenommen wurden. Bezüglich dieser vorenthaltenen Informationen hat die Scientology Kirche e. V. uns um Überprüfung gebeten.

Sämtliche „V-Ordner" wurden daraufhin noch einmal durchgesehen und die darin enthaltenen Dokumente einzeln bewertet. Es hat sich gezeigt, dass im Ergebnis weitere Informationen hätten zugänglich gemacht werden können. Wir haben ein

umfangreiches **Prüfungsprotokoll** erstellt, aus dem ersichtlich ist, in welchen Fällen der Scientology Kirche e. V. nach unserer Auffassung weitere Unterlagen zustanden und bezogen auf welche Dokumente Meinungsdifferenzen zwischen dem Sektenbeauftragten und uns verblieben sind.

Schwerpunkt der Diskussion war die Frage, inwieweit eine Schädigung der Beziehung zu anderen Ländern oder zum Bund zu befürchten ist, wenn Dokumente offenbart werden, die der schleswig-holsteinischen Ministerpräsidentin, der Staatskanzlei oder einem Ministerium im Rahmen länderübergreifender Zusammenarbeit aus anderen Ländern zwecks Information oder Diskussion zugesandt bzw. überlassen worden sind. Hier ist zu bedenken, dass die Offenbarung solcher Informationen schon dann zu einer Schädigung der Beziehung führen kann, wenn sie gegen den Willen der Verfasser bzw. betroffenen Stellen erfolgt. Der **Vertrauensschutz** für die jeweiligen Stellen des Bundes und der Länder muss deshalb prinzipiell beachtet werden. Eine Offenbarungspraxis, die auf etwaige Bekundungen oder Absprachen oder auch auf die rechtliche Situation der betroffenen Stellen keine Rücksicht nähme, liefe Gefahr, das Land zu isolieren. Wir haben die Zugangsverweigerung akzeptiert, wenn glaubhaft gemacht werden konnte, dass die Offenbarung von Dokumenten mit länderübergreifender Bedeutung zu den genannten Folgen führen würde. Gleichwohl bleibt festzuhalten, dass das Informationsfreiheitsgesetz eine eigenständige Entscheidung der schleswig-holsteinischen Behörden verlangt und diese nicht nur von der Zustimmung anderer Stellen abhängig gemacht werden kann.

Inzwischen haben die Scientologen auch Einblick in die Unterlagen genommen, die nach unserer Einschätzung zusätzlich zugänglich zu machen waren.

- **Akteneinsicht bei einer Staatsanwaltschaft?**

Ein Petent hatte sich beim Eingabenausschuss des Landtages über bestimmte Entscheidungen einer Staatsanwaltschaft beschwert. Der **Generalstaatsanwalt** wurde als dienstaufsichtsführende Behörde vom Eingabenausschuss um eine Stellungnahme gebeten. Der Petent beantragte daraufhin beim Generalstaatsanwalt Einsicht in dessen Unterlagen zum Eingabeverfahren, was dieser ablehnte.

Wir haben uns der Meinung des Generalstaatsanwalts angeschlossen. Das Informationsfreiheitsgesetz findet auf Gerichte und Strafverfolgungsbehörden keine Anwendung, soweit sie als Organe der Rechtspflege tätig sind. Dies bezieht sich nicht nur auf die unmittelbare Strafverfolgung, sondern gilt auch für den Generalstaatsanwalt, wenn er sich im Rahmen seiner Stellung als **Dienstaufsichtsbehörde** auf einzelne Ermittlungsverfahren beziehen muss, die bei einer Staatsanwaltschaft geführt worden sind – unabhängig davon, ob die betreffenden Verfahren bereits abgeschlossen sind.

- **Abfallablagerung in der Nachbarschaft**

Ein Gemeindebewohner zeigte bei der Unteren Abfallentsorgungsbehörde des Kreises einen abfallrechtlich relevanten Sachverhalt an und bat um Tätigwerden.

Die Behörde führte einen Ortstermin durch und forderte den verantwortlichen Eigentümer des Grundstücks zur **Abfallbeseitigung** auf. Die vom Anzeigenerstatter erbetene Kopie des an den Eigentümer gerichteten Schreibens wurde ihm versagt, weil er an dem Verfahren nicht beteiligt sei und es sich um personenbezogene Daten handele, die auch nach Maßgabe des Informationsfreiheitsgesetzes nicht herausgegeben werden dürften. Im Übrigen sei ihm bereits Auskunft erteilt worden.

Wir wiesen den Kreis darauf hin, dass nicht das Informationsfreiheitsgesetz des Landes, sondern das speziellere **Umweltinformationsgesetz** des Bundes einschlägig war, welches an den Schutz personenbezogener Daten Dritter weniger hohe Anforderungen stellt als das Informationsfreiheitsgesetz. Bei der gebotenen Abwägung zwischen dem öffentlichen Interesse am freien Zugang zu den Umweltinformationen und der geschützten Persönlichkeitssphäre des abfallrechtlich Verantwortlichen war zu berücksichtigen, dass der Petent die wesentlichen schutzwürdigen Daten ohnehin schon kannte und somit der Eingriff in die Rechte des Betroffenen nicht sehr schwerwiegend war. Die Behörde verwies darauf, dass es nach dem Umweltinformationsgesetz in das Ermessen der Behörden gestellt sei, in welcher Form dem Informationsbegehren nachgekommen wird, und zog sich darauf zurück, dass sie sich im Rahmen des Auswahlermessens dafür entschieden habe, dem Petenten nur eine Auskunft zu erteilen. Dem Petenten blieb nur der Rechtsweg.

- **Kommunaler Architektenwettbewerb**

Eine kreisangehörige Stadt plante den Neubau einer Grundschule und lobte hierfür einen beschränkten Realisierungswettbewerb aus. Die eingereichten **Angebote** enthielten **Kostenberechnungen**, **Kalkulationen** und **Pläne**. Am Abgabetermin wurden die Angebote im Beisein des Bürgermeisters, der Mitbewerber und städtischer Mitarbeiter geöffnet und verlesen. Die anschließenden Beratungen der Ausschüsse über die Entwürfe und die Kostenkalkulationen fanden unter Ausschluss der Öffentlichkeit statt. Nachdem der Hauptausschuss über die Vergabe des Auftrags entschieden hatte, musste der unterlegene Architekt in der Presse lesen, dass sein Angebot um Längen teurer gewesen sein sollte als das seines Konkurrenten. Weil er dies nicht so recht glauben wollte, begehrte er Einsicht in die eingereichten Unterlagen seines Konkurrenten. Dies wurde ihm mit der Begründung verwehrt, dass es sich um Betriebs- und Geschäftsgeheimnisse handele, die nicht offenbart werden dürften.

Betriebs- und Geschäftsgeheimnisse können dem Informationsrecht nur entgegenstehen, wenn es um nicht offenkundige Tatsachen geht, die im Zusammenhang mit einem wirtschaftlichen Geschäftsbetrieb stehen, nach dem Willen des Unternehmers geheim gehalten werden sollen und die den Gegenstand eines berechtigten wirtschaftlichen Interesses des Unternehmers bilden. Wir haben die Stadt darauf hingewiesen, dass bei der Prüfung eines darauf gerichteten Zugangsantrags zu berücksichtigen ist, dass die jeweiligen Merkmale allein zum entscheidungserheblichen Zeitpunkt vorliegen müssen. Insbesondere an dem erforderlichen Geheimhaltungswillen des Unternehmens kann es fehlen, wenn bereits eine gemeinsame

Eröffnung der Angebote stattgefunden und die Kommune den Auftrag schon erteilt hat. Selbst bei Annahme eines Geheimnisses wären ferner die Interessen des Unternehmens gegen das Offenbarungsinteresse der Allgemeinheit abzuwägen.

Hinsichtlich des öffentlichen Interesses haben wir auf die finanzielle und gesellschaftliche Bedeutung eines Schulneubaus hingewiesen. Die Öffentlichkeit darf sich dafür interessieren, ob die Stadt zwischen inhaltlich gleichwertigen Angeboten entschieden hat, ob die Angebote die geltenden Vorgaben und Richtlinien einhalten und ob das Auswahlverfahren insgesamt wettbewerbs- und sachgerecht durchgeführt worden ist. Sowohl bei der Vergabe **öffentlicher Aufträge** als auch im **Beschaffungswesen** kommt dem Recht auf Informationszugang eine wichtige Rolle zu. Wenn Politik und Verwaltung mit einer größeren Kontrolle von außen rechnen müssen, wird auch das Maß der Eigenkontrolle steigen. Die gesteigerte Transparenz fördert daher nicht nur das Kostenbewusstsein, sondern ist zugleich ein Instrument sowohl zur Korruptionsprävention als auch zur Bekämpfung der Korruption. Nach unserer Vermittlung hat die Stadt ihre Rechtsauffassung revidiert und sich bereit erklärt, dem Antrag des Petenten stattzugeben.

- **Von welcher Qualität ist das Trinkwasser?**

Die Bewohner einer amtsangehörigen Gemeinde müssen in regelmäßigen Abständen ihr **Brunnenwasser** untersuchen lassen, weil ihre Grundstücke nicht an die zentrale Trinkwasserversorgung angeschlossen sind. Bestehen Anhaltspunkte dafür, dass der Genuss des Brunnenwassers gesundheitsschädlich sein könnte, muss zum Zwecke der Gefahrenabwehr nach der geltenden Trinkwasserverordnung eine so genannte „erweiterte“ Untersuchung veranlasst werden.

Im Rahmen der Auseinandersetzung über die Rechtmäßigkeit dieser Verpflichtung beantragte ein Bewohner der Gemeinde bei der zuständigen Kreisgesundheitsbehörde eine „vollumfängliche“ Auskunft über die Ergebnisse der in seiner Gemeinde durchgeführten erweiterten Untersuchungen und berief sich dabei auf das **Umweltinformationsgesetz**. Nachdem er vom Kreis lediglich eine allgemeine „Beanstandungsquote“ mitgeteilt bekommen hatte, wandte er sich an das Ministerium für Arbeit, Gesundheit und Soziales. Dieses verwies auf datenschutzrechtliche Hindernisse, weil sich die Gutachten auf private Einzelbrunnen bezögen.

Wir haben die Kreisgesundheitsbehörde darauf hingewiesen, dass das hier einschlägige Umweltinformationsgesetz kein pauschales Verbot der Offenbarung personenbezogener Daten enthält, sondern den Zugang nur verwehrt, wenn durch das Bekanntwerden der personenbezogenen Daten schutzwürdige Interessen des Betroffenen beeinträchtigt würden. Um etwaige persönliche Interessen des Betroffenen zu ermitteln, wäre dieser zuvor anzuhören. Um sich dieses Verfahren zu ersparen und dennoch sowohl den datenschutzrechtlichen Belangen der betroffenen Brunnenbesitzer als auch dem berechtigten Informationsinteresse des Petenten gerecht zu werden, haben wir vorgeschlagen, die Untersuchungsergebnisse von vornherein durch Trennung von den personen- bzw. grundstücksbezogenen Daten zu **anonymisieren** bzw. so zusammenzufassen, dass sich auch für ortskundige Leser kein Personenbezug mehr herstellen lässt.

- **Welche Gebührenhöhe ist noch angemessen?**

Ein Petent wollte sich über die Haushaltslage seiner Gemeinde informieren und beantragte bei der Amtsverwaltung die Überlassung von **Kopien** des aktuellen Haushalts sowie die Rechenschaftsberichte vorangegangener Jahre. Ihm wurde mitgeteilt, dass es sich hier um über 300 Seiten handele und er **1 DM pro Seite** zahlen müsse. Der Petent rechnete dem Amt vor, dass sein eigener Kopierer in der Lage sei, 35 Kopien in der Minute zu einem Stückpreis von 0,037 DM herzustellen („ohne Profit, inklusive Papier, Toner und Wartung"). Außerdem käme man für die Herstellung der beantragten Kopien auf einen Zeitaufwand von 10,26 Minuten. Bei dem vom Amt veranschlagten Gesamtpreis ergäbe dies einen Stundenlohn von 2099,42 DM. Das Amt entgegnete hierauf, dass die Erstellung von Kopien ohnehin nur infrage komme, wenn eine Einsichtnahme oder eine Auskunftserteilung nicht möglich seien. Alternativ wurde ihm angeboten, die erbetenen Unterlagen in den Räumen des Amtes einzusehen.

Wir haben das Amt auf zweierlei hingewiesen:

Bei der Ausgestaltung des Informationszugangs bleibt es der Entscheidung des Antragstellers überlassen, in welcher Form ihm die begehrten Unterlagen zugänglich gemacht werden. Die Möglichkeiten des direkten Zugangs zum jeweiligen Informationsträger (z. B. durch Akteneinsicht), der Auskunftserteilung oder aber der Anfertigung von Kopien stehen für ihn gleichberechtigt zur **Auswahl**. Etwas anderes gilt nur dann, wenn keine ausreichenden zeitlichen, sachlichen und räumlichen Möglichkeiten für den direkten Informationszugang zur Verfügung stehen oder wenn bestimmte Daten vorenthalten werden müssen und von den übrigen Informationen nicht sinnvoll getrennt werden können.

Der Europäische Gerichtshof hat entschieden, dass die Kostenerhebung nicht dazu genutzt werden darf, die gesamten tatsächlichen, auch mittelbaren Kosten, die dem öffentlichen Haushalt durch eine Zusammenstellung von Unterlagen entstehen, auf Einzelne abzuwälzen, die einen Antrag auf Informationsgewährung stellen. Der Preis ist deshalb so zu gestalten, dass zwischen dem bei der Behörde tatsächlich zu betreibenden personellen und sachlichen Verwaltungsaufwand und der Bedeutung oder dem wirtschaftlichen Wert der Amtshandlung für den Antragsteller ein angemessenes Verhältnis besteht. Dabei ist der Wert der Verwaltungsleistung objektiv zu bestimmen und kann etwa anhand vergleichbarer, am Markt angebotener Leistungen ermittelt werden. Bei der Herstellung von Kopien ist auch zu berücksichtigen, dass sich deren Preis auf dem Markt heutzutage in Bereichen um die 0,10 DM pro Seite bewegt und dank der Automation des Kopiervorgangs mit zunehmender Stückzahl sinkt, weil der dabei entstehende Aufwand nicht proportional steigt. Demgemäß dürften die in einigen Gebührentarifen noch zu findenden pauschalen Preise von 1 DM/Seite – und dies unabhängig von der Anzahl der Seiten – heute nicht mehr zu rechtfertigen sein. Eine angemessene Gebührenerhebung für Kopien sollte nach unserer Auffassung Bagatellgrenzen und mit steigender Anzahl der Kopien eine Staffelung vorsehen, die den gleichzeitig sinkenden Aufwand berücksichtigt. Die Amtsverwaltung hat sich bereit erklärt, mit dem Petenten einen „fairen Preis" zu vereinbaren.

- **Die erste Beanstandung**

Eine Gemeinde plante ein neues Gewerbegebiet. Sie erstellte einen entsprechenden Bebauungsplan und führte das nach dem Baugesetzbuch vorgeschriebene Verfahren durch, in dem sowohl die Bürgerinnen und Bürger als auch die Träger öffentlicher Belange beteiligt wurden. Es wurde eine Verkehrszählung in Auftrag gegeben und eine Bürgerversammlung durchgeführt. In der Gemeinde gründete sich eine Interessengemeinschaft, deren Mitglieder bei der Verwaltung nach dem Ergebnis der Verkehrszählung und dem Protokoll der Bürgerversammlung fragten. Während der Einsichtnahme beantragten sie Kopien hiervon sowie eine Kopie der eingereichten **Stellungnahmen** der **Träger öffentlicher Belange**. Dies wurde dem Bürgermeister offenbar zu viel, und er verwies darauf, dass die Unterlagen bereits ausgelegen hätten. Schließlich erklärte er sich dazu bereit, dem Auskunftsersuchen insoweit zu entsprechen, als das Protokoll der Bürgerversammlung in Kopie herausgegeben wurde.

Tatsächlich schreibt das **Baugesetzbuch** eine möglichst frühzeitige und umfassende Beteiligung der Bürgerinnen und Bürger vor. Die Entwürfe der Bauleitpläne mit dem Erläuterungsbericht oder der Begründung sind befristet öffentlich auszulegen, um die Möglichkeit zu geben, Anregungen und Einwendungen gegen die Planung vorzubringen. Dies lässt aber weder den Schluss zu, dass andere im Zusammenhang mit der Bauplanung stehende Unterlagen vom Zugang ausgenommen sind, noch, dass ein Zugang zu sämtlichen Unterlagen nach Ablauf der Monatsfrist ausgeschlossen ist.

Ist die Aufstellung des Bebauungsplans noch nicht abgeschlossen, lässt sich zwar der **Schutz** der behördlichen **Entscheidungsbildung** ins Feld führen. Nach dem Informationsfreiheitsgesetz werden Entwürfe zu Entscheidungen sowie Arbeiten und Beschlüsse zu ihrer unmittelbaren Vorbereitung nicht bekannt gegeben, wenn dadurch der Erfolg der Entscheidung vereitelt würde. Von diesen Vorbereitungsarbeiten werden jedoch **extern** erstellte **Stellungnahmen** ausdrücklich ausgenommen, sodass insbesondere auch die von anderen Trägern öffentlicher Belange abgegebenen Stellungnahmen zu konkreten Planvorhaben nach dem Willen des Gesetzgebers nicht vorenthalten werden dürfen, weil sie nicht zum Zwecke der Entscheidungsvorbereitung selbst erstellt wurden, sondern lediglich als externe Entscheidungshilfe zu betrachten sind.

Da sich die Gemeinde nicht von unserer Rechtsauffassung überzeugen lassen hat, haben wir eine **förmliche Beanstandung** ausgesprochen.

13 Was es sonst noch zu berichten gibt

13.1 Kampfhundeverordnung und Steuergeheimnis

Auf den ersten Blick fällt es schwer, eine Beziehung zwischen der Kampfhundeverordnung und dem Steuergeheimnis herzustellen. Trotzdem lagen uns im vergangenen Jahr hierzu stapelweise Anfragen vor. Die betreffenden Kommunen hatten nämlich die Absicht, alle Hundehalter anzuschreiben und mittels Fragebogen zu ermitteln, wer von ihnen einen so genannten Kampfhund besitzt. Hierzu wollten die Ordnungsämter die Adressen aus dem Hundesteuerbestand nutzen und waren ärgerlich, als die Kollegen der Steuerabteilungen die Herausgabe unter Hinweis auf das Steuergeheimnis verweigerten. Deren Argumentation war schlüssig: Die Umsetzung der Kampfhundeverordnung sei eine ordnungsrechtliche Maßnahme und diene nicht dem Besteuerungsverfahren. Die Offenbarung steuerlicher Verhältnisse sei aber nur zur Verfolgung von Verbrechen und einigen anderen schweren Straftaten zulässig. Wir haben darauf hingewiesen, dass die Hundehalter nicht zur Abgabe der Erhebungsbögen verpflichtet sind, weil die Kampfhundeverordnung eine Erklärungspflicht nicht vorsieht. Wenn es aber nur auf die Erfassung freiwillig gemachter Angaben ankommt, kann die Versendung der Vordrucke auch durch das Steueramt erfolgen, sodass es nicht zu unbefugten Offenbarungen steuerlicher Verhältnisse kommt. Ein Hundehalter, der seinen Bullterrier freiwillig registrieren lässt, bricht nicht das Steuergeheimnis. Die Daten desjenigen, der nicht reagiert, werden dem Ordnungsamt nicht bekannt. Die von vielen kritisierte geringe Effektivität derartiger Aktionen lag also jedenfalls nicht im Steuergeheimnis begründet.

13.2 AIDS-Beratung ohne Grenzen

Ein Petent beschwerte sich, dass seine Akte in einer AIDS-Beratungsstelle nicht nur von seinem Sozialarbeiter, sondern auch von allen anderen Kollegen gelesen werde. Dies war im konkreten Fall besonders heikel, weil persönliche Kontakte zwischen dem Petenten und einem Mitarbeiter der Beratungsstelle bestanden. Sozialarbeiter unterliegen aus gutem Grund der beruflichen Schweigepflicht. Dies gilt auch gegenüber Kollegen, die selbst zur Geheimhaltung verpflichtet sind. Wünscht der Rat Suchende also ein vertrauliches Gespräch unter vier Augen, so ist dieser Wunsch für den Sozialarbeiter bindend. Ohne Einwilligung des Hilfe Suchenden dürfen die Daten auch intern grundsätzlich nicht weitergegeben werden. Wird die Beratung durch ein Team wahrgenommen, muss diese Vorgehensweise zuvor mit den Betroffenen abgestimmt werden. Dies kann z. B. durch Informationsbroschüren über die Verfahrensweisen der Beratungsstelle, die vor dem ersten Beratungsgespräch ausgehändigt werden, erfolgen. Aus Gründen der Rechtssicherheit sollte stets eine schriftliche Einwilligung eingeholt werden, wenn der Berater personenbezogene Daten seiner Beratungsfälle an weitere Personen weitergeben möchte. Beratungsstellen haben uns bestätigt, dass sich diese Transparenz positiv auf das Vertrauensverhältnis auswirkt bzw. eine fehlende Unterrichtung die Hilfeleistung nachhaltig beeinträchtigen kann.

13.3 Mailingaktion der Krebsgesellschaft

Groß war die Irritation, als ein Petent Werbung von der Schleswig-Holsteinischen Krebsgesellschaft e. V. erhielt, lag doch sein Vater aufgrund eines Krebsleidens gerade im Sterben. Noch größer wurden die Befürchtungen, als er feststellte, dass nur die Nachbarn die gleiche Werbesendung erhalten hatten, die bzw. deren Angehörige vor kurzer Zeit wegen eines Krebsleidens in der gleichen Klinik wie sein Vater behandelt worden waren. „Gesunde“ Nachbarn hatten keine Post bekommen. Hatte womöglich das Krankenhaus die Anschriften von Patienten weitergegeben?

Die Krebsgesellschaft erklärte uns, dass jährlich drei bis vier Werbeaktionen bundesweit durchgeführt werden. Jeweils etwa eine Million Haushalte erhielten im Rahmen dieser Mailingaktionen Post; auf Schleswig-Holstein entfielen ca. 115.000 Briefsendungen. Man versicherte uns sowohl vonseiten der Gesellschaft als auch des Krankenhauses, dass die Adressdaten nicht aus medizinischen Behandlungen stammen. Nachforschungen ergaben, dass die Adressen von einer Vermittlungsagentur aus der Schweiz gekauft worden waren. Diese Agentur hatte die Adressen wiederum von einem Schweizer Adresshändler erworben. Die Schweizer Firmen erklärten uns, die Daten aus Telefonbüchern des Jahres 1997 entnommen und mit weiteren öffentlichen Quellen abgeglichen zu haben. Nach einem wechselnden Zufallsprinzip würden dann bestimmte Haushalte angeschrieben. Die Mailingaktionen der Krebsgesellschaften hätten nicht nur das Ziel der Versorgung der Bevölkerung mit Informationen, sondern auch das des Einwerbens von Spenden. Daher erfolge die Auswahl der Adressen zudem nach dem Kriterium der von den Wohnadressen abgeleiteten angenommenen Spendenbereitschaft. Trotz intensiver Prüfung – über die Grenzen von Schleswig-Holstein hinaus – konnte der Verdacht des Petenten nicht bestätigt werden. Ein ungutes Gefühl blieb jedoch, nicht nur bei dem Petenten. Die Schleswig-Holsteinische Krebsgesellschaft e. V. hat reagiert. Den konkreten Fall sowie eine Vielzahl weiterer Anfragen will man zum Anlass nehmen, bei zukünftigen Mailingaktionen durch entsprechende Informationen zur Herkunft der Adressen für eine größere Transparenz zu sorgen.

13.4 Der geschwätzige Mutterpass

Werdende Mütter erhalten zu Beginn der Schwangerschaft einen Mutterpass, der zu einem wichtigen Wegbegleiter für die Schwangere wird. Bei jedem Arztbesuch wird darin der Verlauf der Schwangerschaft vermerkt. In den neun Monaten wird die werdende Mutter diesen Pass einer Vielzahl von Ärzten, eventuell aber auch dem Arbeitgeber, dem Sozialamt oder anderen Stellen vorlegen. Der Arzt einer gynäkologischen Abteilung eines Krankenhauses monierte, dass in dem Dokument die Angabe „Allein erziehend – ja/nein“ vermerkt ist. Eine Schwangere werde auch dann als allein erziehend eingestuft, wenn sie zwar in fester Beziehung, aber ohne Trauschein lebt. Dieses Merkmal sei medizinisch nicht erforderlich. Keine Mutter ist gesetzlich verpflichtet, einen Mutterpass bzw. ein Kinderuntersuchungsheft (für die Vorsorgeuntersuchungen U1 bis U9) zu führen. Die

Ausstellung und Nutzung dieser Dokumente ist freiwillig; eine Leistungsgewährung der Krankenkassen kann hiervon nicht abhängig gemacht werden. Dessen ungeachtet ist der Mutterpass bzw. das Kinderuntersuchungsheft aus medizinischer Sicht eine sinnvolle Einrichtung. Werden aber nicht erforderliche Daten eingetragen, so kann aus einer sinnvollen Sache schnell ein Instrument der Diskriminierung werden. Der Bundesausschuss der Ärzte und Krankenkassen hat das Datenfeld „Allein erziehend“ nach anfänglichem Zögern gestrichen.

13.5 Telefonkosten- und Internet-Surf-Erlass

Heftiges Rauschen im Blätterwald und in den sonstigen Medien hat der Bundesfinanzminister mit seiner Absicht hervorgerufen, die Nutzung dienstlicher/geschäftlicher Kommunikationsgeräte (Telefone, PC, Laptops) zu privaten Zwecken und privater Geräte zu dienstlichen/geschäftlichen Zwecken auf den Pfennig genau abzurechnen und entsprechend steuerlich zu berücksichtigen. Dies hätte zu detaillierten Aufzeichnungen des gesamten Kommunikationsverhaltens der Betroffenen geführt. Nach einhelliger Auffassung der Interessenverbände der Steuerpflichtigen, der Wirtschaft und der IT-Industrie sowie der Datenschützer war dieses perfektionistische Verfahren als ein unverhältnismäßiger Eingriff in die Privatsphäre anzusehen. Weiterhin bestanden Zweifel, ob dies überhaupt mit dem Telekommunikationsrecht zu vereinbaren war. Der Bundesfinanzminister hat sich den vielfältigen Protesten gebeugt und einer pauschalierten steuerlichen Berücksichtigung der Kosten bzw. der geldwerten Vorteile zugestimmt.

13.6 IKOTECH II resistent gegen Loveletter-Virus

Das Auftreten des Loveletter-Virus im Mai 2000 hat in zahlreichen Unternehmen und Behörden zu erheblichen Problemen geführt. In der Presse wurde hierüber ausführlich berichtet. Obwohl die über das CAMPUS-Netz verknüpften und nach dem IKOTECH-II-Standard ausgerüsteten obersten Landesbehörden sogar von Behörden anderer Bundesländer und der Bundesverwaltung mit verseuchten Mails bombardiert worden sind, konnte der Virus hier keinen Schaden anrichten und wurde auch nicht weiterversandt. Der IKOTECH-II-Standard enthält Konfigurationselemente, die die Arbeitsplatzrechner gegen derartige Attacken recht effektiv abschirmen:

- Benutzer haben keinen Zugriff auf die Betriebssystemebene und können nur auf ihrer „Schreibtischoberfläche“ agieren.
- Die Dateien selbst müssen außerdem durch die Systemverwaltung für die betreffenden Benutzer explizit freigegeben worden sein.
- Die Benutzer haben kein Schreibrecht auf die Verzeichnisse der Konfigurationseinstellungen.
- Auf jedem Arbeitsplatz ist ein Virenscanner installiert.

Nur das Zusammenspiel dieser Faktoren hat die notwendige Resistenz bewirkt. Der Virenscanner allein hätte z. B. keine Wirkung erzielt, da ihm „Loveletter“

zunächst nicht bekannt war. Hierbei handelt es sich um ein klassisches Beispiel dafür, dass es gute Sicherheitslösungen gibt, die gleichwohl nicht überall eingesetzt werden (vgl. Tz. 7.5.2). Alle Behörden, die Ärger mit dem Virus hatten oder ihn weiter verbreitet haben, müssen sich vorwerfen lassen, dass ihre Sicherheitsmaßnahmen nicht dem Stand der Technik entsprachen; dies war nicht schicksalhaft, sondern fahrlässig.

13.7 Geschwindigkeitsmessungen als verkehrserzieherische Maßnahme

Eine Gemeindeverwaltung beabsichtigte, in Tempo-30-Zonen Geschwindigkeitsmessungen durchzuführen, bei denen zu schnell fahrende Autos angehalten werden und die Fahrer im Rahmen eines verkehrserzieherischen Gesprächs vor allem mit Kindern und Jugendlichen der Gemeinde konfrontiert werden sollten. Die Gemeinde versprach sich gerade von einer eventuellen persönlichen Bekanntschaft aufgrund von Nachbarschaft der Beteiligten eine größere Einsicht der betroffenen Verkehrsteilnehmer in die verkehrsgefährdenden Auswirkungen ihres Fahrverhaltens. Auch wenn der pädagogische Ansatz dieser Idee anzuerkennen ist und die Gefährdung von Kindern durch Raser sicherlich auch neue Wege erfordert, um auf Autofahrer einzuwirken, muss eine problematische Prangerwirkung für die betroffenen Autofahrer vermieden werden. Die Gemeinde würde im Rahmen dieses Vorhabens in Zusammenarbeit mit der Polizei personenbezogene Daten erheben und an Dritte (Kinder und Jugendliche) weitergeben. Eine Rechtsgrundlage hierfür gibt es nicht. Die Gemeinde müsste deshalb das Einverständnis der jeweiligen Autofahrer zu einem Gespräch mit den Kindern und Jugendlichen einholen.

13.8 Unberechtigte Akteneinsicht einer Versicherung

Bei einem Verkehrsunfall erlitt ein Petent erhebliche Verletzungen, die seine Berufs- und Erwerbsunfähigkeit zur Folge hatten. Während die Sachschäden anstandslos von der gegnerischen Versicherung beglichen wurden, blieben die Schadenersatz- sowie die Schmerzensgeldforderungen unberücksichtigt. Über den Rechtsanwalt dieser Versicherung erfuhr er, dass man dort einen anonymen Hinweis auf diverse gegen ihn gerichtete Strafverfahren erhalten und Einsicht in die dazugehörigen Vorgänge genommen habe. Unsere Nachprüfung ergab, dass die Akteneinsicht von der Staatsanwaltschaft zu Unrecht gestattet worden war, da die Versicherung kein berechtigtes Interesse darlegen konnte. Die eingesehenen Strafakten betrafen Vorwürfe, die keinen sachlichen Zusammenhang mit dem vorliegenden Versicherungsfall aufwiesen. Dies wurde als ein erheblicher datenschutzrechtlicher Verstoß beanstandet. Die betreffende Staatsanwaltschaft hat den Fehler eingeräumt und uns mitgeteilt, künftig bei Prüfungen von Akteneinsichtsersuchen einen engeren Maßstab anzulegen.

14 Rückblick

14.1 Elektronisches Grundbuch

Bei der Einführung des elektronischen Grundbuches, die das Land gemeinsam mit Mecklenburg-Vorpommern und Brandenburg unternehmen wollte, haben wir wiederholt darauf hingewiesen, dass an die Datensicherheit besonders hohe Anforderungen zu stellen sind (vgl. 21. TB, Tz. 5.1). Insbesondere hatten wir unter der Überschrift „Wie unterschreibt der Grundbuchbeamte elektronisch?“ dargelegt, wie ein Signierverfahren, das den Anforderungen der einschlägigen Gesetze genügt, aussehen müsste. Dazu gehört u. a., dass es ein Trustcenter gibt, das die digitalen Schlüssel verwaltet, dass die Schlüssel auf hinreichend sicheren Chipkarten gespeichert sind und es ein auf Dauer ausgerichtetes Verfahren zur Wahrung der Integrität der gespeicherten Daten geben muss. Einige Zeit lang schien es so, als seien diese Anforderungen nur schwer durchzusetzen. Nachdem die Arbeiten nur schleppend vorankamen (vgl. 22. TB, Tz. 4.3.1), wurde die Zusammenarbeit der Länder im Jahr 2000 endgültig aufgegeben. In einem neuen Projekt, das zusammen mit Baden-Württemberg gestartet wurde, soll das dort betriebene System FOLIA, das bisher lediglich eine elektronische Eingabehilfe bei der Grundbuchführung darstellt, in zwei Ausbaustufen zu einem vollständigen elektronischen Grundbuch ausgebaut werden. Erfreulicherweise konnten wir feststellen, das die von uns angemahnten Anforderungen an die Datensicherheit in dem neuen Projekt als selbstverständlich und dem Stand der Technik entsprechend vorgesehen worden sind. Es ist zu hoffen, dass das Justizministerium auch bei der konkreten Ausgestaltung der Verfahren an dieser grundsätzlich richtigen Ausrichtung festhält.

14.2 ViCLAS-Datenbank

Mithilfe der aus Nordamerika stammenden Methode der Fallanalyse auf Grundlage detaillierter Fragebögen über Täter- und Opferpersönlichkeiten wird versucht, besonders herausragende Verbrechen durch speziell geschulte Mitarbeiter aufzuklären (vgl. 22. TB, Tz. 4.2.5). Inzwischen ist die Errichtungsanordnung für die ViCLAS-Verbunddatei beim BKA in Kraft getreten. Sie sieht die personenbezogene Speicherung von Opferdaten auf Grundlage von Einwilligungen mit einer Prüffrist von jeweils fünf Jahren vor, und zwar unabhängig davon, ob der Fall des konkreten Opfers bereits aufgeklärt wurde. Als Argument gegen unseren Einwand, der Zweck der Datei könne aufgrund der detaillierten Angaben über Opferpersönlichkeit und Tatgeschehen auch mit anonymisierten Opferdaten hergestellt werden, verweist die Polizei auf einen einzelnen Fall, in dem der Nachname der Opfer die Taten zu einer Serie zusammenfügte. Außerdem habe das Opfer in der Regel in seine Speicherung in der ViCLAS-Datei eingewilligt. Die Speicherung von Opferdaten steht jedoch auch nach Auffassung des Innenministeriums unter dem Vorbehalt der Erforderlichkeit. Die Frage der Speicherung von Opferdaten aus aufgeklärten Fällen war vor einigen Jahren bereits im Rahmen der schleswig-holsteinischen POLDOK-Datei strittig geblieben (vgl. 19. TB, Tz. 4.2.5). Wir hatten uns auch damals mit unseren Argumenten für eine Anonymisierung von Opferdaten nicht durchsetzen können.

14.3 Verwaltungsinformatiker werden gesucht, aber in Schleswig-Holstein noch immer nicht ausgebildet

Vor zwei Jahren haben wir darauf hingewiesen, dass die Anforderungen an die verwaltungsrechtlichen und systemtechnischen Qualifikationen von Mitarbeiterinnen und Mitarbeitern in IT-Stellen stetig steigen, weil die automatisierten Verwaltungsabläufe immer komplexer werden (vgl. 21. TB, Tz. 6.3). Die Behörden bekommen deshalb erhebliche Probleme, entsprechend ausgebildetes Personal für diese Bereiche zu finden. Verwaltungsfachleuten fehlt in der Regel der informationstechnische Background, Informatiker müssen „teuer“ bezahlt werden und entfalten die erforderliche Produktivität erst, nachdem sie auf dem verwaltungsrechtlichen Gebiet geschult worden sind. Unsere Forderung, an den schleswig-holsteinischen Fachhochschulen Studiengänge für Verwaltungsinformatiker einzurichten, wurde daher allseits begrüßt. Insbesondere die Leiter kleinerer Behörden waren von unserer Idee angetan, da bei ihnen die IT-Administratoren diese Tätigkeit nicht „hauptamtlich“ ausüben, sondern „daneben auch noch“ bzw. im Wesentlichen normale Verwaltungstätigkeiten zu erledigen haben. Dabei fehlt in diesen Verwaltungen nicht selten das IT-Fachwissen, um sich z. B. unseriöser Hard- und Softwareangebote und überdimensionierter IT-Lösungen zu erwehren. Trotz alledem hat sich in den vergangenen Jahren in Schleswig-Holstein nichts bewegt. In anderen Bundesländern sind derartige Studiengänge schon im Angebot der Hochschulen, zumindest aber in Vorbereitung. In Schleswig-Holstein ist man sich zwar darüber einig, dass alle gewinnen würden, die Hochschulen, die Studenten und die Verwaltungen. Bei dieser Erkenntnis wird es jedoch augenscheinlich bleiben.

14.4 Datenschutz als Mittel zur Verwaltungsmodernisierung – auf Kontinuität angelegt

Häufig sind die datenschutzrechtlichen Aktivitäten von Behörden nur darauf ausgerichtet, punktuelle Problemstellungen kurzfristig zu lösen. Ist dies geschehen, tritt der Datenschutz als Managementaufgabe schnell wieder in den Hintergrund. Einige Verwaltungen haben allerdings im Laufe der letzten Jahre erkannt, dass das ausschließliche Reagieren auf „aktuelle Krisen“ höchst ineffektiv ist und dass nur die kontinuierliche Auseinandersetzung mit datenschutzrechtlichen und sicherheitstechnischen Fragen auch im Hinblick auf die Verwaltungsmodernisierung zu befriedigenden Lösungen führt. Der Kreis Schleswig-Flensburg hat sich vor zwei Jahren entschieden, diesen Weg zu gehen (vgl. 22. TB, Tz. 6.6). Er hat nicht nur in einem definierten Verfahren ein allgemeines Sicherheitskonzept erstellt, sondern nutzt die bewährten Zusammenarbeitsstrukturen zwischen der Behördenleitung, den Fachbereichen, der IT-Stelle und den behördlichen Datenschutzbeauftragten auch für so komplexe Projekte wie „Anschluss des lokalen Netzes der Kreisverwaltung an das Internet“. Auch der Kreis Ostholstein hat sich diese Verfahrensweise zu Nutze gemacht. Das dortige Projekt zum Internet-Anschluss steht bereits unmittelbar vor der „Produktivphase“. Offenbar aufgrund der guten Erfahrungen ihrer Kollegen mit dieser Vorgehensweise strebt der Kreis Nordfriesland eine Kooperation mit dem Kreis Schleswig-Flensburg an.

14.5 Verantwortung für die Datensicherheit in den Finanzämtern klargestellt

Es hatte vor einigen Jahren den Anschein, dass die Verantwortung für die Datensicherheit in den Finanzämtern zwischen den Finanzamtsvorstehern und der Oberfinanzdirektion zulasten des Steuergeheimnisses hin und her geschoben werden sollte (vgl. 22. TB, Tz. 4.9.1). Diese etwas verfahrene Situation ist bereinigt worden. Nachdem wir Gelegenheit hatten, im Rahmen einer Vorsteherdienstbesprechung die von uns kritisierten Schwachstellen noch einmal allen Vorstehern darzustellen, ist seitens der Oberfinanzdirektion die Zuständigkeit eindeutig festgelegt worden. Sie liegt bei den Leitern der Finanzämter. Erste Konsequenzen wurden sichtbar, als die GMSH als Gebäudeeigentümer einem Vorsteher vorschreiben wollte, welche Regularien für die Steueraktenvernichtung zu gelten hätten. Dieser hat unter Hinweis auf seine Verantwortung eine hinreichend sichere Verfahrensweise durchgesetzt. Ähnliche Konflikte wird die GMSH auch bei anderen Finanzämtern zu erwarten haben, wenn sie weiterhin glaubt, bei der landesweiten Ausschreibung von Entsorgungsdienstleistungen aus Kostengründen das Sicherheitsniveau in diesem sensiblen Bereich senken zu können.

15 Beispiele dafür, was die Bürger von unserer Tätigkeit haben

1. *Das Landesamt für soziale Dienste hatte bei Anträgen auf Gewährung von **Erziehungsgeld** prinzipiell die Vorlage des Einkommensteuerbescheides des Vorjahres gefordert, was weder vom Gesetzgeber vorgesehen, noch für die Bearbeitung der Anträge erforderlich war. Nach unserer Intervention wurde das Verfahren so gestaltet, dass der Einkommensnachweis auch ohne die Offenbarung aller Steuerbescheiddaten erbracht werden kann.*

2. *Die Online-Shops unter der Domain www.schleswig-holstein.de verwenden „**langlebige**“ **Cookies**, die es ermöglicht hätten, ein personenbezogenes Nutzungsprofil anzulegen. Außerdem war die Zustimmungserklärung zur Verwendung der persönlichen Daten zu Werbezwecken so voreingestellt, dass die Kunden ihrerseits aktiv werden mussten, um diese Art der Datennutzung zu verhindern. Wir machten die Betreiberfirma darauf aufmerksam, dass Cookies mit nur einer Stunde „Lebensdauer“ ausreichend sein sollten und dass die Voreinstellung der Zustimmung keine Einwilligung im Sinne des Datenschutzes darstellt. Die Probleme wurden mittlerweile beseitigt.*

3. *Offenbar unbemerkt von der Staatsanwaltschaft funktionierte die Löschfunktion in den staatsanwaltschaftlichen Verfahrensregistern des Systems **MESTA** nicht. Dies hatte zur Konsequenz, dass für die Betroffenen äußerst belastende Daten auch nach Fristablauf gespeichert blieben. Nachdem wir dies bei der Nachprüfung eines Falles entdeckt hatten, ist eine Behebung des Programmfehlers auf den Weg gebracht worden.*

4. *Einige Unternehmen veröffentlichten sensible Mitarbeiterdaten am jeweiligen **schwarzen Brett** ihrer Betriebe. Jeder wusste z. B., wer wie lange krank war. Wir konnten die Firmen überzeugen, von dieser Praxis künftig abzusehen.*

5. *Sicherheitstechnisch hochbrisante **Fernwartungen** wurden bei Behörden in Schleswig-Holstein häufig ohne sichere Rahmenbedingungen durchgeführt. Dadurch bestand das Risiko, dass die Vertraulichkeit von Daten vorsätzlich oder fahrlässig verletzt wurde. Nach unseren Beanstandungen werden Fernwartungen grundsätzlich nach präzisen schriftlichen Vereinbarungen durchgeführt; alle Aktivitäten werden außerdem protokolliert.*

6. *Bislang wurde offenbar bei den Staatsanwaltschaften nicht in jedem Fall geprüft, ob eine Versicherung auch wirklich tragfähige Gründe hatte, um **Akteneinsicht** in abgeschlossene Ermittlungsverfahren zu bekommen. Nachdem wir in einem solchen Fall die Einsichtgewährung als rechtlich unzulässig bewertet hatten, wurden die Mitarbeiter der Staatsanwaltschaft auf ihre Pflicht hingewiesen, künftig genau zu prüfen, ob ein ausreichend begründetes berechtigtes Interesse an der Einsichtnahme vorliegt.*

7. *Banken verlangten von Eigenheimbauern lange nach Abschluss von Darlehensverträgen nachträglich eine laufende und umfassende Offenbarung ihrer **Vermögensverhältnisse**. Darlehensnehmer wandten sich an uns, weil der in Anspruch genommene Kredit durch Hypotheken hinreichend gesichert war und durch regelmäßige Zahlungen ordnungsgemäß bedient wurde. Wir bewirkten, dass die Banken von ihrem überzogenen Auskunftsverlangen Abstand nahmen.*

8. *Die frei zugänglichen Mülltonnen einer Behörde waren gefüllt mit Unterlagen über **Rentenangelegenheiten**, auf dem Parkplatz davor lagen adressierte Briefumschläge. Sensible Sozialdaten waren durch eine unzulängliche Organisation der Entsorgung dem Zugriff unbefugter Dritter ausgesetzt. Gemeinsam mit der Behördenleitung wurde daraufhin das Konzept zur Vernichtung konventioneller Datenträger neu strukturiert, und die Mitarbeiter des Rentenversicherungsträgers wurden über ihre Datensicherungspflichten unterrichtet.*

9. *Zur Feststellung, ob Krankenhäuser **Notfallpatienten** aus medizinisch nicht gerechtfertigten Gründen ablehnen, wollte das Ministerium für Arbeit, Gesundheit und Soziales bei den Rettungsdiensten eine Erhebung durchführen, in der auch die Namen der jeweiligen Ärztinnen und Ärzte erfasst werden sollten. Die Ärztekammer wandte sich an uns mit der Befürchtung, die genannten Ärzte könnten mit strafrechtlichen oder sonstigen Sanktionen überzogen werden. Wir konnten erreichen, dass nicht der Name, sondern nur die allgemeine Funktion des Arztes erfasst wurde.*

10. *Staatsanwaltschaft und Polizei beabsichtigten, zur Erfassung von Straftätern in der **bundesweiten Gendatei** künftig auf eine richterliche Prüfung zu verzichten. Stattdessen sollten sich die Betroffenen mit der Untersuchung ihrer DNA und der Dateispeicherung einverstanden erklären. Nach unserer ablehnenden Stellungnahme modifizierte die Staatsanwaltschaft ihr Konzept, sodass nach wie vor ein richterlicher Beschluss zu beantragen ist. Das Bundesverfassungsgericht hat in einer Entscheidung inzwischen unsere Position gestützt.*

11. *Bislang war bei der Vermittlung von Arbeitsstellen für straffällige Personen unklar, wie Informationen über eine mögliche Wiederholungsgefährdung des Verurteilten übermittelt werden konnten, ohne dessen Resozialisierung zu gefährden. Dadurch konnte es passieren, dass entweder notwendige Warnhinweise nicht gegeben wurden oder durch routinemäßige Hinweise die **Resozialisierung** gefährdet war. Durch ein gemeinsam mit dem Justizministerium erarbeitetes Verfahrensmodell konnten wir erreichen, dass die Vermittlungsstellen – so genannte Freie Träger der Straffälligenhilfe – von der Staatsanwaltschaft einen Hinweis über zu vermeidende Einsatzbereiche, nicht jedoch Informationen über das gesamte strafrechtliche Vorleben des Betroffenen bekommen.*

12. *Seit der letzten Änderung des Landesmeldegesetzes müssen Kinder bis zur Vollendung des 27. Lebensjahres auch die Daten ihrer Eltern bei der melderechtlichen Anmeldung nachweisen. Bei einer kreisfreien Stadt wurden zu diesem Zweck von den Meldepflichtigen regelmäßig Kopien der Personalausweise der Eltern gefordert und gegebenenfalls bei Nichtvorlage ein Bußgeldverfahren eingeleitet. Aufgrund unseres Hinweises, dass solche Unterlagen nicht der Verfügungsgewalt und damit der Auskunftspflicht der meldepflichtigen Kinder unterliegen, sind die anhängigen Bußgeldverfahren eingestellt worden. Soweit Betroffene künftig keinen ausreichenden Nachweis erbringen können, soll im Wege der Amtsermittlung eine telefonische Bestätigung von der Wohnsitzgemeinde der Eltern eingeholt werden.*

13. *Urlaubsgastgebern von Gefangenen im Rahmen des Hafturlaubes wurde bislang ein Einwilligungsformular zur Einholung von Auskünften über die Gastgeber vorgelegt, das nicht erkennen ließ, an welche Stellen die JVA herantreten wollte, um sich von der Geeignetheit der **Urlaubsadresse** zu überzeugen, und was mit den erhobenen Daten danach geschieht. Dies konnte die betroffenen Gastgeber in unangenehme Situationen bringen. Auf unsere Anregung hin wurde ein neuer Vordruck eingeführt, der die beabsichtigte Datenerhebung und -verarbeitung klarer beschreibt.*

14. *Viele **Bankkunden** fühlten sich bei der Benutzung von Selbstbedienungsterminals von anderen Kunden beobachtet. Wir wirkten darauf hin, dass die Kreditinstitute künftig verstärkt Terminals mit Sichtschutzfilter verwenden. Bei Banken und Sparkassen, die übergangsweise noch alte Terminals nutzen, veranlassten wir die Einrichtung von Diskretionszonen.*

15. *Über ihre so genannten Multimediarechner tauscht die Polizei **E-Mails** mit Bürgern aus. Die Betroffenen wurden nicht auf das Ausspähungsrisiko hingewiesen. Jetzt bietet die Polizei ausdrücklich die Verschlüsselung von E-Mails an. Außerdem werden entsprechende „Warnhinweise" erteilt.*

16. *Informationen über **Auftragssperren** wurden bislang nach dem Gießkannenprinzip breit gestreut. Dadurch konnte für Firmen großer Schaden entstehen, insbesondere wenn sich später die Gründe für die Auftragssperre als nicht stichhaltig erwiesen. Nach unserer Intervention hat die Gebäudemanagement Schleswig-Holstein den Sachbereich neu organisiert und eine Dienstanweisung vorbereitet.*

17. *Bislang blieben belastende Informationen auch dann auf Dauer in Sicherheitsüberprüfungsakten gespeichert, wenn sie verjährt und in allen anderen Registern bereits gelöscht waren. „**Jugendsünden**" konnten so über Jahrzehnte gespeichert bleiben. Nunmehr sollen derartige nicht mehr benötigte Informationen ausgesondert und vernichtet werden.*

18. *Bislang wurde die Tatsache des **Sozialhilfebezuges** von Ausländern routinemäßig an die Ausländerbehörden übermittelt, auch wenn dies im Einzelfall nicht erforderlich war. Nach einer neuen Regelung entfällt die Übermittlung künftig in den Fällen, in denen die übermittelnde Stelle die fehlende Erforderlichkeit erkennen kann.*

19. *Bei der öffentlichen Auslegung von Planungsunterlagen im Rahmen von **Planfeststellungsverfahren** wurden die Grundstückseigentümer namentlich genannt. Künftig wird das Landesamt für Straßenbau und Straßenverkehr die Grundstücke nur mit Nummern bezeichnen, die erst bei Bedarf den Grundstückseigentümern zugeordnet werden.*

20. *Patientendaten dürfen an **privatärztliche Verrechnungsstellen** nur mit schriftlicher Einwilligung des Patienten weitergegeben werden. Dies wurde bislang nicht durchgängig beachtet. Nunmehr hat die Privatärztliche Verrechnungsstelle Schleswig-Holstein/Hamburg alle Mitglieder per Rundschreiben auf die Rechtslage hingewiesen und außerdem Mustertexte zur Verfügung gestellt.*

21. *Psychotherapeuten mussten dem Zulassungsausschuss für Ärzte Falldokumentationen vorlegen. Dadurch konnten sensible **Therapiedaten** offenbart werden. Wir veranlassten den Zulassungsausschuss, künftig auch pseudonymisierte Fälle zu akzeptieren.*

16 DATENSCHUTZAKADEMIE Schleswig-Holstein

Terminübersicht für die Kurse der DATENSCHUTZAKADEMIE Schleswig-Holstein 2001

Kurse/Seminare/Workshops	Kurz-bez.	Zeit	Ort
Landesdatenschutzgesetz 2000	R 5	07.02.2001	KYC-Kiel
Systemdatenschutz nach LDSG 2000	T 5	08.02.2001	KYC-Kiel
Behördliche Datenschutzbeauftragte nach LDSG 2000	BDSB 5	09.02.2001	KYC-Kiel
Technischer Datenschutz an Schulen	LT 4	27.02.2001	IPTS
Landesdatenschutzgesetz 2000	R 6	06.03.2001	KYC-Kiel
Systemdatenschutz nach LDSG 2000	T 6	07.03.2001	KYC-Kiel
Behördliche Datenschutzbeauftragte nach LDSG 2000	BDSB 6	08.03.2001	KYC-Kiel
Datenschutz an der Schule	L26	15.03.2001	IPTS
Behördliche Datenschutzbeauftragte Recht	DR 1	26. – 27.03.2001	Leck
Datensicherheitsrecht, Prüfung und Bewertung von Sicherheitsmaßnahmen durch behördliche Datenschutzbeauftragte	DT 1	28. – 30.03.2001	Leck
Windows NT Sicherheit I	NT-I 1	03. – 06.04.2001	Leck
Landesdatenschutzgesetz 2000	R 7	25.04.2001	Bordesholm
Systemdatenschutz nach LDSG 2000	T 7	26.04.2001	Bordesholm
Datenschutz an der Schule	L27	02.05.2001	IPTS
Informationsfreiheitsgesetz Schleswig-Holstein	IFG 1	03.05.2001	KYC-Kiel
Einstieg in das Datenschutzrecht	E 10	09.05.2001	KYC-Kiel
Schutz von Personaldaten	P 9	10. – 11.05.2001	Bordesholm
Landesdatenschutzgesetz 2000	R 8	28.05.2001	Bordesholm
Systemdatenschutz nach LDSG 2000	T 8	29.05.2001	Bordesholm
Technischer Datenschutz an Schulen	LT 5	29.05.2001	IPTS
Datenschutz bei der Internet-Nutzung	NET 3	29. – 30.05.2001	KYC-Kiel
Technik und Recht von Firewalls	FW 7	31.05.2001	KYC-Kiel
Einführung Datenschutz im Schulsekretariat	ES 9	13.06.2001	Bordesholm
Windows NT Sicherheit II	NT-II 1	12. – 15.06.2001	Leck
Landesdatenschutzgesetz 2000	R 9	25.06.2001	Bordesholm
Systemdatenschutz nach LDSG 2000	T 9	26.06.2001	Bordesholm
Informationsfreiheitsgesetz Schleswig-Holstein	IFG 2	10.07.2001	KYC-Kiel
Einführung Kommunalbereich	EK 9	11.07.2001	KYC-Kiel
Behördliche Datenschutzbeauftragte nach LDSG 2000	BDSB 7	12.07.2001	Bordesholm
Beauftragte für Sozialdatenschutz	S 9	03. – 07.09.2001	Leck
Führung von Personalakten	PA 9	10. – 11.09.2001	Bordesholm
Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung im Anwendungsbereich des LDSG	SIL 1	14.09.2001	KYC-Kiel
Datenschutz in der Wirtschaft – Schwerpunkte der Datenschutzaufsicht in Schleswig-Holstein	DWI 1	18.09.2001	KYC-Kiel
Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung im Anwendungsbereich des BDSG	SIB 1	19.09.2001	KYC-Kiel
Einführung Datenschutz im Schulsekretariat	ES 10	20.09.2001	Bordesholm

Kurse/Seminare/Workshops	Kurz-bez.	Zeit	Ort
IT-Revision	ITR 1	24.09.2001	Bordesholm
Datenschutz an der Schule	L28	26.09.2001	IPTS
Windows NT Sicherheit I	NT-I 2	25. – 28.09.2001	Leck
Behördliche Datenschutzbeauftragte Recht	DR 2	08. – 09.10.2001	Leck
Datensicherheitsrecht, Prüfung und Bewertung von Sicherheitsmaßnahmen durch behördliche Datenschutzbeauftragte	DT 2	10. – 12.10.2001	Leck
Personaldatenverarbeitung im Rahmen des Mitbestimmungsrechts	PR 5	10.10.2001	Bordesholm
Datenschutz im Sozialamt	SOZ 3	16.10.2001	KYC-Kiel
Das neue Bundesdatenschutzgesetz	BDSG 1	17.10.2001	KYC-Kiel
Landesdatenschutzgesetz 2000	R 10	05.11.2001	Bordesholm
Systemdatenschutz nach LDSG 2000	T 10	06.11.2001	Bordesholm
Datenschutz bei der Internet-Nutzung	NET 4	13. – 14.11.2001	KYC-Kiel
Technik und Recht von Firewalls	FW 8	15.11.2001	KYC-Kiel
Workshop zur Datensicherheit	SIW 7	14. – 16.11.2001	Leck
Datenschutz an der Schule	L29	22.11.2001	IPTS
Behördliche Datenschutzbeauftragte nach LDSG 2000	BDSB 8	27.11.2001	Bordesholm
Einstieg in das Datenschutzrecht	E 11	04.12.2001	KYC-Kiel
Workshop für Datenschutzbeauftragte	DW 5	05.12.2001	KYC-Kiel
Informationsfreiheitsgesetz Schleswig-Holstein	IFG 3	06.12.2001	KYC-Kiel
Technischer Datenschutz an Schulen	LT 6	11.12.2001	IPTS
Windows NT Sicherheit II	NT-II 2	11. – 14.12.2001	Leck
Das neue Bundesdatenschutzgesetz	BDSG 2	18.12.2001	KYC-Kiel

Das Jahresprogramm 2001 der DATENSCHUTZAKADEMIE Schleswig-Holstein mit näheren Informationen zu den Veranstaltungen und Anmeldeformularen kann kostenlos angefordert werden.

Schleswig-Holstein
DATENSCHUTZAKADEMIE

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Düsternbrooker Weg 82, 24105 Kiel
ab 01.06.2001: Holstenstr. 98, 24103 Kiel
Fax: 0431/988-1223
E-Mail: akademie@datenschutzzentrum.de

Das Programm ist auch auf unserer Homepage im Internet verfügbar:

www.datenschutzzentrum.de/akademie/

http://

17 Sommerakademie 2001

Die Sommerakademie 2001 findet am

10. September 2001 im Kieler Schloss

statt. In diesem Jahr treffen sich Fachleute und Interessierte zum Thema

Datenschutz als Wettbewerbsvorteil

In der Vergangenheit wurde der Datenschutz gelegentlich als Wettbewerbsnachteil empfunden. Bei der Verabschiedung des ersten Bundesdatenschutzgesetzes wurde beispielsweise davor gewarnt, den deutschen Unternehmen könnten nicht vertretbare hohe Kosten entstehen, die die Wirtschaft im Ausland nicht zu tragen habe. Seit dem In-Kraft-Treten der Europäischen Datenschutzrichtlinie ist dieser Argumentation der Boden entzogen, denn sie führt im Ergebnis in allen Mitgliedstaaten zu einem vergleichbaren Datenschutzstandard. Sogar Drittländer werden zu angemessenen Datenschutzmaßnahmen veranlasst.

Seit einigen Jahren hat sich die Nachfrage der Bürgerinnen und Bürger nach einem effizienten, praktikablen Datenschutz spürbar erhöht, nicht nur in Deutschland und Europa, sondern insbesondere auch in den USA. Bei der Suche nach den Gründen für die bislang eher bescheidenen Erfolge beim E-Commerce wird deutlich, dass eine der Ursachen für die zögerliche Haltung der Kunden im fehlenden Vertrauen in das Datenschutz- und Datensicherheitsangebot der Internet-Branche liegt. Die Menschen erwarten offenbar nicht nur günstige Preise und bequeme Einkaufsmodalitäten, sondern auch einen pfleglichen Umgang mit ihren personenbezogenen Daten. Die New Economy wird auf Dauer ohne überzeugendes Datenschutzangebot nicht auskommen.

Die Diskussion über Safe-Harbor-Principles, Datenschutzaudit, Gütesiegel und Privacy Policies zeigt, dass viele Unternehmen verstanden haben, dass sie den Kunden auch auf dem Gebiet des Datenschutzes etwas bieten müssen. Ein überzeugender, nachprüfbarer Datenschutzservice könnte sich in Zukunft als Wettbewerbsvorteil erweisen. Mehr noch: Der Standort eines Unternehmens in einem Land mit gutem Datenschutzstandard könnte helfen, das Vertrauen des Publikums zu erringen. Wird der Datenschutz sogar zum Wettbewerbsvorteil für die Regionen in der globalen Wirtschaft?

Die Sommerakademie 2001 geht der Frage nach, was dran ist an der These vom „Datenschutz als Wettbewerbsvorteil“. Sie möchte den Fakten auf den Grund gehen und darauf aufbauend ermitteln, welche Änderungen in der Datenschutzgesetzgebung und -politik notwendig sind, damit der Datenschutz tatsächlich sein Image von einer hoheitlich auferlegten Pflicht hin zu einer gerne wahrgenommenen – weil Vorteile versprechenden – Obliegenheit verändert. In Vorträgen und Diskussionen mit Wissenschaftlern, Wirtschaftsfachleuten und Experten aus dem

In- und Ausland soll näher beleuchtet werden, ob und unter welchen Voraussetzungen die Konvergenz von Grundrechtsschutz und marktwirtschaftlichem Denken gelingen kann.

An der Vorbereitung und Durchführung der Sommerakademie 2001 wirken u. a. mit:

Heinz-Werner **Arens**, Präsident des Schleswig-Holsteinischen Landtages; Dr. Bruno **Baeriswyl**, Datenschutzbeauftragter des Kantons Zürich; Grietje **Bettin**, Mitglied des Deutschen Bundestages; Dr. Johann **Bizer**, Johann Wolfgang Goethe-Universität, Frankfurt; Dr. John **Borking**, Vizepräsident der Registratiekamer, Den Haag; Wolfgang **Brockhaus**, Geschäftsführer der TÜV Nord Security GmbH, Hamburg; Prof. Dr. Alfred **Büllesbach**, Konzernbeauftragter für Datenschutz der DaimlerChrysler AG, Stuttgart; Prof. Dr. Hans H. **Driftmann**, Präsident der UVNord – Vereinigung der Unternehmensverbände in Hamburg und Schleswig-Holstein; Dr. Ralf **Ehrhardt**, Geschäftsführer der Curiavant Internet GmbH, Nürnberg; Dr. Wolfgang **Ewer**, Fachanwalt für Verwaltungsrecht, Vorsitzender des Umweltgutachterausschusses beim Bundesumweltministerium, Kiel; Dr. Riccardo **Genghini**, Notar in Mailand; Georg **Gorrissen**, Landrat des Kreises Segeberg; Dr. Günter **Hörmann**, Geschäftsführer der Verbraucher-Zentrale Hamburg e. V.; Werner **Hornberger**, Datenschutzbeauftragter der SAP AG, Walldorf; Dr. Joachim **Jacob**, Bundesbeauftragter für den Datenschutz, Bonn; Thomas **Königshofen**, Konzerndatenschutzbeauftragter der Deutschen Telekom AG, Bonn; Christopher **Kuner**, Morrison & Foerster, Brüssel; Otto Christian **Lindemann**, Vorstandssprecher und Vorstand Neue Medien der Beate Uhse AG, Flensburg; Prof. Dr. Edda **Müller**, Vorstand des Bundesverbandes der Verbraucherzentralen und Verbraucherverbände, Berlin; Prof. Dr. Günter **Müller**, Albert-Ludwigs-Universität, Freiburg; Burckhard **Nedden**, Landesbeauftragter für den Datenschutz Niedersachsen; Prof. Dr. Horst W. **Opaschowski**, wissenschaftlicher Leiter des BAT-Freizeit-Forschungsinstituts, Hamburg; Hans-Joachim **Otto**, Mitglied des Deutschen Bundestages; Prof. Dr. Andreas **Pfitzmann**, Technische Universität Dresden; Dr. Kai **Rannenberg**, Microsoft Research Cambridge; Prof. Dr. Alexander **Roßnagel**, Universität Gesamthochschule Kassel; Heide **Simonis**, Ministerpräsidentin des Landes Schleswig-Holstein; Prof. Dr. Albert **von Mutius**, Lorenz-von Stein-Institut für Verwaltungswissenschaften, Vorsitzender des Kuratoriums der DATENSCHUTZAKADEMIE Schleswig-Holstein; Dr. Armgard **von Reeden**, Privacy Officer für IBM EMEA (Europa, Naher Osten und Afrika), Brüssel; Prof. Dr. Reinhard **Voßbein**, Unternehmens- und Informations-Management (UIMC), Wuppertal; Michael **Waidner**, IBM Zürich Research Laboratory; Prof. Dr. Peter **Wedde**, quid! Projektbüro, Frankfurt; Dr. Thilo **Weichert**, stellvertretender Landesbeauftragter für den Datenschutz Schleswig-Holstein; Dr. Helmut **Bäumler**, Landesbeauftragter für den Datenschutz in Schleswig-Holstein.

Information und Anmeldung beim
Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein
Düsternbrooker Weg 82 / 24105 Kiel

Neue Adresse ab 01.06.2001: Holstenstraße 98 / 24103 Kiel

Telefon: 0431/988-1200 / Telefax: 0431/988-1223
E-Mail: mail@datenschutzzentrum.de

www.datenschutzzentrum.de/somak/somak01/somak01.htm

Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein

Geschäftsverteilungsplan einschließlich Teilzeitstellen

Düsternbrooker Weg 82, 24105 Kiel
Postfach 71 21, 24171 Kiel

Neue Adresse ab 01.06.2001:
Holstenstraße 98, 24103 Kiel
Postfach 71 16, 24171 Kiel

Telefon: 0431/988-1200, Telefax: 0431/988-1223
E-Mail: mail@datenschutzzentrum.de
Homepage: http://www.datenschutzzentrum.de

Leiter des ULD SH und Landesbeauftragter für den Datenschutz:	**Dr. Helmut Bäumler**
Dienstanschluss:	0431/988-1200
Vorzimmer:	Monika Harks App. 1202
Stellvertreter des Landesbeauftragten für den Datenschutz:	**Dr. Thilo Weichert** App. 1205
Gleichstellungsbeauftragte:	Dr. Susanne Rublack App. 1204
Vorsitzende des Personalrats:	Marit Köhntopp App. 1214
Behördlicher Datenschutzbeauftragter:	Thomas Lenz App. 1219

Referat LD 1
Dr. Helmut Bäumler
App. 1200

Silke Molt App. 1203	Vorbereitung der Sitzungen der Konferenz der Datenschutzbeauftragten Haushalt, Beschaffung Allgemeine Fortbildung Allgemeine Verwaltungsangelegenheiten der Dienststelle Reisekostenabrechnung Personalangelegenheiten
Monika Harks App. 1202	Öffentlichkeitsarbeit Vorbereitung von Veranstaltungen Vorbereitung von Publikationen Interne Fortbildung Führung der Urlaubs-, Kranken- und Dienstbefreiungsdatei Aufbewahrung der Zeitwertkarten
Dr. Folker Westphal App. 1208	Herausgabe von Publikationen in elektronischer und Papierform Präsentation von Informationen im Internet Betreuung der DATENSCHUTZAKADEMIE Schleswig-Holstein
Frank Möller App. 1396	Vorbereitung von elektronischen Publikationen
Heike Reimann App. 1209 Katrin Caspari App. 1210	Registratur Beschaffung von Büromaterial Sekretariat

Referat LD 2

Lukas Gundermann App. 1215	Grundsatzfragen des Datenschutzes Recht der neuen Medien Novellierung des Landesdatenschutzgesetzes Elektronisches Grundbuch
Jürgen von der Ohe App. 1206	Datenschutz im Bereich des Personal-, Wahl-, Melde-, Ausweis-, Kommunal-, Gewerbe-, Bau-, Wirtschafts- und Personenstandswesens

LD 21

Dr. Claudia Golembiewski App. 1395	Juristische Betreuung des Projektes „AN.ON“

Referat LD 3	
Uwe Jürgens App. 1211	Datenschutz im Bereich der Steuerverwaltung
Heiko Behrendt App. 1212	Systemdatenschutz, insbesondere Grundsatzfragen der Datensicherheit und der ordnungsgemäßen Anwendung der DV-Programme
Thomas Lenz App. 1219	Prüfung von Rechenzentren Prüfung und Beratung von Behörden, soweit Fragen der automatisierten Datenverarbeitung berührt sind Mitwirkung bei der Erstellung von Gutachten
Referat LD 4	
Dr. Thilo Weichert App. 1205	Datenschutz im Ausländerbereich Datenschutz im Bereich der Parlamentsverwaltung
Torsten Koop App. 1218	Datenschutz im Sozial- und medizinischen Bereich
Holger Brocks App. 1207	Datenschutz im Bereich der Landwirtschaftsverwaltung, des Kataster-, Statistik-, Verkehrs-, Umweltschutz-, Planungs-, Zivil- und Katastrophenschutzwesens und im Kultusbereich sowie in Bereichen, für die keine andere Zuständigkeit festgelegt ist, fachübergreifende Fragen der Wissenschaft und der Forschung
LD 41	
Margitta Welz App. 1222	Juristische Betreuung des Projekts „Sichere IT-Nutzung in Aus- und Weiterbildung“
Referat LD 5	
Dr. Susanne Rublack App. 1204	Internationales Datenschutzrecht
Torsten Wähling App. 1228	Datenschutz im Polizei-, Verfassungsschutz- und Justizbereich
Silke Molt App. 1203	

Referat LD 6	
Marit Köhntopp App. 1214	Grundsatzfragen der neuen Medien und Informations-technologien Technischer Datenschutz Technikfolgenabschätzung EDV-Einsatz der Dienststelle Leitung der Modellprojekte
Jan Ziegler App. 1213	EDV-Einsatz der Dienststelle Anbindung der Dienststelle an das Internet und andere Netze Führung des Verzeichnisses gem. § 7 Abs. 4 LDSG
Gebhard Uehlken App. 1229	Interne Schulung
Markus Wiese App. 1392	
Andreas Schmidt App. 1393	Betreuung des Projekts „Anonyme und unbeobachtete Internet-Nutzung“ unter Aspekten des Datenschutzes
Dr. Thomas Probst App. 1217	Betreuung des Projekts „BioTrusT“ unter Aspekten des Datenschutzes
Martin Rost App. 1391	Betreuung des Projekts „Virtuelles Datenschutzbüro“
Roman Maczkowsky App. 1247	
Referat LD 7	
Birthe Köster App. 1216	Grundsatzfragen des Informationszugangsrechts
Referat LD 8	
Dr. Thomas Petri App. 1394	Datenschutz im nichtöffentlichen Bereich
Hans Heinrich Sieh App. 1253	
Referat LD 9	
Dr. Anja Diek App. 1398	Gütesiegel und Datenschutzaudit

Beim **ULD SH** erhältliche Publikationen:

Neues Datenschutzrecht in Schleswig-Holstein
Text des Landesdatenschutzgesetzes, der Datenschutzverordnung, des Informationsfreiheitsgesetzes, der Regelungen zum Datenschutzaudit und Datenschutzgütesiegel und des Bundesdatenschutzgesetzes (Neuauflage ab Juni 2001)

Tätigkeitsbericht
des letzten Jahres als Landtagsdrucksache

Faltblätter
Safer Surfen!: Verschlüsseln – Ich?
Safer Surfen!: Selbst sicher(n)!
Safer Surfen!: Ich bin drin! ... Und meine Daten?
Datenschutz im Melderecht ... und was Sie persönlich davon haben
Virtuelles Datenschutzbüro – Virtual Privacy Office
Sicherheit durch Anonymität – Security by Anonymity
Datenschutzgerechte Biometrie – Privacy-compliant Biometrics
Das Informationsfreiheitsgesetz Schleswig-Holstein

Broschüren
backUP-Magazin für IT-Sicherheit (Reihe)
Datenschutz leicht gemacht – Praxistipps zum Datenschutzrecht (Reihe)
Sich wohl fühlen in der Informationsgesellschaft – Das ULD stellt sich vor

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

DATENSCHUTZAKADEMIE Schleswig-Holstein
Jahresprogramm 2001

Schleswig-holsteinische Datenschutzinformationen im Internet
Datenschutzinformationen aus Schleswig-Holstein sind natürlich auch im weltweiten Datennetz zugänglich: **http://www.datenschutzzentrum.de** (Homepage des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein). Zurzeit sind die Rechtsnormen des Bundes und des Landes zum Datenschutz, das Informationsfreiheitsgesetz, das Programm der DATENSCHUTZAKADEMIE Schleswig-Holstein, Informationen zu den Sommerakademien, die Tätigkeitsberichte der letzten Jahre, Pressemitteilungen und weitere Publikationen im elektronischen Format abrufbar. Weiterhin ist dort der öffentliche Schlüssel des Unabhängigen Landeszentrums für Datenschutz erhältlich.

Datenschutz auf CD-ROM
Wie jedes Jahr bringen wir eine CD-ROM mit dem Inhalt des Tätigkeitsberichtes und der zum Zeitpunkt der Veröffentlichung dieses Berichtes auf der Homepage bereitstehenden Informationen heraus. Für Benutzer, die über kein eigenes Programm verfügen, um die internetgerechten Dateien anzuschauen, wird ein einfacher Offline-Browser mitgeliefert. Die CD-ROM kann beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein kostenlos angefordert werden.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z