SCHLESWIG-HOLSTEINISCHER LANDTAG **Drucksache 15/3300**
15. Wahlperiode 2004-05-06

Bericht

des Unabhängigen Landeszentrums für Datenschutz

Schleswig-Holstein

Tätigkeitsbericht 2004

Tätigkeitsbericht 2004

des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

Berichtszeitraum: 2003, Redaktionsschluss: 25.02.2004
Landtagsdrucksache 15/3300

(26. 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 Tüpfelchen auf dem i

Im 24. Tätigkeitsbericht (Tz. 1.3) hatten wir die Prognose gewagt, das Unabhängige Landeszentrum für Datenschutz werde sich von einer reinen Aufsichtsbehörde immer mehr zu einem **Innovationszentrum** weiterentwickeln. In den vergangenen zwei Jahren ist dieser Prozess so weit fortgeschritten, dass nunmehr auch der entsprechende organisatorische Rahmen geschaffen werden konnte. Die steigende Zahl von eigenen Modellprojekten, die zunehmenden Angebote aus der Wirtschaft und aus der Wissenschaft an das ULD zur Beteiligung an Projekten und der Erfolg der abgeschlossenen Projekte (vgl. Tz. 8) haben die Einrichtung eines neuen Arbeitsbereiches mit der Bezeichnung Unabhängiges Landeszentrum für Datenschutz – Innovationszentrum (ULD-i) notwendig gemacht.

Das ULD-i wird unsere Projekte im Datenschutz- und Datensicherheitsbereich künftig professionell von der Antragsphase bis zur Abwicklung begleiten. Vor allem wird das ULD-i Partner aus der Wirtschaft und Wissenschaft der Region für gemeinsame Projekte zusammenführen. Damit in engem Zusammenhang steht die weitere Aufgabe, die Ergebnisse von Modellprojekten und das dabei entstandene Know-how in die Praxis, und das heißt in erster Linie in konkrete Produkte, zu überführen. Die IT-Unternehmen der Region sollen in Zusammenarbeit mit den bewährten Institutionen wie der Industrie- und Handelskammer, der Technologietransferzentrale, den Hochschulen des Landes, insbesondere dem Multimedia-Center in Kiel und der International School of New Media in Lübeck, sowie den Verbänden der IT-Branche mit dem neuesten **Know-how** aus dem Bereich der **Privacy Enhancing Technologies** versorgt werden. Die Anschubfinanzierung für ULD-i stammt aus den Fördermitteln des Regionalprogramms 2000, das von der Europäischen Union finanziell getragen wird.

Kurz vor Redaktionsschluss dieses Berichtes kam das Land Schleswig-Holstein in einem Innovationswettbewerb, an dem sich 126 europäische Regionen beteiligen konnten, mit dem ULD-Projekt „Datenschutz-Gütesiegel“ in der Kategorie Informationsgesellschaft unter die besten, d. h. innovativsten drei Regionen. Dass man mit dem Thema „Datenschutz“ in einem Innovationswettbewerb der Europäischen Union ganz vorne landen kann, ist eine vor wenigen Jahren noch kaum vorstellbare Entwicklung. Nichts könnte den Wandel des Unabhängigen Landeszentrums für Datenschutz von der traditionellen Aufsichtsbehörde hin zu einem Motor der **technologischen Innovation** besser dokumentieren als die Gründung des **ULD-Innovationszentrums.**

1.2 Die Hausaufgaben gemacht

Neben diesen Neuerungen liefen bei uns auch im Berichtsjahr die typischen Tätigkeiten einer Datenschutzkontroll- und Aufsichtsbehörde ungeschmälert weiter. Die Bürgerinnen und Bürger konnten sich darauf verlassen, dass wir uns bei der **Verteidigung der Grundrechte** gegen Zumutungen der Politik oder gegen unverantwortliche technische Entwicklungen stets an vorderster Linie befanden

(vgl. Tz. 4.2.2, 4.2.4, 4.2.5, 4.5.1, 7.1). Mit unserer Aktion „Rote Karte für Internet-Schnüffler“ und im Rahmen von Stellungnahmen und Presseerklärungen haben wir, wann immer es aus unserer Sicht notwendig war, energisch, vernehmbar und in der Sache eindeutig Partei für das Recht auf informationelle Selbstbestimmung ergriffen.

Die **datenschutzrechtlichen Kontrollen** wurden auch im Berichtsjahr angemeldet oder unangemeldet kontinuierlich fortgesetzt (vgl. Tz. 4.3.1, 4.7.12, 4.7.14, 5.2, 5.6, 6.7.1, 6.7.2, 6.7.3). Inzwischen wurde mit einem flächendeckenden Kontrollprogramm begonnen, an dessen Ende in absehbarer Zeit alle Kommunen in Schleswig-Holstein in puncto Datensicherheit überprüft sein werden (vgl. Tz. 6.7).

Entsprechend dem seit Jahren bestehenden Trend wurde auch die **Beratung** von Wirtschaft, Verwaltung und IT-Branche bei der Einführung neuer Technologien und Verfahren fortgesetzt. Beispiele für den manchmal zähen, zunehmend aber angenehm konstruktiven Dialog mit den Machern der Informationstechnik finden sich unter Tz. 2, 4.7.5, 4.7.6, 4.7.10, 4.8.1, 6.1, 6.3, 6.5, 6.6, 8.3, 8.4, 8.5, 9.1.3, 10.1, 10.2, 10.3, 10.4, 10.6, 10.7, 10.8, 11.2, 11.3, 11.4. Hinter diesen Textziffern und den dort geschilderten Beratungen neuer technischer Entwicklungen verbergen sich viele stille, häufig kleine, manchmal auch große Erfolgsgeschichten des Datenschutzes. Das geringe Aufheben, das gemeinhin um diese Beratungstätigkeit im Vorfeld neuer Verfahren gemacht wird, steht jedenfalls in einem umgekehrten Verhältnis zu den großen Effekten, die mit einer datenschutzgerechten Informationstechnik erzielt werden.

1.3 Datenschutz-Audit und Datenschutz-Gütesiegel in Schleswig-Holstein: Herr Schily, übernehmen Sie!

Datenschutz-Audit und Datenschutz-Gütesiegel sind den Kinderschuhen entwachsen und haben sich zu **erfolgreichen Innovationsinstrumenten** des Datenschutzes entwickelt. Die Zertifizierungsanträge aus der Wirtschaft laufen auch nach dem Ende der von der EU geförderten Modellprojekte (vgl. Tz. 8.1) unvermindert weiter. Schon jetzt bewegt sich das Datenschutz-Gütesiegel von den Fallzahlen her im Bereich der seit Jahren in Deutschland etablierten Zertifizierungsverfahren IT-Grundschutz und Common Criteria.

Die Behörden in Schleswig-Holstein nehmen bei **Beschaffungen** zunehmend ihre Verpflichtung aus dem LDSG wahr, vorrangig Produkte mit dem Datenschutz-Gütesiegel einzusetzen; das Gebäudemanagement Schleswig-Holstein ist mit gutem Beispiel vorangegangen (Tz. 9.1.5). Erstmals konnten im Berichtszeitraum Firmen von ihren Erfahrungen mit dem Datenschutz-Gütesiegel berichten. Offenbar zahlt sich das Gütesiegel aus. Ein Unternehmen ließ beispielsweise verlautbaren, dass sich die Aufwendungen binnen weniger Wochen amortisiert hätten.

Leider ist der Wirkungskreis des schleswig-holsteinischen Gütesiegels aus Gründen der Gesetzgebungszuständigkeit begrenzt. Bis der Bund endlich die gesetzlichen Voraussetzungen auf **Bundesebene** schafft, versuchen sich die Unternehmen zu behelfen, so gut es geht. Manche gehen dazu über, uns um Bescheinigungen

darüber zu bitten, dass ihr Produkt die Voraussetzungen für ein schleswig-holsteinisches Gütesiegel erfüllen würde, wenn es denn zulässig wäre, ein solches zu beantragen. Schon davon erhofft man sich also Marktvorteile. Bleibt nur die Aufforderung an den Bundesinnenminister: **„Herr Schily, übernehmen Sie!“**

http://www.datenschutzzentrum.de/audit/obschily.htm

2 Datenschutz in Deutschland

Das Thema der nächsten Jahre: Biometrie

Mit dem technischen Fortschritt zu kleineren und immer leistungsfähigeren Mikrochips gewinnen biometrische Verfahren eine immer größere Bedeutung. Biometrie steht für eine Technologie, mit deren Hilfe die **einzelne Person** anhand **unverwechselbarer**, häufig **unveränderlicher** mit ihr verbundener „lebensechter“ **Kennzeichen** von anderen unterschieden werden kann. Solche Verfahren sind nicht neu: Zumindest aus Kriminalfällen ist jedem das Verfahren zum Vergleich von Fingerabdrücken bekannt. Auch der Abgleich von Gesichtsfotos ist ein biometrisches Verfahren, das zur Unterscheidung von Personen dient. Die fortschreitende Digitalisierung hat die Leistungsfähigkeit biometrischer Verfahren erhöht, aber auch ihre spezifischen Datenschutzrisiken. Elektronisch gesteuerte Sensoren vermessen einzelne Körperteile, ihre digitalen Abbilder können auf kleinsten Speichermedien abgelegt, automatisiert mit anderen Personendaten verglichen und schließlich mit Zusatzinformationen über den Merkmalsträger versehen werden.

Neben dem Vergleich von Fotografien und Fingerabdrücken werden mittlerweile auch DNA-Analysen von Körpergeweben wie beispielsweise von Hautpartikeln oder Haaren zum Zwecke der Identifizierung durchgeführt. Zur **Verfolgung von Straftaten** gibt es in der Strafprozessordnung hierfür eine Rechtsgrundlage, über deren Ausweitung derzeit rechtspolitisch auf Bundesebene gestritten wird. Riskant sind diese Verfahren wegen der für den eigentlichen Zweck nicht benötigten „überschießenden“ Informationen. Neben der Analyse der so genannten „nicht codierenden Teile“ fallen regelmäßig auch **Zusatzinformationen** über die einzelne Person an. Sie können eine Bestimmung des Geschlechts, des Alters, die Zugehörigkeit zu einer bestimmten Ethnie, aber auch die Kenntnis über bestimmte Krankheiten ermöglichen.

Die besondere Sensibilität solcher Informationen erschließt sich dem Betroffenen spätestens dann, wenn eine **Versicherung** oder der Arbeitgeber vor Abschluss eines Vertrages die für eine eindeutige Identifizierung gewonnenen biometrischen Informationen zur Bestimmung einer Risikogruppe verwenden will: Der Arbeitgeber ist aber kein Arzt, und auch die Versicherung ist weniger an der Gesundheit ihrer Kunden als an der Minimierung ihrer eigenen Ausfallrisiken interessiert. Dem einen oder anderen mag dies noch als Zukunftsmusik erscheinen. Allzu fern sind solche Anwendungen allerdings nicht, wie Beispiele aus dem Ausland zeigen. Von Fachkreisen wird daher schon lange das Verbot eines so genannten „Negativattestes“ gefordert, mit dessen Hilfe sich beispielsweise Versicherungen oder Arbeitgeber das Nichtvorhandensein einer bestimmten Eigenschaft, insbesondere einer Krankheit bestätigen lassen wollen, um einen für sie unwirtschaftlichen Vertragsschluss vermeiden zu können. Welche Dimensionen die **wirtschaftlichen Interessen** annehmen können, zeigt das Beispiel von genetischen Datenbanken z. B. in Island, deren Aufbau von der Pharmaindustrie betrieben wird. Ihr Ziel ist nicht weniger als die Kartierung der genetischen Informationen der **gesamten Bevölkerung**.

Auch keine Zukunftsmusik, sondern Realität ist die Anwendung biometrischer Verfahren zur Identifizierung von berechtigten Personen in Wirtschaft und Verwaltung. Vor allem der Zugang zu Hochsicherheitssystemen und -bereichen wird mittlerweile mithilfe von vorab gespeicherten biometrischen Informationen der **Zugangsberechtigten** gesteuert. Eine elektronische Schleuse gibt den Weg erst frei, wenn das biometrische Merkmal des Besuchers mit dem bereits vorab in einer Datenbank gespeicherten Merkmal übereinstimmt. Für diese Anwendung ist der Fingerabdruck weit verbreitet, gefolgt von dem Abdruck der gesamten Hand sowie der Vermessung der Iris. Beim Fingerabdruck beispielsweise untersucht und vermisst ein Sensor den Verlauf der Papillarlinien und hält insbesondere Lage sowie Art der so genannten „Minutien“ fest, die bei jedem Menschen anders verlaufen. Andere Verfahren von bislang noch geringer praktischer Bedeutung sind die Gesichtserkennung, die insbesondere wegen ihrer technischen Verknüpfung mit einer automatisierten Videoüberwachung zukünftig von Bedeutung sein wird, der Anschlag bei der Bedienung der Tasten eines Terminals, den der Kunde beispielsweise bei einem Geldautomaten oder einem Computer bedient, oder die allerdings noch nicht weit entwickelte Spracherkennung.

Konjunktur hat die öffentliche Förderung der Biometrie seit den Terroranschlägen vom 11. September 2001. Was bislang nur für Hochsicherheitstrakte und kleine Benutzergruppen praktikabel erschien, soll nun Schritt für Schritt für den Aufbau einer international kompatiblen **Identifikationsinfrastruktur** eingeführt werden. Im Vordergrund steht das Ziel, die Ströme ein- und ausreisender Personen zu überwachen und zu kontrollieren. Die ersten rechtlichen Voraussetzungen für die Aufnahme digitalisierter biometrischer Merkmale in Personalausweise und Reisepässe sind in Deutschland mit dem Terrorismusbekämpfungsgesetz aus dem Jahr 2002 getroffen worden. Rechtlich ist es nunmehr möglich, die Ausweisdokumente mit Chips auszustatten, auf denen bestimmte biometrische Merkmale der Ausweisinhaber gespeichert werden, die dann zu Kontrollzwecken von den zuständigen Behörden ausgelesen werden können. Ein erster Feldversuch mit der Erfassung der Iris ist auf freiwilliger Basis im Februar 2004 vom Bundesgrenzschutz am **Frankfurter Flughafen** gestartet worden. Erfahrungen werden von deutschen Behörden auch bei der Vergabe von Visa an Ausländerinnen und Ausländer aus Drittstaaten gesammelt – so in Lagos/Nigeria mit Fingerabdrücken und in Jakarta/ Indonesien mit einer digitalen Gesichtserkennung (vgl. Tz. 4.4).

Die internationale Dimension dieser **Biometriepolitik** verdeutlicht ein Beschluss der Justiz- und Innenminister der Mitgliedstaaten der **Europäischen Union** vom 27. November 2003, mit dem unionsweit eine grundsätzliche politische Einigung über die Einführung biometrischer Merkmale in VISA und Aufenthaltstiteln von Bürgern aus Drittstaaten erzielt wurde. Künftig sollen das Gesichtsbild sowie die Abdrücke von zwei Fingern in einen in das Ausweisdokument implementierten Chip aufgenommen werden. Ferner soll 2004 über die Einzelheiten der Einführung eines „Europäischen Visumsinformationssystems“ entschieden werden, das schengenweit einen Abgleich der Visumsanträge ermöglichen soll, um auf diese Weise Mehrfachanträge unterbinden zu können.

Was zunächst nur für Ausländer aus Drittstaaten gilt, wird bald auch für die Unionsbürger zum Standard werden. Für Anfang 2004 hat die EU-Kommission Vorschläge zur Einführung biometrischer Merkmale in die **Pässe der Unionsbür-**

ger angekündigt. Nach einem Beschluss des Rates vom 19./20. Juni 2003 soll die EU-Kommission ein einheitliches Konzept biometrischer Merkmale in Ausweisdokumenten gewährleisten. Für zusätzlichen Handlungsdruck sorgen vor allem die Vereinigten Staaten von Amerika, da auch EU-Bürger ab dem 24. Oktober 2004 für die Einreise in die USA Pässe mit biometrischen Merkmalen vorweisen müssen. Andernfalls unterliegen auch EU-Bürger zukünftig einer Visumspflicht; Visa werden künftig von den USA nur gegen die Bereitstellung biometrischer Merkmale, und zwar in Form eines Fotos sowie zweier digitaler Fingerabdrücke, erteilt.

Voraussetzung für die Verfügbarkeit biometrischer Merkmale in nationalen Ausweisdokumenten ist die **Interoperabilität** der nationalen Systeme. Derzeit werden die technischen Anforderungen und Schnittstellen von den internationalen Standardisierungsgremien genormt. Für die Gestaltung der Reisedokumente sind insbesondere die Arbeiten der Internationalen Luftfahrtorganisation (ICAO) von Bedeutung. Mit Rücksicht auf ihre weltweite Verwendung, insbesondere in den wirtschaftlich nicht entwickelten Staaten der Dritten und Vierten Welt, wird als Mindeststandard das Lichtbild vorgeschlagen. Darüber hinaus ermöglicht die Standardisierung aber auch die Aufnahme des Fingerabdruckes und/oder eines Irisabbildes.

Die politischen Entscheidungen für die Einführung von biometrischen Verfahren sind gefallen. Nun gilt es, durch eine möglichst **datenschutzfreundliche Gestaltung** dieser Anwendungen Schäden für die informationelle Selbstbestimmung zu verhindern. So macht es beispielsweise sowohl aus Sicht des Datenschutzes als auch aus Sicherheitsgründen einen großen Unterschied, ob die biometrischen Merkmale aller Bürgerinnen und Bürger in einer Zentraldatei oder in vernetzbaren dezentralen Dateien gespeichert werden oder ob die Authentifizierung des Ausweisinhabers auf einen Abgleich des aktuell gemessenen biometrischen Merkmals mit dem auf dem Ausweis gespeicherten beschränkt bleibt. In der ersten Variante droht eine neue Form der Überwachungskultur – in der zweiten Variante lassen sich die Risiken minimieren, ohne die angestrebten Sicherheitsgewinne zu vernachlässigen. Von Bedeutung sind aber auch der Schutz der biometrischen Merkmale vor einem unberechtigten Zugriff sowie ihre für den Betroffenen transparente Verwendung. Mit Rücksicht auf ihre Eindeutigkeit und Unveränderlichkeit gilt es auszuschließen, dass biometrische Merkmale durch die elektronischen Netze „vagabundieren“. Sie müssen im Prinzip in der **Verfügungsgewalt der Betroffenen** bleiben.

Der Gesetzgeber verbindet mit der Einführung biometrischer Verfahren große Erwartungen; er sollte sich aber auch der Risiken bewusst sein und sie konstruktiv zu minimieren versuchen. Wir haben uns in den vergangenen Jahren mit den datenschutzrechtlichen und sicherheitstechnischen Implikationen biometrischer Verfahren intensiv beschäftigt. Durch unsere Mitarbeit im Projekt **BioTrust** (vgl. 24. TB, Tz. 9.3) signalisierten wir die Zukunftsrelevanz dieses Themas. In zwei ausführlichen Gutachten für das **Büro für Technikfolgenabschätzung beim Deutschen Bundestag** (TAB) haben wir im Jahr 2001 sowie 2003 die Wirkungsweise biometrischer Verfahren analysiert und dem Gesetzgeber und der Öffentlichkeit Handlungsempfehlungen unterbreitet. Im Zusammenhang mit dem Terrorismusbekämpfungsgesetz haben wir in einer weiteren Expertise die **verfassungs-**

rechtlichen Grenzen für einen Einsatz biometrischer Verfahren aufgezeigt. Danach müssen biometrische Daten auf Ausweisdokumenten auch aus verfassungsrechtlichen Gründen in der ausschließlichen Verfügungsgewalt der Bürgerinnen und Bürger verbleiben. Das Beispiel der Biometrie zeigt wie kein anderes, dass die datenschutzgerechte Gestaltung der besonderen technischen und rechtlichen Kompetenz bedarf. Das Unabhängige Landeszentrum für Datenschutz bemüht sich darum, diesen Sachverstand den Bürgerinnen und Bürgern dieses Landes, aber auch den Mitgliedern in Parlament und Regierung zur Verfügung zu stellen.

3 Datenschutz im Landtag

Nach der erfolgreichen Durchführung von zwei Datenschutz-Audits und der Etablierung eines wirkungsvollen Datenschutzmanagementsystems ist der Schutz personenbezogener Daten im Parlament des Landes schon fast zur Routine geworden.

Das im Jahr 2001 eingerichtete Datenschutzgremium des Landtags Schleswig-Holstein, in dem wir beratend vertreten sind, erweist sich als eine segensreiche Einrichtung. Dort werden schon im Konzeptstadium von Planungen auftauchende Datenschutzfragen erörtert und den verantwortlichen Gremien Beratung angeboten. So wird sichergestellt, dass im Rahmen des Landtagsumbaus beim **Sicherheitskonzept** keine Bewegungsprofile von Abgeordneten im Hause erstellt werden können, aus denen abzulesen ist, welcher Abgeordnete sich wann mit wem und wo getroffen hat.

Eine seiner Hauptaufgaben sieht das Gremium also darin, den Datenschutz im Parlament präventiv sicherzustellen. Daher wurde von ihm z. B. die Durchführung von Datenschutz-Audits angeregt (vgl. 25. TB, Tz. 3.2). Dem dient auch die Information der Abgeordneten durch das Informationsblatt „**Tipps und Hinweise**“:

www.sh-landtag.de/parlament/datenschutz/hinweise-fuer-abge.pdf

und das „Hinweisblatt für Abgeordnete zum datenschutzgerechten **Umgang mit Petitionsdaten**“:

www.sh-landtag.de/parlament/datenschutz/
hinweise-fuer-abge-petitionsdaten.pdf

Im Laufe des Jahres gingen die ersten **Datenschutzbeschwerden** ein, für deren Behandlung das Datenschutzgremium als Kontrollinstanz des von der Exekutive unabhängigen Parlaments zuständig ist. In einem Fall musste das Gremium allerdings einer religiösen Sekte die Auskunft über die Beratungen im Petitionsausschuss verweigern, weil hier das parlamentarische Beratungsgeheimnis die Transparenzansprüche der Petenten verdrängte.

Was ist zu tun?
Die erfolgreiche Arbeit des Datenschutzgremiums sollte fortgeführt werden.

4 Datenschutz in der Verwaltung

4.1 Kommunalbereich

4.1.1 Welches Datenschutzrecht gilt für Stadtwerke?

Die Privatisierung öffentlicher Aufgaben ist sehr populär, insbesondere wenn es um Stadt- und Gemeindewerke geht. Das LDSG verhindert zwar, dass durch eine unkontrollierte „Flucht in das Privatrecht“ die datenschutzrechtlichen Standards verfallen. Soweit sich der Staat allerdings von Aufgaben dauerhaft verabschiedet, kann auch das LDSG nicht mehr angewendet werden.

Es gibt einige Geschäftsbereiche ehemals kommunaler Betriebe, für die nach wie vor das LDSG gilt. Für andere ist das BDSG anwendbar. In der Praxis kommt es auch zu **Mischkonstellationen**, die die Frage aufwerfen, nach welchen Vorschriften behördliche bzw. betriebliche Datenschutzbeauftragte zu bestellen sind.

Nach dem LDSG gelten Organisationen auch dann als öffentliche Stellen, wenn sie zwar als juristische Person des Privatrechts (wie z. B. GmbH oder AG) organisiert sind, jedoch wirtschaftlich von den dahinter stehenden Verwaltungsträgern beherrscht werden, und wenn sie Aufgaben der öffentlichen Verwaltung wahrnehmen. Dazu gehörten nach älterer Rechtsprechung die Versorgung der Bürger mit grundlegenden **Infrastrukturleistungen** wie Gas, Wasser und Strom. Wir hatten daher bisher die Auffassung vertreten, die meisten von Stadtwerken wahrgenommenen Aufgaben seien Aufgaben der öffentlichen Verwaltung im Sinne des LDSG (vgl. 23. TB, Tz. 4.1.4).

Aufgaben der öffentlichen Verwaltung?

Allerdings hat der Staat mittlerweile einen Teil dieser Aufgaben in den privaten Sektor abgegeben. Dies galt zunächst vor allem für den Bereich der **Telekommunikation**. Zwischenzeitlich wurde auch die **Stromversorgung** aus dem staatlichen Monopol in den Wettbewerb überführt. Rechtliche Grundlage dafür war die Umsetzung einer EG-Richtlinie im Energiewirtschaftsgesetz (EnWG). Eine vergleichbare Regelung gibt es für die **Gasversorgung**, wo ebenfalls eine europäische Richtlinie die Liberalisierung vorschreibt. Die Versorgung mit Strom und Gas kann damit nicht länger als Aufgabe der öffentlichen Verwaltung angesehen werden. Dies hat zur Folge, dass für die Datenverarbeitung in diesen Geschäftsfeldern nicht das LDSG, sondern der dritte Abschnitt des BDSG für private Unternehmen anzuwenden ist.

Allerdings gibt es nach wie vor einige Bereiche, die als Aufgaben der öffentlichen Verwaltung angesehen werden müssen und für die nach wie vor das LDSG gilt. Dies trifft z. B. auf die **Trinkwasserversorgung** zu. Eine Liberalisierung des Wassermarktes hat bisher nicht stattgefunden. In diesem Bereich besteht noch der Anschluss- und Benutzungszwang, der regelmäßig von den Gemeinden und Kreisen per Satzung durchgesetzt wird, um die erforderliche Trinkwasserqualität gewährleisten zu können. Auch die **Abwasserbeseitigung** und die Versorgung

mit **Fernwärme** sind weiterhin als Aufgaben der öffentlichen Verwaltung anzusehen. Der öffentliche **Personennahverkehr** ist nach dem Regionalisierungsgesetz (RegG) eine öffentliche Aufgabe, nicht aber der Charter- und Fernverkehr.

Diese Differenzierung kann zur Folge haben, dass in **einem Unternehmen** personenbezogene Daten aus verschiedenen Geschäftsbereichen **unterschiedlichen Datenschutzgesetzen** unterfallen. Bei der Nutzung einer gemeinsamen Kundendatenbank für die Geschäftsbereiche ist dies zu berücksichtigen. Grunddaten der Kunden können zusammen mit den Zusatzdaten aus den Bereichen Strom und Gas nach den Vorschriften des BDSG verarbeitet werden, wogegen im Übrigen die kundenfreundlicheren Regelungen des LDSG zu beachten sind. Natürlich sind die Stadtwerke rechtlich nicht gehindert, auch bei der Verarbeitung von Daten aus den Bereichen, die dem BDSG unterfallen, die materiellen Regelungen des LDSG zugrunde zu legen.

Im Wortlaut:
§§ 1 und 2 Regionalisierungsgesetz

§ 1 Öffentliche Aufgabe, Zuständigkeit

(1) Die Sicherstellung einer ausreichenden Bedienung der Bevölkerung mit Verkehrsleistungen im öffentlichen Personennahverkehr ist eine Aufgabe der Daseinsvorsorge.
(2) Die Stellen, die diese Aufgabe wahrnehmen, werden durch Landesrecht bestimmt.

§ 2 Begriffsbestimmungen

Öffentlicher Personennahverkehr im Sinne dieses Gesetzes ist die allgemein zugängliche Beförderung von Personen mit Verkehrsmitteln im Linienverkehr, die überwiegend dazu bestimmt sind, die Verkehrsnachfrage im Stadt-, Vorort- oder Regionalverkehr zu befriedigen. Das ist im Zweifel der Fall, wenn in der Mehrzahl der Beförderungsfälle eines Verkehrsmittels die gesamte Reiseweite 50 Kilometer oder die gesamte Reisezeit eine Stunde nicht übersteigt.

Auch für übergreifende Verarbeitungen personenbezogener Daten vor allem im Bereich **Personalwesen** muss differenziert werden, ob die jeweilige Tätigkeit eher mit den Bereichen Strom und Gas oder Wasser und Fernwärme zusammenhängt. Hier bietet es sich an, zur Sicherheit auf die materiellen Vorgaben des LDSG abzustellen, die in der Regel einen besseren Datenschutz gewährleisten.

Bestellung von Datenschutzbeauftragten?

Ein wesentlicher Unterschied zwischen den Regelungen des LDSG und denen des BDSG ergibt sich im Hinblick auf die Bestellung von **Datenschutzbeauftragten**. Während diese nach dem BDSG für die Betriebe verpflichtend ist, sieht das LDSG die Bestellung von behördlichen Datenschutzbeauftragten lediglich als Möglichkeit vor. Allerdings kann nach dem BDSG auch ein externer Beauftragter bestellt werden, wogegen nach dem LDSG ein Mitarbeiter der Stelle selbst die Funktion wahrnehmen muss und allenfalls die Bestellung eines gemeinsamen Beauftragten mehrerer Stellen in Betracht kommt. Danach wäre es an sich geboten, lediglich für die Datenverarbeitungen, die dem BDSG unterliegen, einen (gegebenenfalls externen) Datenschutzbeauftragten zu bestellen. Im Hinblick auf die übrigen Datenverarbeitungsprozesse käme die (zusätzliche) freiwillige Bestellung eines internen (oder gemeinsamen) Datenschutzbeauftragten in Betracht. Ein

solches Vorgehen wäre wenig realitätsnah und auch unzweckmäßig. Da die Bestellung nach dem BDSG verpflichtend vorgeschrieben ist, muss davon ausgegangen werden, dass die Stadtwerke für den entsprechenden Bereich Datenschutzbeauftragte benennen. Es macht keinen Sinn, darüber hinaus auch für den dem LDSG unterfallenden Bereich zusätzlich einen weiteren Datenschutzbeauftragten zu bestellen.

Die Problematik der Bestellung **externer Datenschutzbeauftragter** ist bei diesen Stellen auch für die dem LDSG unterliegenden Daten in der Regel nicht so groß wie bei anderen öffentlichen Stellen und vor allem bei Behörden. Nach dem LDSG stehen den Datenschutzbeauftragten umfassende Kontrollrechte zu, die sie auch zum Zugriff auf die zu kontrollierenden Daten ermächtigen. Da bei den Behörden in vielen Fällen sehr **sensible Daten** über die Bürger vorliegen, ist die Wahrnehmung des Amtes als behördlicher Datenschutzbeauftragter im Regelfall eigenen Mitarbeitern vorbehalten. Damit soll eine übermäßige Öffnung der behördlichen Datenbestände für Verwaltungsexterne vermieden werden. Bei den hier in Rede stehenden Stadt- und Gemeindewerken liegen allerdings in aller Regel keine allzu sensiblen Daten vor.

Deshalb kann in solchen Fällen von der bisherigen Auslegung des LDSG abgegangen werden, wonach nur Mitarbeiter von öffentlichen Stellen zu Datenschutzbeauftragten bestellt werden dürfen. Aus unserer Sicht ist es auch akzeptabel, wenn bei einem Unternehmen, das als öffentliche Stelle anzusehen ist, das aber zudem auch Daten verarbeitet, die unter das BDSG fallen, einheitlich für beide Bereiche ein Datenschutzbeauftragter bestellt wird. Dabei kann es sich unseres Erachtens auch um einen nach dem BDSG zulässigen **externen Datenschutzbeauftragten** handeln.

Was ist zu tun?
Stadt- und Gemeindewerke sollten in jedem Fall die Datenschutzinteressen ihrer Kunden beachten und sich im Zweifel an die strengeren materiellen Vorgaben des LDSG halten.

4.1.2 Erhebung von Kalkulationsdaten für die Änderung von Abgabensatzungen

Sollen die Bemessungsgrundlagen einer Abgabensatzung geändert werden, benötigt die Kommune zur Kalkulation der zu erwartenden Einnahmen bereits im Vorwege Daten von den Betroffenen. Eine solche Verarbeitung personenbezogener Daten erfordert in jedem Fall eine ausreichende Befugnisgrundlage.

In einer Gemeinde war beabsichtigt, die **Bemessungsgrundlagen** für die Erhebung der Abwassergebühren umzustellen. Statt nach der Menge sollte sich die Höhe der Gebühr künftig nach der Nutzungsart und Größe der bebauten Flächen richten. Der Gemeinde war nur die Höhe des Gesamtgebührenbedarfs bekannt. Um daraus die für eine Satzungsänderung notwendige Festlegung der Höhe des Gebührenmaßstabs ableiten zu können, mussten die umlagefähigen Flächen der betroffenen Grundstücke ermittelt werden. Hierfür kam nur eine Datenerhebung bei den Betroffenen in Betracht.

Der für die Umstellung des Gebührenmaßstabes vorhandene Ratsbeschluss reichte als Befugnisgrundlage für die beabsichtigte **zwangsweise Datenerhebung** nicht aus, da diese nur durch eine Rechtsvorschrift im datenschutzrechtlichen Sinne legitimiert werden konnte. Auch die vorhandene Abwassergebührensatzung kam als Ermächtigung nicht in Betracht. Sie erlaubte nämlich nur eine Erhebung von Daten über den Frischwasserbezug. Die Gemeinde kam deshalb nicht umhin, die Ermittlung der umlagefähigen Flächen vor der Datenerhebung bei den Betroffenen in einer **Nachtragssatzung** zu regeln.

Was ist zu tun?
Kommunen müssen darauf achten, dass Datenerhebungen aus Anlass der beabsichtigten Änderung von Gebührenmaßstäben einer Satzungsregelung bedürfen.

4.1.3 Auskünfte an politische Mandatsträger

Änderungen bei den Auskunftsansprüchen kommunaler Mandatsträger in der Gemeindeordnung führten zu Unsicherheiten in der Praxis. Um eine landeseinheitliche Handhabung zu ermöglichen, haben wir dazu Anwendungshinweise veröffentlicht.

Mit der Änderung der Gemeindeordnung (GO) zum April 2003 wurden die individuellen **Auskunftsansprüche der Gemeindevertreter** und bürgerlichen Ausschussmitglieder gegenüber dem Bürgermeister erweitert. Vorbild der Regelung war das Informationsfreiheitsgesetz.

Durch die Neuregelung des § 30 GO ergeben sich gegenüber der bisherigen Rechtslage **drei Veränderungen** des Auskunftsrechts:

- Wegfall der Begrenzung der Auskünfte zum Zweck der „Vorbereitung oder Kontrolle der Ausführung einzelner Beschlüsse“,
- Erweiterung des Anspruches auf „Aufgaben zur Erfüllung nach Weisung“,
- bürgerlichen Mitgliedern der Ausschüsse steht künftig ein Auskunftsanspruch über Vorgänge ihres Aufgabenbereiches zu.

Im Wortlaut:
§ 30 Abs. 1 und 2 Gemeindeordnung (GO)

(1) Einzelnen Gemeindevertreterinnen oder -vertretern hat die Bürgermeisterin oder der Bürgermeister in allen Selbstverwaltungsangelegenheiten und zu allen Aufgaben zur Erfüllung nach Weisung auf Verlangen Auskunft zu erteilen und Akteneinsicht zu gewähren. Gleiches gilt für die nicht der Gemeindevertretung angehörenden Mitglieder von Ausschüssen für den Aufgabenbereich ihres Ausschusses sowie Mitglieder von Ortsbeiräten und sonstigen Beiräten für die Angelegenheiten ihres Beirates.

(2) Auskunft und Akteneinsicht dürfen nicht gewährt werden, wenn die Vorgänge nach einem Gesetz geheim zu halten sind oder das Bekanntwerden des Inhalts die berechtigten Interessen Einzelner beeinträchtigen kann. Soweit Auskunft und Akteneinsicht zulässig sind, dürfen diese Rechte bei Personalakten nur den Mitgliedern des Personalausschusses und den Mitgliedern des Hauptausschusses bei der Wahrnehmung personalrechtlicher Befugnisse gewährt werden. Gleiches gilt für Mitglieder anderer Ausschüsse für Akten, deren Inhalt spezialgesetzlich geschützt ist.

Für Vorgänge, die personenbezogene Daten betreffen, ergeben sich hieraus erhebliche Beschränkungen. Zu beachten sind Gesetze, die zur Geheimhaltung verpflichten, z. B. die Datenschutzgesetze des Bundes und des Landes sowie bereichsspezifische Datenschutzvorschriften wie etwa der Sozialdatenschutz und das Steuergeheimnis. Ein tragender Grundsatz des Datenschutzrechts ist das **Erforderlichkeitsprinzip**. Danach ist eine Verarbeitung personenbezogener Daten nur dann zulässig, wenn (und soweit) sie zur rechtmäßigen Erfüllung der durch Rechtsvorschrift zugewiesenen Aufgaben der Daten verarbeitenden Stelle erforderlich ist. Für die Auskunftsansprüche von Gemeinderatsmitgliedern und Ausschussmitgliedern bedeutet dies, dass sie nicht allein mit den allgemeinen Aufgaben der Gemeindevertretung bzw. der Ausschüsse begründet werden können. Die begehrten Informationen müssen vielmehr im Zusammenhang mit einer **konkreten Aufgabenerfüllung** des einzelnen Auskunftsbegehrenden stehen. Insoweit kommt es durch die Neuregelung faktisch zu keiner Erweiterung des Auskunftsrechts im Hinblick auf die Bekanntgabe personenbezogener Daten.

Dieser funktionale **Zusammenhang** zwischen **Aufgabe** und **Informationsanspruch** führt dazu, dass jedes Ausschussmitglied nur diejenigen Auskünfte bzw. Akten verlangen kann, die in seine funktionale Zuständigkeit fallen. Beispiele: Personalakten nur an Personalausschuss- bzw. Hauptausschussmitglieder, Bauakten nur an Bauausschussmitglieder und Steuerakten nur an Finanzausschussmitglieder.

Die Auskunftsverpflichtung gegenüber der Gemeindevertretung nach § 36 Abs. 2 GO erstreckt sich nunmehr ausdrücklich auch auf **Aufgaben zur Erfüllung nach Weisung**. Gleichzeitig ist die GO um einen Auskunftsanspruch für die Ausschüsse ergänzt worden.

Im Wortlaut: § 36 Abs. 2 GO

(2) Die Bürgermeisterin oder der Bürgermeister ist verpflichtet, der Gemeindevertretung und einzelnen Gemeindevertreterinnen oder -vertretern zu allen Selbstverwaltungsaufgaben sowie zu den Aufgaben zur Erfüllung nach Weisung Auskunft zu erteilen; sie oder er kann sich hierbei vertreten lassen, wenn nicht eine Fraktion oder ein Drittel der gesetzlichen Zahl der Gemeindevertreterinnen und -vertreter widerspricht. Der Bürgermeisterin oder dem Bürgermeister ist auf Wunsch das Wort zu erteilen. Sie oder er kann zu den Tagesordnungspunkten Anträge stellen.

Dem Wortlaut nach sind die Auskunftsansprüche **während der Sitzungen** nicht beschränkt. Von dem individuellen Anspruch unterscheiden sie sich dadurch, dass sie sich nur auf Auskunft erstrecken. Dies kann aber nicht dazu führen, die Persönlichkeitsrechte dem Informationsrecht von Gemeindevertretung und Ausschüssen schrankenlos unterzuordnen. Die Regelungen über diese **Gremienauskunftsansprüche** enthalten insoweit offensichtlich eine Regelungslücke. § 30 Abs. 2 GO, der einen vergleichbaren Problemkreis regelt, ist geeignet, diese Lücke zu füllen. Er sollte folglich auch für die Erfüllung dieser Auskunftsansprüche analog angewandt werden. Ansonsten könnten die einem generellen Auskunftsrecht entgegenstehenden Rechte Dritter, denen § 30 Abs. 2 GO gerade Rechnung tragen will, durch Verlagerung der Anfrage in die Sitzung der Gemeindevertretung bzw. der Ausschüsse unterlaufen werden. Dies gilt insbesondere auch deshalb, weil durch die Erweiterung der Auskunftsansprüche auf Pflichtaufgaben zur Erfüllung

nach Weisung Auskünfte über Vorgänge verlangt werden könnten, die nicht zur originären Zuständigkeit der Gemeindevertretung gehören.

Nähere Informationen unter:


www.datenschutzzentrum.de/material/themen/bekannt/auskbmgo.htm

Was ist zu tun?
Kommunen müssen bei Auskünften an politische Mandatsträger die in den Hinweisen aufgezeigten Grenzen beachten.

4.1.4 Ostsee-Card

Die vorgesehene Einführung eines Chipkartensystems zur Zahlung der Kurabgabe und zur Nutzung touristischer Angebote bietet auf technischer Ebene die Möglichkeit, sehr detaillierte Profile über das Verhalten der Kurgäste zu erstellen. Werden die bisher in Absprache mit uns vorgesehenen Schutzvorkehrungen realisiert, kann das System gleichwohl datenschutzkonform betrieben werden.

Fast alle größeren Kurorte an der schleswig-holsteinischen Ostseeküste, die von ihren Gästen eine Kurabgabe verlangen, schlossen sich im Jahr 2002 mit dem Ziel zusammen, ein einheitliches, chipkartenbasiertes Verfahren zur Erhebung der **Kurabgabe** einzuführen. Damit soll es möglich werden, mit der in einer Gemeinde erworbenen Kurkarte auch die Einrichtungen der anderen Teilnehmergemeinden in Anspruch zu nehmen. Das Besondere an dem Modell ist, dass auch private Anbieter mit ihren Leistungen in das Verfahren aufgenommen werden. Es können preisgünstigere Pakete gebucht werden, in denen der Besuch interessanter und häufig frequentierter Freizeiteinrichtungen im Land Schleswig-Holstein enthalten ist. Dieses Modell gibt es zwar schon in einigen Regionen, wo regionale Rabattkarten für Touristen angeboten werden. Das Zusammenführen dieses Elementes mit einer chipkartenbasierten Lösung zur Erhebung der Kurabgabe für eine ganze Region ist jedoch deutschlandweit einmalig. Sie unterscheidet sich von den regionalen Karten vor allem darin, dass keine Freiwilligkeit hinsichtlich des Erwerbs der Karte besteht. Jeder Kurgast muss eine entsprechende Karte erwerben. Damit führt er zugleich seinen Kurbeitrag ab und ist zur Nutzung der kommunalen Einrichtungen berechtigt.

Da jeder Nutzungsvorgang und jede Kontrolle elektronisch erfasst werden, wäre es theoretisch möglich, ein **feinmaschiges Datenprofil** einzelner Kurgäste anzulegen – vom Strandzugang über den Gebrauch öffentlicher Verkehrsmittel bis hin zum Besuch touristischer Angebote.

Wir beraten den Ostseebäderverband datenschutzrechtlich. Die Datenverarbeitung im Hintergrundsystem, in dem die Daten gespeichert werden, soll datenschutzgerecht gestaltet werden, sodass ein unmittelbarer **Zugriff** auf die Datensätze einzelner Personen ohne Zutun der Betroffenen **ausgeschlossen** ist. Zum Zeitpunkt

der Abfassung des Tätigkeitsberichts waren noch einige Details zu klären. Dazu gehörte insbesondere die Frage nach den Zugriffsrechten auf die auf der Karte gespeicherten Informationen. Nach unserer Auffassung muss dafür gesorgt werden, dass nicht jede Stelle, die berechtigt ist, auf der Karte eigene Leistungen abzubuchen, wie z. B. touristische Anbieter vor Ort, zugleich erkennen können, welche sonstigen Leistungen die Kurgäste noch auf der Karte haben, welche sie schon in Anspruch genommen haben und wie lange sie noch in dem Urlaubsort bleiben werden.

Was ist zu tun?
Der Ostseebäderverband und sonstige beteiligte Stellen sollten wie bisher konstruktiv mit uns daran arbeiten, dass für dieses sehr publikumsrelevante Verfahren datenschutzgerechte Lösungen gefunden und umgesetzt werden.

4.1.5 Übermittlung von Meldedaten an Bürgermeisterkandidaten

Die Übermittlung von Meldedaten zu Wahlwerbezwecken ist bereits mit Abgabe der Bewerbung an die Bewerber für ein Bürgermeisteramt zulässig. Ein Missbrauch der Daten ist in der Praxis nicht ausgeschlossen.

Im Rahmen einer Bürgermeisterwahl hatte ein Betroffener einen Wahlbrief erhalten, obwohl der betreffende Bürgermeisterkandidat zu diesem Zeitpunkt noch keine Zulassung als Bewerber hatte. Bei der zuständigen Gemeinde lag zwar eine **Bewerbung** vor, die Nominierung durch den Gemeindewahlausschuss stand aber noch aus. Gleichwohl waren dem Bewerber bereits Meldedaten für Wahlwerbezwecke zur Verfügung gestellt worden.

Nach Auffassung des Innenministeriums gebietet es der Grundsatz der Wahlgleichheit, jeder Wahlbewerberin oder jedem Wahlbewerber grundsätzlich die gleiche Chance im Wettbewerb um die Wählerstimmen offen zu halten. Die **Chancengleichheit** wäre verletzt, wenn Parteien (Fraktionen) unter Beachtung der im Landesmeldegesetz festgesetzten 6-Monatsfrist Melderegisterauskünfte zur Direktwahl erhielten, einzelnen Wahlbewerberinnen oder Wahlbewerbern zur Direktwahl (insbesondere den unabhängigen Einzelbewerberinnen oder Einzelbewerbern) dieses aber erst nach ihrer Zulassung als Kandidat möglich wäre. Die Zulassung erfolgt nämlich in der Regel erst 44 Tage vor der Wahl, sodass die Einzelbewerber einen wesentlich kürzeren Zeitraum zur Nutzung der Meldedaten für Wahlwerbezwecke zur Verfügung hätten. Daher müsse es auch einzelnen Direktwahlbewerberinnen oder Direktwahlbewerbern möglich sein, nach Einreichung des Wahlvorschlages im Zeitraum von 6 Monaten vor der Wahl Melderegisterauskünfte zum Zwecke der Wahlwerbung erhalten zu können.

Die vom Innenministerium vertretene Auffassung führt zu dem Problem, dass damit im Prinzip **jedermann die Möglichkeit** eröffnet wird, sich Zugang zu Meldedaten zu verschaffen. Es genügt bereits die Abgabe einer gegebenenfalls auch unvollständigen oder nicht plausiblen Bewerbung um das Amt eines Bürgermeisters für eine Meldedatenübermittlung. Ist noch keine Zulassung des Bewerbers durch den Wahlprüfungsausschuss erfolgt, so sollte die Übermittlung der Meldedaten unter der Bedingung erfolgen, dass bei einer Ablehnung der Bewer-

bung durch den Gemeindewahlausschuss die erhaltenen Daten unverzüglich zu löschen oder zurückzugeben sind.

Was ist zu tun?
Etwaige Missbrauchsfälle sollten zum Anlass genommen werden, die vorhandene Datenübermittlungsregelung zu überprüfen. Die Meldebehörden sollten daran denken, dass Betroffene bei jeder Ausstellung eines Personalausweises oder Passes über ihre Widerspruchsrechte gegen Datenübermittlungen zu Wahlwerbezwecken aufzuklären sind.

4.1.6 Vermerk des Kirchenaustritts im Familienbuch

Bereits zum Zeitpunkt der Eheschließung sollte man sich genau überlegen, ob man eine Eintragung der Religionszugehörigkeit in das Familienbuch wünscht. Wird das Einverständnis dazu erteilt, ist auch die spätere Eintragung eines eventuellen Kirchenaustritts unvermeidbar.

Aus Anlass seiner Eheschließung benötigte ein Mann eine beglaubigte **Abschrift aus dem Familienbuch** der Eltern. Daraus war zu entnehmen, dass die Eltern bereits seit langem aus der Kirche ausgetreten waren. Die Eltern sahen darin eine Verletzung ihrer Persönlichkeitsrechte, zumal sie seinerzeit über die Eintragung nicht einmal informiert worden waren.

Nach dem **Personenstandsgesetz** hat der Standesbeamte im Anschluss an die Eheschließung das Familienbuch anzulegen. Darin werden u. a. die rechtliche Zugehörigkeit oder Nichtzugehörigkeit zu einer Kirche, Religionsgemeinschaft oder Weltanschauungsgemeinschaft der Eheleute eingetragen, allerdings nur, wenn diese ihr Einverständnis dazu erteilen. In dem geprüften Fall war dies bei der Eheschließung geschehen.

Ist eine Eintragung einmal erfolgt, muss gegebenenfalls auch der spätere Austritt aus der Kirche in das Familienbuch eingetragen werden. Dies ist erforderlich, weil die Personenstandsbücher sowie daraus hergestellte Abschriften Beweiskraft haben und die ursprüngliche Eintragung über die Mitgliedschaft in der Kirche sonst falsch wäre. Das Familienbuch ist deshalb **ständig fortzuführen**. Eine Eintragung bedarf in diesem Zusammenhang weder eines Antrags noch der Einwilligung der Beteiligten.

Eine Aufklärung der Betroffenen über die Tatsache der Eintragung war zum damaligen Zeitpunkt (im Jahr 1978) noch nicht vorgeschrieben. Erst mit der Novellierung des Datenschutzrechts Anfang 1992 ist hier eine Verbesserung erfolgt. **Betroffene** sind seitdem z. B. beim Kirchenaustritt über die Weiterverarbeitung ihrer Daten **aufzuklären**.

Was ist zu tun?
Standesbeamte sollten Betroffene bereits bei der Eheschließung über die dargestellten Regelungen zur Führung des Familienbuches aufklären. Gleiches gilt für Eintragungen im Falle eines Kirchenaustritts.

4.1.7 Meldedatenübermittlung an die GEZ trotz Auskunftssperre?

Durch die Einrichtung einer Auskunftssperre im Melderegister sollen wichtige Rechtsgüter wie Leben, Gesundheit und persönliche Freiheit der Betroffenen unter besonderen Schutz gestellt werden. Um dieses Ziel zu erreichen, müssen auch die Kontrollmitteilungen an die Gebühreneinzugszentrale der Rundfunkanstalten (GEZ) unterbleiben.

Nach heftigen Streitigkeiten mit dem Ehemann war eine Frau in ein Frauenhaus gezogen. Die Meldebehörde hatte bei der Ummeldung zum Schutz der Frau eine Auskunftssperre vermerkt. Nur drei Wochen später stand der Ehemann, vor dem die Frau geflohen war, vor der Tür des Frauenhauses. Im Gespräch mit der Leiterin gab er an, die **neue Anschrift** per Telefon **von der GEZ** erhalten zu haben.

Dieses Beispiel zeigt deutlich, dass der Schutz der Betroffenen im Falle einer **Auskunftssperre** noch immer nicht ausreicht. Die Meldebehörden sind nämlich zurzeit verpflichtet, auch in diesen Fällen bei der Anmeldung Kontrollmitteilungen an die GEZ zu fertigen. Es ist weder ein Hinweis auf die Auskunftssperre vorgesehen, noch müsste die GEZ einen solchen Hinweis beachten.

Eine effektive Lösung des Problems ist nur möglich, wenn in Fällen einer solchen Auskunftssperre eine regelmäßige Datenübermittlung an die GEZ unterbleibt. Im Hinblick auf die anstehende **Novellierung des Landesmeldegesetzes** haben wir deshalb vorgeschlagen, die Ermächtigungsgrundlage für regelmäßige Datenübermittlung an die GEZ entsprechend zu beschränken. Das Innenministerium hat den Vorschlag begrüßt und ihn in seinen Referentenentwurf übernommen.

Was ist zu tun?
Der Gesetzgeber sollte bei der anstehenden Novellierung des Landesmeldegesetzes die Übermittlung von Kontrollmitteilungen an die GEZ im Falle einer Auskunftssperre ausschließen.

4.1.8 Ständig Änderungen im Melderecht

Die Halbwertzeiten gesetzlicher Regelungen im Melderecht werden immer kürzer. Der eigentliche Zweck des Meldewesens, nämlich die Identität der Einwohner und deren Wohnungen nachzuweisen, tritt immer mehr in den Hintergrund.

Im Jahr 2000 wurde im Landesrecht die **Personalausweisnummer** wegen fehlender Erforderlichkeit aus dem Katalog der Melderegisterdaten herausgenommen. Zu groß erschien die Gefahr, dass faktisch ein maschinenlesbares Personenkennzeichen entstehen würde. Die Ereignisse des 11. September 2001 beendeten offensichtlich diese Befürchtungen. Durch die Änderung des Melderechtsrahmengesetzes Anfang 2002 wurde die Personalausweisnummer überraschend wieder in den Datenkatalog des Melderegisters aufgenommen. Eine offizielle Begründung dafür ist uns nicht bekannt.

Ihren Fortgang nahm diese Entwicklung mit der **Novellierung des Waffenrechts**. Plötzlich war es erforderlich, die Inhaber waffenrechtlicher Erlaubnisse hinsichtlich ihres Aufenthaltsortes lückenlos zu kontrollieren. Dies setzte zwingend eine Speicherung waffenrechtlicher Erlaubnisse im Melderegister voraus, was vom Bundesgesetzgeber mit Artikel 5 des Gesetzes zur Neuregelung des Waffenrechts im Oktober 2002 erlaubt wurde. Zweifel, ob dadurch ein unbefugter Waffenbesitz oder -gebrauch tatsächlich verhindert werden kann, sind angebracht.

Den neuesten Coup enthält das Steueränderungsgesetz 2003. Danach sollen zum Zweck der Zuteilung einer dauerhaften Identitätsnummer die Meldebehörden dem Bundesamt für Finanzen die Daten aller gemeldeten Einwohner übermitteln. Danach sind alle Geburten sowie Personen anzuzeigen, die noch keine Nummer erhalten haben. Nach Vergabe der **Identifikationsnummer** soll diese vom Bundesamt für Finanzen an die Meldebehörden zurückgemeldet und dort im **Melderegister** gespeichert werden, um bei Veränderungen im Datensatz entsprechende Kontrollmitteilungen zu fertigen (vgl. Tz. 4.9.1). Dieses **einheitliche Personenkennzeichen** erhält durch die Speicherung bei den Meldebehörden eine besondere Qualität. Natürlich werden auch die Meldebehörden selbst dieses Datum zu Identifikationszwecken benutzen. Daran können auch noch so restriktive Zweckbindungsregelungen nichts ändern. Zudem stellt sich die Frage, wann die Begehrlichkeiten anderer Stellen so groß werden, dass man die vorgesehenen Verwendungsbeschränkungen aufweicht.

Nach unserer Auffassung muss es möglich sein, durch automatisierte Veränderungsmitteilungen der Meldebehörden ein steuerliches Zentralregister beim Bundesamt für Finanzen zu pflegen, ohne dabei gleichzeitig ein einheitliches Personenkennzeichen entstehen zu lassen. Als Zuordnungsmerkmale sollten Vor- und Familienname, Geburtsdatum sowie die alte Anschrift genügen.

Was ist zu tun?
Der Gesetzgeber sollte sich an den eigentlichen Zweck der Melderegister erinnern und deshalb eine Datenspeicherung für andere Verfahren im Melderegister nicht zulassen.

4.2 Polizeibereich

4.2.1 Bewährungshelfer als Hilfssheriff?

Wann darf ein Bewährungshelfer Daten seiner Probanden an die Polizei übermitteln? Was ist, wenn vonseiten des Gerichts eine Führungsaufsicht angeordnet worden ist? In beiden Fällen darf (gegebenenfalls muss) die Polizei eingeschaltet werden, wenn „Gefahr im Verzug“ ist.

Die Überwachung der Lebensführung eines zu einer Bewährungsstrafe Verurteilten obliegt nach den Bestimmungen der Strafprozessordnung dem Gericht. Der **Bewährungshelfer** wirkt an dieser gerichtlichen Überwachung mit. Der Bewährungshelfer kann die Polizei unterrichten, wenn er Anhaltspunkte dafür hat, dass sein Proband neue Straftaten begehen wird. Diese müssen aber so konkret sein, dass ein Eingreifen der Polizei **zur Gefahrenabwehr** auf der Grundlage des Poli-

zeirechts zu rechtfertigen ist. Nur wenn die Polizei überhaupt etwas unternehmen darf, macht es Sinn, sie zu unterrichten. Darüber hinausgehende „Kontrollmitteilungen“ vertragen sich nicht mit dem **Grundgedanken der Bewährungshilfe**, da der Verurteilte in der Bewährungszeit zeigen soll, dass er in der Lage ist, ein straffreies Leben zu führen. Würde man ihn von vornherein für so gefährlich halten, dass von ihm Gefahren für die Allgemeinheit drohen, käme eine Strafaussetzung zur Bewährung ohnehin nicht in Betracht.

Bei der richterlich oder gesetzlich angeordneten **Führungsaufsicht**, die das Gesetz für bestimmte Straftaten vorsieht, untersteht der Verurteilte einer Aufsichtsstelle. Das Gericht bestellt ihm einen Bewährungshelfer. Die Aufsichtsstelle überwacht mit Unterstützung des Bewährungshelfers das Verhalten des Verurteilten und die **Erfüllung von Weisungen**. Zweck dieser Überwachung ist es, gefährliche Entwicklungen beim Verurteilten rechtzeitig festzustellen und die Erfüllung von gerichtlich angeordneten Weisungen (z. B. sich nicht an bestimmten Orten aufzuhalten) sicherzustellen. Grundsätzlich darf die Polizei aber auch hier nur eingeschaltet werden, wenn dies zur Vermeidung von Straftaten notwendig ist.

Bei der Entscheidung, wann eine Datenübermittlung an die Polizei in Betracht kommt, ist also zu berücksichtigen, dass der Gesetzgeber das **Zusammenwirken** von Gericht, Bewährungshilfe, Aufsichtsstelle und Polizei **fein austariert** hat. In einer den Gerichten und Polizeibehörden des Landes bekannt gegebenen Stellungnahme hat sich das schleswig-holsteinische Justizministerium unserer Auffassung (vgl. auch 22. TB, Tz. 4.3.2) angeschlossen.

Was ist zu tun?
Bewährungshelfer dürfen keine routinemäßigen Datenübermittlungen an die Polizei vornehmen, sondern erst tätig werden, wenn sie Anhaltspunkte für neue Straftaten ihres Probanden haben.

4.2.2 Undifferenzierte Erweiterung der DNA-Analyse?

Gegenwärtig gibt es mehrere Gesetzesinitiativen auf Bundes- und Landesebene mit dem Ziel, die rechtlichen Anforderungen an die Entnahme und Untersuchung von Körperzellen und für die Speicherung der dabei gewonnenen DNA-Identifizierungsmuster in der zentralen DNA-Analysedatei des BKA abzusenken. Schleswig-Holstein zeichnete sich bislang durch eine gemäßigte und abgewogene Innenpolitik aus. Äußerungen des Innenministers könnten auf einen Kurswechsel in der schleswig-holsteinischen Innenpolitik hindeuten.

Bei dem Einsatz der DNA-Analyse für Zwecke der Strafverfolgung handelt es sich um ein relativ neues Instrument, mit dessen Hilfe schon in kurzer Zeit beachtliche Erfolge erzielt werden konnten. Es ist deshalb verständlich, dass über einen erweiterten Einsatz nachgedacht wird. Das Datenschutzrecht steht dem nicht prinzipiell entgegen. Es sind allerdings die **verfassungsrechtlichen Vorgaben**, insbesondere das Verhältnismäßigkeitsprinzip und die Rechtsprechung des Bundesverfassungsgerichts zu beachten.

Deshalb besteht kein Anlass zu einer undifferenzierten Betrachtungsweise, wie sie jüngst von führenden Bundes- und Landespolitikern angestellt worden ist. Die nach derzeitiger Rechtslage zulässigen Fälle sind noch nicht einmal vollständig beim BKA erfasst. Eine Angleichung der Erfassungsvoraussetzungen für DNA-Analysen an die routinemäßige erkennungsdienstliche Behandlung ist zudem kein taugliches Mittel, weil deren Voraussetzungen keineswegs präzise geregelt sind. Manche Politiker erwecken den unzutreffenden Eindruck, als seien dem genetischen Fingerabdruck weniger Informationen zu entnehmen als einem polizeilichen Lichtbild. Diese Bewertung greift zu kurz. Denn Betroffene haben es überhaupt nicht in der Hand, an welchen Orten sie genetische Spuren, wie zum Beispiel Haare oder Speichel, zurücklassen. Seine besondere Brisanz erhält der genetische Fingerabdruck durch die Kombination von **elektronischer Auswertbarkeit** für die Polizei und die mangelnde Kontrollmöglichkeit für die Betroffenen. Der Vorschlag des Innenministers setzt sich im Übrigen nicht mit der Rechtsprechung des Bundesverfassungsgerichts auseinander. Dieses hatte in seinen Entscheidungen gerade den Richtervorbehalt als einen wichtigen Aspekt der Rechtsschutzgarantie hervorgehoben.

Die in jüngster Zeit zunehmend zu hörende Einschätzung, die DNA-Analyse sei ohne jedes Risiko, geht fehl. Bereits heute ist es möglich, aus dem genetischen Fingerabdruck **Zusatzinformationen** über Alter, Geschlecht, Zuordnung zu Ethnien oder einzelne Krankheiten zu gewinnen. Angesichts der in den vergangenen Jahren erlebten ungemein stürmischen Entwicklung auf dem Gebiet der DNA-Analyse ist heute für niemanden absehbar, welche neuen Möglichkeiten diese Technik schon in wenigen Jahren bieten wird.

www.datenschutzzentrum.de/material/themen/polizei/dnaanalyse.htm

Was ist zu tun?
Der Gesetzgeber ist aufgefordert, bei gesetzlichen Änderungen im Bereich der DNA-Analyse Augenmaß zu bewahren.

4.2.3 Einsatzleitstellensystem Lübeck – dritter Anlauf

Die datenschutzgerechte technische Ausgestaltung des Einsatzleitstellensystems (ELS) der Polizeiinspektion Lübeck verzögert sich aufgrund fehlender finanzieller Mittel um ein weiteres Jahr. Vom Innenministerium wurde die Umsetzung der notwendigen technischen Vorkehrungen nunmehr für das Jahr 2004 zugesichert.

Wie bereits in früheren Tätigkeitsberichten (vgl. 24. TB, Tz. 4.2.4; 25. TB, Tz. 4.2.5) dargelegt, besteht mit den Verantwortlichen bei der Polizei Einigkeit darüber, dass die Recherchemöglichkeiten im ELS weit über das rechtlich zulässige Maß hinausgehen. Eine für das Jahr 2003 angekündigte Implementierung von technischen Tools, welche gewährleisten sollen, dass nur die Daten von tatverdächtigen bzw. für Gefahren verantwortlichen Personen für die Bewältigung von polizeilichen Einsatzlagen abgerufen werden können, konnte wegen **fehlender finanzieller Mittel** nicht umgesetzt werden. Nach Angaben des Innenministe-

riums sollen sich die Kosten für die aus datenschutzrechtlicher Sicht erforderlichen technischen Vorkehrungen auf ca. 9000 € belaufen. Da es sich bei dem genutzten System mittlerweile nicht mehr um die neueste Softwareversion handele, werde die bei der Einsatzleitstelle in Lübeck eingesetzte Software von der Herstellerfirma nicht mehr im Rahmen des Supports gepflegt; deshalb sei zusätzlich ein Releasewechsel erforderlich. Dieser soll zusätzlich mit Kosten von ca. 95.000 € zu Buche schlagen. Ein Releasewechsel wäre allerdings nicht erforderlich und der in Rede stehende hohe „Mehraufwand“ nicht aufzuwenden gewesen, wenn die datenschutzrechtlichen Aspekte bereits bei der Planung des Systems Berücksichtigung gefunden hätten.

Nach Darstellung des Innenministeriums standen die benötigten finanziellen Mittel der Polizei für das Jahr 2003 nicht zur Verfügung. Die Umsetzung dieses Projektes soll nun im **Jahr 2004** mit **höchster Priorität** erfolgen. Eine Zwischenlösung sieht vor, dass durch konkrete Vorgaben in einer Dienstanweisung sowie durch verstärkte Kontrollen insbesondere im Rahmen der Dienstaufsicht die Einhaltung der rechtlichen Vorgaben gewährleistet wird.

Was ist zu tun?
Bei solchen Projekten sollten künftig die datenschutzrechtlichen Aspekte schon bei der Planung berücksichtigt werden, damit ein derartiger finanzieller „Mehraufwand“ aufgrund von Versäumnissen von vornherein vermieden werden kann.

4.2.4 Rasterfahndung: Außer Spesen nichts gewesen

Nach den Terroranschlägen des 11. September 2001 hat sich auch die schleswig-holsteinische Polizei an der bundesweit durchgeführten Rasterfahndung beteiligt. Nennenswerte Erfolge sind dabei offenbar nicht zu verzeichnen gewesen. Der Landesgesetzgeber sollte dies bei der im Jahr 2005 durchzuführenden Evaluierung der Rechtsgrundlagen für die Rasterfahndung nicht außer Acht lassen.

Über die Rasterfahndung berichteten wir bereits im Rahmen des 24. und 25. Tätigkeitsberichts (Tz. 4.2.2 und 4.2.4). Wir hatten insbesondere moniert, dass der Kern der Rasterfahndung, der automatisierte Abgleich schleswig-holsteinischer Daten mit den beim Bundeskriminalamt (BKA) vorgehaltenen Abgleichsdateien, vom **Bundeskriminalamt** ohne Befugnisgrundlage durchgeführt wurde. Das BKA hatte uns eine Kontrolle der Verwendung der schleswig-holsteinischen Daten aus „grundsätzlichen Erwägungen der föderalen Kompetenzverteilung“ verweigert. Die dort durchgeführten Datenabgleiche sind im Frühjahr 2003 abgeschlossen worden; im März 2003 hatte das Landeskriminalamt die Löschung der übersandten Daten aus der Verbunddatei und den Abgleichdateien beantragt. Das BKA hat die Löschung bestätigt. Nach Beendigung der Benachrichtigung der Betroffenen wurden auch die in Schleswig-Holstein noch vorhandenen Datensätze vollständig gelöscht.

Konkrete Verdachtsmomente im Hinblick auf terroristische Taten haben sich aus den schleswig-holsteinischen Prüffällen offenbar **nicht ergeben**. Welcher Schluss lässt sich daraus ziehen? Fest steht, dass die Rasterfahndung eine beson-

ders eingriffsintensive Maßnahme darstellt, denn sie stellt die grundgesetzlich verankerte **Unschuldsvermutung** auf den Kopf. In das Blickfeld der Polizei geraten unbescholtene Bürger, die erst im Nachhinein davon erfahren, dass sie in die Rasterung mit einbezogen worden sind. Auch wenn das schleswig-holsteinische Landesverwaltungsgesetz hohe Anforderungen an das Verfahren stellt, lässt doch der Umstand, dass offensichtlich auch bundesweit trotz des sehr hohen personellen Aufwandes keine messbaren Erfolge zu verzeichnen waren, **Zweifel** an der **Eignung** und Verhältnismäßigkeit der **Rasterfahndung** aufkommen.

Was ist zu tun?
Der Landesgesetzgeber sollte im Rahmen der Evaluierung der Vorschriften zur Rasterfahndung aus den Erfahrungen mit der erfolglosen Rasterfahndung die Konsequenzen ziehen.

4.2.5 Evaluation der Telefonüberwachung zeigt schwere Mängel auf

Die Ergebnisse des im Mai 2003 vom Max-Planck-Institut in Freiburg vorgelegten Gutachtens „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach §§ 100 a, 100 b StPO und anderer verdeckter Ermittlungsmaßnahmen“ sowie eine Studie der Uni Bielefeld zu diesem Themenkreis legen es nahe, die gesetzlichen Bestimmungen zur Telefonkommunikationsüberwachung (TKÜ) zu überarbeiten.

Die Zahl der Überwachungsanordnungen hat sich in Deutschland seit 1995 nahezu verfünffacht. In dem Gutachten wird der Fall einer einzigen Anordnung mit 30.500 abgehörten Gesprächen geschildert. In 21 % der Anordnungen kam es zum Abhören von 1000 bis 5000 Gesprächen, in weiteren 8 % sogar von mehr als 5000 Gesprächen. Das Gutachten kommt zu dem Ergebnis, dass ein „statistisch signifikanter Zusammenhang zwischen dem Erfolg der TKÜ-Maßnahme und den Katalogstraftaten, aufgrund derer ermittelt wird, nicht feststellbar ist“. Zwar waren bei 60 % der untersuchten Verfahren Ermittlungserfolge im weitesten Sinne zu verzeichnen, es wurden aber nur in **17 %** der Fälle **unmittelbare Erfolge** für das Verfahren, das die Rechtfertigung für die Abhörmaßnahmen bieten sollte, erzielt. Auch in Anklagen und Urteilen spielen die Ergebnisse der TKÜ lediglich eine untergeordnete Rolle.

Welche Schlussfolgerung ist daraus zu ziehen? Die nicht zu leugnende **zunehmende Überwachung** der Telekommunikation hat aus einem nur im äußersten Fall zulässigen Rechtseingriff ein alltägliches Standardmittel der Strafverfolgung werden lassen. Dies ist in einem freiheitlichen Rechtsstaat nicht hinnehmbar. Das auf dem Spiel stehende grundgesetzliche Telekommunikationsgeheimnis fordert ein **umgehendes Tätigwerden** des Gesetzgebers.

- Der Katalog des § 100 a StPO ist seit Jahren immer weiter ausgedehnt worden, ohne dass ermittelt worden wäre, was jeweils vorangegangene Gesetzesänderungen in der Praxis ergeben haben. Hier muss eine **Beschränkung** auf solche **Straftaten** stattfinden, die im Hinblick auf Art und Schwere der aufzuklärenden Straftaten tatsächlich TKÜ-Maßnahmen rechtfertigen.

- Bestehende Defizite im Bereich der Begründung und Prüfung von TKÜ-Maßnahmen müssen beseitigt werden. Die zuständigen Ermittlungsinstanzen müssen rechtlich und tatsächlich gezwungen werden, TKÜ-Maßnahmen nur als **Ultima Ratio** anzuordnen.
- Die **nachträgliche Benachrichtigung** Betroffener ist nach der Rechtsprechung des Bundesverfassungsgerichts eine unabdingbare Verfahrensvoraussetzung für die Zulassung der TKÜ. Der Gesetzgeber muss dafür sorgen, dass diese auch effektiv umgesetzt wird.

Absolutes Muss ist eine begleitende **Wirkungs- und Wirksamkeitskontrolle** der Überwachung. Hervorzuheben ist, dass die Erkenntnisse des Gutachtens nur eine Momentaufnahme – vor allem von Verfahren aus dem Jahr 1998 mit einer inzwischen bereits überholten Überwachungstechnik – widerspiegeln. Der Grundrechtsschutz in diesem dynamischen Bereich setzt voraus, dass **unabhängige Instanzen** – z. B. Richter, Wissenschaftler und Datenschützer – in den laufenden Verfahren die Wirkungen der TKÜ beurteilen und dass hierüber berichtet wird. Die Pläne der Bundesregierung, im Rahmen der Novellierung des Telekommunikationsgesetzes die Berichtspflichten stattdessen abzubauen, sind daher vollkommen unakzeptabel. Wer es ernst meint mit der Abwehr von Tendenzen hin zu einem Überwachungsstaat, der muss staatliche Geheimermittlungen einem fortdauernden demokratischen „check and balance“ aussetzen.

Was ist zu tun?
Der Gesetzgeber muss die formellen und materiellen Voraussetzungen für die TKÜ einer grundlegenden Revision unterziehen.

4.2.6 Einführung von INPOL-SH und @rtus

Bei der Landespolizei stehen im Bereich der elektronischen Datenverarbeitung grundlegende Neuerungen an, die im Rahmen einer datenschutzrechtlichen Vorabkontrolle begleitet werden. Es handelt sich um das polizeiliche Vorgangsbearbeitungssystem @rtus und um INPOL-SH als Nachfolger der Polizeilichen Erkenntnisdatei (PED). Eine abschließende Vorabkontrolle ist zum gegenwärtigen Zeitpunkt nicht möglich, da noch Schnittstellen zu klären sind.

Auch wenn versichert worden ist, dass ein Einsatz von **@rtus** als so genanntes **Informationsbeschaffungssystem** nicht in Betracht kommt, lassen die Funktionalitäten des Systems auch andere Rückschlüsse zu. So kann die Rolle von Beschuldigten **landesweit** recherchiert werden, womit der Einstieg in ein überregionales, d. h. dienststellenübergreifendes Informationssystem erreicht sein dürfte. Unklarheiten bestehen vor allem hinsichtlich der elektronischen Aufbewahrungsfristen, die für elektronische Vorgänge und Dokumente nicht nur unterschiedlich lang bemessen sind, sondern auch eine Speicherung nach Abschluss des Verfahrens hinaus zulassen. Hier stellt sich eine Fülle von Fragen. Zum einen ist eine **Erforderlichkeit** der Vorhaltung der Dokumente in elektronischer Form über den Verfahrensabschluss hinaus nicht erkennbar. Zum anderen muss die Polizei klären, ob die längerfristige Speicherung von Dokumenten den Vorgang

nicht zu einer Art **Kriminalakten-Teilstück** macht. Weiterhin muss die **Authentizität** des elektronischen Datenbestandes gewährleistet sein. Aus Gründen der Transparenz sollte für die Dienststellenleiter zudem erkennbar sein, welche Mitarbeiter welche Zugriffsberechtigungen haben, denn es ist durchaus möglich, dass Mitarbeiter als Anwender auf mehreren Dienststellen registriert sind. Ein wesentlicher, von der Polizei noch zu klärender Punkt liegt darin, dass ihre **Kontrollmöglichkeit** in Bezug auf ihren eigenen bei dataport untergebrachten Server, der auch von dort administriert wird, derzeit nicht gegeben ist.

Als **INPOL-SH** wird sowohl das Informationssystem der schleswig-holsteinischen Polizei als auch das Zugangssystem zu INPOL-Zentral bezeichnet. Es ist als Nachfolgesystem der PED das Kernstück der polizeilichen Informationsverarbeitung in Schleswig-Holstein, denn es handelt sich um den **zentralen Datenbestand** der Polizei, auf den ca. 6500 Mitarbeiter Zugriff haben. Deshalb sind neben Aspekten der **Vertraulichkeit** gegenüber allen Personen innerhalb und außerhalb der Verwaltung, die nicht mit der Strafverfolgung oder Gefahrenabwehr befasst sind, insbesondere auch die Aspekte der **Datenintegrität** bei der Verfahrensgestaltung zu beachten. Die Sicherheitsanforderungen an das Verfahren INPOL-SH müssen daher beide Bereiche auf einem einheitlich hohen Niveau abdecken. Eine besondere Problematik ergibt sich daraus, dass an der Entwicklung, der Einführung und dem Betrieb des Systems eine Vielzahl von eigenverantwortlich handelnden und gleichzeitig weisungsgebundenen Organisationseinheiten beteiligt ist. Ohne eine genaue Zuständigkeitsabgrenzung und Beschreibung der Ablauforganisation dürfte die **Ordnungsmäßigkeit der personenbezogenen Datenverarbeitung** bei diesem Maß an Arbeitsteilung nicht zu gewährleisten sein.

Das Verfahren INPOL-SH weist in datensicherheitstechnischer Sicht noch Schwachstellen auf, die dringend behoben werden müssen. Die sich hieraus ergebenden Probleme haben wir der Polizei im Einzelnen dargestellt und eine Abhilfe dringend angeraten.

Was ist zu tun?
Die Polizei muss die Konzepte nachbessern. Dabei sollte überlegt werden, ob nicht eine Zentralisierung der Aufgaben bei einer entscheidungsbefugten Stelle geboten ist.

4.3 Justizverwaltung

4.3.1 Positives aus der Justizvollzugsanstalt

Im Jahr 2002 wurde eine umfangreiche datenschutzrechtliche Querschnittskontrolle in einer schleswig-holsteinischen Justizvollzugsanstalt vorgenommen. Im vergangenen Jahr sind nahezu 90 % der beanstandeten Mängel behoben worden.

Die Zielstrebigkeit, mit der die Verantwortlichen der Justizvollzugsanstalt Neumünster die von uns aufgezeigten Datenschutzdefizite beseitigt und ihre Verfahrensweisen datenschutzgerecht gestaltet haben, ist bemerkenswert. Dies unter-

streicht die gute Zusammenarbeit zwischen der JVA und den Prüfern bereits während der Prüfung. Von Anfang an wurde seitens der JVA Neumünster signalisiert, im Umgang mit Daten über einsitzende Gefangene **Sensibilität** und **Verantwortungsbewusstsein** zeigen zu wollen.

- So werden künftig die **medizinischen Gutachten** von der übrigen Gefangenenpersonalakte getrennt und in einem gesonderten Briefumschlag in den Aktenschränken der Vollzugsgeschäftsstelle aufbewahrt. Die Zugriffsberechtigungen werden durch die jeweiligen Vollzugsleiter festgelegt.
- Die Entnahme bzw. der Verbleib von **Lichtbildern** wird künftig in der jeweiligen Gefangenenpersonalakte dokumentiert. Die Beschriftung aller Lichtbilder wird sichergestellt, damit eine sichere Zuordnung zu den Gefangenen möglich ist.
- Die Führung von zahlreichen, in der Regel mehrere Jahre umfassenden **Buchwerken** ist eingestellt worden. Nunmehr werden diese Informationssammlungen jahrgangsweise geführt, sodass die jeweiligen Aufbewahrungsfristen eingehalten und die Unterlagen fristgerecht vernichtet werden können.

Darüber hinaus ist der Datenschutz in einer Fülle von weiteren Punkten verbessert worden. Die Verantwortlichen der JVA Neumünster haben in diesem Zusammenhang die Aussage getroffen, dass durch die *„Einsparung von Buchwerk und anderen Nachweisen“* dazu beigetragen wird, *„dass künftig Unterlagen mit personenbezogenen Daten in merklich geringerem Umfang gelagert werden“*. Datenvermeidung und Datensparsamkeit führen also zu **mehr Effizienz** im Strafvollzugsalltag.

Nur in wenigen Punkten bestehen noch **unterschiedliche Auffassungen** bzw. steht die Umsetzung der erforderlichen Maßnahmen noch aus. Insbesondere im Zusammenhang mit der elektronischen Datenverarbeitung besteht ein größerer Änderungsbedarf, damit die Sicherheitsanforderungen des Landesdatenschutzgesetzes sowie der Datenschutzverordnung erfüllt werden. Folgende Punkte sind darüber hinaus noch mit den Verantwortlichen zu klären:

- Bereitstellung von persönlichen Schließfächern für Gefangene, um ein Minimum an informationeller Selbstbestimmung in den Hafträumen zu gewährleisten,
- Durchführung der Haftraumrevision grundsätzlich durch zwei Justizvollzugsbeamte, wenn der betreffende Gefangene aus strafvollzugsrechtlichen Gründen nicht anwesend sein darf.

Was ist zu tun?
Die noch offen stehenden Punkte sollten rasch einer Lösung zugeführt werden.

4.3.2 Wenn der Staatsanwalt keine Zeit mehr für den Datenschutz hat

Ein Staatsanwalt darf nicht ungeprüft komplette Ermittlungsakten an die Versorgungsverwaltung herausgeben. Dies gilt auch für die Prüfung, ob dem Opfer einer Straftat eine Entschädigung zusteht. Auch hier ist das Erforderlichkeitsprinzip zu beachten.

Bei einer Kontrolle des Behörden-Transport-Service, über den der Post- und Aktenaustausch zwischen Behörden abgewickelt wird, war in Hamburg die **Ermittlungsakte** einer schleswig-holsteinischen Staatsanwaltschaft **offen aufgefunden** worden. Darin ging es um den Tatbestand des sexuellen Missbrauchs Schutzbefohlener. In dem Vorgang befanden sich Unterlagen mit sensiblem Inhalt über Dritte (Beschuldigter und Opfer anderer Strafverfahren). Diese Vorgänge waren komplett an die Versorgungsverwaltung übersandt worden. Besonders pikant war, dass aus den offen übersandten Vorgängen auch ersichtlich war, dass gegen einen in einem anderen Ermittlungsverfahren Tatverdächtigen **Telefonüberwachungsmaßnahmen** und eine **Wohnungsdurchsuchung** vorgenommen worden waren.

Wer die offene Übersendung der Akten zu verantworten hatte, war nicht mehr zu klären. Hier stand Aussage gegen Aussage. Unabhängig davon war aber die Übersendung der **vollständigen Ermittlungsakte** an das Versorgungsamt nicht zulässig. Nach der Strafprozessordnung darf nur dann, wenn die Erteilung von Auskünften einen unverhältnismäßigen Aufwand verursachen würde, ausnahmsweise Akteneinsicht gewährt werden. Da in diesem Fall ein komplexer Vorgang entstanden war, hätten die Dritte betreffenden Aktenbestandteile abgetrennt werden müssen und nicht mit übersandt werden dürfen. Der damit verbundene Aufwand hätte sich aus unserer Sicht in vertretbarem Rahmen gehalten. Wenn die Staatsanwaltschaft ihre Akten schon nicht von vornherein so organisiert, dass selektive Datenübermittlungen leicht möglich sind, bedeutet das nicht, dass man sich quasi als Regelfall auf die Durchbrechung des Erforderlichkeitsgrundsatzes berufen kann mit der Begründung, die Aussonderung der nicht erforderlichen Teile mache Mühe.

Die Vorschriften der **Richtlinien für das Straf- und Bußgeldverfahren** (RiStBV) sehen aus guten Gründen vor, dass besonders schutzwürdige Daten von vornherein getrennt zu heften sind. Die bei den Staatsanwaltschaften vorhandene hohe Arbeitsbelastung soll nicht verkannt werden. Dies kann jedoch kein Blankoscheck dafür sein, dass sensible Daten über Beschuldigte und über unbescholtene Dritte ohne Erforderlichkeit an andere Behörden übersandt werden. Dies haben wir der Staatsanwaltschaft mitgeteilt.

Was ist zu tun?
Die Staatsanwaltschaften sollten ihre Verfahrensakten so organisieren, dass bei Übermittlungsvorgängen schutzwürdige Daten Dritter ohne großen Aufwand entfernt und zurückbehalten werden können, wenn sie für den Empfänger nicht erforderlich sind.

4.4 Ausländerverwaltung

Auch im dritten Jahr nach den Anschlägen des 11. September 2001 werden die Maßnahmen zur biometrischen Reisekontrolle weiter verstärkt. Künftig sollen schon Visa-Antragsteller biometrisch erfasst werden.

Die weltweiten terroristischen Anschläge der letzten Jahre haben nachhaltige Auswirkungen auf die Kontrolle des grenzüberschreitenden Personenverkehrs. Praktisch sämtliche Aktivitäten verfolgen das Ziel einer möglichst eindeutigen Identifizierung der Reisenden. Dabei setzt sich inzwischen als Standard die **biometrische Erfassung** und Überprüfung durch (vgl. Tz. 2).

Mit dem Anfang 2002 in Kraft getretenen Terrorismusbekämpfungsgesetz wurden die rechtlichen Grundlagen für die biometrische Erfassung von Ausländerinnen und Ausländern ausgeweitet. Wurden bisher die Fingerabdrücke der Flüchtlinge erfasst und zentral gespeichert, so sollen künftig schon die **Visa-Antragsteller** aus so genannten Problemstaaten biometrisch identifiziert werden. Zudem wurde eine Rechtsgrundlage für biometrische Ausländerausweisdokumente geschaffen (vgl. 24. TB, Tz. 4.5.2). Inzwischen startete im nigerianischen Lagos ein Pilotprojekt, bei dem sämtliche Antragsteller auf Erteilung eines Visums ihre Fingerabdrücke abgeben müssen, sowie ein Gesichtserkennungsverfahren im indonesischen Jakarta. Ein weiterer Testlauf mit Iriserkennung soll in einem anderen Staat folgen. Das beste der drei Verfahren soll dann zum Standard bei Visaverfahren in 32 Ländern werden.

Ein weiteres Beispiel zielt darauf ab, Flüchtlingen ohne Ausweispapiere aufgefundene Reisepässe oder sonstige Reisedokumente zuzuordnen, um deren Identität bzw. Herkunftsstaat ausfindig zu machen. Zu diesem Zweck soll bundesweit eine **zentrale Passabgleichsstelle** eingerichtet werden. Es soll ein elektronisches Verfahren eingesetzt werden, bei dem die Passbilder der gefundenen Dokumente mit den Gesichtsprofilen der passlosen Ausländer verglichen werden. Mit den Datenschutzbeauftragten anderer Länder stimmen wir darin überein, dass ein solches Verfahren derzeit gesetzlich nicht zulässig ist.

Parallel dazu wird weltweit an der Entwicklung von Standards für die **biometrische Aufrüstung der Reisepässe** gearbeitet. Eine „Arbeitsgruppe Immigrationsexperten“ der acht führenden Industriestaaten (G8) entwickelte erste Überlegungen zu einem „vollständigen gemeinsamen technischen Interoperabilitätsstandard“. Die EU-Regierungschefs erteilten der EU-Kommission den Auftrag, die Aufnahme von biometrischen Merkmalen in Ausweisen vorzubereiten. Die Kommission unterbreitete im Herbst 2003 entsprechende Vorschläge, zu denen auch eine Speicherung im europaweiten **Schengen Informationssystem** gehört. Eine neue Konvention der Internationalen Arbeitsorganisation sieht international gültige Biometrieausweise für Seeleute vor. In der weltweiten Standardisierung engagiert sich insbesondere auch die Internationale Zivile Luftfahrtorganisation.

Zwar wird bei den europäischen Planungen auf die Anwendbarkeit der Europäischen Datenschutzrichtlinie hingewiesen. Konkrete Vorschläge zur spezifischen Umsetzung der **Zweckbindung der biometrischen Daten** bestehen aber nicht

einmal auf nationaler, geschweige denn auf supra- bzw. internationaler Ebene. Heikel ist dies, da die biometrischen Ausweisangaben, je nach eingesetztem technischen Verfahren, auch für andere Zwecke, insbesondere Strafverfolgungszwecke, genutzt werden können. Im Fall einer Standardisierung könnten die Identifizierungsdaten zu einem weltweit einheitlichen Personenkennzeichen werden.

Was ist zu tun?
In einem internationalen Abkommen über die Aufnahme von biometrischen Merkmalen in Reisedokumente müssen datenschutzrechtliche Vorkehrungen vorgesehen werden, die eine Zweckentfremdung der Identifizierungsdaten verhindern.

4.5 Verkehr und Wirtschaft

4.5.1 Verkehrstotalüberwachung durch das Lkw-Mautsystem?

Die Diskussion über das Lkw-Mautsystem der Firma TollCollect drehte sich monatelang nur um Fragen der Funktionsfähigkeit des Systems und der Kosten. Es sind aber auch noch wichtige datenschutzrechtliche Fragen zu klären.

Im Sommer 2003 konkretisierten sich Befürchtungen, dass das sehr aufwändige Lkw-Mauterfassungs- und Abrechnungssystem zu einer weitgehenden **Überwachung des Straßenverkehrs** mithilfe von Satellitennavigation, Mobilfunkkontrolle und Videoüberwachung geeignet ist. Die Mautabrechnung soll nämlich vorrangig mithilfe von in den Lastkraftwagen installierten **OnBoardUnits**, den so genannten OBUs, erfolgen. Die OBUs vergleichen ständig die aktuellen GPS-Koordinaten mit einer im Gerät gespeicherten Straßenkarte. Wird dadurch erkannt, dass sich der Lkw auf einer mautpflichtigen Strecke befindet, so beginnt der Gebührenzähler zu laufen. Anhand der GPS- und Tachosignale wird die Plausibilität der gemessenen Werte überprüft. Verlässt der Lkw die mautpflichtige Strecke, so meldet das im OBU installierte Mobilfunkgerät automatisch die errechnete Maut samt der gefahrenen Strecke an die TollCollect-Zentrale, die der Spedition die Fahrt in Rechnung stellt.

? OBU

Die OBU ist ein autoradiogroßes Gerät, das an die Lkw-Elektronik angeschlossen ist und über einen Tachosensor, einen GPS-Satellitenempfänger, einen Infrarotsender sowie ein Mobilfunkteil verfügt. Damit werden die gefahrenen mautpflichtigen Kilometer ermittelt, die Maut berechnet und die entsprechenden Daten elektronisch übermittelt.

Mithilfe von derzeit knapp 200 **Kontrollbrücken** über Autobahnen mit Videoüberwachung und Infrarotsensor soll überprüft werden, ob alle mautpflichtigen Fahrzeuge auch tatsächlich abrechnen. Hierzu werden die Frontbilder von sämtlichen Fahrzeugen – also auch der Pkws – per Video erfasst und die Kfz-Kennzeichen über ein automatisches Mustererkennungsverfahren eingelesen. Diese Daten werden wieder gelöscht, wenn die OBU per Infrarotsignal mitteilt, dass der Mautpflicht entsprochen wird. Bei der Durchfahrt unter der Brücke werden zudem die

Fahrzeuge automatisch vermessen. Ergibt sich dabei, dass keine Mautpflicht besteht, z. B. weil es sich bei dem Fahrzeug um einen Pkw und nicht um einen Lkw handelt, so werden auch die hierzu gehörenden Videodaten gelöscht. Lkws ohne OBU haben die Möglichkeit, vorab Strecken unter Angabe des Kfz-Kennzeichens über Internet oder an Bezahlterminals an Tankstellen vorzubuchen. Ergibt sich, dass das eingelesene Kennzeichen mit dem der Vorbuchung übereinstimmt, so werden auch diese Bilder gelöscht. Kommt es aber nicht zu einem Treffer, so wird das aufgenommene Foto als Beweismittel gespeichert; dem Besitzer des Kfz wird ein Bußgeldbescheid zugestellt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte schon im Jahr 2001 darauf gedrängt, eine datensparsame Technik bei der Mauterfassung zu realisieren. Das TollCollect-Verfahren birgt dagegen ein erhebliches Überwachungspotenzial: Über die **Videoüberwachung** kann nicht nur nach Lkws, sondern auch nach Pkws gefahndet werden, deren Bilder zunächst vollständig erfasst werden. Ist die technische Infrastruktur erst einmal aufgebaut, genügt eine kleine Gesetzesänderung. Da es sich bei der OBU um ein ganz „normales“ Mobiltelefon handelt, lässt sich zudem mithilfe der **Mobilfunkverbindungsdaten** – die z. B. über die „stille SMS“ erzeugt werden können – eine Lokalisierung des Lkw auf wenige hundert Meter genau vornehmen.

? Stille SMS

Bei der stillen SMS wird ein Mobilfunkgerät z. B. von der Polizei angerufen, ohne dass dies für den Besitzer erkennbar wäre. Durch die bei diesem Kommunikationsvorgang entstehenden Verbindungsdaten kann dann die Polizei unbemerkt die Lokalisierung des Gerätes vornehmen. Bei in Lkw eingebauten OBUs könnte so verdeckt der Standort festgestellt werden.

Zwar sieht das Autobahnmautgesetz eine „ausschließliche“ Zweckbeschränkung der Mautdaten vor. Doch stellte das **Amtsgericht Gummersbach** bereits fest, dass sich dadurch kein Verarbeitungs- und Verwertungsverbot für Strafverfolgungsbehörden ergeben könne. Daher sahen wir uns veranlasst, die Verfahrensbeteiligten auf die datenschutzrechtlichen Gefahren hinzuweisen. Weder der Betreiber noch das Bundesverkehrsministerium sehen allerdings relevante Datenschutzrisiken.

Was ist zu tun?
Die öffentliche Debatte über die Lkw-Maut sollte sich nicht auf die technische Machbarkeit beschränken, sondern sich auch mit den Gefahren für die Freiheit befassen.

4.5.2 Datenschutzgerechte Korruptionsregister

Wie kann gewährleistet werden, dass Anbieter in öffentlichen Ausschreibungsverfahren, die sich als korrupt und unzuverlässig erwiesen haben, nicht den Zuschlag bekommen? Die Lösung soll ein Korruptionsregister bringen. Hierbei müssen aber Rechtsstandards beachtet werden.

Noch kurz vor der Bundestagswahl 2002 versuchte die Bundesregierung, durch Änderung des Gesetzes gegen Wettbewerbsbeschränkungen ein **bundesweites Korruptionsregister** einzuführen. Nachdem dieses Vorhaben am Widerstand des Bundesrates gescheitert war und auch keine Erfolgsaussichten für eine erneute Bundesinitiative bestanden, wurden Landespolitiker aktiv. Zumindest für Schleswig-Holstein sollte ein solches Register realisiert werden. In einigen Bundesländern gibt es bereits solche Register, jedoch ohne gesetzliche Grundlage. Auf dem Erlasswege können und dürfen aber die Grundrechte auf Datenschutz und auf freie wirtschaftliche Betätigung nicht eingeschränkt werden. Notwendig ist deshalb eine gesetzliche Grundlage.

Nach der Anhörung zu einem Gesetzentwurf im **Landtag** wurden wir gebeten, **Vorschläge** für ein datenschutzgerechtes Korruptionsregistergesetz zu machen. Angesichts der Dauer von Straf- und Ordnungswidrigkeitenverfahren im Wirtschaftsbereich lag ein zentrales Problem darin, schon während der Ermittlungen eine Speicherung zuzulassen, ohne dass hierbei die Rechtsposition des jeweiligen Unternehmens bzw. der Beschuldigten unverhältnismäßig beeinträchtigt würde. Unstreitig ist, dass die Unschuldsvermutung eine Registerspeicherung nicht von vornherein ausschließt. Wohl aber müssen durch Benachrichtigungen, Widerspruchs- und Löschansprüche die Grundsätze des rechtlichen Gehörs, des fairen Verfahrens und der informationellen Selbstbestimmung gewahrt bleiben. Unsere Formulierungsvorschläge haben wir nicht nur den Fraktionen unterbreitet, sondern auch im Interesse einer breiten öffentlichen Diskussion im Internet veröffentlicht:


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

Danach könnte ein **Landesregister** eingerichtet werden, bei dem ab einer bestimmten Auftragshöhe Landesstellen anfrage- und meldepflichtig sind. Aber auch Anfragen und Meldungen von sonstigen Stellen könnten bearbeitet bzw. gespeichert werden, sodass eine über die Landesgrenzen hinausgehende Kommunikation möglich wäre. Eine zentrale Funktion käme den präzisen Regelungen der Speicherungskriterien und den Auskunfts- und Korrekturansprüchen der betroffenen Personen und Unternehmen zu.

Die **Reaktionen** anderer Gutachter wie auch der Politik auf unsere Vorschläge waren fast durchgängig **positiv**. Aus der Bürgerschaft Hamburg kam eine Anfrage, ob die ULD-Formulierungsvorschläge übernommen werden könnten. Auch bei einer Anhörung im Landtag von Nordrhein-Westfalen wurden unsere Vorschläge zustimmend kommentiert und in das weitere dortige Gesetzgebungsverfahren einbezogen. In Schleswig-Holstein wurden die Regelungsvorschläge leicht modifiziert in das weitere Gesetzgebungsverfahren eingebracht.

Was ist zu tun?
Gegen ein Korruptionsregister ist aus Datenschutzsicht nichts grundsätzlich einzuwenden. Doch müssen dabei die rechtsstaatlichen Standards, insbesondere der Gesetzesvorbehalt bei Grundrechtseingriffen, beachtet werden.

4.6 Schutz von Sozialdaten

4.6.1 Rauer Wind bei der Sozialhilfe

Überschuldete kommunale Haushalte veranlassen die Kreise und Gemeinden jeden Euro zweimal umzudrehen, bevor sie ihn ausgeben. Sozialämter prüfen vor der Bewilligung einer Sozialhilfeleistung sehr genau, ob und in welcher Höhe ein Anspruch besteht. Aber auch die Hilfe Suchenden hinterfragen verstärkt Ablehnungen, wie die im letzten Jahr deutlich gestiegene Zahl von Beratungswünschen und Eingaben in diesem Bereich zeigt.

Vielfach wurden wir mit der Frage der Zulässigkeit der Durchführung von **Hausbesuchen** befasst. Mehrere Oberbürgermeister, Stadträte und Amtsleiter kündigten in Tageszeitungen verstärkte Kontrolltätigkeiten durch extra eingerichtete **Ermittlungsdienste** an. Unsere Nachfragen zeigten, dass die von uns im 23. Tätigkeitsbericht unter Tz. 4.7.3 veröffentlichten praktischen Handlungshilfen oft nicht bekannt waren und noch öfter nicht beachtet wurden.

Auf Anfragen von Hilfe Suchenden, ob sie denn tatsächlich bei der Beantragung von Sozialhilfe **Kontoauszüge** vorlegen und zudem eine **Bankvollmacht** unterschreiben müssen, verwiesen wir auf die Veröffentlichung im Amtsblatt Schleswig-Holstein vom November 1998, wonach die Anforderung von Kontoauszügen in begrenztem Umfang zulässig, die Forderung nach einer Bankvollmacht jedoch unzulässig ist (vgl. 21. TB, Tz. 4.7.4, und 23. TB, Tz. 4.7.4).

Bei der Hilfegewährung wollen sich viele Sozialämter von den Betroffenen nicht in die Karten blicken lassen, weshalb wir häufig bei der Durchsetzung der **Rechte auf Auskunft und Akteneinsicht** vermitteln mussten. Gründe für die Verweigerung dieser Rechte bestehen im Bereich der Sozialhilfe nur in wenigen seltenen Fällen.

Was ist zu tun?
Zum Sparen gibt es vermutlich auch im Bereich der Sozialhilfe derzeit keine Alternative. Die Hilfebedürftigen sind deshalb nicht völlig rechtlos.

4.6.2 Misstrauen unter Sozialämtern

Darf ein Sozialamt die vollständige Sozialhilfeakte mit sämtlichen Informationen über einen Hilfe Suchenden an ein anderes Sozialamt übersenden, damit dort der Anspruch auf Kostenerstattung geprüft werden kann?

Ein Bürgermeister freut sich grundsätzlich über jeden neuen Bürger in seinem Ort, verspricht dies doch zunächst einmal mehr Einnahmen für die kommunale Kasse. Über einen neuen Sozialhilfeempfänger wird diese Freude wegen der zu erwartenden Ausgaben eher getrübt sein. Um diese Enttäuschung etwas zu lindern, hat der Gesetzgeber vorgesehen, dass die Sozialhilfekosten für Neubürger in den ersten zwei Jahren der alten Wohnsitzgemeinde in Rechnung gestellt werden. Im Rahmen dieser **Kostenerstattung** erhält die alte Wohnsitzgemeinde jährlich eine Aufstellung der gezahlten Sozialhilfe. Bei Geld hört oft die Freundschaft auf: Voller Argwohn werden die Rechnungen daraufhin geprüft, ob die neue Gemeinde etwa zu großzügig Sozialhilfe gezahlt hat. Vertrauen ist gut, Kontrolle ist besser. Nach diesem Motto fordert so manches Sozialamt zur Prüfung der Rechnung die **vollständigen Sozialhilfeakten** der Abgewanderten an.

Sozialhilfeakten enthalten eine Vielzahl von zum Teil äußerst sensiblen Daten. Ist es wirklich erforderlich, dass vollständige Sozialhilfeakten nur zum Zwecke der Rechnungsprüfung bundesweit hin- und hergeschickt werden? Wir meinen: Nein. Mit unseren im Amtsblatt Schleswig-Holstein im November 1998 veröffentlichten Hinweisen zur Zulässigkeit der Übersendung von Sozialhilfeakten unterrichteten wir die beteiligten Stellen (vgl. 22. TB, Tz. 4.6.3). Die Sozialämter in Schleswig-Holstein bestätigten uns, dass zur Prüfung der Rechnung die Sozialhilfeakte nicht benötigt werde. Man verzichtet daher auf die **pauschale Anforderung** der Akten. Dieses Vertrauen zwischen den Sozialämtern in Schleswig-Holstein hat sich in den letzten fünf Jahren bewährt. Unnötige Arbeit entfällt; außerdem wird das Prinzip der Datensparsamkeit beachtet.

An dieser Stelle könnte der Bericht mit einer Erfolgsmeldung enden, wären da nicht **Sozialämter** in **anderen Bundesländern**, die sich weigerten, die Kosten zu erstatten. Die Aktenübersendung wurde zur Zahlungsbedingung gemacht. Selbstverständlich war man in Schleswig-Holstein bereit, konkrete Fragen zur Rechtmäßigkeit der Berechnung zu beantworten, aber vollständige Akten mit hochsensiblen Daten an Gemeinden in anderen Bundesländern zu schicken, das wollte man nun doch nicht. Allerdings wollte man auch nicht auf den Kosten sitzen bleiben.

Dies war Anlass für eine **bundesweite Erörterung** zwischen den Landesbeauftragten. Leider mussten wir feststellen, dass nicht alle unsere Kollegen unsere Auffassung teilten. Manche argumentierten, ein Sozialamt müsse umfassend die Rechtmäßigkeit von Erstattungsforderungen prüfen können. Und das gehe nur durch Kontrolle der vollständigen fremden Akten. Einen Verwaltungsgrundsatz des Vertrauens zwischen Sozialämtern gäbe es nicht. Es wurde lediglich zugestanden, dass zur Prüfung, ob sich ein Sachbearbeiter verrechnet hat, nicht die Inhalte vertraulicher Beratungsgespräche nötig sind.

Wir vertreten weiterhin die Auffassung, dass

- grundsätzlich eine dezidierte Kostenaufstellung ausreicht,
- im Einzelfall die Beantwortung konkreter Fragen zu Umfang und Zusammensetzung der gewährten Sozialhilfe berechtigt sein kann,
- nur in besonderen Fällen Akten, und dann auch nur beschränkt auf den berechnungsrelevanten Teil der Akte, übersandt werden dürfen.

Kurs SOZ

Was ist zu tun?
Bei der Abrechnung der Kostenerstattung folgt aus den Grundsätzen der Datensparsamkeit und Datenvermeidung, dass die Übersendung von vollständigen Sozialhilfeakten grundsätzlich unzulässig ist. Unsere Bekanntmachung im Amtsblatt Schleswig-Holstein vom November 1998 gilt unverändert.

4.6.3 Datenschutz für Hinweisgeber?

Denunzianten oder Anschwärzer nennen sie die einen, Informanten, Hinweisgeber oder Mitbürger mit Zivilcourage die anderen. Hat man als Betroffener gegenüber dem Sozialamt einen Anspruch darauf, den Namen eines Hinweisgebers zu erfahren?

Jeder, der eine Zeit lang bei einem Sozialleistungsträger, z. B. einem Sozial- oder Jugendamt gearbeitet hat, kennt sie, die hilfsbereiten Bürger. Ungefragt sind manche bereit, ihre privaten Beobachtungen dem Amt mitzuteilen. Manchmal bringen sie einen Sozialleistungsmissbrauch ans Tageslicht, gelegentlich sind die Hinweise aber auch falsch oder gar bewusst gelogen. Die eigentliche **Motivation von Hinweisgebern** liegt gelegentlich auch im persönlichen Bereich und besteht in der Absicht, zu schaden. Stets wird das Vertrauen zwischen Hilfe Suchendem und Sachbearbeiter nachhaltig gestört, denn Letzterer ist fast immer in der Pflicht, einem Hinweis nachzugehen.

Natürlich will der Hilfe Suchende oft erfahren, wer ihn beim Sozialamt angeschwärzt hat. Der Sozialdatenschutz wird von dem Gedanken der Transparenz getragen. Jeder Betroffene hat Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten. Er hat auch das Recht, die Herkunft der Daten zu erfahren. Die Auskunftserteilung darf aber unterbleiben, wenn berechtigte Interessen Dritter, hier des Hinweisgebers, überwiegen. Der Sozialleistungsträger muss also eine **Interessenabwägung** vornehmen. In der Rechtsprechung hat sich eine „Faustregel“ herauskristallisiert: Hat der Hinweisgeber wider besseres Wissen oder leichtfertig falsche Behauptungen aufgestellt, so kann dem Betroffenen Auskunft erteilt werden. Stellt sich der Hinweis aber als richtig heraus, so muss die Auskunftserteilung unterbleiben, wenn dies der Hinweisgeber so will.

Kurs SOZ

Was ist zu tun?
Bei allem Bestreben, Sozialhilfemissbrauch zu verhindern, muss das Recht, sich gegen unberechtigte Vorwürfe wehren zu können, gewahrt bleiben. Begehrt ein Hilfe Suchender Kenntnis über die Identität eines Hinweisgebers, muss eine Abwägung zwischen dem Auskunftsinteresse des Betroffenen und dem Geheimhaltungsinteresse des Hinweisgebers erfolgen.

4.6.4 Datenschutzgerechte Antragsvordrucke

Nach dem Bundessozialhilfegesetz erhält Hilfe, wer sich nicht selbst helfen kann oder erforderliche Hilfe nicht von anderen erhält. Sie setzt ein, sobald dem Träger der Sozialhilfe die Bedürftigkeit bekannt wird. Um den Sozialhilfeanspruch berechnen zu können, benötigen die Sozialämter konkrete Angaben zum Einkommen und zum Bedarf. Die dabei verwendeten Antragsvordrucke entsprechen leider nicht immer den Vorschriften.

Die Berechnung des Sozialhilfeanspruches ist bundesweit einheitlich geregelt, doch gleicht kaum ein Antragsvordruck dem anderen. Die Beschwerden, die bei uns eingehen, zeigen, dass jedes Sozialamt andere Fragen stellt. Wir stellen fest, dass oftmals unnötigerweise auch sensibelste Daten gesammelt werden. Seit vielen Jahren drängen wir daher auf eine **einheitliche datenschutzgerechte Gestaltung** von Vordrucken. Wir initiierten Abstimmungsgespräche zwischen dem Schleswig-Holsteinischen Landkreistag und dem Deutschen Gemeindeverlag (vgl. 22. TB, Tz. 13.1). Einigen Sozialämtern, z. B. der Stadt Reinbek und dem Kreis Herzogtum Lauenburg, ging dieses nicht schnell bzw. weit genug. Sie stimmten die Gestaltung ihrer Vordrucke direkt mit uns ab. Ein zu begrüßendes Engagement.

Ein strittiger Punkt ist derzeit noch die Erhebung von Daten über Mitglieder der **Haushaltsgemeinschaft**, die selbst keine Sozialhilfe erhalten. Gewährt ein Onkel seinem Neffen oder die Schwester ihrem Bruder in einer finanziellen Notsituation Unterkunft, so wird nach den Bestimmungen des Bundessozialhilfegesetzes vermutet, dass der Hilfe Suchende von seinen Verwandten auch finanziell unterstützt wird. In den meisten Antragsvordrucken sind daher Fragen zu „Schwestern“ und „Onkeln“ enthalten. Ohne dass diese etwas ahnen, werden so ihre Daten wie Name, Einkommen, Belastungen, Staatsangehörigkeit, Beruf- und Schulbildung, Familienstand, Vermögen, aber auch Informationen zu etwaigen Behinderungen erfasst. Nicht der betroffene Onkel, sondern der Hilfe suchende Neffe wird gefragt. Wir halten diese Datenerhebung über Dritte für nicht erforderlich und für unzulässig. Erst wenn der Onkel erklärt, dass er bereit ist, seinen Neffen auch finanziell zu unterstützen, sind weitere Fragen gerechtfertigt, um den möglichen Unterhaltsbeitrag feststellen zu können. Die Fragen sind allerdings dem Onkel selbst, nicht dem Neffen zu stellen.

Kurs SOZ

Leider gibt es viele weitere wenig datenschutzfreundliche Beispiele. Der Antragsvordruck auf Gewährung von Leistungen nach dem Grundsicherungsgesetz des Kreises Steinburg enthielt etwa eine pauschale Erklärung zur **Entbindung von der ärztlichen Schweigepflicht** und dem Bankgeheimnis. Der Kreis teilte unsere, auch vom Sozialministerium vertretene Meinung, dass dies zu weit ging, nicht.

Wir mussten die Kommunalaufsicht des Innenministeriums einschalten, um dieses rechtswidrige Verfahren zu beenden.

Was ist zu tun?
Antragsvordrucke sind so zu gestalten, dass nur die Daten erhoben werden, die zur Aufgabenerfüllung erforderlich sind. Unser Ziel, dass zukünftig jeder Hilfe Suchende in jedem Sozialamt unseres Landes die gleichen Fragen beantworten muss, haben wir noch nicht erreicht.

4.7 Schutz des Patientengeheimnisses

4.7.1 Datenschutz inmitten der Verteilungskämpfe

Angesichts der Automatisierung des Gesundheitswesens und der nicht enden wollenden **Kämpfe um die Gesundheitskosten** haben sich der Medizin- und der Krankenkassenbereich zu zentralen Konflikt- und Betätigungsfeldern des Datenschutzes entwickelt. Uns kommt dabei nicht nur die Funktion des Kontrolleurs zu, sondern auch die Rolle **des Informationsvermittlers, des Beraters und Streitschlichters**. Diese Rolle wird von den Beteiligten in der Regel angenommen, da sowohl die technischen, vor allem aber die rechtlichen Rahmenbedingungen derart kompliziert geworden sind, dass kompetenter Datenschutzrat als Hilfe verstanden und gerne berücksichtigt wird.

4.7.2 Aktion „Datenschutz in meiner Arztpraxis“ zeigt Wirkung

Die gemeinsam mit der Ärztekammer und der Zahnärztekammer durchgeführte Aktion zur Aufklärung und Sensibilisierung im Hinblick auf den Schutz des Patientengeheimnisses geht in das dritte Jahr. Sie verfehlt ihre Wirkung nicht.

Über den Start unserer Aktion und eine erste Zwischenbilanz berichteten wir (24. TB, Tz. 4.8.8; 25. TB, Tz. 4.8.9). Bestätigt durch den Zuspruch vieler Patienten und ermutigt durch die zunehmende Zahl der teilnehmenden Zahnärzte und Ärzte geht die Aktion „Datenschutz in meiner Arztpraxis“ in die nächste Runde. Sie hat sich zu einem kleinen **Exportschlager** entwickelt. Immer mehr Ärztekammern, Ärzte und Berufsschulen aus dem ganzen Bundesgebiet fragen nach, ob das unter

www.datenschutzzentrum.de/medizin/arztprax/

veröffentlichte **Informationsangebot** genutzt werden darf. Hiergegen haben wir bei nicht kommerziell orientiertem Interesse keine Einwände, wenn auf die Quelle hingewiesen wird. Die Aktionspartner und wir werten dies als Beleg dafür, dass wir eine „Marktlücke“ geschlossen haben.

Auch in Schleswig-Holstein erhält unsere Aktion weiteren Zuspruch. Der von uns und den Aktionspartnern entwickelte Datenschutzselbstcheck für Arztpraxen wurde in vielen **Berufsschulen** zwischenzeitlich zum Standardlehrmaterial. In

über 40 Klassen von Auszubildenden zum Beruf der Zahnarzt- bzw. Arzthelferin haben wir dieses Thema inzwischen behandelt. Über die Aktion wurde in einer Vielzahl von Fachzeitschriften berichtet.

Mithilfe der Ärztekammer bzw. der Zahnärztekammer Schleswig-Holstein haben wir **Fragebögen** landesweit an ca. 600 Praxen gesandt. Wir wollten wissen, wie es zwei Jahre nach dem Start der Aktion um das Patientengeheimnis bestellt ist. Aufgrund eines relativ hohen Rücklaufs von Zahnärzten und trotz eines geringeren von Ärzten konnten wir eine hohe Sensibilität bei dem Umgang mit konventionellen Patientenakten feststellen. Zugleich wurden aber Defizite bei der elektronischen Verarbeitung und bei der Einschaltung Dritter, z. B. den Privatärztlichen Verrechnungsstellen, offensichtlich. Die Ergebnisse und ein kurzer Kommentar sind veröffentlicht unter:

www.datenschutzzentrum.de/medizin/arztprax/fragebogen03.htm

Auch im nächsten Jahr wird die Aktion „Datenschutz in meiner Arztpraxis“ ein Schwerpunkt unserer Arbeit bleiben. Es gilt weiterhin Nachlässige und Bequeme in der Ärzteschaft zu überzeugen.

Was ist zu tun?
Zahnärzte und Ärzte sollten im Bewusstsein ihrer rechtlichen Verpflichtung zur Wahrung der ärztlichen Schweigepflicht die Hilfsangebote unserer Aktion „Datenschutz in meiner Arztpraxis“ zur Optimierung der Abläufe in ihrer Praxis nutzen.

4.7.3 „Aktion Datenschutz“ jetzt auch in Krankenhäusern

Nicht nur in Arzt- und Zahnarztpraxen, auch in Kliniken und Krankenhäusern ist das Patientengeheimnis zu wahren. Die verantwortlichen Mitarbeiterinnen und Mitarbeiter in Krankenhäusern erhalten von uns die notwendigen Hilfestellungen.

Die erfolgreiche Aktion „Datenschutz in meiner Arztpraxis“ hat sich auch bei den Ärzten in den Krankenhäusern herumgesprochen. Nachfragen, nicht nur aus Schleswig-Holstein, wann es diese Aktion auch für Krankenhäuser geben wird, häuften sich. Dies veranlasste uns, den aus Kapazitätsgründen für einen späteren Zeitpunkt geplanten Schritt der Ausweitung auf den stationären Bereich bereits jetzt zu gehen. Dieser Teil der Aktion findet nicht nur in enger Zusammenarbeit mit der Ärztekammer, sondern auch mit der **Krankenhausgesellschaft Schleswig-Holstein** (KGSH) statt. Ihr sind die privaten und öffentlichen Kliniken in Schleswig-Holstein angeschlossen. Die KGSH griff unsere Initiative positiv auf und sagte ihre Unterstützung zu.

Mit **Fortbildungsveranstaltungen** der DATENSCHUTZAKADEMIE Schleswig-Holstein und einer im Internet veröffentlichten Ausarbeitung versuchten wir zunächst, Grundlageninformationen zu verbreiten.


www.datenschutzzentrum.de/medizin/krankenh/patdskh.htm

Als Nächstes wurde den Krankenhäusern in Schleswig-Holstein eine **Checkliste** zur Verfügung gestellt. Diese ermöglicht eine Bestandsaufnahme, um etwaige Schwachstellen bei der Beachtung des Patientengeheimnisses zu erkennen. Ergänzend wurden weitere umfangreiche Informationsmaterialien zur Verfügung gestellt, etwa das Muster einer Archivordnung.


www.datenschutzzentrum.de/medizin/krankenh/index.htm

Durch die Teilnahme am Flensburger Forum für IT-Anwendungen im Gesundheitswesen, wo IT-Spezialisten, Verantwortliche aus der Verwaltung und Mediziner zusammenkommen, und auf ähnlichen Veranstaltungen versuchen wir, unsere Lösungen im **Dialog mit den Praktikern** vor Ort weiterzuentwickeln.

Was ist zu tun?
Durch die Ausweitung der Aktion „Datenschutz in meiner Arztpraxis“ wird den Ärztinnen und Ärzten in den Krankenhäusern Schleswig-Holsteins die Möglichkeit geboten, aktiv zur Optimierung des Patientengeheimnisses beizutragen.

4.7.4 Projekte auf dünnem Eis

Bei den Planungen zur Verbesserung der Gesundheitsversorgung und zur Kosteneinsparung bei den Krankenkassen spielt der Datenschutz leider immer noch keine wichtige Rolle. Oft bleibt allerdings nicht nur der Datenschutz auf der Strecke, sondern das Projekt selbst.

Während die Kooperation zwischen den Krankenkassen bzw. den Kassenärztlichen Vereinigungen des Landes und uns sehr eng ist, gilt dies für Projekte auf Bundesebene leider nicht. Eine Konsequenz ist, dass gelegentlich beträchtliche Summen für Projekte ausgegeben werden, die sich als rechtswidrig oder als praktisch nicht durchführbar erweisen. So sollte in Schleswig-Holstein ein Verfahren zur Verhinderung der **missbräuchlichen Nutzung von Krankenversicherungskarten** eingeführt werden. Zu diesem Zweck sollten die Krankenkassen einem privaten Dienstleister quartalsweise die Daten aller gesperrten Karten ohne Namensangabe weitergeben. Der Dienstleister sollte daraus Datenträger erstellen, die den Arztpraxissoftwarehäusern und von diesen wiederum im Rahmen der Softwarewartung den Ärzten zur Verfügung gestellt werden sollten. Die Idee war gut, die Umsetzung nicht: Es war in keiner Weise sichergestellt, dass die Daten bei dem privaten Dienstleister, den Softwarehäusern und den Ärzten hinreichend gesichert würden. Die Zuordnung zu konkreten Personen war nicht ausgeschlossen. Bei einer rechtzeitigen datenschutzrechtlichen Beratung hätten die Fehlinvestitionen vermieden werden können.

Zu den Neuerungen im Jahr 2004 gehört auch eine Regelung, die es den Krankenkassen erlaubt, zur Gewinnung von Mitgliedern Daten aus öffentlichen Quellen zu verarbeiten, wenn die Betroffenen dem nicht widersprechen bzw. keine schutzwürdigen Interessen entgegenstehen. Damit ist es den Kassen möglich, Adress- und Telefonbücher oder öffentlich zugängliche elektronisch gespeicherte Adressdaten für **Werbezwecke** zu nutzen. Nicht zulässig ist es aber, derartige Primärdaten derart anzureichern, dass Personenprofile entstehen. Daher haben wir der AOK mitgeteilt, dass die Nutzung einer großen Datenbank eines Direktmarketingunternehmens, die auf einer Vororterhebung basiert, schutzwürdige Betroffeneninteressen verletzt. Die Anmietung von Adressen bei Adressenhändlern, die diese z. B. bei Konsumentenbefragungen erlangt haben, ist keine Datenbeschaffung aus öffentlichen Quellen. Die rechtmäßig erlangten Daten dürfen ausschließlich mit folgenden Sozialdaten der Krankenkasse abgeglichen werden: Namen, Geburtsdatum, Geschlecht und Anschrift. Dadurch wird sichergestellt, dass keine Vermischung von Sozialdaten und Werbedaten erfolgt.

Was ist zu tun?
Bei den Reformprojekten im Bereich der gesetzlichen Krankenversicherung muss von Anfang an datenschutzrechtlicher Sachverstand berücksichtigt werden, da praktisch immer der Umgang mit höchst sensiblen Daten zur Disposition steht; andernfalls drohen die Projekte gegen die Wand zu fahren.

4.7.5 Disease-Management-Programm

Mit so genannten Disease-Management-Programmen (DMP) sollen chronisch Kranke besser ärztlich betreut werden. Hierfür sollen von unabhängigen Arbeitsgemeinschaften sensible Behandlungsdaten verarbeitet werden. Entgegen den Vorschriften des Sozialdatenschutzes will das Bundesversicherungsamt diese Aufgabe auch durch private, eventuell sogar ausländische Firmen vornehmen lassen.

Die äußerst anspruchsvolle Aufgabe, durch eine arztübergreifende medizinische Dokumentation eine patientenadäquate Versorgung zu sichern, ohne dabei für die Krankenkassen den „gläsernen Patienten“ zu schaffen, wurde in zähen Verhandlungen dadurch gelöst, dass die pseudonyme Dokumentation nicht von den Krankenkassen selbst vorgenommen wird, sondern von **selbstständigen Arbeitsgemeinschaften**, an denen neben den Kassen auch die Ärzteschaft über die Kassenärztlichen Vereinigungen beteiligt ist (vgl. 25. TB, Tz. 4.8.1). Die Datenverarbeitung bei diesen Arbeitsgemeinschaften unterliegt im Interesse des Schutzes des Sozial- und des Patientengeheimnisses hohen Sicherheitsanforderungen. Daher regelt das Sozialgesetzbuch auch, dass der überwiegende Teil der Datenverarbeitung unter direkter Verantwortung einer öffentlichen Stelle erfolgen muss und nicht an private Stellen ausgelagert werden darf.

Diese eindeutige gesetzliche Regelung wurde vom Bundesversicherungsamt (BVA), das die staatliche Aufsicht über die Durchführung der DMP ausübt, von Anfang an ignoriert. Das BVA fordert von den Beteiligten, dass sie die Datenverarbeitung **europaweit ausschreiben**. Das BVA geht davon aus, dass selbst ausländische private Stellen die gesamte Datenverarbeitung der Chronikerprogramme übernehmen könnten. Obwohl die Datenschutzbeauftragten des Bundes und der Länder immer wieder auf die Unzulässigkeit dieser Vorgehensweise hingewiesen haben, beharrte das BVA auf seiner Position. Die Konsequenzen für die chronisch Kranken wie für die Krankenkassen sind gravierend: Die Patienten können nicht sicher sein, dass ihre sensiblen Daten gemäß den hohen Datenschutzstandards des Sozialgesetzbuches verarbeitet werden. Die Krankenkassen werden gezwungen, äußerst kosten- und zeitintensive Ausschreibungen vorzunehmen und im Fall einer entsprechenden Auftragsvergabe Datenverarbeitungsstrukturen, deren Rechtswidrigkeit bei vernünftiger Rechtsanwendung unzweifelhaft ist, zu etablieren. Weitere Konsequenz ist, dass sehenden Auges vom BVA Millioneninvestitionen für eine gesetzwidrige Aktion zulasten der Krankenkassen veranlasst werden.

? DMP

DMP steht für Disease-Management-Programm. Dabei erstellen die Krankenkassen gemeinsam mit der Kassenärztlichen Vereinigung für chronisch Kranke jeweils individuelle Patientendokumentationen, die zur Optimierung der Behandlung genutzt werden sollen, indem eine gezielte Beratung erfolgt, Behandlungsschritte koordiniert, kontrolliert und an den neuesten wissenschaftlichen Erkenntnissen ausgerichtet werden. Bei den hierbei entstehenden Dokumentationen handelt es sich um höchst sensible elektronische Datensammlungen.

Daher haben wir gemeinsam mit anderen Datenschutzbeauftragten das BVA aufgefordert, das Sozialgesetzbuch zu beachten und auf die Forderung nach einer europaweiten, private Firmen mit erfassenden Ausschreibung zu verzichten.


www.datenschutzzentrum.de/medizin/gkv/dmp_bva.htm

Was ist zu tun?
Die Ausschreibungen sind zu stoppen und in gesetzeskonformer Weise zu wiederholen.

4.7.6 Gesundheitskarte Schleswig-Holstein

Im Jahr 2003 wurde mit der praktischen Erprobung einer umfassenden Gesundheitschipkarte beim regionalen Praxisnetz Flensburg begonnen. Viele Datenschutzfragen harren noch einer Antwort.

Die Erprobung einer **erweiterten Gesundheitschipkarte** kommt nur langsam voran (vgl. 25. TB, Tz. 4.8.2). Nach einer Änderung im Sozialgesetzbuch V besteht seit Jahresbeginn 2004 für die elektronische Gesundheitskarte eine rechtliche Grundlage. Diese überträgt dem einzelnen Patienten eine umfassende Mitbestimmungsmöglichkeit hinsichtlich der Datennutzung und setzt hierfür wirksame Einwilligungserklärungen voraus.

Ende 2003 wurde mit dem begrenzten Wirkbetrieb der Karte im **Flensburger Raum** begonnen. Dabei stehen die Integration eines Lichtbildes sowie die Möglichkeit des Einspielens von weiteren Versicherten- und Notfalldaten auf den Chip durch die behandelnden Ärzte im Mittelpunkt. Durch eine umfassende Information, verbunden mit einer Einwilligungserklärung, soll erkundet werden, wie groß die Akzeptanz bei den Patienten für eine solche Karte ist. Aus Datenschutzsicht sind noch viele Fragen offen. So ist es für uns nicht erkennbar, weshalb im Arztrechner ein Bild des Patienten gespeichert werden muss.

Was ist zu tun?
Innovationen im Gesundheitsbereich haben dann gute Akzeptanzchancen, wenn das Patientengeheimnis von Anfang an gewahrt wird.

4.7.7 Anforderung von Kurzberichten durch Krankenkassen

Die Kosten für stationäre Behandlungen rechnen die Krankenhäuser mit der jeweiligen gesetzlichen Krankenkasse direkt ab. Das Sozialgesetzbuch V enthält eine abschließende Aufzählung der Patientendaten, die der Krankenkasse zur Prüfung der Erforderlichkeit der stationären Behandlung übermittelt werden dürfen.

Der Datenhunger der Krankenkassen war schon oft Gegenstand unserer Berichte. In unserem 22. Tätigkeitsbericht forderten wir unter Tz. 4.7.3: „Keine **Krankenhausentlassungsberichte** an Krankenkassen“. Die Krankenkassen versuchten auch immer wieder, an Arztbriefe oder OP-Berichte zu gelangen. Mal wurde den Krankenhäusern gedroht, ohne die Daten gäbe es kein Geld. Mal legten die Krankenkassen von ihren Versicherten unterschriebene Schweigepflichtentbindungserklärungen vor, mit denen die gesetzliche Regelung umgangen werden sollte.

Die Krankenkassen in Schleswig-Holstein berichteten uns andererseits von so mancher stationären Krankenhausbehandlung, bei deren näherer Betrachtung sich herausstellte, dass sie nicht notwendig war. Die gesetzlich vorgesehene Prüfung der Notwendigkeit nimmt der Medizinische Dienst der Krankenversicherungen (MDK) vor. Ein solcher **Auftrag an den MDK** wird immer dann erteilt, wenn sich Zweifel an der Erforderlichkeit der Behandlung ergeben. Dies geschieht – so die Kassen – in mehr Fällen als notwendig, nur weil sie nicht die „richtigen“, d. h. die zur Vorprüfung ausreichenden Daten erhalten würden.

Folgendes **Beispiel** soll diese Problematik beleuchten: Ein Patient wird stationär für einige Tage im Krankenhaus aufgenommen. Auf der Abrechnung für die Krankenkasse steht als Diagnose „Grippe“. Ist bei einer Grippe wirklich eine stationäre Behandlung erforderlich? Eine Grippeerkrankung ist grundsätzlich nur ambulant zu behandeln, Zweifel an der Erforderlichkeit des Krankenhausaufenthaltes sind also vorprogrammiert. Nach dem bisherigen Verfahren musste die Krankenkasse den MDK um Prüfung bitten. Erst nach dieser Prüfung erfuhr die Krankenkasse, dass Komplikationen, z. B. aufgrund des Alters des Patienten, eine stationäre Behandlung notwendig machten.

Diese aufwändigen und letztlich oft überflüssigen Prüfungen belasteten den MDK, die Krankenkassen, die Krankenhäuser und die Patienten. Es galt deshalb gemeinsam eine Lösung für dieses Problem zu suchen. Die Spitzenverbände der Krankenkassen und die Krankenhausgesellschaft Schleswig-Holstein verhandelten im Berichtsjahr unter Vermittlung einer Schiedsstelle einen neuen Vertrag zur Prüfung der Notwendigkeit und Dauer der Krankenhausbehandlung. Bezüglich der Anforderung von Kurzberichten durch die Kassen wurden wir frühzeitig beteiligt. Die Krankenkassen räumten ein, dass der entstandene Wildwuchs bei der Anforderung von weiteren Unterlagen nicht nur unzulässig, sondern auch uneffektiv sei. Es zeigte sich, dass es oft ausreichend ist, wenn im Einzelfall neben der eigentlichen Diagnose („Grippe“) Informationen zur **Ausprägung der Haupt- und Nebendiagnosen** („Komplikationen“) oder zu den **besonderen Mitteln eines Krankenhauses** (z. B. technische Ausstattung) gegeben werden. Wir sind der Auffassung, dass diese Daten von dem im SGB V enthaltenen Katalog mit erfasst sind. Die Krankenhäuser dürfen solche Daten übermitteln, mit denen die Krankenkassen eine erste **Plausibilitätsprüfung** der Notwendigkeit und Dauer der stationären Behandlung durchführen können.

Unsere Bewertung wurde zur Grundlage des zwischen den Spitzenverbänden der Krankenkassen und der Krankenhausgesellschaft Schleswig-Holstein abgeschlossenen neuen Vertrags. Dieser Vertrag beinhaltet einen Mustervordruck für die **Anforderung von Kurzberichten**, durch den festgelegt wird, welche Daten an eine Krankenkasse übermittelt werden sollen. Weiter gilt, dass die Anforderung von Kurzberichten nur in begründeten Einzelfällen, also nicht pauschal erfolgen darf. So müssen Krankenkassen zukünftig gegenüber den Krankenhäusern angeben, warum ein Kurzbericht angefordert wird. Die Anforderung weiterer Unterlagen ist nicht zulässig. So ist sichergestellt, dass die Rechtsunsicherheit bei der Anforderung von Unterlagen wie Entlassungsberichten ein Ende hat. Das Verfahren ist transparent, für alle Beteiligten verständlich und rechtlich durch die Vorschriften des Sozialgesetzbuches V gedeckt.

Was ist zu tun?
Krankenkassen und Krankenhäuser müssen sich an den in Schleswig-Holstein geschlossenen Vertrag bezüglich der Zulässigkeit der Anforderung von Kurzberichten halten.

4.7.8 Stiften Versicherungen zur Geheimnisverletzung an?

Bei privaten Krankenversicherungen scheint das Patientengeheimnis ihrer Mitglieder nicht an erster Stelle der Prioritätenliste zu stehen. Sie operieren weiter mit unzulänglichen Schweigepflichtentbindungsklauseln.

Bereits im letzten Bericht stellten wir die Problematik der **pauschalen Schweigepflichtentbindungserklärungen** dar, die sich private Krankenversicherungen, aber auch Unfall-, Renten- und Lebensversicherungen, bei Vertragsschluss geben lassen (vgl. 25. TB, Tz. 4.8.3). Darin sollen die Versicherten unterschreiben, dass die Versicherungen bei behandelnden Ärzten Patientendaten abfragen dürfen. Zum Zweck der Risikobeurteilung bei Vertragsabschluss soll dies noch fünf Jahre nach Antragstellung zulässig sein und sich auf die Behandlungen der letzten zehn

Jahre erstrecken können. Für die Beurteilung der Leistungspflicht soll die Entbindung sogar unbefristet für die Zukunft gelten.

Wir haben gemeinsam mit den anderen im „Düsseldorfer Kreis“ organisierten Aufsichtsbehörden den Gesamtverband der Versicherungswirtschaft als Zusammenschluss aller Versicherer darauf hingewiesen, dass die seit 15 Jahren verwendeten Erklärungstexte nicht mit der Rechtslage übereinstimmen. Seit der Umsetzung der Europäischen Datenschutzrichtlinie im Bundesdatenschutzgesetz 2001 ist eine **hinreichend bestimmte Erklärung** notwendig. Hiervon kann bei den gebräuchlichen Formulartexten keine Rede sein: Die Versicherten können bei Vertragsschluss nicht erkennen, welche Patientendaten in 10, 20 oder gar 30 Jahren anfallen und ob sie damit einverstanden sind, dass diese ungefragt an ein Versicherungsunternehmen weitergegeben werden dürfen. Diese Einschätzung der Aufsichtsbehörden wird auch von der Ärztekammer und der Zahnärztekammer Schleswig-Holstein geteilt.

Die **Versicherungswirtschaft** weigert sich, ihre Formulare neu zu gestalten. Statt im Interesse ihrer Versicherten eine kundenfreundliche Lösung zu suchen, zaubert sie immer wieder neue **Ausflüchte** aus dem Hut. Bei den Leistungsanträgen und dem Einreichen von Rechnungen würden die Versicherten oft keine Vordrucke verwenden, auf die man eine hinreichend konkrete Entbindung der Schweigepflicht aufnehmen könnte. Eine nachträgliche Einholung der Erklärung sei zu teuer und zu aufwändig, obwohl nach eigenen Angaben nur in 0,5 % der Fälle eine Nachprüfung der eingereichten Rechnungen durch eine Rückfrage beim Arzt erfolgt. Schließlich wurden Archivierungsprobleme vorgetragen, als kenne dieser Wirtschaftssektor die Segnungen moderner Aktenablagesysteme noch nicht. Aus Eingaben ist uns bekannt, dass das Anfordern von Unterlagen – auch beim Patienten – für die Versicherungswirtschaft kein Problem darstellt, wenn dadurch Zahlungen vermieden werden können.

Das Verhalten der Versicherungswirtschaft ist nicht nur **kundenunfreundlich**. Es ist auch ein Beitrag dazu, dass die in rechtlichen Fragen oft nicht geschulten Ärzte zur Verletzung ihrer Schweigepflicht verleitet werden. Da die rechtlichen Möglichkeiten der Aufsichtsbehörden im vorliegenden Fall erschöpft sind, geben wir Ärzten und Patienten den Ratschlag, Datenbeschaffungsversuche von Versicherungen mittels unwirksamer Einwilligungserklärungen zurückzuweisen. Wir behalten uns vor, das Vorgehen der Versicherungen auch strafrechtlich untersuchen zu lassen.

Was ist zu tun?
Die Versicherungswirtschaft wäre gut beraten, ihren Widerstand gegen eine rechtskonforme Vorgehensweise abzulegen.

4.7.9 Datenerhebung bei der Erstanamnese

Da staunte eine Mutter nicht schlecht: Schon vor dem ersten Termin ihres Kindes bei einem Kieferorthopäden wurde ihr ein dreiseitiger Fragebogen übersandt. Am Telefon wurde ihr mitgeteilt, dass eine Behandlung nur erfolgen könne, wenn sie die Fragen beantworten würde. Diese „Neugier" ging der Mutter eindeutig zu weit.

Der Vordruck enthielt Fragen wie:

- Wo lebt der Patient (Mutter/Vater/Großeltern/Adoptiveltern/Heim/Internat)?
- Bestehen bei den Geschwistern oder Eltern Zahnunregelmäßigkeiten?
- Verlief die Schwangerschaft bzw. die Geburt normal?
- Wie groß und schwer war der Patient bei der Geburt?
- Wie lange wurde das Kind gestillt, und wurde in dieser Zeit zugefüttert?
- Wann lernte der Patient das Gehen und wann das Sprechen?
- Welche Probleme hat der Patient mit der Sprachentwicklung?
- Leidet oder litt der Patient an Spreizfüßen?
- Wurde der Patient jemals operiert, wenn ja, warum?

Der Kieferorthopäde meinte, dass jede Frage ihre medizinische Berechtigung habe. Die Zahnärztekammer bestätigte, dass ein Patient seinem Arzt vertrauen und sich auf dessen fachliche Vorgehensweise einlassen müsse. Gegebenenfalls sei ein anderer Arzt aufzusuchen. Die Mutter war mit dieser Antwort nicht zufrieden. Sie wollte ja ihrem Arzt vertrauen, aber vor dem Vertrauen kommt das Verstehen. Ein Arzt benötigt als Grundlage für eine effiziente Behandlung sicher bestimmte Informationen über den Patienten. Insofern leuchten auch pauschale Fragen nach Alter, Größe, Gewicht und **Vorerkrankungen** ein. Aber warum muss ein Kieferorthopäde wissen, ob der Patient unter Haltungsschäden leidet? Er meinte dazu, Haltungsschäden könnten sich auch auf die Stellung der Kiefer auswirken, was bei der Anfertigung der Zahnspange zu beachten sei.

Gefragt werden sollte grundsätzlich nur das, was für die Durchführung der gewünschten Behandlung medizinisch erforderlich ist. Der Arzt muss seine Patienten über den Zusammenhang der Fragen mit der gewünschten Behandlung **aufklären**, ansonsten besteht die Gefahr, dass seine Fragen nicht oder nicht korrekt beantwortet werden. In vielen Fällen mag eine Information im Fragebogen ausreichen. Der Patient sollte aber auf keinen Fall das Gefühl haben, dass schon die Rückfrage beim Arzt als Misstrauen gewertet wird. Da ein Fragebogen immer eine Vielzahl von – eventuell nicht relevanten – Fragen enthält, sollte dem Patienten die Möglichkeit gegeben werden, einzelne Fragen nicht zu beantworten.

Anamnesebögen können ein sinnvolles Hilfsinstrument für den Arzt sein, wenn sie zweckgerichtet und patientengerecht ausgestaltet und eingesetzt werden. In unseren, im Internet unter

www.datenschutz.de/medizin/arztprax/anamnese.htm

veröffentlichten **Hinweisen** sind die wichtigsten dabei zu beachtenden Punkte dargestellt.

Was ist zu tun?
Bei der Erstanamnese sind nur die Daten zu erheben, die aus medizinischer Sicht für die gewünschte Behandlung erforderlich sind. Wir empfehlen, unsere „Hinweise zur Verwendung von standardisierten Anamnesefragebögen“ zu beachten.

4.7.10 Verordnungsmonitoring bei niedergelassenen Ärzten

Was machen Pharmafirmen mit den Rezept- und Verordnungsdaten, die Ärzte ihnen in elektronischer Form „zum Zweck der Auswertung“ zur Verfügung stellen sollen? Wir haben keinen Anhaltspunkt für Missbrauch, aber die Verfahren müssen wesentlich transparenter sein.

> ***? Verordnungsmonitoring***
>
> *Die Erstattungsfähigkeit von Verordnungen durch Ärzte hängt davon ab, dass die Ärzte sich an einen gewissen vorgegebenen Rahmen halten. Um einen Überblick hierüber zu erhalten, erfolgt durch private EDV-Dienstleister für den jeweiligen Arzt ein Verordnungsmonitoring. Hierfür stellt der Arzt Teile seiner elektronischen Patientendokumentation zur Verfügung. Die daraus erstellten Statistiken sind nicht nur für den Arzt von Interesse, sondern auch für die Pharmawirtschaft.*

Liest man die Werbung von EDV-Dienstleistern, die Ärzten das so genannte Verordnungsmonitoring anbieten, so muss man das Schlimmste befürchten: Da ist davon die Rede, dass den Ärzten ein Sorglospaket mit einem dauernden Überblick über das eigene Verordnungsverhalten inklusive Systemwartung zur Verfügung gestellt wird, wenn sie ihre Rezeptdaten elektronisch zur Verfügung stellen. Es stellt sich beim Lesen der **Hochglanzbroschüren** der Verdacht ein, dass diese Dienstleister sich die Patientendaten direkt über das Internet aus dem Arztrechner absaugen. Natürlich erfahren die Patienten von diesem Verordnungsmonitoring nichts. Wäre also der erste Eindruck richtig, so würde in Deutschland in großem Umfang das Patientengeheimnis mit Füßen getreten.

Eine Prüfung der auf dem Markt angebotenen Verfahren zeigte, dass teilweise datenschutzrechtliche Mängel bestehen. Eine millionenfache Verletzung des Patientengeheimnisses erfolgt jedoch nicht. So konnten wir nicht feststellen, dass die Dienstleister sich die Daten eigenmächtig von den Arztrechnern holen. Vielmehr muss der Arzt diese Daten von sich aus elektronisch versenden, wobei er durch ein automatisiertes Verfahren angehalten wird, diese zuvor zu aggregieren oder zumindest zu pseudonymisieren, sodass der Dienstleister **keine Klardaten** über Patienten erhält. Da wir nicht feststellen konnten, dass anhand dieser Daten eine Reidentifizierung der Patientendaten möglich ist, stellten wir auch keine Verletzung des Patientengeheimnisses fest. Offensichtlich geben die Dienstleister die erhaltenen Daten nicht personenbezogen, sondern nur aggregiert an die Pharmaindustrie weiter, die diese Daten dann für Marketingzwecke nutzen.

Weder die Software- noch die Monitoringanbieter vermitteln aber gegenüber den Ärzten eine **transparente Datenschutzpolicy**. Nicht nur, dass das Verfahren der Aggregierung bzw. Pseudonymisierung weitgehend unklar dargestellt wird, auch

bezüglich der Gefahren, die mit einer Verbindung der Praxisrechner mit dem Internet verbunden sind, wird der Ärzteschaft kein reiner Wein eingeschenkt. Tatsächlich sind schon viele Arztpraxisrechner mit dem Internet verbunden, ohne dass eine sichere Abschottung der Patientendaten erfolgt. Insofern ist es schon fast ein Wunder, dass in der Öffentlichkeit noch nicht mehr Fälle bekannt geworden sind, in denen Hacker sich über das Internet illegal Patientendaten beschafft haben.

Wir haben die Monitoringanbieter auf die bestehenden Schwachstellen hingewiesen und sie aufgefordert, die Defizite zu beheben. Die ausführliche Darstellung unserer Untersuchung haben wir auch den Patienten und der Ärzteschaft über unsere Webseite zur Verfügung gestellt unter

www.datenschutzzentrum.de/medizin/arztprax/monitoring.htm

Was ist zu tun?
Das Vertrauen der Ärzte in das Verordnungsmonitoring könnte durch mehr Transparenz gestärkt werden.

4.7.11 Arztbrief an mündige Patienten

Nach Beendigung der stationären Behandlung in einer Klinik werden Krankenhausentlassungsberichte oder abschließende Arztbriefe geschrieben. Diese enthalten detaillierte Angaben zu Anamnese, Vorbefunden, Diagnosen und durchgeführten Behandlungen. Warum erhalten in den wenigsten Fällen die Patienten selbst diese Arztbriefe, jedoch fast immer die einweisenden Ärzte bzw. die Hausärzte?

Das Patientengeheimnis gilt grundsätzlich auch zwischen dem Arzt eines Krankenhauses und dem behandelnden Hausarzt. Nur wenn der Patient damit einverstanden ist, darf dem Hausarzt ein Arztbrief zugesandt werden. Nach den Ärztlichen Berufsordnungen ist das **Einverständnis** des Patienten **anzunehmen**, wenn mehrere Ärzte gleichzeitig oder nacheinander denselben Patienten untersuchen oder behandeln. Dies entbindet den Arzt im Krankenhaus jedoch nicht von der Pflicht, den tatsächlichen Willen des Patienten so weit wie möglich zu ergründen.

Schon bei der **Aufnahme** im Krankenhaus wird gefragt, wer der behandelnde (Haus-)Arzt ist bzw. welcher Arzt die Einweisung veranlasst hat. Alleine der Umstand, dass ein Patient bei dieser Frage einen Arzt benennt, bedeutet aber nicht zwangsläufig, dass er eine Unterrichtung dieses Arztes über die Krankenhausbehandlung wünscht. Bei der Aufnahme sollte daher auch gefragt werden, ob der Patient damit einverstanden ist, dass den von ihm benannten Ärzten ein Arztbrief übersandt wird. Ist diese Frage frühzeitig geklärt, müssen sich die behandelnden Ärzte nicht mehr später während der eigentlichen Behandlung hierum kümmern.

Möglich ist auch, dem Patienten den Arztbrief zur Weiterleitung zu übergeben. So hat der Patient selbst die Möglichkeit zu entscheiden, welchem Arzt er diesen weitergibt. Grundsätzlich sollte auch der Patient eine Kopie erhalten. Dieses Vor-

gehen fördert den **mündigen Patienten** und macht spätere Nachfragen und Auskunftsforderungen überflüssig. Mehr zu den Patientenrechten haben wir veröffentlicht unter

www.datenschutzzentrum.de/medizin/arztprax/dsrdpat1.htm

Was ist zu tun?
Zu Beginn der stationären Aufnahme sollte der Patient gefragt werden, ob der Hausarzt, der einweisende Arzt oder ein anderer Arzt einen Arztbrief oder Krankenhausentlassungsbericht erhalten soll.

4.7.12 Kosmetiksalon mit Zugriff auf Arztpraxisdaten

Das Patientengeheimnis ist natürlich auch dann zu beachten, wenn ein Hautarzt nebenbei einen Kosmetiksalon betreibt.

Zunächst wollten wir es gar nicht glauben: Eine Petentin schilderte uns, dass sie bei einem Hautarzt in Behandlung war. Als sie sich wenig später in einem Kosmetiksalon eine vom Arzt empfohlene Creme besorgen wollte und nach ihrem Namen gefragt wurde, habe sie feststellen müssen, dass es der Kosmetikerin möglich war, direkt auf den **Praxisrechner des Arztes** mit Behandlungsterminen, Diagnosen und verordneten Medikamenten zuzugreifen. Bei unserer Recherche zeigte sich, dass die Vorwürfe nicht aus der Luft gegriffen waren: Das Kosmetikgeschäft gehörte demselben Arzt, auf dessen Rechner zugegriffen werden konnte. Er verwies auf ein Schild mit der Information, dass das Kosmetikgeschäft im Auftrag des Hautarztes handele. Die Kosmetikangestellten seien auf das Patientengeheimnis verpflichtet. Ein Anwalt habe bestätigt, dass dies den rechtlichen Anforderungen genüge.

Wir haben dem Arzt mitgeteilt, dass die von ihm eingeräumte Zugriffsmöglichkeit auf Patientendaten eine grundsätzlich strafbare Verletzung seiner ärztlichen Schweigepflicht war. Daran ändert auch der Umstand nichts, dass er selbst Besitzer des Kosmetiksalons ist. Ein Hinweisschild und die Verschwiegenheitsverpflichtung der Angestellten können die für eine Offenbarung nötige Einwilligung nicht ersetzen. Nachdem wir eine technische Anordnung androhten, war der Arzt auch bereit, die beiden verbundenen **Systeme zu trennen** und künftig getrennt zu betreiben.

Was ist zu tun?
Ärzte müssen darauf achten, dass ausschließlich die im Rahmen der Behandlung beschäftigten Praxismitarbeiterinnen und -mitarbeiter Zugriff auf Patientendaten haben dürfen.

4.7.13 Das Patientengeheimnis bei komplizierten Familienverhältnissen

Das Patientengeheimnis ist auch gegenüber Familienmitgliedern zu beachten, z. B. auch gegenüber dem Stiefvater von Kindern.

Ein getrennt lebender Ehemann wollte das alleinige Sorgerecht für sein Kind erlangen. Er behauptete, die Mutter sei nicht in der Lage, das Kind zu versorgen. Sie zeige keine Verantwortung und neige dem Alkohol zu. All dies habe er von dem behandelnden Kinderarzt erfahren, der nicht nur das gemeinsame Kind, sondern auch zwei Kinder der Frau aus erster Ehe jahrelang behandelt hatte. Der Kinderarzt habe ihm mitgeteilt, dass die Mutter Arzttermine der Stiefkinder wegen persönlicher Probleme nicht habe wahrnehmen können. Der Vater benannte den **Kinderarzt** als **Zeugen** für das anstehende **Sorgerechtsverfahren**.

Für die Mutter brach eine Welt zusammen. Ihr Ehemann hatte bis zur Trennung nicht einen Arzttermin wahrgenommen. Sie hatte dem Kinderarzt stets vertraut. Es konnte nicht zulässig sein, dass der Ehemann Auskunft über die Stiefkinder und ihre Vergangenheit erhalte. Der Kinderarzt bestätigte uns gegenüber das Gespräch mit dem Ehemann: Schließlich müsste doch auch ein Stiefvater ein Recht auf Auskunft haben. Hier lag der Kinderarzt falsch. Die **ärztliche Schweigepflicht** galt auch **gegenüber dem Stiefvater**. Nur im Fall der Adoption und nach Übertragung des Sorgerechtes wäre er berechtigt gewesen, Auskunft zu verlangen. Der Arzt konnte auch nicht davon ausgehen, dass die sorgeberechtigte Mutter ihre Einwilligung erteilt hatte, da der Stiefvater vor der Trennung zu keinem Zeitpunkt Arzttermine bei ihm wahrgenommen hatte. Zudem richtete sich das Auskunftsersuchen offensichtlich gegen die Interessen der Mutter. Bevor der Arzt das Gespräch mit dem Stiefvater führte, hätte er bei der Mutter eine schriftliche Einwilligung einholen müssen.

Was ist zu tun?
Bevor ein Arzt Dritten über Patienten Auskunft erteilt, muss er seine Befugnis hierzu prüfen. Bei minderjährigen, noch nicht selbst einsichtsfähigen Patienten ist grundsätzlich der Sorgeberechtigte zu befragen.

4.7.14 Psychiatriealtakten mit Ewigkeitswert?

Patienten eines Krankenhauses betrachteten das Lesen von Psychiatrieakten als interessantes „Freizeitangebot“. Die Prüfung des Archivs brachte eine ungeordnete Archivierung zutage.

Für Krankenunterlagen über eine stationäre Behandlung besteht eine Aufbewahrungsfrist von mindestens zehn bzw. ein **Aufbewahrungsrecht von 30 Jahren**. Nach Ablauf dieser Aufbewahrungsfristen sind die Unterlagen von öffentlichen Krankenhäusern dem Landesarchiv anzubieten oder, sofern sie von dort nicht als „archivwürdig“ bewertet werden, ordnungsgemäß zu vernichten. Eine längere Aufbewahrung als 30 Jahre ist im Einzelfall zulässig, wenn dies aus medizinischen (psychotherapeutischen) Gründen oder zur Durchführung von rechtlichen Auseinandersetzungen, bei denen die Akte beweiserheblich ist, erforderlich ist.

Die Verwaltung des Archivgutes sollte deshalb in einer Archivordnung geregelt sein. Ein Muster hierfür haben wir veröffentlicht unter

www.datenschutzzentrum.de/material/themen/gesund/muarcho.htm

Nachdem vor einiger Zeit ein Patient die unklaren Verhältnisse im Zusammenhang mit seiner psychiatrischen Behandlung gerügt hatte, sagte uns der Direktor der betroffenen Klinik für Psychiatrie und Psychotherapie der CAU zu, diese Regeln künftig zu beachten.

Zwei Jahre später berichtete uns ein anderer Patient des gleichen Krankenhauses jedoch von einem besonderen „Freizeitangebot“: In einem unverschlossenen und frei zugänglichen Raum im Dachgeschoss direkt neben der Bibliothek würden sich **Kisten mit Patientenakten** aus den Jahren 1938 bis 1944 stapeln. Die Möglichkeit, diese Patientenakten zu lesen, sei ein Insidertipp unter den Patienten. Der Hinweis war für uns Anlass, noch am gleichen Tag eine Prüfung vor Ort durchzuführen. Unsere Feststellungen waren alles andere als erfreulich.

In nicht weniger als neun Räumen wurden Krankenunterlagen verschiedener psychiatrischer und psychotherapeutischer Kliniken aufbewahrt. Zwar waren die Räume zum Zeitpunkt unserer Prüfung verschlossen, doch Beanstandungen gab es reichlich. Das als „Nervenberg“ bezeichnete **Klinikgelände in Kiel** besteht seit ca. 1900. Genauso alt waren diverse von uns gefundene Patientenunterlagen. Im Raum neben der Bibliothek fanden wir Patientenakten aus der Zeit des Dritten Reichs. Es existierten weder eine Archivordnung noch andere Regelungen, die hätten sicherstellen können, dass nur Befugte zu diesen äußerst sensiblen Unterlagen Zugang haben.

Aufgrund unserer Kritik erklärte der Klinikdirektor, dass nach Absprache mit dem Landesarchiv die Krankenunterlagen aus den Jahren vor 1950 sowie aus der Folgezeit jene Akten, bei denen der Nachname des Patienten mit dem Buchstaben „D“ beginnt, dort ordnungsgemäß archiviert werden. Die Akten, die nicht aus rechtlichen oder medizinischen Gründen länger als 30 Jahre aufbewahrt werden müssen, würden umgehend vernichtet. In Anlehnung an unsere Musterarchivordnung wurde eine **Dienstvorschrift** erlassen.

Was ist zu tun?
Die Aufbewahrung von Patientenunterlagen ist durch eine Archivordnung zu regeln. Die Löschfristen sind genau zu beachten. Angesichts der gemachten Erfahrungen werden wir die Umsetzung der angekündigten Schritte in der Psychiatrie des Kieler Klinikums überprüfen.

4.7.15 Wegen Verletzung des Patientengeheimnisses zur Kasse gebeten

Guter Wille und Aufklärung ändern nichts an dem Umstand, dass es sich bei dem Bruch des Patientengeheimnisses um eine Straftat handelt, die auf Antrag des Betroffenen verfolg- und sanktionierbar ist.

Vonseiten der **Justiz** wird in diesem Bereich leider nicht immer ein zeitgemäßes Datenschutzbewusstsein gezeigt. So wurden wir über einen Vorgang informiert, bei dem ein Praxisnachfolger ohne eine wirksame Einwilligung des Patienten Auskünfte aus der Behandlungsakte an eine private Versicherung gegeben hatte. Hierin lag eine doppelte Verletzung des Patientengeheimnisses. Zunächst erfolgte die Nutzung der Patientenakte durch den Praxisnachfolger, ohne dass sich der Vorgänger die Übergabe an den Nachfolger hatte genehmigen lassen. Des Weiteren war die Übermittlung der Daten an die Versicherung ohne eine Entbindung von der Schweigepflicht unzulässig. Die Staatsanwaltschaft und der Generalstaatsanwalt stellten das Verfahren trotzdem ein. Auf die Beschwerde des Betroffenen hin wurden diese Entscheidungen sogar vom Schleswig-Holsteinischen Oberlandesgericht bestätigt mit der lapidaren Feststellung, es fehle an den „objektiven Voraussetzungen einer Verletzung von Privatgeheimnissen“. Solche strafrechtlichen Entscheidungen haben hinsichtlich der datenschutzrechtlichen Bewertung durch die Aufsichtsbehörde keine Bindungswirkung. Sie stehen im krassen Gegensatz zu den Beanstandungen, die wir für notwendig halten.

In anderen Fällen war jedoch die Kooperation mit der Staatsanwaltschaft besser. Dies war z. B. der Fall bei der im letzten Tätigkeitsbericht dargestellten illegalen Aktenentsorgung (vgl. 25. TB, Tz. 4.8.8), die mit einer Einstellung des Verfahrens nach Zahlung eines **Bußgeldes** beendet wurde. In einem weiteren Fall des Bruchs des Patientengeheimnisses durch eine mangelhafte Entsorgung von Patientendaten gab die Staatsanwaltschaft das Verfahren an uns als zuständige Ordnungswidrigkeitenbehörde ab. Wir verhängten ein angemessenes Bußgeld.

Was ist zu tun?
Auch Staatsanwälte sollten im Rahmen ihrer Zuständigkeit den Schutz des Patientengeheimnisses unterstützen.

4.8 Kultur und Bildung

4.8.1 Wann dürfen Schulverwaltungsrechner online gehen?

Schulverwaltungen sollen nach den Vorstellungen des Bildungsministeriums zukünftig personenbezogene und statistische Daten untereinander und mit anderen öffentlichen Stellen des Landes über das Internet austauschen. Dies ist bisher aus Sicherheitsgründen im Schulrecht untersagt. Unsere Lösungsvorschläge für eine sichere elektronische Datenübermittlung liegen seit über einem Jahr vor.

Ein elektronischer Datenaustausch ist schneller und kostengünstiger als ein papiergebundener. Dies hat das Bildungsministerium auch hinsichtlich der Schul-

verwaltungen erkannt. Die Kommunikation der Schulen mit dem Ministerium und den Schulaufsichtsbehörden über E-Mail würde Einsparungen ermöglichen. Auch die Meldungen zur Schulstatistik und der Austausch im Zusammenhang mit der „Betreuten Grundschule“ könnte mittels elektronischer Kommunikation erfolgen. Bisher dürfen die **Schulverwaltungsrechner** nach einer Regelung der Datenschutzverordnung Schule jedoch **nicht** an das **Internet** angebunden werden. Hintergrund dieser Regelung ist, dass wegen der Vielfalt der eingesetzten Systeme und einer nicht gewährleisteten flächendeckenden professionellen Systemadministration ein solcher Anschluss als nicht hinreichend sicher angesehen wird. Davon unberührt wurde nunmehr die elektronische Datenübermittlung der Schülerstatistik auf den Weg gebracht. Um nicht gegen die Datenschutzverordnung Schule zu verstoßen, erfolgen die Datenübermittlungen an das Statistische Landesamt mittels Datenträgeraustausch, d. h. auf Disketten.

Der Druck auf die Schulverwaltungen, mit anderen öffentlichen und privaten Stellen **elektronisch** zu **kommunizieren**, wird jedoch täglich größer. Damit steigt die Gefahr, dass Schulverwaltungssysteme, in denen personenbezogene Daten gespeichert sind, unter Missachtung der Regelungen der Datenschutzverordnung Schule an das Internet angebunden werden und damit die Sicherheit für die Daten der Schülerinnen, Schüler, Eltern und Lehrkräfte nicht mehr gewährleistet ist.

Kurse
L, LT, L-INT

In Kenntnis dieser Situation haben wir dem Bildungsministerium bereits im Jahre 2001 den **Vorschlag** gemacht, die Schulverwaltungssysteme an das **Landesnetz** anzubinden. Dies halten wir für die beste Lösung, da die Schulen sich so auf gesichertem Weg mit den Schulaufsichtsbehörden, dem Bildungsministerium und dem Statistischen Landesamt austauschen könnten. Auch wäre so ein geschützter Zugang zum Internet möglich, der den E-Mail-Austausch mit anderen Stellen außerhalb des Landesnetzes zuließe. Trotz einiger Gespräche wurden bisher keine Fortschritte bei der Lösung dieser Fragestellungen erzielt.

Was ist zu tun?
Das Bildungsministerium sollte sich für eine einheitliche, datenschutzgerechte und sichere Lösung der Anbindung der Schulen ans Internet entscheiden. Am Datenschutz liegt es jedenfalls wieder einmal nicht.

4.8.2 Bilder auf der Schulhomepage

„Bildnisse“ von Personen dürfen nur mit deren Einverständnis verbreitet werden. Dies schreibt seit 1907 das Kunst- und Urheberrechtsgesetz vor. Leider scheint dies nicht allen Schulleitungen bekannt zu sein.

Eingaben von besorgten Eltern, aber auch Anfragen von Schulleiterinnen und Schulleitern machen uns immer wieder auf die Praxis aufmerksam, Bilder von Schülerinnen und Schülern auf schuleigenen Homepages ohne Einverständnis der Eltern bzw. der Betroffenen zu veröffentlichen. Die Präsentation solcher Bilder geht von Einzel- über Klassenfotos bis zu Bildern, die von Kindern in den Unterrichtsräumen gemacht wurden. Die Verbreitung im Internet führt dazu, dass diese Bilder **weltweit abrufbar**, kopierbar und veränderbar sind.

Dies gilt auch für Bilder. Wegen der damit verbundenen Gefahren für die Persönlichkeitsrechte der Betroffenen, den eindeutigen Rechtsgrundlagen für die Datenübermittlung an Private im Schulgesetz und dem Recht am eigenen Bild der Betroffenen ist es erforderlich, vor der Veröffentlichung von Bildern auf Schulhomepages zunächst die **Einwilligung** der Betroffenen oder der Eltern einzuholen. Dabei ist auf die genannten Gefahren in jedem Falle hinzuweisen. Wenn die Schulleitung Bilder von Schülerinnen und Schülern auf ihrer Homepage veröffentlichen will, sollte sie diese in jedem Falle nicht mit den Namen der Betroffenen versehen.

Was ist zu tun?
Veröffentlichungen von Bildern auf der Schulhomepage sind nur mit Einwilligung der Betroffenen bzw. deren Eltern zulässig. Es ist darauf zu achten, dass die Betroffenen vorher umfassend aufgeklärt werden. Namensnennungen sollten vermieden werden.

4.8.3 Videoüberwachung im Klassenraum

Videoüberwachung stellt einen starken Eingriff in die Persönlichkeitsrechte der Betroffenen dar. Deshalb stehen wir der Videoüberwachung – insbesondere in Schulen – sehr kritisch gegenüber (vgl. auch Tz. 5.10). Doch es gibt Situationen, in denen eine Videoüberwachung das Mittel der Wahl ist.

Durch eine Eingabe wurden wir darauf aufmerksam gemacht, dass eine Berufliche Schule einen Physikraum mittels Videokamera überwacht und die Überwachungsbilder speichert. Im Gespräch mit der Schulleitung und den zuständigen Lehrkräften wurde deutlich, dass diese Videoüberwachung tatsächlich notwendig ist. Der **Physikraum** ist mit hochwertigen Arbeitstischen ausgestattet, die von Schülerinnen und Schülern wiederholt beschädigt wurden. So wurden Einritzungen und unauslöschbare Kritzeleien auf den Tischen hinterlassen. Die Verantwortlichen konnten trotz anwesender Lehrkraft nicht in flagranti ertappt werden, sodass sie nicht zur Rechenschaft gezogen werden konnten. Die Schulleitung versuchte unter Einschaltung der Schüler- und Elternvertretung die Missstände zu unterbinden. Diese Bemühungen blieben jedoch erfolglos.

Aufgrund des vorliegenden Sachverhaltes und insbesondere im Hinblick auf die hohen Kosten für die Beseitigung der Beschädigungen war gegen die Videoüberwachung nichts einzuwenden. Allerdings haben wir darauf aufmerksam gemacht, dass seitens der Schule sichergestellt werden muss, dass die Videoaufzeichnungen **schnellstmöglichst gelöscht** werden, wenn keine strafbaren Handlungen dokumentiert sind. Ferner muss durch Hinweisschilder auf die Videoüberwachung hingewiesen werden. Die Schule muss eine schriftliche Regelung treffen, unter welchen Bedingungen welche Personen Zugang zu dem Videomaterial erhalten. Darüber hinaus wurde sichergestellt, dass die Videoaufzeichnungen nicht zur Feststellung von Täuschungsversuchen bei Klassenarbeiten herangezogen werden, die in diesem Raum ebenfalls gefertigt werden.

Was ist zu tun?
Videoüberwachung kann nur das letzte Mittel darstellen, um strafbare Handlungen zu verhindern bzw. nachzuweisen. Beim Betrieb sind die gesetzlichen Vorgaben zu beachten.

4.8.4 Wann eine Blankoentschuldigung nicht reicht

Schulen dürfen von Eltern eine Begründung für Unterrichtsversäumnisse verlangen. Dies kann dann erforderlich sein, wenn immer wieder pauschale Entschuldigungen für Versäumnisse bestimmter Fächer vorgelegt werden.

Eine Schule wandte sich mit der Frage an uns, ob es angehe, dass sich der Vater eines schulpflichtigen Kindes aus „datenschutzrechtlichen Gründen“ weigert, der Schule Auskunft darüber zu geben, warum sein Kind regelmäßig nicht am **Sportunterricht** teilnimmt. Der Vater hatte für die Entschuldigung ein Formular entwickelt, welches er jeweils lediglich mit dem aktuellen Datum versah.

Wir sind zu dem Ergebnis gekommen, dass bei Unterrichtsversäumnissen zwar grundsätzlich eine Entschuldigung der Eltern bzw. der volljährigen Schülerinnen und Schüler ohne eingehende Begründung ausreichend ist. Erfolgen jedoch solche Entschuldigungen für regelmäßig wiederkehrende Unterrichtsversäumnisse in einem speziellen Fach, so hat die Schule nach dem Schulgesetz sogar die Pflicht zu prüfen, aus welchem Grunde das Kind immer wieder fehlt. Insbesondere beim Sportunterricht muss die Schule prüfen, ob die Schülerin oder der Schüler aus gesundheitlichen Gründen keinen oder nur eingeschränkten Sport während des Unterrichts ausüben kann. Hierüber müssen zunächst die Eltern Auskunft geben. Die **Auskunftsverpflichtung** ergibt sich aus dem Schulgesetz. Erst bei Vorliegen einer Begründung für die Fehlzeiten kann die Schule entscheiden, ob ergänzend eine schulärztliche Untersuchung erfolgen muss. Weigern sich die Eltern weiterhin, die Unterrichtsversäumnisse zu begründen, kann die Schule sogar ohne Einverständnis der Eltern eine schulärztliche Untersuchung verlangen und durchführen lassen.

Was ist zu tun?
Unter bestimmten Voraussetzungen müssen Eltern Auskunft über Schulversäumnisse geben.

4.9 Steuerverwaltung

4.9.1 Wuchernde Steuergesetzgebung

Die aktuelle Steuergesetzgebung ist so unübersichtlich geworden, dass es in der Öffentlichkeit gar nicht aufgefallen ist, dass demnächst alle in Deutschland gemeldeten Menschen von ihrer Geburt an bis über den Tod hinaus unter einem eindeutigen steuerlichen Personenkennzeichen beim Bundesamt für Finanzen registriert werden.

In kaum einem anderen Rechtsgebiet sind die „**Innovationszyklen**“ so kurz wie im Steuerrecht. Es gibt nur wenige Spezialisten, die alle im letzten Jahr realisierten, derzeit in den parlamentarischen Beratungen befindlichen und für das nächste Jahr geplanten Gesetzesänderungen in ihren Konsequenzen überblicken. Aus unserer Sicht sind drei Komplexe zu unterscheiden:

- Änderungen an den Steuertarifen und Abbau von Steuervergünstigungen,
- Anpassung des steuerlichen Verfahrensrechts an die EU-Datenschutzrichtlinie und an E-Government-Angebote,
- Ausbau der Kontrollsysteme zur Vermeidung von Steuerhinterziehungen und zur Erfassung aller Steuerfälle.

Die Vereinfachung des Steuerrechts durch Änderungen der Tarifstruktur und durch Abbau von Steuervergünstigungen ist aus Datenschutzsicht zu unterstützen, wenn sie dazu führt, dass den Finanzämtern gegenüber weniger Angaben als bisher gemacht werden müssen. Hier liegt zweifellos ein großes Potenzial zur **Datenvermeidung** und **Datensparsamkeit**.

Bei der Anpassung der Abgabenordnung (AO) an die Standards, die durch die **EU-Datenschutzrichtlinie** und die Datenschutzgesetze des Bundes und der Länder vorgegeben sind, handelt es sich um einen seit Jahren – in auffälligem Gegensatz zu den eingangs beschriebenen sonstigen hektischen Aktivitäten – verschleppten „Dauerbrenner“ (vgl. 25. TB, Tz. 4.6). Dies würde die Datenschutzbeauftragten nicht so sehr stören, wenn es nicht fortwährend strittige Diskussionen gäbe, in denen die Steuerverwaltung den Standpunkt vertritt, die aus ihrer Sicht zu strengen Datenschutzgesetze seien auf das Besteuerungsverfahren nicht anwendbar, weil die nicht der EU-Richtlinie entsprechende AO bereits abschließende und ausreichende Datenschutzregelungen enthalte. Auch mit der elektronischen Unterschrift im Besteuerungsverfahren ist man bisher nicht sehr erfolgreich, da sich eine signaturgesetzkonforme Lösung noch nicht abzeichnet (vgl. 25. TB, Tz. 4.10.2).

Einen Paukenschlag gab es Ende 2003 mit den gesetzlichen Regelungen zur **Identifikationsnummer** und zur **Wirtschaftsidentifikationsnummer**. Bereits in den letzten Jahren hat es immer wieder gesetzgeberische Initiativen gegeben, Betrügereien beim Vorsteuerabzug im Rahmen der Umsatzsteuerfestsetzung durch zentrale Erfassungssysteme (Stichwort „ZAUBER“) zu begegnen und die papierenen Lohnsteuerkarten durch einen elektronischen Meldedienst an eine Zentralstelle zu ersetzen (Stichwort „ELSTER-Lohn“). Die Verwendung der Steuernummer als

Identifikationsmerkmal (vgl. 25. TB, Tz. 4.10.4) bzw. die Bildung einer Arbeitnehmerkennung aus dem Namen und den Geburtsdaten haben sich jedoch offenbar nicht als praktikabel erwiesen. Deshalb hat man jetzt zum großen Wurf ausgeholt.

Das „2. Gesetz zur Änderung steuerlicher Vorschriften – Steueränderungsgesetz 2003“ enthält die **Generalvollmacht** für die Schaffung eines steuerlichen **Personenkennzeichens** für alle natürlichen Personen sowie alle juristischen Personen und Personenvereinigungen, sofern sie „wirtschaftlich tätig“ sind.

Das Verfahren ist **lückenlos**. Alle 5500 Meldebehörden in Deutschland übermitteln die entsprechenden Datensätze (zunächst also ca. 80 Millionen) an das Bundesamt für Finanzen. Dieses ermittelt die Identifikationsnummer und schickt sie an die betreffende Meldebehörde zurück, die sie zu speichern hat, damit Änderungsmeldungen (z. B. Umzüge) unter dieser Nummer übermittelt werden können (vgl. Tz. 4.1.8). Jedes neugeborene Kind erhält also unmittelbar nach seiner Registrierung im Melderegister seine Identifikationsnummer, die es über sein Lebensende hinaus behält.

Alle Personen und **Stellen**, die mit den Finanzämtern bezogen auf konkrete Steuerfälle kommunizieren (Banken, Sparkassen, Arbeitgeber, Sozialbehörden usw.), müssen künftig entweder ausschließlich oder ergänzend zum Namen bzw. zur Steuernummer diese Identifikationsnummer verwenden. Sie sind also verpflichtet, sie zu speichern.

Eine Verwendung der Identifikationsnummer für **andere** als für steuerliche **Zwecke** ist zwar untersagt, aber wohl kaum zu verhindern. Deshalb ist die Behauptung in der Gesetzesbegründung und in amtlichen Verlautbarungen, dass es sich nicht um das bereits vor Jahren vom Bundesverfassungsgericht als verfassungswidrig bezeichnete allgemeine Personenkennzeichen handelt, nur formal, nicht aber faktisch richtig.

Im Wortlaut:
§ 139 Abs. 1 Abgabenordnung

Das Bundesamt für Finanzen teilt jedem Steuerpflichtigen zum Zwecke der eindeutigen Identifizierung im Besteuerungsverfahren ein einheitliches und dauerhaftes Merkmal (Identifizierungsmerkmal) zu, das bei Anträgen, Erklärungen oder Mitteilungen gegenüber Finanzbehörden anzugeben ist ...

§ 139 b Abs. 2 Abgabenordnung

Die Finanzbehörden dürfen die Identifikationsnummer nur erheben und verwenden, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist oder eine Rechtsvorschrift die Erhebung oder Verwendung der Identifikationsnummer ausdrücklich erlaubt oder anordnet. Andere öffentliche oder nichtöffentliche Stellen dürfen die Identifikationsnummer nur erheben oder verwenden, soweit dies für Datenübermittlungen zwischen ihnen und den Finanzbehörden erforderlich ist oder eine Rechtsvorschrift die Erhebung oder Verwendung der Identifikationsnummer ausdrücklich erlaubt oder anordnet.

§ 139 b Abs. 3 Abgabenordnung

Das Bundesamt für Finanzen speichert zu natürlichen Personen folgende Daten: Identifikationsnummer, Wirtschafts-Identifikationsnummer, Familienname, frühere Namen, Vornamen, Doktorgrad, Ordens-/Künstlernamen, Tag und Ort der Geburt, Geschlecht, gegenwärtige oder letzte Anschrift, zuständige Finanzämter, Sterbetag.

Trotz erheblicher Vorbehalte der Datenschutzbeauftragten ist das Gesetz Ende 2003 von der Öffentlichkeit kaum bemerkt verabschiedet worden. Nur eine einzige private Datenschutzorganisation (vgl. www.datenschutzverein.de) und wenige Informationsdienste und Zeitungen haben den Sinn und Zweck dieser gravierenden Maßnahme hinterfragt. Eine für jedermann verständliche Beschreibung der neuen Verfahrensweise der Finanzämter und eine Erläuterung, wie auf der Grundlage der Identifikationsnummer mehr Steuergerechtigkeit herbeigeführt werden kann, sucht man in den **Gesetzesmaterialien** und auf der Homepage des Bundesministeriums für Finanzen vergebens. Die Tatsache, dass sich nicht – wie beim Versuch, eine allgemeine Personenkennziffer einzuführen, oder im Zusammenhang mit der Volkszählung – in der Öffentlichkeit ein Proteststurm erhoben hat, kann man als einen Indikator dafür ansehen, wie „belastbar" die Bevölkerung inzwischen im Hinblick auf Einschränkungen ihrer Rechte geworden ist.

Dies mag damit zusammenhängen, dass das Verfahren bisher noch nicht gestartet wurde, weil im Bundesamt für Finanzen zunächst die **technischen Voraussetzungen** geschaffen werden müssen. Im Übrigen sind auch bei 5500 Meldebehörden, bei allen Banken, Sparkassen usw. die Datenbanken und die Programme zu erweitern. Der Startschuss wird erst durch eine Rechtsverordnung gegeben, in der auch

- die organisatorischen und technischen Maßnahmen zur Wahrung des Steuergeheimnisses,
- die Richtlinien zur Vergabe,
- die Löschfristen und
- die Form und das Verfahren der Datenübermittlungen

festzulegen sind. Kritiker hoffen, dass dieser Startschuss nie gegeben wird, ihre Gründe sind nachvollziehbar.

Was ist zu tun?
Bevor die Steuerpersonenkennziffer tatsächlich eingeführt wird, sollte überzeugend dargelegt werden, dass ihr Nutzen im Hinblick auf die Steuergerechtigkeit die mit ihr verbundenen Risiken erheblich überwiegt. Die Finanzverwaltung sollte das Informationsdefizit zügig beheben und den Startschuss erst geben, wenn auch ein gesellschaftspolitischer Konsens hergestellt ist.

4.9.2 Steuergeheimnis bei Privatinsolvenzen

Werden Eheleute zusammen veranlagt, muss der eine Partner es dulden, dass seine steuerlichen Verhältnisse in einem Insolvenzverfahren des anderen Partners bekannt werden.

Bis vor wenigen Jahren hatte das **Steuergeheimnis** bei den Steuerpflichtigen und in der breiten Öffentlichkeit durchaus den Ruf der Unantastbarkeit. Man ging ganz selbstverständlich davon aus, dass die Finanzämter sich zwar nicht scheuten, Gewinne aus betrügerischen oder gar sittenwidrigen Geschäften zu besteuern,

andererseits aber über die bei der Besteuerung gewonnenen Erkenntnisse über private und geschäftliche Vorgänge ein striktes Stillschweigen bewahrten. Das Steuer- und das Patientengeheimnis waren die traditionellen Trutzburgen des praktizierten Datenschutzes. Beide Festungen, insbesondere das Steuergeheimnis, haben in jüngster Zeit erhebliche Risse bekommen.

Die Ursache liegt darin, dass immer mehr gesetzliche Regelungen die Nutzung von Daten aus dem Besteuerungsverfahren für andere Zwecke (z. B. Verfolgung von Schwarzarbeit, Sozialversicherungsbetrug, Geldwäsche usw.) zulassen. Obwohl die meisten Bürgerinnen und Bürger die Verfolgung derartiger Delikte gutheißen, verstärkt sich offenbar ihr Gefühl, dass das Steuergeheimnis auch nicht mehr das ist, was es einmal war. Hierauf deutet die **Zahl der Beschwerden** gegen die Verfahrensweisen der Finanzämter hin, die vermeintlich einen Bruch des Steuergeheimnisses zur Folge haben (vgl. z. B. die Angst vor dem Missbrauch der Steuernummern, vgl. Tz. 14.1). Die Sensibilität in diesem Bereich ist signifikant gestiegen. Deshalb sind viele Steuerpflichtige enttäuscht, wenn auch in solchen Fällen, in denen ihnen ihr „gesunder Menschenverstand" sagt, dass das Verhalten des betreffenden Finanzamtes nicht korrekt sein kann, dargelegt werden muss, dass letztlich alles nach Recht und Gesetz abgewickelt worden ist. Exemplarisch hierfür ist folgender Sachverhalt:

Ein Ehepaar hatte in seiner Einkommenssteuererklärung die Zusammenveranlagung gewählt. Lange vor der Eheschließung war der eine Ehepartner mit einem Unternehmen in Konkurs geraten und wollte nunmehr die Angelegenheit im Wege der **Verbraucherinsolvenz** bereinigen. Da in dem so genannten vereinfachten Insolvenzverfahren die Aufgaben des Insolvenzverwalters von einem Betreuer (in der Regel einem Rechtsanwalt) wahrgenommen werden, tritt dieser im Besteuerungsverfahren als gesetzlicher Vertreter bzw. Vermögensverwalter auf.

> **?** ***Verbraucherinsolvenz***
>
> *Es handelt sich um ein 1999 eingeführtes mehrstufiges Verfahren. Entscheidend ist, dass nach dem gescheiterten Versuch, zu einer Einigung zwischen Gläubigern und Schuldner zu kommen, der Schuldner für die Dauer von sieben Jahren den pfändbaren Teil seines Einkommens an einen Treuhänder abtreten muss. Dieser verteilt die Beträge an die Gläubiger. Nach Ablauf dieser Zeit kann das Gericht die Restschulden erlassen.*

Dies hat zur Folge, dass Steuerbescheide ihm und nicht dem tatsächlichen Steuerpflichtigen zugestellt werden.

Als die **Ehefrau** hiervon erfuhr, war sie über die Tatsache, dass ihre gesamten steuerlichen Verhältnisse in dem Insolvenzverfahren transparent wurden, gar nicht erfreut. Als das Finanzamt dann auch noch nur kurz und bündig mitteilte, dieses entspräche den gesetzlichen Regelungen, bat sie uns um Beratung. Wir haben ihr erläutert, dass hinter dieser Regelung die Überlegung steht, dass die Ansprüche des Schuldners gegenüber Dritten (in diesem Fall ein Finanzamt) nicht mehr vom Schuldner selbst, sondern von seinem gesetzlichen Vertreter geltend gemacht werden sollen. Dieser musste also auch die gemeinsamen Steuerbescheide sehen, um gegebenenfalls durch Einsprüche höhere Erstattungsbeträge zu erreichen und die korrekte Aufteilung der erstatteten Beträge zu überprüfen. Wenn das Finanz-

amt diese Erläuterungen von vornherein gegeben hätte, wäre der Eindruck des Bruches des Steuergeheimnisses wahrscheinlich gar nicht erst entstanden.

Was ist zu tun?
Die Finanzämter sollten die Steuerpflichtigen rechtzeitig über die Rechtslage aufklären, wenn sie Daten aus dem Besteuerungsverfahren weitergeben (müssen).

4.9.3 Steuergeheimnis versus besondere Berufsgeheimnisse

Betriebsprüfungen bei Steuerpflichtigen, die gegenüber den Finanzämtern ein Auskunfts- und Urkundenvorlageverweigerungsrecht besitzen, werfen die Frage auf, wie die zu zahlenden Steuern richtig ermittelt werden können, wenn die Finanzbeamten nicht alle Belege einsehen dürfen.

Ärzte, Rechtsanwälte, Notare und andere Steuerbürger, die einem besonderen Berufsgeheimnis unterliegen, stecken ebenso in einem Dilemma wie die Betriebsprüfer, die die korrekte Besteuerung aller Einnahmen und die Berücksichtigung aller abzugsfähigen Ausgaben dieser Berufsgruppen zu überwachen haben. Der Grund hierfür liegt in den Regelungen der Abgabenordnung, nach denen ihnen ein **Auskunfts-** und **Urkundenvorlageverweigerungsrecht** zusteht.

Im Wortlaut:
§ 102 Abs. 1 Abgabenordnung

Auskünfte können [ferner] verweigern ...

3a. Verteidiger
3b. Rechtsanwälte, Patentanwälte, Notar, Steuerberater ...
3c. Ärzte, Zahnärzte

§ 104 Abs. 1 Abgabenordnung

Soweit die Auskunft verweigert werden darf, kann auch die Erstattung eines Gutachtens und die Vorlage von Urkunden oder Wertsachen verweigert werden.

Wie aber soll ein Finanzbeamter die **Vollständigkeit der Buchhaltung** überprüfen, wenn nicht durch einen Vergleich mit den Durchschriften der Honorarrechnungen? Wie kann z. B. ein Rechtsanwalt begründen, dass Reisekosten im Zusammenhang mit einem Mandantenbesuch stehen, wenn nicht durch Vorlage des entsprechenden Schriftwechsels? Diese Problematik ist bereits im Zusammenhang mit der Führung von Fahrtenbüchern diskutiert worden (vgl. 19. TB, Tz. 4.10.3). Auch in diesen Fällen fordern nämlich die Berufsordnungen, das Patienten- bzw. Mandantengeheimnis zu wahren. Im Extremfall könnte die Verschwiegenheitspflicht dazu führen, dass das Finanzamt die Einnahmen und Ausgaben schätzt, was sich in der Regel negativ für den Steuerpflichtigen auswirkt.

Das Problem ist vor dem Hintergrund zu sehen, dass es bisher weder in der Rechtsprechung noch in der datenschutzrechtlichen Literatur als Verstoß gegen die Geheimhaltungsvorschriften angesehen wird,

- wenn Ärzte, Rechtsanwälte, Steuerberater usw. Honorarforderungen einklagen und durch Dritte (Gerichtsvollzieher, Inkassobüros) beitreiben lassen,

- wenn sie ihre Buchhaltung und steuerliche Betreuung durch Steuerberater erstellen bzw. abwickeln lassen,
- wenn Wirtschaftsprüfer die Buchführung (einschließlich des gesamten Kontokorrents) von Krankenhäusern in der Rechtsform juristischer Personen privaten Rechts (GmbH, KG) prüfen und testieren,
- wenn Rechnungshöfe und Rechnungsprüfungsämter das Abrechnungsgebahren öffentlicher Krankenhäuser überprüfen und
- wenn schließlich auch Datenschutzbeauftragte und Datenschutzaufsichtsbehörden im Rahmen ihrer Prüfungen und Beratungen solche Daten zur Kenntnis nehmen.

Wegen dieser unterschiedlichen Verfahrensweise ist es dringend geboten, die Grundfrage zu klären, in welchem Umfang und unter welchen Voraussetzungen Berufsgeheimnisträger berechtigt sind, aus dem originären geheimgeschützten Datenbestand personenbezogene Daten zu selektieren, um die Vertragsabwicklung zu ermöglichen bzw. **eigene berechtigte Interessen** zu wahren. Anders formuliert: Ergeben sich aus dem Vertragsverhältnis zwischen dem Betroffenen und dem „Geheimnisträger“ für Letzteren Rechte, bestimmte personenbezogene Daten zu bestimmten Zwecken zu offenbaren?

Kein Zweifel besteht, dass dies – wenn überhaupt – nur im erforderlichen Umfang geschehen darf. Außerdem ist zu beachten, dass die Geheimhaltungspflichten und die damit korrespondierenden Auskunfts- und Herausgabeverweigerungsrechte primär zum **Schutz der Betroffenen** und nicht der Daten verarbeitenden Stellen geschaffen worden sind.

Da es sich nicht nur um ein steuerrechtliches Problem handelt, haben wir angeregt, dass sich mit diesem Thema nicht nur der Arbeitskreis „Steuer“, sondern auch die Arbeitskreise „Soziales“ und „Justiz“ der Konferenz der Datenschutzbeauftragten sowie gegebenenfalls der „Düsseldorfer Kreis“ als zuständiges Gremium der Aufsichtsbehörden befassen. Dies wird in den nächsten Monaten geschehen. Ziel der Beratungen wird es sein, in allen Fällen eine **vergleichbare Verfahrensweise** zu erreichen, die die Rechte der Betroffenen nicht unzumutbar beeinträchtigt und mit dem geltenden Recht vereinbar ist.

Was ist zu tun?
Die Gremien der datenschutzrechtlichen Kontrollinstanzen und der bereichsspezifischen Aufsichtsbehörden (berufsständische Kammern) sollten sich darüber verständigen, ob und wenn ja welche Teile der Datenbestände, die einer besonderen beruflichen Schweigepflicht unterliegen, Dritten zugänglich gemacht werden dürfen.

4.10 Personalverwaltung

4.10.1 Führung von Personalteilakten für Reisekostenunterlagen

Reisekostenunterlagen sind als materielle Bestandteile der Personalakte vor unbefugter Einsicht zu schützen. Eine Aufbewahrung der Vorgänge in der Kasse entspricht nicht den Verfahrensregelungen des Personalaktenrechts. Sie unterliegen gleichwohl dem Personalakteneinsichtsrecht der Betroffenen.

Im Rahmen einer Revision hatte ein Rechnungsprüfungsamt von der geprüften Personalverwaltung verlangt, Reisekostenunterlagen künftig den Kassenanweisungen beizufügen. Die Personalverwaltung bat uns um Beratung, da man die Behandlung der Unterlagen als Personalteilakte für geboten hielt.

Nach dem **Landesbeamtengesetz** (LBG), das insoweit auch für Angestellte und Arbeiter gilt, gehören zur Personalakte alle Unterlagen (einschließlich der in Dateien gespeicherten), die die Mitarbeiterin oder den Mitarbeiter betreffen und die mit ihrem oder seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten). Nach § 106 h Abs. 2 LBG wird für Unterlagen über Reisekosten eine besondere Aufbewahrungsfrist von fünf Jahren festgelegt.

Im Wortlaut:
§ 106 h Abs. 2 S. 1 LBG

Unterlagen über Beihilfen, Heilfürsorge, Heilverfahren, Unterstützungen, Erholungsurlaub, Erkrankungen, Umzugs- und Reisekosten sind fünf Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorganges abgeschlossen wurde, aufzubewahren.

Über alle Mitarbeiterinnen und Mitarbeiter im öffentlichen Dienst sind daher **Personalakten** zu führen; sie sind **vertraulich zu behandeln** und vor unbefugter Einsicht zu schützen. **Zugang zu Personalakten** dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und zwar nur, soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist; dies gilt auch für den Zugang im automatisierten Abrufverfahren. Würde man Reisekostenunterlagen den Kassenanweisungen beifügen, hätte dies zur Folge, dass die Unterlagen in der Kasse nicht personenbezogen, sondern chronologisch sortiert bei der jeweiligen Haushaltsstelle abgelegt würden. Zudem hätten Beschäftigte der Kasse **unbefugt Zugang** zu Personalakten, da sie organisatorisch nicht Teil der Personalverwaltung sind. Daneben würden erhebliche Probleme auftreten, falls ein Mitarbeiter von seinem Recht auf vollständige Einsicht in seine Personalakte, die auch die Reisekostenunterlagen einschließt, Gebrauch machen wollte.

Wir haben deshalb empfohlen, Reisekostenunterlagen auch künftig im Bereich der Personalverwaltung als **Personalteilakte** aufzubewahren. In diesem Fall bestehen keine Bedenken dagegen, wenn im Rahmen der Rechnungsprüfung die kassenmäßigen Buchungen unter Einbeziehung der Personalakten kontrolliert werden, weil die Verarbeitung personenbezogener Daten zur Ausübung von Aufsichts- und Kontrollbefugnissen sowie zur Rechnungsprüfung nicht als Verarbeitung für andere Zwecke gilt. Das betreffende Rechnungsprüfungsamt hat sich der von uns vertretenen Auffassung zwischenzeitlich angeschlossen.

Schleswig-Holstein DATENSCHUTZAKADEMIE
Kurse P, PA

Was ist zu tun?
Personalverwaltungen sollten sich vergewissern, ob ihre Aufbewahrung von Reisekostenunterlagen nach Abschluss der Bearbeitung den Maßgaben des Personalaktenrechts entspricht.

4.10.2 Diagnose auf Rezepten naher Angehöriger

Die Verordnung von Arzneimitteln durch nahe Angehörige unterliegt einer besonderen Nachprüfung durch die Beihilfestellen. Die Begründung und damit die Notwendigkeit für die verfahrensmäßige Abweichung gegenüber einem Normalfall halten wir für zweifelhaft.

Ein Beihilfeberechtigter, dessen Sohn als Arzt tätig ist, hatte uns einen **Beihilfebescheid** vorgelegt, in dem von ihm gefordert wurde, bei der Verordnung von Arzneimitteln durch nahe Angehörige auf jedem Rezept die Diagnose anzugeben. Wir konnten weder den Beihilfevorschriften selbst noch den dazu vom Bundesinnenministerium ergangenen Hinweisen eine entsprechende Regelung entnehmen. Es war nicht erkennbar, zu welchem Zweck die Diagnose angegeben werden sollte. Unseres Erachtens ist jedenfalls die Beihilfefähigkeit der Aufwendungen nicht von der Diagnose abhängig, sondern allenfalls von der Art der verordneten Medikamente. Ein Nachweis, dass die Aufwendungen tatsächlich entstanden sind, wird durch die Abrechnungsbescheinigung der Apotheke erbracht.

Auf unsere Anregung hin wurde die Angelegenheit vom Finanzministerium in die **Bund-Länder-Kommission** für das Beihilferecht eingebracht. Dort hielt man allerdings an der Auffassung fest, dass die Beihilfestelle auch die Notwendigkeit der Aufwendungen für verordnete Arzneimittel prüfen müsse. Besonders gelte dies für Rezeptierungen in Fällen, in denen z. B. Arztleistungen aus sittlichen und moralischen Gründen nicht in Rechnung gestellt werden und deswegen auch von der Beihilfefähigkeit ausgeschlossen sind. Hierunter fallen insbesondere die Behandlung naher Angehöriger, deren Aufwendungen beihilferechtlich nicht anerkannt werden können. Insofern sei gerade auch in diesen Fällen – wie auch in den Fällen der Selbstbehandlung – der Diagnosenachweis auf den Rezepten erforderlich.

Uns kann diese Argumentationslinie nicht überzeugen. Gleichwohl sehen wir im Hinblick auf die Entscheidung der Bund-Länder-Kommission derzeit keine Möglichkeit, eine Änderung der Verwaltungspraxis herbeizuführen. Als **Teillösung** des Problems konnten wir dem Petenten nur empfehlen, die Eintragung der Diagnose auf dem Rezept erst nach dessen Einlösung bei der Apotheke durch den Sohn vornehmen zu lassen. So kann vermieden werden, dass Angaben über die Art der Erkrankung gegenüber der Apotheke offenbart werden.

5 Datenschutz in der Wirtschaft

5.1 Zielvereinbarungen führen zu besserem Datenschutz

Macht Datenschutz Spaß? Nicht jeder wird diese Frage mit einem Ja beantworten. Und doch begreifen fortschrittliche Unternehmen den Datenschutz zunehmend als ein Instrument, mit dem man das Vertrauen des Kunden gewinnen kann. Selbst Firmen, die typischerweise keine Privatkunden haben, integrieren effektive Datenschutzmanagementsysteme in eine „Total-Quality-Philosophie". Bis der Bundesgesetzgeber endlich Audits regelt, können Zielvereinbarungen nützlich sein.

Ein aktuelles Beispiel hierfür stellen die **Sauer-Danfoss GmbH & Co. oHG** und **Sauer-Danfoss-Informatic GmbH** in Neumünster dar. Die beiden Unternehmen wandten sich an uns und baten um eine Überprüfung ihrer Datenschutzorganisation, weil sie sich hiervon eine weitere Verbesserung des Datenschutzes und der betrieblichen Zusammenarbeit innerhalb der Belegschaft erhofften. In der Folge unterzogen wir die betrieblichen Abläufe einer Prüfung auf „Herz und Nieren" und nahmen eine **Stärken-Schwächen-Analyse** vor. Für die Beseitigung der festgestellten Schwächen erarbeiteten wir zusammen mit der Geschäftsführung, den Datenschutzbeauftragten und dem Betriebsrat Lösungswege, die die Unternehmen nun schrittweise umsetzen.

Insbesondere in Bezug auf die **Datenschutzorganisation** haben die Unternehmen die gesetzlichen Vorgaben des BDSG in moderner Form umgesetzt.

- Nach dem Bundesdatenschutzgesetz ist grundsätzlich für jede verantwortliche Stelle ein **betrieblicher Datenschutzbeauftragter** zu bestellen, der auf die Einhaltung der Datenschutzbestimmungen hinzuwirken hat. Unternehmen haben die Verpflichtung, den Datenschutzbeauftragten in dieser Aufgabe zu unterstützen. Häufig geschieht dies allerdings nicht oder nur unzureichend. Um solche Defizite zu vermeiden, wurde von den Firmen ein gemeinsamer „**Betriebsausschuss Datenschutz**" ins Leben gerufen. Er setzt sich aus Vertretern der Geschäftsführung, des Betriebsrates und den beiden Datenschutzbeauftragten zusammen und hat die Funktion, die Datenschutzbeauftragten in ihren Aufgaben zu unterstützen und datenschutzrechtlich relevante Entscheidungen der Unternehmen vorzubereiten und umzusetzen.
- Für **jedes neu einzuführende Verfahren** sehen die Unternehmen eine spezielle **Vorabkontrolle** vor. Will ein Verantwortlicher ein neues Verfahren oder eine neue Anwendung einsetzen, schaltet er den Datenschutzbeauftragten ein und beschreibt das Verfahren bzw. die Anwendung nach einem vorgegebenen Fragenkatalog. Der Datenschutzbeauftragte prüft anhand dieser Angaben, ob und in welchem Umfang personenbezogene Daten verarbeitet werden und gibt dazu eine datenschutzrechtliche Beurteilung ab. Anschließend geht die Sache zum Betriebsausschuss Datenschutz und zum Betriebsrat. Bei Bedarf wird eine Betriebsvereinbarung abgeschlossen. Auf diese Weise werden alle relevanten Stellen zügig in einem standardisierten Verfahren eingebunden und ihr Sachverstand genutzt.

Die ersten Erfahrungen mit dieser Vorgehensweise sind ausgesprochen positiv. Der Schwerpunkt wird auf einen **präventiven Datenschutz** gelegt, der Verstöße bereits im Ansatz vermeidet. Die generelle Vorabkontrolle führt dabei zu einer **Sensibilisierung** der für die Datenverarbeitung verantwortlichen Funktionsträger, da sie geplante Verfahren und Anwendungen von vornherein auf ihre datenschutzrechtliche Zulässigkeit und Zweckmäßigkeit überprüfen. Durch die frühzeitige Einbindung aller Betriebspartner wird zudem die **Akzeptanz** der Verfahren im Unternehmen nachhaltig erhöht. Mittlerweile wenden sich Verantwortliche teilweise sogar an den Betriebsausschuss mit der Bitte, auch Altverfahren zu überprüfen.

Ins Auge gefasst werden Formen eines hausinternen **Audits**, um die gewonnenen datenschutzrechtlichen Fortschritte nicht durch Zeitablauf verloren gehen zu lassen. Auch wenn die Beratungsprüfung durch uns aufgrund der fehlenden Bundesgesetzgebung nicht zu einem Datenschutzzertifikat führen konnte, dokumentiert das Beispiel, dass fortschrittliche Unternehmen Datenschutz-Audits auf freiwilliger Basis befürworten würden.

Was ist zu tun?
Datenschutz kann als Instrument dienen, unternehmensinterne Abläufe so zu gestalten, dass dies zur Verbesserung des Betriebsklimas im Unternehmen beiträgt. Zielvereinbarungen zum Datenschutz der Mitarbeiter, betriebsinterne Audits und Produktgütesiegel fördern solche Prozesse, weil sie den Unternehmen Unterstützung und zusätzliches Know-how bieten.

5.2 Was Detektive nicht dürfen

Detekteien und Sicherheitsunternehmen greifen in erheblichem Umfang in die Privatsphäre ihrer „Zielpersonen" ein. Die Überprüfung eines Unternehmens ergab, dass es in der Branche offenbar erhebliche Wissensmängel bezüglich des Datenschutzes gibt.

Wer kennt nicht die zahllosen Detektivfilme im Fernsehen? Detektive und Sicherheitsunternehmen leben davon, fremde Menschen im Auftrag anderer zu beobachten. Die damit verbundenen erheblichen **Gefährdungen für die Persönlichkeitsrechte** der Betroffenen waren für uns der Anlass, eines dieser Unternehmen zu überprüfen. Dabei zeigte es sich, dass wesentliche Bestimmungen des Datenschutzrechts schlichtweg nicht bekannt waren:

- Nach dem Bundesdatenschutzgesetz sind Unternehmen ab einer gewissen Größe grundsätzlich verpflichtet, einen **Datenschutzbeauftragten** zu bestellen, der auf die Einhaltung datenschutzrechtlicher Bestimmungen hinwirkt. Das Unternehmen wusste davon nichts.
- Es fehlte das gesetzlich vorgeschriebene **Verfahrensregister**. Diese Verfahrensübersicht dient der Bestandsaufnahme automatisierter Datenverarbeitungsverfahren und damit als Grundlage für ein Datenschutzcontrolling.
- Zum Zeitpunkt der Prüfung übernahm das Unternehmen in erheblichem Umfang Aufträge zur **Observation**. Meist verdächtigten die Auftraggeber ihre

Mitarbeiter „krank zu feiern“. Eine solche Vermutung kann es vielleicht rechtfertigen, dass Arbeitnehmer daraufhin kontrolliert werden, ob sie wirklich krank sind. In keinem Fall ist es jedoch zulässig, sie in ihrer gesamten Privatsphäre auszuspionieren und darüber den Auftraggeber zu informieren.

- Die **Videoüberwachung** im Rahmen des **Objektschutzes** wurde nicht transparent gemacht.

Wir wiesen das Unternehmen auf diese und weitere Mängel hin. In einer ersten Reaktion hat sich das Sicherheitsunternehmen einsichtig gezeigt und die wichtigsten Mängel beseitigt. Den problematischen Observationsdienst stellte die Firma ganz ein.

Was ist zu tun?
Unternehmen der Sicherheitsbranche haben wie alle anderen Unternehmen die allgemeinen Datenschutzregeln zu beachten. Insbesondere bei Observationsaufträgen darf die Privatsphäre der Betroffenen nicht generell infrage gestellt werden.

5.3 Adresshandel und Direktmarketing

5.3.1 Der Preis der Rabattpunkte

Kundenbindungssysteme mit Karten zum Sammeln von Rabattpunkten finden bei Verbrauchern und Unternehmen zunehmend Anwendung. In einem Gutachten haben wir untersucht, welche Voraussetzungen für den datenschutzgerechten Betrieb solcher Systeme erfüllt sein müssen.

In jüngster Zeit sind eine Fülle von Rabattkarten auf den Markt geworfen worden (vgl. 24. TB, Tz. 6.4.1). Im Vordergrund stehen **unternehmens- und branchenübergreifende Rabattkarten** für mehrere Unternehmen. Der Kunde steht mittlerweile einem kaum überschaubaren Angebot gegenüber. Gegenüber den Verlockungen der Bonuspunkte und Sonderaktionen standen bisher die datenschutzrechtlichen Risiken für die Kunden im Hintergrund der Diskussion. Wenn überhaupt, dann erfährt der Kunde nämlich zumeist nur im **Kleingedruckten**, warum die Rabattkarten für die Unternehmen so lukrativ sind.

Über seine bis dahin anonymen Kunden erhält ein Unternehmen mittels Rabattkarte eine Menge personenbezogener und kommerziell nutzbarer Informationen. Dies beginnt bei der Beantragung, für die der Kunde seinen Namen, seine Anschrift und häufig auch sein Geburtsdatum offenbaren soll. Oftmals werden darüber hinaus Informationen zu Beruf, Einkommen oder Konsuminteressen der Kunden erhoben. Verknüpft mit den Umsatzdaten, die bei jedem Einsatz der Kundenkarte anfallen, lassen sich **Kundenkonsumprofile** erstellen, die Auskunft über viele Fragen geben können. So können etwa Vorlieben des Kunden abgeleitet und für eine optimierte Werbeansprache nutzbar gemacht werden. Mit einer Analyse des Kundenprofils können aber auch Aussagen zur Bonität des Kunden gewonnen werden, die eine wichtige Grundlage zur Beurteilung seiner Kreditwürdigkeit bilden.

Die zunehmende Verunsicherung über die datenschutzgerechte Gestaltung solcher Bonussysteme hat den **Verbraucherzentrale Bundesverband e.V. (vzbv)** veranlasst, sich eingehend mit dieser Thematik zu befassen. Er hat uns beauftragt, ein Gutachten über Kundenbindungssysteme und Datenschutz zu erstellen. Darin haben wir zunächst die **Anforderungen** aufgezeigt, die Kundenbindungssysteme im Hinblick auf den Datenschutz erfüllen müssen. Sollen neben Name und Anschrift weitere Kundendaten zum Zweck der Werbung und Marktforschung genutzt werden, ist dafür stets eine **Einwilligung** des Kunden erforderlich. Von einer wirksamen Einwilligung ist nur auszugehen, wenn der Kunde umfassend über die Datenverarbeitung im Rahmen des Kundenbindungsprogramms aufgeklärt wurde, insbesondere über die verantwortliche Stelle, die Art der zu verarbeitenden Daten sowie die Zwecke und die einzelnen Vorgänge der Datenverarbeitung. Sollen die Kundendaten genutzt werden, um daraus Kundenprofile zu erstellen und auszuwerten, muss der Kunde auch hierauf hingewiesen werden. Die Einwilligung muss ausdrücklich erfolgen, was eine aktive Handlung des Kunden (etwa durch gesonderte Unterschrift oder Ankreuzen einer Zustimmung) erfordert.

In der Praxis werden diese Anforderungen zumeist nicht erfüllt. Sämtliche Kundenbindungssysteme, die wir im Rahmen der Gutachtenerstellung unter die Lupe genommen haben, wiesen im Hinblick auf den Datenschutz Defizite auf. Weit verbreitet sind z. B. Einwilligungserklärungen, die den Kunden auffordern, den Text der Erklärung durchzustreichen, soweit er damit nicht einverstanden ist. Macht der Kunde davon keinen Gebrauch, dann erklärt er automatisch seine Einwilligung in die dort beschriebene, oft sehr weit gehende und komplexe Datenverarbeitung. Damit wird eine **Einwilligung** auch derjenigen Kunden **fingiert**, die die Aufforderung zur Streichung übersehen haben oder die sich nicht trauen, die vom Unternehmen vorgegebenen Bedingungen zurückzuweisen.

Unzureichend ist in den meisten Fällen auch die **Information des Kunden** über die Verarbeitung seiner Daten. Oft werden die Daten, die im Rahmen des Bonusprogramms verarbeitet werden, nicht präzise benannt. Unklar bleibt in der Regel auch, durch wen die Kundendaten verarbeitet werden. Dies gilt insbesondere für Kundenbindungssysteme, an denen mehrere Unternehmen beteiligt sind. Hier muss der Kunde genau erfahren, welche der Unternehmen welche Informationen über ihn nutzen.

Das für den vzbv erstellte Gutachten ist im Internet abrufbar unter

www.vzbv.de/mediapics/gutachten_kundenbindungssysteme_2003.pdf
www.datenschutzzentrum.de/wirtschaft/kundbisy.htm

Was ist zu tun?
Wollen Unternehmen durch Bonusprogramme Kunden langfristig binden, so sollten sie sich um deren Vertrauen bemühen. Datenschutzrechtlich einwandfreies Verhalten ist dabei hilfreich.

5.3.2 Schwarze Schafe im Adress- und Direkthandel

Bürgerinnen und Bürger fühlen sich von der ungefragten Zusendung von Werbezuschriften erheblich belästigt. Die beträchtliche Zahl der Beschwerden gegen die Verarbeitung und Nutzung von personenbezogenen Daten zu Werbezwecken im Jahr 2002 wurde 2003 nochmals deutlich übertroffen.

Die häufigsten Eingaben betrafen die **unverlangte Zusendung von Werbeanschreiben**. Die meisten Verbraucher verstehen nicht, warum Unternehmen ihre Daten ohne ihre Kenntnis verwenden dürfen. Wenn sie zu Werbezwecken angeschrieben werden, fragen sie sich, woher das Unternehmen Informationen über sie erhalten hat. Deshalb verpflichtet der Gesetzgeber die Werbewirtschaft dazu, die Betroffenen über ihr Recht zu informieren, der Nutzung ihrer Daten zu Zwecken der Werbung, der Markt- und Meinungsforschung zu widersprechen. Widerspricht ein angeschriebener Bürger der besagten Nutzung, so hat das Unternehmen seine Adressdaten zu sperren, weiter gehende Datennutzungen zu Werbezwecken sind verboten. Verlangt ein Betroffener Auskunft über die zu seiner Person gespeicherten Daten, hat das Unternehmen ihm diese erbetene Information unverzüglich zu erteilen.

Leider gibt es auch in Schleswig-Holstein **schwarze Schafe**, die diese Verbraucherrechte missachten. Die Unterrichtung über das Widerspruchsrecht fehlt ebenso häufig, wie manche Firmen **Auskunftsverlangen** von Bürgern schlichtweg ignorieren. In den meisten Fällen genügte es zwar, die Unternehmen darauf hinzuweisen, dass sie gegen gesetzliche Vorschriften verstoßen. Manche Unternehmen haben unsere Hinweise sogar dankbar aufgenommen, weil sie durch eine korrekte Verfahrensweise eine stärkere Akzeptanz ihrer Werbung erwarten. Manche Unternehmen missachten die Verbraucherrechte aber bewusst und wiederholt.

Deshalb haben wir gemeinsam mit der Verbraucherschutzzentrale des Landes und mit dem Verbraucherzentrale Bundesverband eine Broschüre mit dem Titel „99 + 1 Beispiele und viele Tipps zum BDSG“ herausgegeben, die Bürger über ihre Rechte informiert und ihnen Tipps gibt, sie auch durchzusetzen. Für Unternehmen enthält die Broschüre Hinweise, wie sich ein **verbraucherfreundlicher Datenschutz** mit relativ geringem Aufwand realisieren lässt. Sie ist im Internet abrufbar unter

www.datenschutzzentrum.de/download/BDSG_Handbuch.pdf

Was ist zu tun?
Unternehmen der Werbewirtschaft sind verpflichtet, die Rechte der Bürger auf Widerspruch und Auskunft zu beachten. Schwarze Schafe müssen künftig mit strengeren Sanktionen rechnen.

5.4 Auf Datenjagd bei Minderjährigen

Zahlreiche Webseiten locken Kinder und Jugendliche mit Spielen und besonderen Informationsangeboten. Doch Vorsicht ist angesagt, wenn solche Offerten an die Bedingung geknüpft werden, der betroffene Minderjährige müsse Daten über sich und seine Familie preisgeben.

Will ein Webdiensteanbieter von Minderjährigen personenbezogene Informationen erheben, muss er die **besondere Schutzwürdigkeit** seiner „Kunden" beachten. Unabdingbar sind dabei eine kind- bzw. jugendgerechte Information über die geplante Datenverarbeitung. Bei einwilligungspflichtigen Verarbeitungsprozessen muss darüber hinaus sichergestellt sein, dass sie nur mit Zustimmung der Erziehungsberechtigten erfolgt.

Bei einer routinemäßigen Kontrolle einer Webseite, die in erster Linie für Kinder gedacht war, stellten wir fest, dass die beschriebenen Anforderungen nicht erfüllt waren. Der Webseitenbetreiber bot Kindern die Mitgliedschaft in einem **virtuellen „Freundeklub"** an, in dem sie sich über ihre Fragen und Probleme austauschen konnten. Daneben „informierte" er die Teilnehmer des Forums über seine Angebote. Dabei mussten sich die betroffenen Minderjährigen für die Mitgliedschaft in dem Freundeklub registrieren lassen und damit Informationen über sich preisgeben. Der Webanbieter klärte seine kleinen Gäste nicht über Art, Umfang und Zweck etwaiger Datenauswertungen auf. Uns gegenüber machte er geltend, die Registrierung diene ausschließlich dem Schutz der Kinder, um missbräuchlichen Ausforschungen und Belästigungen vorzubeugen. Erforderlich war gleichwohl eine **Information der Minderjährigen**, die ihrem Erfahrungshorizont gerecht wird. Da der Umfang der geplanten Datenverarbeitung den erforderlichen Rahmen sprengte, musste zudem eine Einwilligung der Eltern sichergestellt werden. Da deren Authentisierung ausschließlich über das Internet erfolgen sollte, musste mit hinreichender Sicherheit gewährleistet werden, dass die Einwilligung in die Nutzung von Adressdaten auch tatsächlich von den Erziehungsberechtigten stammt.

Auf diese Erfordernisse angesprochen, erwies sich der Webseitenbetreiber als durchaus einsichtig. Über die geplanten Datenverarbeitungen werden die Minderjährigen künftig altersgerecht informiert. Im Rahmen des Registrierungsverfahrens werden sie aufgefordert, ihre Eltern zur Einwilligung hinzuzuziehen. Um zu erreichen, dass die Erziehungsberechtigten tatsächlich von der Registrierung Kenntnis erlangen und mit ihr einverstanden sind, wird nach der Anmeldung unmittelbar eine **Bestätigungsmail** eingeholt und diese Information nach einem bestimmten, hinreichend großen Zeitraum (nach mehreren Wochen bzw. einem Monat) nochmals per Mail bestätigt. Durch diese Vorgehensweise wird ausgeschlossen, dass Dritte unter Vorgabe einer anderen Identität ein dauerhaftes „Newsletter-Spamming" verursachen. Das Beispiel zeigt, wie im World Wide Web Datenschutz und Jugendschutz verbunden werden können.

Was ist zu tun?
Webangebote für Kinder dürfen nicht dazu führen, dass die Kids ausgeforscht werden. Wird ein Forum angeboten, in dem Kinder ihre Identität preisgeben, muss sichergestellt sein, dass die Erziehungsberechtigten hierzu ihre Einwilligung erteilen.

5.5 Gläserne Belegschaften?

Die moderne Industrie ist auf automatisierte Produktionssteuerung und auf Werkzeuge zur Revision angewiesen. Solche Instrumente ermöglichen zugleich umfassende Auswertungen des Arbeitnehmerverhaltens und bringen erhebliche Gefährdungen für die Rechte der Betroffenen mit sich.

Der Datenschutzbeauftragte eines Konzernunternehmens wandte sich an uns, weil die Geschäftsführung eine neue **Revisionssoftware** einführen wollte. Diese dient der Aufdeckung von Verlustquellen, die durch Manipulationen oder Fehlbedienungen von Kassen entstehen. Die Software macht sich zunutze, dass die Kassendaten sämtlicher Märkte des Unternehmens zentral erfasst und gespeichert werden. Sie ermöglicht eine Analyse dieser Datenbestände unter verschiedenen Gesichtspunkten (Data Mining), z. B. An- und Abmeldungen von Kassen, Nutzung elektronischer Zahlungsmittel, Kassenaktivitäten ohne Verkauf usw. Aufgrund der besonderen Funktionalität des Produktes können dabei Vorgänge einzelner Kassen zentral ausgewertet werden.

Nach dem geltenden Datenschutzrecht waren die geplanten Eingriffe in das Persönlichkeitsrecht der Mitarbeiter nicht zu rechtfertigen. Die eingesetzte Software ermöglichte Datenanalysen, die weit über die erforderliche Betrugsprävention hinausgingen und das **Verhalten der Arbeitnehmer systematisch ausforschten**. Einer solchen umfassenden Überwachung ihres Verhaltens am Arbeitsplatz stehen die schutzwürdigen Belange der Arbeitnehmer entgegen. Natürlich hat ein Unternehmen ein berechtigtes Interesse daran, Betrugsversuche aufzudecken und die Verantwortlichen zu identifizieren. Das darf aber nicht dazu führen, dass Arbeitnehmer am Arbeitsplatz ihre Privatsphäre völlig preisgeben müssen.

Auch wenn eine Betriebsvereinbarung im gewissen Umfang Datenverarbeitungsprozesse ermöglichen kann, muss sie im Einklang mit höherrangigem Recht stehen. Nach unseren Hinweisen auf die Rechtslage schlossen deshalb das Unternehmen und sein Gesamtbetriebsrat eine **Gesamtbetriebsvereinbarung** ab, welche den Einsatz der Revisionssoftware auf die Zwecke der Aufdeckung von vorsätzlichen Kassenmanipulationen und von **Kassenfehlgebrauch** (z. B. Tippfehler oder versehentliche Fehlbuchungen) beschränkt. Dabei soll der Kassenfehlgebrauch für die betroffenen Arbeitnehmer keine arbeitsrechtlichen Sanktionen nach sich ziehen. Der Kassenfehlgebrauch einzelner Betroffener soll für die unmittelbaren Vorgesetzten unbekannt bleiben. Das Verfahren sieht umfangreiche technische und organisatorische Maßnahmen vor, die die Rechte der Betroffenen wahren. Überdies wurden die betroffenen Mitarbeiter über die Einführung der Revisionssoftware allgemein verständlich informiert.

Was ist zu tun?
Schließen die Betriebspartner in einem Unternehmen Betriebsvereinbarungen ab, die den Einsatz von Überwachungsanlagen betreffen, muss ein angemessener Ausgleich zwischen berechtigten Interessen der Firma und den schutzwürdigen Interessen der Betroffenen geschaffen werden.

5.6 Datenschutz bei Unternehmensfusionen

Bei Unternehmensfusionen können komplizierte rechtliche Fragen auftreten. Eine Fusionsentscheidung zieht zwar zwangsläufig Datenverarbeitungsvorgänge nach sich, das Datenschutzrecht steht aber einer Fusion als solcher nicht entgegen.

Nachdem eine bevorstehende Bankenfusion mit dem Argument der datenschutzrechtlichen Unzulässigkeit angegriffen wurde, wandte sich eines der beteiligten Kreditinstitute an uns und bat uns um die Beurteilung der Zulässigkeit von **Datentransfers** im Rahmen eines Unternehmenszusammenschlusses.

Die Durchführung von Bankgeschäften mit Privatkunden unterliegt als Dienstleistung dem Wettbewerb mit privaten Stellen. Ungeachtet der Stellung des Kreditinstituts als Anstalt des öffentlichen Rechts oder als privatrechtliche Organisation gelten für die Verarbeitung personenbezogener Kundendaten durch Kreditinstitute die Vorschriften des Bundesdatenschutzgesetzes (BDSG). Speziellere Rechtsvorschriften gehen allerdings den Vorschriften des BDSG vor. Das einschlägige **Umwandlungsgesetz** nimmt aber keine Stellung zur Übermittlung von personenbezogenen Daten im Rahmen einer Verschmelzung und steht daher einer Anwendung des BDSG nicht im Wege.

Das BDSG findet nur auf „personenbezogene Daten“ Anwendung, also auf solche Informationen, die Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person enthalten. Die neu gegründete Gesellschaft tritt als **Gesamtrechtsnachfolgerin** in die Vertragsbeziehungen mit dem betroffenen Kunden ein. Soweit eine Datenverarbeitung durch das Kreditinstitut vor der Fusion zur Vertragsabwicklung mit dem Betroffenen erforderlich war, ist sie es nach dem Zusammenschluss für die neu gegründete Gesellschaft auch, es sei denn, der betroffene Kunde beendet das Vertragsverhältnis durch Kündigung.

Problematisch können Übermittlungen personenbezogener **Kundendaten** vor der erfolgten Verschmelzung sein. Sie sind nicht zur Vertragsabwicklung mit dem betroffenen Kunden erforderlich, weil die Fusion als solche für den Bestand des Vertragsverhältnisses mit dem Kunden nicht unmittelbar relevant ist. Der Datenübermittlung können überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen. Solche schutzwürdigen Interessen werden zum Beispiel relevant, wenn Datenbestände im Vertrauen auf eine künftige Fusion übermittelt werden und die Fusion gleichwohl scheitert. Unabdingbar ist deshalb eine **rechtzeitige Information** der betroffenen **Kunden**, damit sie ihre Interessen wahrnehmen können.

In einem anderen Fall erkundigte sich ein Unternehmen nach den Voraussetzungen eines Transfers von **Mitarbeiterdaten** im Rahmen eines **Betriebsüberganges**. Dabei wurde ein Betrieb an ein anderes Unternehmen veräußert. Ein solcher Betriebsübergang ist nicht erforderlich, um den Arbeitsvertrag mit dem Betroffenen zu erfüllen: Zwar tritt der Erwerber eines Betriebs regelmäßig in alle Rechte und Pflichten des alten Arbeitgebers ein. Wenn der Arbeitnehmer jedoch dem

Übergang des Arbeitsverhältnisses widerspricht, kann er hierdurch nach geltendem Recht das Vertragsverhältnis mit dem alten Arbeitgeber fortsetzen. Dementsprechend ist der Betriebsübergang nicht zum Erhalt des Arbeitsverhältnisses erforderlich. Daraus folgt, dass auch die Übermittlung von Arbeitnehmerdaten an den Erwerber nicht zur Erfüllung des Vertragsverhältnisses mit dem Betroffenen dient.

Der Arbeitgeber, der den Betrieb veräußert, muss deshalb vor der Übermittlung von Mitarbeiterdaten eine **Interessenabwägung** zwischen seinen Interessen als Veräußerer und den Interessen der Arbeitnehmer als Betroffenen vornehmen. Die Arbeitnehmer dürften dabei in der Regel mit dem Übergang des Arbeitsverhältnisses einverstanden sein, insbesondere wenn ansonsten betriebsbedingte Beendigungen des Arbeitsverhältnisses drohen. Denkbar ist jedoch auch, dass Betroffene in Einzelfällen ein **schutzwürdiges Interesse** haben, das **gegen die Übermittlung** spricht. Beispielsweise kann ein Mitarbeiter die Abfindung dem Arbeitsplatzerhalt vorziehen, weil er sich beruflich umorientieren will. Oder der Mitarbeiter hatte früher mit dem Käufer des Betriebs ein Vertragsverhältnis, das im Konflikt gelöst wurde. In solchen Ausnahmefällen dürfte ein Arbeitnehmer Wert darauf legen, dass seine Daten nicht zum Betriebserwerber gelangen.

Datenschutzkonform ist folgende **Vorgehensweise**: Im Rahmen der Vertragsverhandlungen und beim Vertragsabschluss dürfen keine personenbezogene Mitarbeiterdaten ohne Zustimmung übermittelt werden. In der Regel genügt aber eine **Widerspruchslösung**: Erfolgt innerhalb einer angemessenen Frist kein Widerspruch des Arbeitnehmers, darf der Arbeitgeber dessen Daten übermitteln. Der Veräußerer kann dem Erwerber aber anonymisierte oder statistische Daten (Wie viele Mitarbeiter sind derzeit im Betrieb beschäftigt? Wie viele davon sind Teilzeitbeschäftigte? Alter, Eintrittsdatum und das Jahresgehalt der Beschäftigten usw.) mitteilen, die ihm eine Beurteilung ermöglichen, ob sich der Erwerb lohnt.

Was ist zu tun?
Mitarbeiterdaten dürfen bei einer Unternehmensfusion grundsätzlich übermittelt werden, wenn die betroffenen Personen Gelegenheit hatten, dem Datentransfer zu widersprechen.

5.7 SCHUFA

Die Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA) plant Erweiterungen ihres Geschäftsfeldes um die Bereiche Wohnungswirtschaft, Versicherungswirtschaft und Inkassounternehmen. Bereits jetzt verarbeitet sie personenbezogene Informationen über etwa 59 Millionen Bürgerinnen und Bürger, also nahezu die gesamte erwachsene Bevölkerung Deutschlands.

Die **Erweiterung des Geschäftsfeldes** über die anerkannte Funktion für die kreditgebende Wirtschaft hinaus führt dazu, dass der Datenbestand der SCHUFA durch die Einbeziehung vielgestaltiger sozialer Zusammenhänge immer umfassender wird. Jede weitere Datenquelle lässt das Persönlichkeitsprofil des betroffenen Menschen detaillierter werden. Die gläserne Bürgerin und der gläserne Bürger werden zunehmend Realität – mit schwer kalkulierbaren Risiken für die Betroffenen.

Die Einbeziehung von Informationen aus weiteren Geschäftsfeldern in einen einheitlichen Datenbestand kann bewirken, dass künftig eine Person z. B. nur deswegen eine **Wohnung** nicht erhält, weil sie – aus welchen Gründen auch immer – eine Handyrechnung nicht bezahlt hat. Gerade die Einbeziehung von Informationen der Inkassounternehmen erhöht die Gefahr, dass alltägliche Streitigkeiten, wie z. B. über eine Handwerkerrechnung, schnell zu einem SCHUFA-Eintrag führen und als Folge etwa ein benötigter Versicherungsschutz nicht zustande kommt. Jeder verlorene Rechtsstreit könnte die Bonität für Kredite, Versicherungen und Mietverträge gefährden.

Die Entscheidung der SCHUFA über die Ausweitung ihrer Geschäftsfelder hat auch Auswirkungen auf Bürger und Unternehmen in Schleswig-Holstein. Deshalb haben wir gemeinsam mit dem Bundesbeauftragten für den Datenschutz und weiteren Landesdatenschutzbehörden auf die Folgen der schleichenden Geschäftserweiterung aufmerksam gemacht. **Unternehmen** der genannten Branchen **aus Schleswig-Holstein**, die die SCHUFA-Daten nutzen wollen, müssen damit rechnen, dass wir die Rechtmäßigkeit von SCHUFA-Abfragen überprüfen und bei Rechtswidrigkeit entsprechend sanktionieren.

Was ist zu tun?
Unternehmen der Wohnungswirtschaft und der Versicherungswirtschaft sollten bedenken, dass die Teilnahme am SCHUFA-Verfahren in seiner derzeitigen Ausgestaltung aus unserer Sicht als rechtswidrig anzusehen ist.

5.8 Versicherungen

Versicherungen und Kreditinstitute, die im Rahmen von Allfinanzkonzepten kooperieren, können mit dem Gesetz in Konflikt geraten, wenn sie nicht beachten, dass Gesundheitsdaten nach dem Datenschutzrecht einen besonderen Schutz genießen.

Nicht schlecht staunte der Kunde einer Sparkasse, als er von ihr Formulare zugesandt bekam, aus denen sich konkret ergab, welche seiner Organe noch einer genaueren ärztlichen Untersuchung bedurften, um einen beantragten Kleinkredit zu erhalten. Was war geschehen? Um den beantragten Kredit abzusichern, sollte der Kunde bei einer Versicherungsgesellschaft, die mit der Sparkasse in einem Verbund zusammenarbeitet, eine **Lebensversicherung** in entsprechender Höhe abschließen. Bevor die Versicherungsgesellschaft den Antrag auf Abschluss einer Lebensversicherung annahm, verlangte sie von dem Kunden eine ärztliche Untersuchung.

So weit, so gut. Doch anstatt die Formulare, mit denen der Kunde zu seinem Hausarzt gehen sollte, direkt an den Kunden zu schicken, leitete die Versicherung die Unterlagen an die kreditgewährende Sparkasse. Immerhin ergaben sich aus den Formularen konkrete Untersuchungserfordernisse, wie z. B. eingehende Untersuchung von Blutdruck und Leber. Die Versicherung konnte ihr Verhalten auf unsere Anfrage nur mit dem Hinweis auf eine **langjährige Praxis** und mit der Verbundpartnerschaft mit der Sparkassenorganisation begründen. Nach unserer Intervention erklärte die Versicherung, ihr Verfahren zu ändern und derartige Untersuchungsbögen künftig nur noch direkt an die Antragsteller zu übersenden.

Was ist zu tun?
Versicherungen dürfen zur Klärung des Risikos im Vorfeld von Vertragsabschlüssen medizinische Informationen von Betroffenen nicht an Dritte weitergeben.

5.9 Rechtsanwälte und Datenschutz

Rechtsanwälte beraten und vertreten ihre Mandanten in vielfältigen Situationen und Anliegen. Das deshalb erforderliche besondere Vertrauensverhältnis zwischen Mandant und Anwalt soll durch die anwaltliche Schweigepflicht abgesichert werden. Daneben ist das Bundesdatenschutzgesetz zu beachten.

Manche **berufsrechtliche Regelungen** zum Geheimnisschutz, wie beispielsweise in der Bundesrechtsanwaltsordnung (BRAO), sind sehr allgemein gehalten. Ergänzend ist deshalb bezüglich der Auskunftspflichten gegenüber dem Betroffenen oder in Fragen der Datensicherheit auf das stärker ausdifferenzierte Bundesdatenschutzgesetz zurückzugreifen.

Im Wortlaut:
§ 43 a Abs. 2 BRAO

Der Rechtsanwalt ist zur Verschwiegenheit verpflichtet. Diese Pflicht bezieht sich auf alles, was ihm in Ausübung seines Berufes bekannt geworden ist. Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

Die Aufsicht über die Einhaltung berufsrechtlicher Regelungen ist den **Rechtsanwaltskammern** übertragen. Für **Fragen des Datenschutzrechts** sind hingegen die **Datenschutzaufsichtsbehörden** für den nichtöffentlichen Bereich zuständig. Soweit hiervon nicht die Prozesstätigkeit betroffen ist, haben wir deshalb auch die Aufgabe, bei Rechtsanwälten Prüfungen durchzuführen. Interessenvertreter der Rechtsanwälte befürchten, dass im Rahmen einer solchen Prüftätigkeit das anwaltliche Berufsgeheimnis unterlaufen werden könnte. Diesen Bedenken trägt das BDSG dadurch Rechnung, dass personenbezogene Daten, die im Rahmen der Prüftätigkeit erlangt wurden, nur zum Zweck der Datenschutzaufsicht verwandt werden dürfen. Besondere Berufsgeheimnisse stehen der Datenschutzaufsicht ausdrücklich nicht entgegen.

Dass datenschutzrechtliche Kontrollen und Nachforschungen aufgrund von Beschwerden notwendig sind, zeigt folgendes Beispiel: Eine Bürgerin musste sich von ihrem Arbeitgeber unangenehme Fragen gefallen lassen, weil ihre Rechtsanwältin ein **Telefax** an ihren Arbeitsplatz übersandt hatte. Dies geschah ohne Absprache und überdies ohne Kennzeichnung als „vertraulich/persönlich“. Damit gab sie Informationen über die frühere soziale Hilfsbedürftigkeit ihrer Mandantin preis. Erst nach unserer Intervention ließ sich die Rechtsanwältin davon überzeugen, dass eine solche Vorgehensweise nicht rechtmäßig ist, und sicherte für die Zukunft eine datenschutzkonforme Kommunikation mit Dritten zu.

Schleswig-Holstein
DATENSCHUTZAKADEMIE
Kurs ANW

Was ist zu tun?
Das Datenschutzrecht ist grundsätzlich auch von Rechtsanwälten zu beachten. Sie unterliegen diesbezüglich auch unserer Kontrolle.

5.10 Videoüberwachung wuchert wie ein Geschwür

Über 400.000 Videokameras überwachen in der Bundesrepublik Deutschland öffentliche Plätze, Bahnhöfe und Geschäftsräume. Die nackte Zahl gibt nur eine vage Vorstellung davon, in welchem Ausmaß die Bürger inzwischen bereits der Dauerüberwachung ausgesetzt sind. Auch in schleswig-holsteinischen Städten wird es immer schwieriger, sich einen Tag lang frei und unbeobachtet bewegen zu können.

Während die Überwachung von sicherheitsrelevanten Räumen (z. B. Kreditinstituten) nachvollziehbar ist, werden immer mehr Kameras zur Abwehr von Bagatellschäden oder lediglich zur Steigerung des **subjektiven Sicherheitsgefühls** installiert. Solche Gründe reichen in der Regel nicht, um den Eingriff in die Privatsphäre der Betroffenen zu rechtfertigen (vgl. Tz. 4.8.3). Dass sich Videoüberwachung auszahlt, ist keineswegs belegt, selbst wenn beträchtliche Sachschäden abgewehrt werden sollen. Auf unsere Nachfrage, wie viele nachweisbare Schäden die Veranlassung für die Installation von Kameras gegeben hätten, blieben uns zahlreiche Betreiber eine Antwort schuldig. In vielen Fällen decken die durch die Überwachung zu vermeidenden Kosten nicht einmal die Kosten der Anschaffung der Anlage. **Videoüberwachung** ist leider **„in“**, die Achtung der Privatsphäre anderer zählt offenbar wenig.

Im Wortlaut: § 6 b Abs. 1 BDSG

Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen ist nur zulässig, soweit sie

1. *zur Aufgabenstellung öffentlicher Stellen,*
2. *zur Wahrnehmung des Hausrechts oder*
3. *zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke*

erforderlich sind und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Besonders häufig wandten sich Bürger an uns, weil bei ihnen die kameragesteuerte Überwachung bereits im **Treppenhaus ihres Wohngebäudes** begann. In den meisten Fällen konnten wir die Betreiber der Kameras von der Rechtswidrigkeit ihres Handelns überzeugen, sodass die Überwachung eingestellt wurde. Nur in wenigen Fällen erwies sich die eingerichtete Videoüberwachung als gerechtfertigt.

Was ist zu tun?
Bevor Unternehmen Videoüberwachungsanlagen errichten, haben sie die gesetzlichen Voraussetzungen sorgfältig zu prüfen: Nicht jedes beliebige Interesse rechtfertigt den erheblichen Eingriff in die Privatsphäre, der durch Videoüberwachung entsteht.

6 Systemdatenschutz

6.1 Sicherheitsmaßnahmen und Restrisiken beim Betriebssystem Windows 2000

Die neuen Betriebssysteme der Firma Microsoft werden nicht in einer „sicheren“ Konfiguration ausgeliefert. Das nötige Maß an Sicherheit muss durch die IT-Betreuer mühsam eingestellt werden. Das hierfür erforderliche Wissen vermittelt unser backUP-Magazin, das sich bereits kurz nach seinem Erscheinen als „Renner“ erweist.

Über die weit reichenden Konsequenzen einer Umstellung der IT-Systeme von einem Betriebssystem auf ein anderes und insbesondere über die Probleme bei der Einführung des Betriebssystems **Windows 2000** der Firma Microsoft haben wir bereits im letzten Jahr berichtet (vgl. 25. TB, Tz. 7.2). Gleichzeitig haben wir angekündigt, im Rahmen unserer backUP-Magazine Handreichungen für die Praxis zu geben. Dies ist zwischenzeitlich geschehen.

Im Juni 2003 konnte nach etwa einjähriger Vorbereitung das Handbuch „**MS-Windows 2000 – Sicherheitsmaßnahmen und Restrisiken**“ an die Systemadministratoren im Lande ausgeliefert werden. Es ist nach dem gleichen Konzept aufgebaut wie sein Vorgänger für das Betriebssystem MS-Windows NT 4.0 (vgl. 23. TB, Tz. 10.1) und hat eine ebenso positive Resonanz gefunden. Dies zeigen die Reaktionen, die wir aus ganz Deutschland empfangen haben. Das Handbuch steht in elektronischer Fassung auf unserer Homepage zum Download zur Verfügung unter

www.datenschutzzentrum.de/material/themen/edv/backup/backup05.htm

Das neue backUP-Magazin erhebt keinen Anspruch auf eine umfassende Vermittlung der Windows 2000-Theorie, vielmehr soll es als ein **praktischer Ratgeber** die IT-Betreuer dabei unterstützen, die datenschutzrelevanten Sicherheitsmaßnahmen auf der Arbeitsplatz- und der Serverebene richtig zu implementieren. Schwachstellen im neuen Betriebssystem werden erläutert und Lösungen für ihre Beseitigung aufgezeigt. Es werden nicht nur systemtechnische Aspekte behandelt, sondern auch Grundsatzfragen in Bezug auf die Sicherheitsproblematik moderner IT-Systeme. Hiermit muss sich heute insbesondere die Leitungsebene einer Daten verarbeitenden Stelle befassen.

Da kaum eine Behörde das Betriebssystem „auf der grünen Wiese“ installieren kann, behandelt ein ganzes Kapitel das Problem der **Migration** von Windows NT 4.0 auf Windows 2000. Hier liegt der Schwerpunkt bei der Frage nach dem Erhalt und der Optimierung von Sicherheitseinstellungen. Außerdem kann das Magazin dazu benutzt werden, bereits unter MS-Windows 2000 realisierte Sicherheitseinstellungen auf ihre Wirksamkeit zu überprüfen.

Wie aufwändig es in der Praxis ist, auch nur die notwendigsten Konfigurationsmaßnahmen vorzunehmen, machen zwei Zahlen deutlich:

- Das Magazin umfasst insgesamt ca. 300 Seiten. Das darin enthaltene Wissensvolumen muss jeder Administrator präsent haben, wenn er sein IT-System unter Sicherheitsaspekten verantwortlich und verantwortbar betreuen will.
- Allein die Checkliste, die eine Hilfestellung bei der Entwicklung eines Sicherheitskonzeptes bzw. bei der Kontrolle bereits durchgeführter Sicherheitsmaßnahmen geben soll, umfasst 128 Positionen in 11 Kategorien.

Schleswig-Holstein DATENSCHUTZAKADEMIE
Kurse WIN-I, SDZ

Kleine Verwaltungen können ein derartig umfangreiches Know-how natürlich nicht vorhalten. Sie nehmen für die Konfiguration ihrer Systeme häufig externe Dienstleister in Anspruch. Dabei setzt sich mehr und mehr die Praxis durch, in den Aufträgen zu fordern, dass die Sicherheitsmaßnahmen entsprechend den Regeln und Vorschlägen des backUP-Magazins zu gestalten sind. Es gibt Anzeichen dafür, dass sich auf diese Weise ein De-facto-Sicherheitsstandard für das am häufigsten eingesetzte Betriebssystem herausbildet. So stellen wir uns **praktizierten Systemdatenschutz** vor.

Was ist zu tun?
Die Verantwortlichen in den Daten verarbeitenden Stellen sollten darauf bestehen, dass von ihren IT-Betreuern die in dem backUP-Magazin „MS Windows 2000 – Sicherheitsmaßnahmen und Restrisiken“ beschriebenen Konfigurationsmaßnahmen als sicherheitstechnischer Mindeststandard realisiert werden.

6.2 Sicherheit am Arbeitsplatz – was Benutzer von den Administratoren verlangen sollten

Datenschutz und Datensicherheit am PC-Arbeitsplatz ist nicht nur Sache der Administratoren. Gerade die für die Verarbeitungsprozesse verantwortlichen Mitarbeiter der Fachbereiche müssen die adäquaten technischen und organisatorischen Maßnahmen fordern, die den Missbrauch von Daten verhindern und deren Vertraulichkeit wahren.

Normalerweise wird das **Sicherheitskonzept** für die PC-Arbeitsplätze einer Daten verarbeitenden Stelle von den IT-Betreuern entwickelt und den Benutzern vor Ort „**gebrauchsfertig**“ präsentiert. Das ist kein grundsätzlich falscher Ansatz. Probleme ergeben sich aber, wenn das Konzept aus Kostengründen, aus Unachtsamkeit oder weil dem zentralen IT-Betreuer die Sicherheitsbedürfnisse der einzelnen Fachabteilungen gar nicht bekannt sind, Lücken aufweist. Dann wiegt sich der IT-Betreuer in der Sicherheit, alles „Mögliche“ getan zu haben, und die Benutzer glauben, die Technik könne nicht anders. In der täglichen Praxis müssen die Benutzer daher oft mit Sicherheitsrisiken leben, die sie eigentlich gar nicht eingehen wollen. Um Kritik an den Entscheidungen der IT-Stelle zu äußern, fehlt ihnen das Wissen bzw. der Präzedenzfall.

Diesen Gegebenheiten trägt das zweite **backUP-Magazin**, das im Jahr 2003 neu herausgebracht wurde, Rechnung. Es hat den Titel „**PC-Arbeitsplatz – So viel Datenschutz muss an jedem Arbeitsplatz sein!**“.

www.datenschutzzentrum.de/material/themen/edv/backup/backup04.htm

Es ist nicht primär für IT-Betreuer, sondern für deren Kunden konzipiert und dreht damit den Spieß um. Den Mitarbeiterinnen und Mitarbeitern in den Fachabteilungen wird erläutert, auf welches Maß an **Systemdatenschutz** sie – auch im eigenen Interesse – einen Anspruch haben. Dabei wird davon ausgegangen, dass ein datenschutzgerechter und sicherheitstechnisch ausgereifter Arbeitsplatz das Risiko reduziert, dass durch Unwissenheit oder Fahrlässigkeit die Benutzer Schäden verursachen, die ihnen angelastet werden. Mitarbeiter, die dieses Risiko vermeiden wollen, sollen in die Lage versetzt werden, konkrete Forderungen zu formulieren und diese in ihrem eigenen Interesse gegenüber der IT-Abteilung durchzusetzen.

Dazu werden z. B. Antworten auf folgende Fragen gegeben:

- Ist Datensicherheit das Gleiche wie Datenschutz?
- Was ist bei Computern anders als bei Akten?
- Wer kann auf meinem Computer arbeiten?
- Wo werden meine Daten gespeichert?
- Kann jemand überwachen, was ich auf meinem Computer mache?
- Warum brauche ich ein Passwort?
- Wann ist eine Verschlüsselung sinnvoll?
- Was muss ich bei der E-Mail-Kommunikation beachten?
- Wie gefährlich ist das Internet?

Außerdem enthält das Magazin eine **Checkliste**, mit deren Hilfe der Benutzer selbst feststellen kann, welche datenschutzrelevanten Defizite an seinem Arbeitsplatz bestehen. Praktische Hilfestellungen für die Optimierung der Aufbau- und Ablauforganisation werden durch drei Musterdienstanweisungen gegeben.

Wünschenswert ist, dass sich nach dem Studium des backUP-Magazins möglichst viele Mitarbeiterinnen und Mitarbeiter zu einem **konstruktiv-kritischen Dialog** mit ihren IT-Betreuern herausgefordert fühlen und auf diese Weise zu einer Verbesserung des Datenschutzes und der Datensicherheit speziell an ihrem Arbeitsplatz beitragen. Natürlich ist kein IT-Betreuer daran gehindert, der Kritik aus den Fachbereichen dadurch vorzubeugen, dass nach einem Abgleich mit den Forderungen und Vorschlägen des ULD bereits präventiv das Sicherheitskonzept fortgeschrieben wird. Dabei sollte das backUP-Magazin von der IT-Abteilung und den Fachbereichen gemeinsam durchgearbeitet werden.

Was ist zu tun?
Die Mitarbeiterinnen und Mitarbeiter in den Fachbereichen sollten bezüglich des Datenschutzes und der Datensicherheit an ihren PC-Arbeitsplätzen klare Forderungen gegenüber dem IT-Bereich formulieren. Die Vorschläge in dem backUP-Magazin sollten wörtlich genommen werden: So viel Datenschutz muss sein!

6.3 Informationsdienst SUSA

Die Kontakte zwischen den Systemadministratoren im Lande und dem ULD müssen intensiviert werden, um den Herausforderungen der immer komplexer werdenden IT-Systeme gerecht zu werden. Zu diesem Zweck wurde die Initiative SUSA gestartet, ein Angebot, von dem bereits viele Systemverantwortliche Gebrauch machen.

In den Verwaltungen des Landes, der Kommunen und der sonstigen öffentlichen Stellen gibt es ca. 400 bis 500 Mitarbeiter, die die Funktion des **Systemadministrators** ausüben. Nur wenige von ihnen sind uns namentlich bekannt, etwa weil durch Prüfungen, Beratungen, Audits oder Schulungsmaßnahmen Kontakte aufgebaut werden konnten. In der Regel handelt es sich um diejenigen, die diese Tätigkeit auf Dauer und im „Hauptamt“ wahrnehmen. Die meisten Mitarbeiterinnen und Mitarbeiter, insbesondere in den IT-Stellen von kleineren Behörden, sind jedoch nur zu 30 bis 50 % ihrer Arbeitszeit als Administrator tätig. Ihre Hauptaufgaben liegen in anderen Fachgebieten. Gleichwohl müssen auch sie dafür sorgen, dass die von ihnen betreuten IT-Systeme so funktionieren, dass die Ergebnisse richtig sind und die verarbeiteten personenbezogenen Daten nicht in unbefugte Hände gelangen. Diese klassischen Sicherheitsanforderungen zu gewährleisten erfordert eine ständige Auseinandersetzung mit den aktuellen Meldungen über Betriebssystem- und Softwarefehler, über Patches, Updates, Service Packs, Resource Kits und Security Tools sowie über die in der Fachliteratur und in Schulungsveranstaltungen veröffentlichten bzw. angebotenen Konfigurationskonzepte.

> **?** ***Systemdatenschutz***
>
> *Der Systemdatenschutz umfasst alle IT-bezogenen Vorkehrungen, die für den Schutz des Rechts auf informationelle Selbstbestimmung förderlich und rechtlich geboten sind. Er beschränkt sich nicht auf rein technische Maßnahmen wie z. B. Firewalls und Verschlüsselungen, sondern schließt auch organisatorische Regelungen ein und geht aufgrund neuer Ansätze wie Datensparsamkeit, frühzeitige Anonymisierung oder Pseudonymisierung, Datenschutz-Audit und Datenschutz-Gütesiegel über die klassischen technischen und organisatorischen Maßnahmen hinaus.*

Aus diesem Grunde haben wir im Juni 2003 unter dem Kürzel SUSA eine Initiative gestartet, die unserem im Landesdatenschutzgesetz festgeschriebenen Beratungsauftrag speziell auch für IT-Betreuer gerecht werden soll. **SUSA** steht für „Systemdatenschutz – ULD-Support für Administratoren“.

Die zentrale Komponente dieser Initiative ist ein auf unserer Homepage angebotener **Informationsdienst**, in dem

- Nachrichten mit sicherheitstechnischem Hintergrund,
- Hinweise auf Artikel in Fachzeitschriften sowie auch andere Veröffentlichungen,
- Termine einschlägiger Veranstaltungen und Fortbildungsangebote und
- vom ULD und anderen Datenschutzinstitutionen herausgegebene Dokumentationen

publiziert werden. Er ist deshalb unterteilt in die Rubriken:

- System-Meldungen,
- System-Bibliothek,
- System-Zeit und
- System-Dokumentation

und unterscheidet sich in einem wesentlichen Punkt von anderen Informationsangeboten im Web: Die **Inhalte** werden nicht nur transportiert, sondern auch unter datenschutzrechtlichen und sicherheitstechnischen Gesichtspunkten **kommentiert**. Sowohl die Auswahl als auch ihre Aufbereitung geschieht unter dem Gesichtspunkt: „Welche Information braucht ein Administrator, und welche Kommentare und Hinweise des ULD sind für ihn bezogen auf die betreffende Information nützlich?“ Zu diesem Zweck wurde ein Redaktionsteam gebildet, das die Aufgabe hat, alle Informationen, die für unsere eigenen Aufgaben von Belang sind, daraufhin zu untersuchen, ob sie auch für die IT-Betreuer im Lande interessant sein könnten. Der **SUSA-Informationsdienst** selbst ist dreistufig aufgebaut:

- Eine Überschrift und ein „Abstract“ beschreiben kurz, worum es geht.
- Es folgt eine kompakte Kommentierung des Sachverhalts.
- Schließlich wird auf die Quellen bzw. Fundstellen (in der Regel durch Links) verwiesen.


www.datenschutzzentrum.de/systemdatenschutz/

Der Informationsdienst wird gut angenommen. Da der WWW-Server des ULD bewusst keine spezifizierten Protokolle über die Nutzer erzeugt, sind genaue **Zugriffszahlen** nicht zu ermitteln (die automatischen Zugriffe der Suchmaschinen sind nicht identifizierbar). Schätzungsweise greifen aber bereits jetzt monatlich ca. 700 Nutzer auf das Angebot zu.

Zusätzlich haben wir eine **Mailinglist für Systemadministratoren** eingerichtet, die für alle Interessenten offen ist. Die An- und Abmeldung zur Mailinglist kann jeder leicht selbst durchführen unter


www.datenschutzzentrum.de/ldsh/listen.htm

Das SUSA-Angebot wird **künftig** um weitere backUP-Magazine speziell für Administratoren und durch die überwachte Durchführung von professionellen Angriffen auf die Sicherheitspolicy der Behörden durch ein Security-Analyseteam **erweitert**. Diese bestellte (und bezahlte) Prüfung soll die Frage beantworten helfen: „Könnte vielleicht nicht doch ein Angreifer an der Sicherheitspolicy vorbei auf vertrauliche Daten zugreifen?“

Was ist zu tun?
Die Systembetreuer im Lande sind eingeladen, den neuen Informationsdienst zu nutzen; sie können sich beim ULD als Administrator registrieren lassen, damit der Informationsaustausch künftig weiter intensiviert werden kann.

6.4 Warum man den Bock nicht zum Gärtner machen darf

Mit so genannten Online-Updates wollen Betriebssystemlieferanten und Anbieter sonstiger Software den Behörden angeblich das Leben einfacher machen. Tatsächlich verschleiern sie damit die Anzahl der zu reparierenden Softwarefehler und gewinnen selbst die Herrschaft über die IT-Systeme. Diese Marketingstrategie verstößt gegen datenschutzrechtliche Vorschriften.

Es ist unter IT-Fachleuten eine Binsenweisheit, dass derjenige, der einen Zugriff mit Änderungsrechten auf die Betriebssystemebene eines Computers hat, ihn in beliebiger Weise manipulieren kann. Deshalb sind professionelle und verantwortungsbewusste Systembetreuer sehr darauf bedacht, dass außer ihnen selbst niemandem derartige Möglichkeiten zur Verfügung stehen. Praktisch alle Hackeraktivitäten haben nämlich zum Ziel, Konfigurationsschwächen oder Betriebssystemfehler auszunutzen, um sich unbefugt **Administrationsrechte** anzueignen. Auf diese Weise ist es möglich, Viren oder Würmer in ein fremdes IT-System zu implantieren. Eine durchbruchfeste Barriere zwischen der Benutzer- und der Administrationsebene eines Rechnersystems ist also die Grundvoraussetz-

Im Wortlaut:
Auszug aus den Lizenzverträgen der Firma Microsoft

„Wenn Sie sich entscheiden, die Update-Funktionen innerhalb des Betriebssystemproduktes oder der Betriebssystemkomponenten zu verwenden, ist es zum Implementieren der Funktionen erforderlich, bestimmte Informationen zum Computersystem, zur Hardware und zur Software zu verwenden. Indem Sie diese Funktionen verwenden, ermächtigen Sie Microsoft oder deren bezeichneten Vertreter zum Zugriff auf die erforderlichen Informationen und zu deren Verwendungen für Updates. Microsoft ist berechtigt, diese Informationen nur zur Verbesserung ihrer Produkte oder zum Liefern von benutzerdefinierten Diensten und Technologien an Sie zu verwenden. Microsoft erklärt sich einverstanden, solche Daten ausschließlich anonym offen zu legen. Das Betriebssystemprodukt oder die Betriebssystemkomponenten enthält bzw. enthalten Komponenten, die die Verwendung bestimmter internetbasierter Dienste ermöglichen und erleichtern. Sie erkennen und stimmen zu, dass Microsoft berechtigt ist, die von Ihnen verwendete Version des Betriebssystemprodukts und/oder seiner Komponenten automatisch zu überprüfen und Updates oder Fixes des Betriebssystemprodukts bereitzustellen, die automatisch auf Ihrem Computer gedownloadet werden.“

zung dafür, dass ein Administrator überhaupt die Verantwortung für das ordnungsgemäße Funktionieren der automatisierten Verfahren übernehmen kann.

Nun ist es Fakt, dass die gängigen Betriebssysteme und die systemnahe Software so fehlerbehaftet sind, dass die Administratoren fortwährend neue **Korrektursoftware** einspielen müssen. Dies ist für die Hersteller der Betriebssysteme (wie z. B. für die Firma Microsoft) peinlich. Noch peinlicher ist es, wenn sich Viren und Würmer explosionsartig weltweit verbreiten und schädigende Wirkungen großen Ausmaßes haben, weil viele IT-Betreuer besagte Patches nicht in ihr System übernommen haben.

Deshalb war z. B. die Firma Microsoft bestrebt, selbst **Online-Updates** für ihre Betriebssysteme durchzuführen und dabei das bestehende Betriebssystem zu analysieren, um spezifizierte Korrekturen und Ergänzungen vorzunehmen. Es handelte sich um ein weltweit praktiziertes Verfahren, das als ein Service gegenüber den Kunden angesehen wurde. Rechtliche und sicherheitstechnische Probleme hat die Firma Microsoft nicht gesehen. Sie ging davon aus, dass die Kunden über Verträge bzw. die Anerkennung der allgemeinen Geschäftsbedingungen ihr Einverständnis zu diesen Maßnahmen geben würden.

In der Fachliteratur werden derartige Vereinbarungen als „**Lizenz zum Spähen**“ bezeichnet. Microsofts Möglichkeiten, den Usern auf die Festplatten zu schauen und nicht nur systembezogene Daten einzuholen, seien enorm. Microsoft prüfe nicht nur, welche der verfügbaren Updates bereits installiert sind und welche fehlen, es würden auch die Versionsnummern von Softwarepaketen, die Plug & Play-IDs der installierten Hardware und andere Kennzahlen ausgelesen und in einem Globally Unique Identifier zusammengefasst. Tests mit einem Network Analyser hätten gezeigt, dass beim ersten Scan eines neu installierten Systems fast zehn MByte Daten an mehrere Microsoft-Server gehen, bevor auch nur eine einzige Datei heruntergeladen wird, und weitere zehn MByte wandern von Microsoft zum Anwender. Dies sei der klassische Fall, dass der Bock zum Gärtner gemacht wird.

> ***Im Wortlaut: § 6 Abs. 2 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.*

Im Hinblick auf die in Schleswig-Holstein geltenden Regelungen im Landesdatenschutzgesetz und in der Datenschutzverordnung ist ein derartiges Online-Update für IT-Systeme, mit denen personenbezogene Daten verarbeitet werden, **schlicht unzulässig**. Das LDSG schreibt nämlich aus den oben genannten Gründen bindend vor, dass Zugriffe, mit denen Änderungen an automatisierten Verfahren (also auch an den den Verfahren zugrunde liegenden Betriebssystemen) bewirkt werden können, nur den dazu ausdrücklich berechtigten Personen möglich sein dürfen.

> ***Im Wortlaut: § 5 Abs. 2 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.*

Bei der Erbringung von Wartungsarbeiten oder von vergleichbaren Unterstützungstätigkeiten durch Stellen oder Personen außerhalb der Daten verarbeitenden Stelle hat diese dafür Sorge zu tragen, dass personenbezogene Daten nur **im Rahmen ihrer Weisungen** verarbeitet werden. Sie hat die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um dies sicherzustellen. Die Aufträge und die ergänzenden Weisungen zu den technischen und organisatorischen Maßnahmen sind schriftlich festzulegen. Vor wesentlichen Änderungen an automatisierten Verfahren, mit denen besonders sensible Daten verarbeitet werden, hat eine Vorabkontrolle durch den Datenschutzbeauftragten zu erfolgen. Schließlich sind alle automatisierten Verfahren vor ihrem erstmaligen Einsatz und nach Änderungen zu dokumentieren und durch die Leitung der Daten verarbeitenden Stelle förmlich freizugeben.

Dies war mit dem von der Firma Microsoft konzipierten Verfahren nicht zu realisieren. Unter datenschutzrechtlichen Aspekten steht nämlich nicht die Frage der Aufwandsminimierung im Vordergrund, sondern die objektive Möglichkeit der Firma Microsoft, unkontrollierbare, nicht revisionsfähige und nicht ausdrücklich genehmigte Veränderungen auf der Betriebssystemebene und an den Datenbeständen eines IT-Systems vornehmen zu können. Dies haben wir nicht nur den Daten verarbeitenden Stellen im Lande über die „System-Meldungen“ der Initiative SUSA (vgl. Tz. 6.3), sondern auch der Firma Microsoft mitgeteilt. Nun war nicht zu erwarten, dass das Unternehmen seine Praxis aufgrund der Bedenken eines einzelnen deutschen Datenschutzbeauftragten ändert. Als sich allerdings die **Konferenz der Datenschutzbeauftragten** des Bundes und der Länder im August 2003 in einer kritischen Entschließung zu automatischen Software-Updates unseren Bedenken anschloss, zeigte sie Wirkung.

www.datenschutz-berlin.de/doc/de/konf/65-66/update.htm

Ohne auf die Argumente der Datenschutzbeauftragten näher einzugehen, wird nunmehr ein Konzept propagiert, bei dem ein so genannter **Software-Update-Server** einen regelmäßigen Kontakt mit der Firma Microsoft hält und die Korrektursoftware herunterlädt. Die Kunden entscheiden, wann und welche Software sie auf ihre Produktivsysteme übertragen.

Die Daten verarbeitenden Stellen haben also weiterhin die Möglichkeit,

- Online-Updates über Testsysteme durchzuführen, die Ergebnisse zu überprüfen und die neuen Versionen erst danach auf die Produktivsysteme zu überspielen oder
- die Updates offline abzuwickeln, die Downloads und Prozesse zu dokumentieren und die Systeme erst nach entsprechenden Tests und Freigaben wieder für die Produktion freizugeben.

Was ist zu tun?
Unabhängig davon, ob die Systemadministration durch eigene Mitarbeiter oder durch externe Dienstleister vorgenommen wird, haben die Daten verarbeitenden Stellen jede Änderung am Betriebssystem und an der sonstigen Software vor dem Einsatz unter Produktionsbedingungen zu testen, zu dokumentieren und förmlich freizugeben. Unkontrollierbare Veränderungen durch die Lieferanten des Betriebssystems scheiden in jedem Fall aus.

6.5 Umbau in der IT-Organisation der Landes

Die Kosten für den Einsatz der Informationstechnik in der Verwaltung sind immer schwieriger zu erwirtschaften. Deshalb kommen die IT-Strukturen überall auf den Prüfstand. Die Landesregierung hat eine Reorganisation vorgenommen, die sicherlich datenschutzrechtlich, wahrscheinlich aber auch wirtschaftlich sinnvoll ist.

Seit dem Beginn der Automatisierung von Verwaltungsabläufen im Lande hat es ein Koordinierungsgremium gegeben, in dem die einzelnen Ministerien ihre IT-Vorhaben miteinander abstimmten und die Schnittstellen für die ressortübergreifenden Maßnahmen definierten. Zunächst wurde es als Automationskommission und nach einer Reorganisation als **IT-Kommission** bezeichnet. In ihr waren neben den IT-Referenten der Ministerien und dem Landesrechnungshof auch die Datenzentrale (jetzt dataport) und das ULD sowie der Personalrat mit beratender Stimme vertreten. Obwohl sich die Kommission unter der Federführung des Innenministeriums eine Geschäftsordnung gab, eine Vielzahl von Richtlinien verabschiedete und die Normierung und Standardisierung der Informationstechnik im Lande maßgeblich vorantrieb, wurde die Ressortverantwortung für die konkreten IT-Maßnahmen nicht angetastet. Die Frage, welche Verbindlichkeit die gefassten Beschlüsse für die einzelnen Verwaltungsbereiche hatten, blieb über Jahre hinweg ohne eine abschließende Antwort. Einstimmig getroffene Entscheidungen waren selbstverständlich verbindlich, bei Mehrheitsentscheidungen relativierte sich diese Verbindlichkeit sehr stark.

Dieser **Schwebezustand** war aus datenschutzrechtlicher Sicht nur so lange hinnehmbar, wie in der Kommission nur über Konzepte diskutiert und entschieden wurde, die eigentliche Verarbeitung personenbezogener Daten aber unter der Regie des einzelnen Fachressorts ablief. Dieser Zustand änderte sich vor einigen Jahren in drei Bereichen:

- Die Haushaltsabteilung des Finanzministeriums installierte in allen Behörden PC-Arbeitsplätze, über die die zentrale Mittelbewirtschaftung (SAP-Verfahren) abgewickelt wurde.
- Das Finanzministerium wurde zuständig für den Betrieb und die Administration der über 300 Telekommunikationsanlagen im Lande.
- Das Innenministerium übernahm die Rolle des Betreibers des CAMPUS-Netzes, später des Landesnetzes und des verwaltungsweiten Maildienstes.

Während das Finanzministerium bei der Mittelbewirtschaftung und der Sprachkommunikation zweifelsfrei in eigener Zuständigkeit/Verantwortung handelte (die Verfahren wurden im „Erlasswege“ eingeführt und betrieben), trat das **Innenministerium** gegenüber den anderen Ressorts als **Dienstleister** auf. Von der IT-Kommission waren so genannte Rahmen- und Anschlussbedingungen erarbeitet worden, die praktisch eine vertragliche Grundlage für die Übernahme von Aufgaben des jeweiligen Fachressorts durch das Innenministerium darstellten. Das Innenministerium bediente sich seinerseits der Datenzentrale als externem Dienstleister. Im datenschutzrechtlichen Sinn war das Innenministerium also Auftragnehmer der anderen Ministerien und somit an deren Weisungen gebunden.

Diese rechtliche **Umkehr der** tatsächlichen „**Machtverhältnisse**“ erlangte deshalb eine so große Bedeutung, weil sowohl im Rahmen des Landesnetzes und der damit verbundenen Services als auch im Rahmen des Projektes IKOTECH III Datenbestände mit personenbezogenen Daten aufgebaut wurden (z. B. beim E-Mail-Management) und außerdem wichtige Sicherheitsfunktionalitäten aus den einzelnen Ressorts in das Innenministerium bzw. zu dataport verlagert worden sind (z. B. der zentrale Verzeichnisdienst und die Firewall). Die Frage, welche Daten verarbeitende Stelle für welche Entscheidungen, Vertragsgestaltungen mit Dritten, Implementierungen, Sicherheitsmaßnahmen, Dokumentationen und Kontrollen der Auftragnehmer die Verantwortung übernehmen konnte, war in den letzten Jahren ein ständiger von uns initiierter Diskussionspunkt in den Beratungen der IT-Kommission.

Diesem Dilemma hat die Ministerpräsidentin mit ihrem „**Organisationserlass über die Geschäftsverteilung der Landesregierung**“ im Jahr 2003 ein Ende bereitet. Der Erlass weist die Zuständigkeit für das „Ressortübergreifende strategische und operative IT-Management“ sowie für die „Zentralen Komponenten und Services der IT-Infrastruktur der Landesverwaltung“ dem Finanzministerium zu. Das bedeutet nicht mehr und nicht weniger, als dass der **Finanzminister** nunmehr für das Landesnetz, das Sprachnetz, die Mailprovider-Funktion, den Verzeichnisdienst, den Internet-Übergang (Firewall), den landesweiten Dienst zur Verschlüsselung und zur elektronischen Unterschrift (PKI) und für alle anderen IT-Maßnahmen, die Ressortgrenzen überschreiten, **zuständig** und damit **verantwortlich** ist. Die IT-Kommission wird zwar weiterhin das Beratungsgremium für Konzepte bleiben, die problematischen Rahmen- und Anschlussbedingungen haben aber ihre Bedeutung verloren und werden nach Aussagen des Finanzministeriums demnächst durch Erlasse ersetzt werden.

Aus datenschutzrechtlicher Sicht hat diese Veränderung eine außerordentliche Bedeutung für die „Evolution“ der automatisierten personenbezogenen Datenverarbeitung in der Landesverwaltung. Die Grenzen der rechtlichen und sicherheitstechnischen **Verantwortungsbereiche** sind damit **eindeutig festgelegt**. Für viele Verarbeitungsprozesse, die bisher in einer Grauzone lagen, ist nunmehr der Finanzminister die Daten verarbeitende Stelle. Werden externe Dienstleister wie z. B. die dataport eingeschaltet, gibt es keine Gemengelage bezüglich der Auftraggebereigenschaft mehr. Die Leistungsbeschreibungen und Sicherheitskonzepte für diejenigen Standards, Hard- und Softwarekomponenten und Verfahrensabläufe, die zwar von den Ressorts genutzt, aber vom Finanzminister verantwortet werden, haben nicht mehr den Charakter eines gemeinsamen (freiwillig zu beach-

tenden) Codex, sondern sind für alle verbindliche Definitionen. Erstmals können auch in diesem Bereich die Ordnungsmäßigkeitsvorschriften des Landesdatenschutzgesetzes und der Datenschutzverordnung (Test, Freigabe, Dokumentation) „trennscharf“ eingehalten werden.

Noch sind allerdings viele Dinge auseinander zu sortieren. Wie die einzelnen Verwaltungsbereiche mit welchen anderen kommunizieren, verantworten sie selbst. Insoweit können die Aufsichtsfunktionen des Finanzministeriums beim Landesnetz verschlankt werden. Das Prinzip der Sicherheitschecks durch „zufällig“ zusammengestellte Teams wird man grundsätzlich überdenken müssen. Es stellt sich auch die Frage, ob das derzeitige Domänenmodell unter den neuen Gegebenheiten Bestand haben kann. Schließlich sind die Infrastrukturprobleme für einen landeseinheitlichen Verschlüsselungs- und Signaturdienst erst ansatzweise gelöst. Ein besonderes Augenmerk wird man auch auf die Frage richten müssen, welche E-Government-Angebote als ressortübergreifend und welche als ressortintern angesehen werden müssen. All dies sind keine „akademischen Sandkastenspiele“, sondern führen unmittelbar zu **konkreten datenschutzrechtlichen Konsequenzen** (Vergabe von Zugriffs- und Änderungsrechten, Erfüllung von Löschungspflichten usw.) und zu sicherheitstechnischen Maßnahmen (eindeutige Authentifizierung, Abschottung von Datenbeständen, Virenabwehr, Schutz der Administrationsebene usw.).

Was ist zu tun?
Die Konsequenzen aus der neuen IT-Aufbauorganisation müssen kurzfristig sichtbar gemacht werden. Die Ordnungsmäßigkeitskriterien des Datenschutzrechts können dabei Hilfestellungen geben. Nur transparente Verarbeitungsprozesse gewährleisten das notwendige Maß an Korrektheit, Sicherheit und Revisionsfähigkeit.

6.6 Land und Kommunen bauen ein großes Computernetz

Wenn die zwischen dem Land und den Kommunen geschlossene E-Government-Vereinbarung in die Praxis umgesetzt worden ist, werden insgesamt ca. 30.000 IT-Arbeitsplätze miteinander vernetzt bzw. vernetzbar sein. Das hierfür erforderliche Sicherheitskonzept muss noch erarbeitet werden.

In der Vergangenheit haben die Kommunen untereinander und mit den Landesbehörden auf ganz konventionelle Weise (per Brief, per Telefon, per Fax) kommuniziert, ohne dass es zu schwerwiegenden Problemen gekommen ist. In jüngster Zeit wird zunehmend auch vom Datenträgeraustausch (Disketten, CD-ROM, USB-Sticks) Gebrauch gemacht und das Internet genutzt, obwohl die mit Letzterem im Zusammenhang stehenden Sicherheitsprobleme nur von wenigen Behörden hinreichend gelöst worden sind (vgl. 24. TB, Tz. 7.1).

Im Zusammenhang mit den **E-Government-Strategien** der Verwaltung wird nun angestrebt, das Landesnetz, die Kommunikationsplattform für die Landesbehörden, auch dem kommunalen Bereich zu öffnen. Hierüber besteht seit Ende 2003 eine Absichtserklärung zwischen dem Land und den kommunalen Landesverbänden. In ihr sind u. a. folgende datenschutzrechtlich relevante Zielsetzungen festgelegt:

- Aufbau einer leistungsfähigen und sicheren technischen Infrastruktur, die von Land und Kommunen unter denselben Bedingungen genutzt werden kann,
- Aufbau von landesweit standardisierten Kreisnetzen als integraler Bestandteil des landesweiten Datennetzes,
- Anschluss der Kommunalverwaltungen an das landesweite Datennetz über die Landesnetzanschlüsse der Kreise als untere Landesbehörden,
- Aufbau eines landesweit wirksamen Verzeichnisdienstes,
- Aufbau einer landesweit einheitlichen Public-Key-Infrastruktur mit digitaler Signatur und Ver- und Entschlüsselungsfunktionen für Datenströme,

> **? *E-Government***
>
> *Der Begriff E-Government – zusammengesetzt aus den beiden Wörtern „electronic" (deutsch: elektronisch, rechnergestützt) und „Government" (deutsch: Verwaltung, Regierung) – bezeichnet die Bemühungen der öffentlichen Verwaltung, ihre Aufgaben und die darauf bezogenen Verwaltungsabläufe mittels der modernen Informations- und Kommunikationstechnologie zu erfüllen. Dabei steht die Nutzung des World Wide Web, also des Internets, häufig als Medium im Mittelpunkt der Betrachtung. E-Government ist gleichsam ein Synonym für die Modernisierung der überkommenen aktendominierten Verwaltung.*

- Aufbau einer zentralen technischen Plattform (Datendrehscheibe) für die Steuerung von landesweiten und bundesweiten Datenströmen aus Anwendungen,
- Aufbau einer Zahlungsplattform für Verwaltungsdienstleistungen.

Wenn diese E-Government-Vereinbarung umgesetzt ist, wird ein Zustand erreicht sein, in dem die Rechnersysteme aller Landes- und Kommunalbehörden miteinander vernetzt bzw. vernetzbar sind. Vom Sicherheitsniveau her ist damit ein **Quantensprung** bezüglich des Anforderungsprofils an die Abschottungs- und Steuerungsmechanismen verbunden. Man darf nämlich nicht übersehen, dass E-Government nicht bedeutet, dass die rechtlichen und Verantwortungsgrenzen zwischen den einzelnen Behörden eingerissen werden. In der Vereinbarung wird richtig festgestellt, dass die geplanten Maßnahmen kein Selbstzweck sind, sondern (nur) die Qualität der Leistungen der öffentlichen Verwaltungen in Schleswig-Holstein verbessern sollen.

Aus **datenschutzrechtlicher** und **sicherheitstechnischer** Sicht ist noch eine Vielzahl von **Vorbedingungen** zu erfüllen, bevor das geplante „Supernetz" in den Echtbetrieb gehen kann. Hierzu gehören z. B. die Lösung folgender noch offener Probleme:

- Die **Betreiberzuständigkeit/-verantwortung** für das Landesnetz ist erst kürzlich von der Landesregierung dem Finanzministerium übertragen worden, da die bisherigen Vereinbarungen zwischen den Ressorts sich nicht als tragfähig erwiesen haben (vgl. Tz. 7.4). Da das Finanzministerium die Kommunen nicht wie Landesbehörden im Erlasswege anweisen kann, sich „landesnetzkonform" zu verhalten, wird es für diesen Bereich Verträge und ihnen zugrunde liegende Leistungsbeschreibungen geben müssen. Datenschutzrechtlich wird das Finanz-

ministerium den Kommunen gegenüber als weisungs/-vertragsgebundener Auftragnehmer agieren.

- Besonders wichtig ist dabei die Frage, ob alle 237 kommunalen Verwaltungseinheiten, die potenziell das Landesnetz nutzen werden, direkt in vertragliche Beziehungen zum Finanzministerium treten. Da man die Kreisnetze als integralen Bestandteil des neuen Netzes ansieht, könnte auch ein **zweistufiges Modell** realisiert werden: Das Landesnetz öffnet sich nur den Kreisen und kreisfreien Städten, die Kreise übernehmen den Betrieb der kreisinternen Kommunikation mit ihren Kommunen über eigene, vom Landesnetz unabhängige Netze. Die kreisübergreifende Kommunikation würde über den Umweg des Landesnetzes erfolgen.

- Da die **Kreise** keine eigene Zuständigkeit für den Betrieb von Kreisnetzen besitzen, können auch sie den kreisangehörigen Kommunen gegenüber nur als weisungs/-vertragsgebundene **Auftragnehmer** auftreten. Die dafür erforderlichen schriftlichen Verträge müssen die sicherheitstechnischen Schnittstellen zwischen den lokalen Netzen der Kommunen und dem Netzwerk der Kreise eindeutig definieren.

- Das Landesnetz hat bisher eine Struktur, die ausschließlich auf die Organisation der Ministerien mit ihren nachgeordneten Behörden zugeschnitten ist. Bereits der Anschluss der Kreise und kreisfreien Städte käme einer Erweiterung um **15 „Ministerien“** gleich. Es bedarf sehr sorgfältiger Prüfungen, ob dies mittels des bisher praktizierten Konzeptes der „geschlossenen Benutzergruppen“ abgebildet werden kann. Ein Einzelanschluss für jede Kommune würde dieses Konzept mit Sicherheit sprengen.

- Nach den Standardisierungsregeln des Landes wird der Verzeichnisdienst auf der Basis des „Active Directory“ der Firma Microsoft realisiert. Wenn in ihm künftig 237 selbstständige Organisationseinheiten der Kommunen und alle bereits jetzt erfassten Landesbehörden mit ihren ca. 30.000 Arbeitsplatzsystemen gemeinsam verwaltet werden sollen, stellt sich das Problem, wer ein **zentrales Management** verantwortet und wer es kontrolliert. Sicherheitstechnisch wäre ein ausschließlich dezentrales Management vorzuziehen. Entsprechende Modelle gibt es in anderen Bundesländern. Die Entscheidung, wer in einer Kommune in welchem Umfang mit einer der anderen Kommunen des betreffenden Kreises, mit dem Kreis selbst, mit Kommunen in anderen Kreisen, mit welchen Behörden des Landes, anderer Länder oder des Bundes, sonstigen öffentlichen oder nichtöffentlichen Stellen (über das Internet) kommunizieren darf, wird man nämlich auch weiterhin den verantwortlichen Bürgermeistern bzw. leitenden Verwaltungsbeamten überlassen müssen.

- Die Verschlüsselung von Daten auf der Grundlage einer **Public-Key-Infrastruktur** dürfte auch landesweit ohne größere Schwierigkeiten möglich sein. Die bisherigen handschriftlichen Unterschriften und Namenszeichen der Mitarbeiterinnen und Mitarbeiter fälschungssicher und revisionsfähig durch elektronische Unterschriften zu ersetzen bedeutet aber, dass sich alle Behörden zu einem signaturgesetzkonformen Verfahren verpflichten müssen. Nur auf diesem Sicherheitsniveau wird es möglich sein, die Mitarbeiterinnen und Mitarbeiter zur Nutzung der elektronischen Unterschrift zu verpflichten.

- Die geplante **Datendrehscheibe** wird mit hoher Wahrscheinlichkeit größere Datenbestände mit personenbezogenem Inhalt zu speichern haben. Da es hierfür keine originäre Zuständigkeit gibt, bedarf es entsprechender vertraglicher Vereinbarungen mit einer Institution, die Behördencharakter hat. Deren Sicherheitsmaßnahmen müssen transparent sein und von allen Beteiligten akzeptiert werden.

Die vorgenannten Datenschutzgesichtspunkte beziehen sich im Wesentlichen auf **Vertraulichkeitsaspekte**. In das noch zu erarbeitende IT-Gesamtkonzept und das daraus abzuleitende Sicherheitskonzept sind zusätzlich auch die Aspekte der **Verfügbarkeit** und der **Integrität** des Gesamtsystems einzuarbeiten. Alles zusammen ist dies eine Aufgabe, die nicht ohne gründliche Vorarbeiten bewältigt werden kann.

Was ist zu tun?
Die Konstrukteure des neuen Supernetzes sollten von der Möglichkeit Gebrauch machen, bereits das IT-Konzept und das Sicherheitskonzept einem Audit nach dem LDSG zu unterziehen. Dazu ist es dienlich, das ULD schon frühzeitig über die konkreten Absichten und Lösungsansätze zu informieren.

6.7 Prüfungen im Bereich Systemdatenschutz

Als Folge der Umstellung der Betriebssysteme in den Daten verarbeitenden Stellen mussten auch unsere Prüfungsteams ihr Wissen um deren Funktionalitäten und Sicherheitsschwächen und -stärken auf den neuesten Stand bringen. Dies war bei uns eine ebenso zeitaufwändige Maßnahme wie in den IT-Stellen der Behörden im Lande. Die dabei gewonnenen Erkenntnisse konnten allerdings bei der Erarbeitung eines backUP-Magazins verarbeitet werden.

Insgesamt mussten also die Prüfungsaktivitäten im Bereich Systemdatenschutz im Jahre 2003 vorübergehend etwas zurückgefahren werden. Diese Phase ist jedoch zwischenzeitlich durch den Start eines neuen Projektes beendet worden. Seit Ende 2003 wird durch ein darauf spezialisiertes Team daran gearbeitet, in absehbarer Zeit eine **Flächendeckung** unserer Kontrollen **im kommunalen Bereich** zu erreichen. Es sollen in nächster Zeit alle 237 Organisationseinheiten mindestens einmal einem Sicherheitscheck unterzogen werden. Dahinter steht die Überlegung, dass die weit überwiegende Mehrzahl der Behördenleiter und IT-Betreuer derartige Kontrollen auch dann begrüßt, wenn es Gründe für Beanstandungen gibt. Für die Verantwortlichen wird nämlich deutlich, in welchen Teilbereichen die realisierten Sicherheitsmaßnahmen ausreichend sind und mit welchen Prioritäten welche Defizite abzubauen sind. Vereinfacht formuliert: Eine Kommune, deren Sicherheitskonzept überprüft worden ist, ist besser dran als diejenige, die noch gar keinen Besuch vom ULD hatte. Diese „Ungleichbehandlung“ gilt es so zügig wie möglich abzubauen.

Neben diesen Routineprüfungen (die in der Regel nicht zu spektakulären Ergebnissen führen) wird es aber auch in Zukunft Kontrollen geben, in denen **grundsätzlichen Sicherheitsproblemen** nachgegangen wird. Die Ergebnisse derartiger Prüfungsmaßnahmen sind nachfolgend dargestellt.

6.7.1 Nach wie vor unsicheres Krankenhausinformationssystem in Itzehoe

Das Krankenhaus Itzehoe nimmt eine unrühmliche Spitzenstellung bezüglich der bei Prüfungen festgestellten Datensicherheitsmängel ein. Mit deren Bereinigung lässt sich diese kommunale Einrichtung viel zu viel Zeit.

Nachdem die Kontrollen im Zweckverbandskrankenhaus Itzehoe gleich zu Beginn eklatante Sicherheitsdefizite in Bezug auf die Zugriffsrechte externer Dienstleister aufgedeckt haben und diese durch das Krankenhaus unverzüglich bereinigt wurden (vgl. 25. TB, Tz. 7.4.1), bestand die Hoffnung, dass im weiteren Verlauf der Prüfung nicht noch mehr derartig gravierende sicherheitstechnische Schwachstellen zutage treten würden. Diese Hoffnung hat sich leider nicht erfüllt. Am Ende der Prüfungsmaßnahme umfasste der **Beanstandungskatalog** mehr als **70 Positionen**. Das hat es in den mehr als 20 Jahren, in denen Krankenhäuser und Stellen mit ähnlich sicherheitskritischen Datenverarbeitungsprozessen geprüft werden, noch nicht gegeben. Die wichtigsten Verstöße gegen die Sicherheitsvorschriften des Landesdatenschutzgesetzes und der Datenschutzverordnung sind:

- Das Krankenhaus verfügt weder über ein in sich geschlossenes IT-Konzept noch über ein Sicherheitskonzept als Grundlage für konkrete technische und organisatorische Maßnahmen.
- Die Administratoren und die Benutzer der IT-Systeme arbeiten ohne ausreichende Dienstanweisungen bzw. Benutzerhandbücher.
- Es ist nicht möglich, sich eine verlässliche Übersicht darüber zu verschaffen, welche Verarbeitungsprozesse auf welchen Rechnersystemen ablaufen.
- Seitens der Krankenhausleitung bestehen keine Vorgaben für die Zuweisung von Zugriffsrechten auf Patientendaten.
- Störungs- und Fehlermeldungen werden nicht auswertbar protokolliert.
- Die Dokumentation der eingesetzten Datenbanken ist nicht ausreichend.
- Für die Internet-Nutzung bestehen keine Vorgaben, die Absicherung ist unzureichend.
- Die E-Mail-Kommunikation mit sensiblen Daten erfolgt unverschlüsselt.
- Die Arbeit der Administratoren wird von der Leitungsebene des Krankenhauses nicht überwacht.
- Die Verwaltung der Benutzerkonten erfolgt ohne eine nachvollziehbare Struktur.
- Die tatsächlich vergebenen Zugriffsrechte sind nicht nachvollziehbar dokumentiert.

- Elektronische Arztbriefe sind nicht hinreichend gegen unbefugte Zugriffe geschützt.
- Die Mitarbeiter der EDV-Abteilung haben einen uneingeschränkten Zugriff auf medizinische Datenbestände.
- Passwörter werden über Jahre hinweg nicht geändert.
- Auf Notebooks werden medizinische Daten unverschlüsselt gespeichert.
- Der Einsatz des Verfahrens „SAP R/3“ ist nicht revisionsfähig dokumentiert, einige Mitarbeiter haben eindeutig zu weit reichende Zugriffsrechte.
- Die Telekommunikationsanlage ist nicht ausreichend abgesichert.
- Die Datenbestände über die Patienten der zur Privatliquidation berechtigten Krankenhausärzte stehen im allgemeinen Zugriff der Krankenhausmitarbeiter.
- Die Controllingabteilung hat einen permanenten und umfassenden Zugriff auf die medizinischen Datenbestände.
- Laborergebnisse stehen allen Mitarbeitern des medizinischen Bereiches zur Verfügung.
- Vom Schulungsraum aus sind Zugriffe auf Echtdaten möglich.

Es bedarf keiner näheren Begründung dafür, dass es sich hierbei um erhebliche Sicherheitsmängel handelt. Dem hat die Krankenhausleitung in den Erörterungen der Prüfungsergebnisse auch nicht widersprochen. Die Tatsache, dass der vorstehende Mängelkatalog auch viele Monate nach Abschluss der Prüfung noch im Präsens formuliert ist, weist darauf hin, dass die **Defizite bisher noch nicht abgestellt** sind. Gründe hierfür sind uns nicht genannt worden. Es liegt uns noch nicht einmal eine abschließende schriftliche Stellungnahme der Krankenhausleitung vor. Ende 2003 ist uns im Zusammenhang mit der Beschwerde eines Patienten zu einem anderen Sachverhalt lediglich mitgeteilt worden, dass eine externe Datenschutzberaterin damit beauftragt worden ist, einen Plan zu machen, welche Maßnahmen vorrangig in Angriff zu nehmen sind. Dies ist zwar ein Lichtblick, aber noch keine Lösung. Fakt bleibt, dass das Krankenhaus Itzehoe damit datenschutzrechtlich und sicherheitstechnisch als „weniger empfehlenswert“ einzustufen ist.

Was ist zu tun?
Es dürfte der Zeitpunkt erreicht sein, an dem sich endlich der Landrat des Kreises Steinburg und der Bürgermeister der Stadt Itzehoe als Repräsentanten des Zweckverbandes der Sache annehmen müssen.

6.7.2 Wissenschaftliche Auswertung des Krebsregisters

Nach der Vertrauensstelle des Krebsregisters bei der Ärztekammer ist auch die Registerstelle selbst überprüft worden. Es gab keine Anhaltspunkte dafür, dass medizinische Daten in unbefugte Hände gelangt sind. Eine Reihe von kleineren Sicherheitsmängeln wurden zwischenzeitlich abgestellt.

Im Jahr 2002 haben wir begonnen, die Sicherheitsmaßnahmen im Zusammenhang mit der Verarbeitung der medizinischen Daten des schleswig-holsteinischen Krebsregisters zu durchleuchten. Da die Datenverarbeitungsprozesse nacheinander zunächst in der Vertrauensstelle bei der Ärztekammer und dann in der Registerstelle des Instituts für Krebsepidemiologie an der Medizinischen Universität Lübeck ablaufen, entsprach auch die **Gesamtprüfungsmaßnahme** dieser Reihenfolge. Die Kontrollen bei der Vertrauensstelle haben keine wesentlichen Beanstandungen ergeben (vgl. 25. TB, Tz. 7.4.3).

Die **Registerstelle** arbeitet überwiegend mit anonymisiertem Datenmaterial. Allerdings sieht das Krebsregister vor, dass bei entsprechenden Einwilligungen der Patienten die Vertrauensstelle für bestimmte Forschungszwecke der Registerstelle die personenbezogenen Informationen zu den epidemiologischen Datensätzen bereitstellen darf. Über diese Vorgänge ist das ULD zu informieren. Für unsere Prüfung konnten wir deshalb einen Zeitpunkt wählen, zu dem in der Registerstelle ein entsprechendes Forschungsvorhaben lief und damit ein sehr hohes Sicherheitsniveau erforderlich war.

Dabei zeigte sich, dass die Verfahrensweise des Instituts nicht in allen Punkten dem Krebsregistergesetz entsprach. Die **wichtigsten Sicherheitsmängel**:

- Um eine nicht ausdrücklich von den Patienten genehmigte Verkettung von personenbezogenen Datensätzen über mehrere Forschungsmaßnahmen hinweg zu verhindern, schreibt das Gesetz vor, dass projektbezogene Identitätsnummern zu vergeben sind. Dies war im konkreten Fall nicht geschehen.
- Im Sicherheitskonzept waren nicht alle tatsächlich eingesetzten IT-Systeme erfasst.
- Die Löschfristen wurden nicht exakt eingehalten.
- Die Arbeitsplatzrechner waren nicht so konsequent gesichert, wie es der Sensibilität der verarbeitenden Daten entsprochen hätte.
- Die Zugriffsrechte hätten spezifischer/restriktiver ausgestaltet werden können.

Trotz dieser Beanstandungen kann die Prüfung aus zwei Gründen als ein Erfolg angesehen werden. Es haben sich keine Anhaltspunkte dafür ergeben, dass die Vertraulichkeit der der Registerstelle anvertrauten personenbezogenen Daten tatsächlich verletzt worden ist. Die oben angeführten Schwachstellen sind vom Institut für Krebsepidemiologie unverzüglich abgestellt worden.

Was ist zu tun?
Um das Vertrauen der Patienten in das Krebsregister zu stärken und den Anforderungen des Krebsregistergesetzes gerecht zu werden, sollte die Registerstelle während der Durchführung personenbezogener Forschungsvorhaben ein Höchstmaß an Datensicherheit gewährleisten.

6.7.3 EDV aus der Steckdose – nicht ohne Risiko

Ein seit längerem schwebendes datenschutzrechtliches Problem mit einem Angebot der Datenzentrale (jetzt dataport) ist durch eine Prüfung konkret zutage getreten. Die Situation ist allerdings paradox: Der Kunde ist zufrieden, obwohl er gegen das Landesdatenschutzgesetz verstößt.

Es hätte eigentlich eine der vielen **Routinesicherheitsüberprüfungen** in einer kleineren Amtsverwaltung im Lande werden sollen. Konfrontiert wurden wir aber mit einer IT-Organisation, die eine Reihe von Grundsatzfragen aufwirft, die bereits im 23. TB (Tz. 7.2) problematisiert worden sind: Es geht dabei um die vollständige Auslagerung der IT-Administration auf einen externen Dienstleister. Der leitende Verwaltungsbeamte der betreffenden Amtsverwaltung stand vor dem Problem, für die Administration des neu zu installierenden IT-Systems keinen geeigneten Mitarbeiter zur Verfügung zu haben. Bei einem Mitarbeiterstab von 17 Personen war das nicht verwunderlich. Da kam ihm ein Angebot der Datenzentrale recht, alle Administrationsaktivitäten zu übernehmen, die Rechner in der Datenzentrale in einer so genannten Server-Farm zu installieren und die Behörde nur mit Terminals ohne jede Betriebssystemfunktionalität auszurüsten (Terminal-Server-Lösung „DZ.net“).

Durch dieses „**Application-Hosting**“ erfolgt ein Rundumservice bezogen auf die Administration, den Support, den Verfahrensbetrieb und die Bereitstellung von Rechenzentrumsressourcen. Der fatale Nebeneffekt derartiger Konstruktionen besteht darin, dass der verantwortliche Betreiber des Systems faktisch keinerlei Kontrollmöglichkeiten bezüglich der korrekten Arbeitsweise seines externen Dienstleisters besitzt. Das Einspielen neuer Softwareversionen, das Eröffnen von Benutzerkonten, das Zuweisen von Zugriffs- und Änderungsrechten usw. erfolgen nach dem Prinzip: Wenn das Vertrauen ausreichend ist, braucht man keine Kontrollen.

Die Amtsverwaltung war sich dieser Tatsache bewusst, sah es aber als das **kleinere Übel** gegenüber dem Aufbau einer eigenen Systemadministration an. Da beeindruckte auch unser Hinweis auf die Verstöße gegen die datenschutzgesetzlichen Regelungen über die Auftragsdatenverarbeitung (z. B. Pflicht zur Erteilung schriftlicher Vorgaben und Kontrolle deren Einhaltung) wenig. Selbst als im Rahmen der Prüfung deutlich wurde, dass die vertraglichen Vereinbarungen zwischen der Amtsverwaltung und der Datenzentrale in sich nicht konsistent waren und die Amtsverwaltung nicht einmal über alle Vertragsbestandteile verfügte, wurde dies mit dem Hinweis darauf, dass doch die Datenverarbeitung reibungslos funktioniere, relativiert, Beanstandungen in unserem Prüfungsbericht hin, Beanstandungen her.

Uns stellte sich die Frage: Wenn denn der Auftraggeber mit den Leistungen seines Auftragnehmers zufrieden ist, kann man dann den Auftragnehmer schelten? Wir haben deshalb der von uns geprüften Kommune empfohlen, ihren externen Dienstleister mit unseren Beanstandungen zu konfrontieren und **Abhilfe** zu fordern. Das ist zwischenzeitlich geschehen. Die Antwort von dataport steht aber noch aus.

Was ist zu tun?
Da es eine Reihe technischer und organisatorischer Lösungsmöglichkeiten gibt, die Kontrollmöglichkeiten der verantwortlichen Stellen zu verbessern, sollte dataport bestrebt sein, sie anzubieten. Es kann nicht im Interesse der Beteiligten liegen, dass auf Dauer gegen geltendes Recht verstoßen wird.

7 Recht und Technik der neuen Medien

7.1 Novellierung des Telekommunikationsgesetzes

Aufgrund mehrerer neuer EG-Richtlinien muss der Bundesgesetzgeber das Telekommunikationsgesetz (TKG) novellieren. Betroffen von den neuen europäischen Direktiven sind auch die Datenschutzregelungen. Während die Bundesregierung eine Strategie der „kleinen" Verschlechterungen verfolgt, hat sich der Bundesrat für die Einführung einer massiven Vorratsspeicherung von Verbindungsdaten ausgesprochen. Eine ganz andere Linie haben die Experten aus Wirtschaft und Datenschutz in einer Sachverständigenanhörung am 9. Februar 2004 eingeschlagen: Zusammenlegung des Teledienste- und Mediendienstedatenschutzes, keine Vorratsdatenspeicherung!

Die Ausgangslage ist an sich günstig. Ein ganzes Richtlinienpaket der Europäischen Union, darunter auch eine Richtlinie über den Datenschutz für elektronische Kommunikationsdienste (2002/58/EG), macht eine Revision des nationalen Telekommunikationsgesetzes (TKG) erforderlich. Die Bundesregierung hätte diese Chancen nutzen können, um einen Webfehler der Datenschutzgesetzgebung aus den Jahren 1996 und 1997 zu beheben und die Datenschutzregelungen für TK-Dienste sowie für Telemedien in einer Regelung zusammenzufassen. Alle reden von **Konvergenz und Bürokratieabbau**: Warum nicht im Datenschutzrecht anfangen? Diensteanbietern und Bürgern wäre mit einem einheitlichen und schlanken Datenschutzrecht für die elektronischen Basisdienste der Informationsgesellschaft allemal gedient.

Bundesregierung und Bundestag haben sich jedoch nur zu einer „**kleinen Lösung**" durchringen können: Immerhin sind nun die Regelungen des TK-Datenschutzes und der einschlägigen Rechtsverordnung (TDSV) in *einer* gesetzlichen Regelung zusammengefasst. Spötter behaupten, zu mehr habe es nicht gelangt, weil der Bundeswirtschaftsminister die beiden für den Datenschutz in Telediensten und TK-Datenschutz zuständigen Referate nicht habe zusammenlegen können: Sie gehören zwei unterschiedlichen Unterabteilungen an. Darüber hinaus weist der am 13. März 2004 vom Bundestag beschlossene Gesetzentwurf eine Reihe von **Verschlechterungen für den Datenschutz** auf:

Noch geltendes Recht ist, dass der Nutzer für den Umgang mit seinen Verbindungsdaten zwischen **drei Möglichkeiten** wählen kann, nämlich einer vollständigen Speicherung der Zielnummern, einer verkürzten Speicherung um die letzten drei Ziffern oder einer sofortigen Löschung. Dabei bleibt es auch. Aber anders als in der Vergangenheit soll der **Normalfall** künftig in der **vollständigen Speicherung** ohne Kürzung bestehen. Das bedeutet für den Nutzer: Nur wenn er aktiv eine andere Wahl trifft, kommt es zur verkürzten Speicherung oder zur vollständigen Löschung. Der Normalfall ist also gerade nicht die datensparsame Lösungsvariante, was letztlich im Interesse der an einem umfassenden Zugriff interessierten Sicherheitsbehörden ist. Zu befürchten ist, dass die datenschutzfreundliche Lösung nur auf die wenigen Nutzer beschränkt bleibt, die in Kenntnis der komplizierten Regelung eine entsprechende Wahl treffen.

Eine weitere gravierende Verschlechterung bedeutet die Aufweichung des bislang geltenden strikten Einwilligungsprinzips für Zwecke der Werbung und Marktforschung. Nach der nun vom Bundestag beschlossenen Regelung dürfen die Diensteanbieter Adressdaten ihrer Kunden – wie die Rufnummer, die Postanschrift und die E-Mail-Adresse – „im Rahmen einer bestehenden Kundenbeziehung“ zur **Beratung**, zur **Werbung für eigene Angebote** und zur **Marktforschung** verwenden. Während bislang Voraussetzung einer solchen Nutzung die konkrete Einwilligung des Teilnehmers war, sind seine Rechte nunmehr auf ein **Widerspruchsrecht** beschränkt.

Einige zunächst vorgesehene **Verschlechterungen** wurden in den Gesetzesberatungen auch auf Intervention der Datenschutzbeauftragten des Bundes und der Länder noch **revidiert**. So bleibt das so genannte „Koppelungsverbot“ erhalten, das den Kunden davor schützt, dass die Leistungserbringung von seiner Einwilligung in eine Datenverarbeitung zu anderen Zwecken abhängig gemacht wird. Schließlich wird auch die Statistik über die Zahl der angeordneten strafprozessualen Überwachungsmaßnahmen entgegen früheren Plänen nicht abgeschafft.

Die besseren Argumente haben sich in den parlamentarischen Gesetzesberatungen zudem an zwei Punkten durchgesetzt: So unterliegen in Zukunft auch Passwörter, PINs und PUKs (Personal Unblocking Key), mit denen die Inhalte und Umstände der Telekommunikation geschützt werden, dem Schutz des Fernmeldegeheimnisses. Bedeutsam ist diese Regelung beispielsweise für den Schutz der auf einer Mailbox hinterlegten Informationen, die der Teilnehmer mithilfe eines Passwortes „von außen“ abrufen kann. Für den Zugriff auf diesen „Schlüssel“ zur vertraulichen Kommunikation wird in Zukunft also ebenso der Richtervorbehalt gelten wie für den Zugriff auf die Inhalte und näheren Umstände der Telekommunikation.

Erfreulich aus Sicht des Datenschutzes ist die Entscheidung des Bundestages, die Anbieter von **Prepaid-Produkten** von der Verpflichtung auszunehmen, Bestandsdaten ihrer Kunden auf Vorrat speichern zu müssen. Diese Regelung folgt Vorgaben des **Bundesverwaltungsgerichts**, das Ende 2003 anders lautende Vorgaben der Regulierungsbehörde für rechtswidrig erklärt hatte. Zu begrüßen ist diese Entscheidung, weil den Teilnehmern ohne eine Registrierungspflicht der Prepaid-Produkte anonyme und damit datensparsame Kommunikationsmöglichkeiten eröffnet werden. Dass sich Straftäter einer Identifizierung ihrer Mobilfunkkommunikation entziehen, indem sie Prepaid-Karten Dritter verwenden, kann durch eine generelle Identifizierungspflicht beim erstmaligen Kauf einer solchen Karte nicht erfolgreich verhindert werden.

Im noch laufenden Gesetzgebungsverfahren hatte sich der Bundesrat mit der Einführung einer **Vorratsspeicherung für Verbindungsdaten** in Höhe von sechs Monaten ausgesprochen. Die Bundesregierung war diesem Vorschlag bislang nur halbherzig entgegengetreten und hatte auf die weiteren Beratungen im parlamentarischen Verfahren verwiesen. Der Bundestag ist dem Vorschlag des Bundesrates jedenfalls nicht gefolgt. Jedem muss klar sein, dass die Einführung einer Vorratsspeicherung allein zu dem Zweck, sie für mögliche Zugriffe der Sicherheitsbehörden verfügbar zu halten, einen gravierenden Verstoß gegen das vom Bundesverfassungsgericht statuierte **Verbot der Vorratsspeicherung** darstellt. Der bloße

Verweis auf die gesetzlichen Aufgaben der unterschiedlichen Sicherheitsbehörden ist als Rechtfertigung eines solchen Eingriffes nicht ausreichend, da es an einer hinreichenden Konkretisierung der einzelnen Zwecke fehlt.

Unterstützung kommt auch vonseiten der TK-Diensteanbieter, deren Branchenverband BITKOM gegenüber dem Deutschen Bundestag darauf hingewiesen hat, dass die massenhafte Speicherung von Verbindungsdaten einer überwältigenden Mehrheit unbescholtener Bürger in keinem Verhältnis zu einem möglichen Sicherheitsgewinn steht. Die einschlägige Klientel organisierter oder terroristischer Kriminalität werde die Vorratsspeicherung ohnehin unterlaufen. Vor diesem Hintergrund ist es wenig überraschend, dass sich **Diensteanbieter** und **Datenschutz gemeinsam** gegen eine Verschärfung der sicherheitsrechtlich motivierten Regelungen ausgesprochen haben. Das Gesetzgebungsverfahren ist noch nicht abgeschlossen. Mit einem Vermittlungsverfahren zwischen Bundestag und Bundesrat im Mai 2004 wird allgemein gerechnet.

Was ist zu tun?
Schleswig-Holstein sollte sich im Bundesrat gegen die vorgesehenen Verschlechterungen im Datenschutz aussprechen und für eine Zusammenführung von TK-Datenschutz und Telemediendatenschutz eintreten. Die Bürgerinnen und Bürger sollten sich gegen die geplante Datenschnüffelei im Internet wehren.

7.2 Rundfunkgebühren und Datenschutz – Ein unlösbarer Widerspruch?

Beim Einzug der Rundfunkgebühren gibt es Ärger wegen diverser Datenschutzverstöße. Es ist an der Zeit, über datenschutzgerechte Varianten der Rundfunkfinanzierung nachzudenken.

Obwohl wir keine eigene Zuständigkeit für die Kontrolle der Datenverarbeitung zur Erhebung der Rundfunkgebühren besitzen, beschäftigte uns dieser Komplex im Berichtszeitraum erneut in unterschiedlichen Konstellationen. Im Frühjahr 2003 wurde ein interner Entwurf zur **Änderung** des zwischen den Bundesländern abgeschlossenen **Rundfunkgebührenstaatsvertrages** bekannt. Hintergrund ist, dass auf der einen Seite die Rundfunkanstalten einen kontinuierlich steigenden Finanzbedarf melden. Auf der anderen Seite wird es zurzeit offenbar für untunlich gehalten, die Rundfunkgebühren anzuheben. Um dieses Dilemma zu lösen, wird versucht, die Ausschöpfungsquote bei der Gebührenerhebung zu steigern.

Aus Datenschutzsicht sah der vorgelegte Entwurf **erhebliche Verschlechterungen** vor. So war geplant, in noch weiterem Umfang als bisher auf die Daten der Meldebehörden zuzugreifen. Zwar findet bereits heute bei jedem melderelevanten Vorgang eine Datenübermittlung an die GEZ statt. Zusätzlich sollte jedoch, um auf einen Schlag alle Meldepflichtigen identifizieren und mit dem Bestand der Gebührenzahler bei der GEZ abgleichen zu können, eine Vorschrift eingeführt werden, wonach die Meldebehörden zu einem bestimmten Stichtag verpflichtet gewesen wären, alle über 16-jährigen Personen in Deutschland an die GEZ zu melden. Der allergrößte Teil dieser Datenübermittlungen wäre nicht erforderlich gewesen, weil die betroffenen Personen entweder bereits Gebührenzahler sind oder für sie keine Gebührenpflicht besteht.

Obwohl als gewisse Erleichterung geplant war, nur noch ein Rundfunkgerät pro Wohnung als gebührenpflichtig anzusehen, sollten alle gemeldeten erwachsenen Bewohner zur Auskunft über alle Umstände, die gebührenrelevant sind, verpflichtet sein. Dies sollte selbst dann gelten, wenn keine Anhaltspunkte für eine Gebührenpflicht bestanden. Darüber hinaus war geplant, dass **weitere öffentliche Register** Veränderungen unmittelbar an die GEZ melden sollten. Dies betraf beispielsweise die berufsständischen Kammern, die Schuldnerverzeichnisse oder das Gewerbezentralregister. Die GEZ sollte auf diese Daten auch online zugreifen dürfen. Weiterhin sollte die bisher von den Datenschutzbeauftragten als rechtswidrig bezeichnete Praxis, wonach die so genannten **Gebührenbeauftragten** ohne Wissen der Betroffenen bei Dritten, beispielsweise bei Nachbarn, Daten erheben, ausdrücklich erlaubt werden. Die Datenschutzbeauftragten des Bundes und der Länder wandten sich in einer Entschließung vom April 2003 gegen diese Vorschläge zur Neuordnung der Rundfunkgebührenerhebung. Nicht zuletzt wegen dieses gut begründeten Widerstands wurden die Pläne nicht weiter verfolgt.

Aber auch **Zuständigkeitsfragen** auf der Grundlage des bestehenden Rechts beschäftigten uns im Berichtszeitraum. Zurzeit haben wir keine Kontrollbefugnisse für die Gebührendatenverarbeitung in Schleswig-Holstein. Die Kontrolle erfolgt durch den Rundfunkdatenschutzbeauftragten des NDR. Entsprechendes gilt für alle anderen Bundesländer mit Ausnahme von Berlin, Bremen, Brandenburg und Hessen, in denen der jeweilige Landesbeauftragte ein Kontrollrecht besitzt. Hintergrund für diese Regelung ist, dass sich die Rundfunkanstalten auch hinsichtlich der Verarbeitung der Rundfunkgebührendaten auf die grundgesetzlich garantierte Rundfunkfreiheit berufen. Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder greift dieses Argument allerdings nicht. Die bestehende Rechtslage in den meisten Bundesländern führt vielmehr dazu, dass eine **unabhängige Datenschutzkontrolle** bei der Gebührendatenverarbeitung, wie sie von der Europäischen Datenschutzrichtlinie verlangt wird, **nicht realisiert** ist. Die Kontrolle durch interne Datenschutzbeauftragte der Rundfunkanstalten kann nicht als gleichwertiger Ersatz für eine unabhängige Kontrolle durch Dritte, von der zu kontrollierenden Institution unabhängige Stellen angesehen werden.

In materieller Hinsicht ist die Praxis von **Einkäufen bei Adresshändlern** durch die GEZ zu kritisieren. Offenbar versuchte die GEZ gezielt Daten solcher Personen zu erwerben, die als Jugendliche mit eigenem Einkommen bei den Eltern wohnen. Allerdings zeugten diverse Eingaben von einer schlechten Datenqualität. So wurden beispielsweise **kleine Kinder angeschrieben** und von der GEZ verängstigt. Für die Betroffenen war es in der Regel schwierig, eine Korrektur der fehlerhaften Datenspeicherungen herbeizuführen. Zwar werden kostenpflichtige Telefon-Hotlines angeboten; gleichwohl bringen Beschwerden dort nach Berichten der Betroffenen nichts, sie werden vielmehr weiterhin mit unfreundlichen Schreiben belästigt.

Ein weiteres Problem stellt die Arbeit der so genannten **Gebührenbeauftragten** dar. Diese Personen sollen möglichst neue, der GEZ noch nicht bekannte Gebührenschuldner ausfindig machen und zur Zahlung veranlassen. Dabei werden sie eigenständig tätig. Nach sowohl in der Presse veröffentlichten als auch bei uns vorliegenden Berichten wird dabei offenbar nicht immer mit lauteren Mitteln vorgegangen. Die Bürger sollten sich von schneidig auftretenden Gebührenbeauf-

tragten nicht einschüchtern lassen – sie müssen insbesondere nicht in die Wohnung gelassen werden.

Problematisch ist auch die Art und Weise, in der die GEZ versucht, Daten außerhalb ihrer rechtlichen Befugnisse zu erheben. So ist es praktisch ausgeschlossen, sich bei der GEZ abzumelden, ohne **Daten dritter Personen** anzugeben. Für diese Art der Datenerhebung gibt es keine Rechtsgrundlage. Nach unserer Erkenntnis werden einfache Abmeldungen ohne die Nennung dritter Personen nicht bearbeitet, sodass die Gebührenschuld weiterhin bestehen bleibt. Dabei ist zu beachten, dass rückständige Rundfunkgebühren öffentlich-rechtliche Forderungen sind. Sie können im Wege der Vollstreckung durch gemeindliche Vollstreckungsbeamte eingezogen werden. Diese müssen dabei – ob sie wollen oder nicht – Amtshilfe leisten, wenn eine entsprechende Forderung besteht.

Diese Fälle zeigen, dass es einen erheblichen **Wildwuchs bei der Erhebung der Rundfunkgebühren** gibt. Es wäre an der Zeit, einen Vorschlag aufzugreifen, den die Datenschutzbeauftragten des Bundes und der Länder bereits im Jahr 2000 in einer Entschließung unterbreitet haben. Würde von einer gebührenbezogenen Finanzierung abgegangen und würden die Kosten für die Rundfunkanstalten aus dem allgemeinen Steueraufkommen bezahlt, so ließen sich all die dargestellten Probleme vermeiden. Eine solche Rundfunkfinanzierung würde den Prinzipien der Datenvermeidung und Datensparsamkeit Rechnung tragen. Auch beweisen Rundfunkanstalten in anderen europäischen Ländern, beispielsweise in Großbritannien, dass sich eine solche Finanzierung durchaus mit anspruchsvollen Programmen und der gebotenen Staatsferne verträgt.

Wir haben die zahlreichen Eingaben zum Anlass genommen, eine Liste von **häufig gestellten Fragen** mit den passenden Antworten im **Internet** zu veröffentlichen, um die Bürger über die wichtigsten Fragen der Datenverarbeitung bei der Rundfunkgebührenerhebung aufzuklären. Die Liste findet sich unter folgender Internet-Adresse:

www.datenschutzzentrum.de/faq/gez.htm

Was ist zu tun?
Das Land Schleswig-Holstein sollte einen innovativen Schritt zur datenschutzgerechten Neuorganisation der Rundfunkfinanzierung gehen und sich für eine aus den Steuern finanzierte öffentlich-rechtliche Rundfunklandschaft stark machen.

7.3 Bundesregierung geht endlich gegen Missbrauch von 0190-Nummern vor

Lange Zeit war dem Missbrauch von 0190er-Nummern Tür und Tor geöffnet. Nun wurde endlich ein Gesetz zum Schutz der Verbraucher erlassen.

Noch im letzten Tätigkeitsbericht (25. TB, Tz. 8.3) haben wir über die Probleme und den Ärger berichtet, den Verbraucher mit dem Missbrauch von so genannten Mehrwertdiensterufnummern hatten (die bisher mit der Kombination 0190 und in

Zukunft mit 0900 beginnen). Windige Geschäftemacher hatten sich die bestehenden Gesetzeslücken zunutze gemacht und beuteten die Unerfahrenheit vieler Internet-Nutzer und Telefonkunden aus. Damit ist jetzt Schluss: Der Bundestag hat im August 2003 ein Gesetz zur Bekämpfung des Missbrauchs von 0190-/0900-Mehrwehrtdiensterufnummern beschlossen. Es fügt in das Telekommunikationsgesetz Regelungen ein, aufgrund derer die **Verbraucher** gegenüber der **Regulierungsbehörde** einen **Auskunftsanspruch** geltend machen können. So können sie erfahren, welcher Anbieter hinter einer bestimmten 0190-Nummer steht. Dies war in der Vergangenheit nicht möglich, weswegen die rechtliche Gegenwehr häufig schwierig bis ausgeschlossen war. Handelt es sich um die bisher vergebenen 0190-Nummern, so wird in einem schriftlichen Verfahren innerhalb von zehn Tagen eine Antwort durch die Regulierungsbehörde erteilt. Bei den neuartigen 0900-Nummern, die ab 2006 ausschließlich verwendet werden, ist die Abfrage über das Internet ohne weitere Voraussetzungen möglich.

Weiterhin sind die Anbieter nach den neuen Regelungen verpflichtet, bei der Werbung für ihre Dienste die **genauen Preise** anzugeben. Bei Diensten, die per Sprachtelefonie erbracht werden, muss, bevor der eigentliche Dienst einsetzt, eine akustische Information über die Höhe des Preises erfolgen. Dies gilt allerdings für Gespräche aus dem Mobilfunknetz erst ab August 2004. Außerdem gibt es eine **Preishöchstgrenze**. So dürfen höchstens 2 € pro Minute oder 30 € einmalig für eine Einwahl verlangt werden. Ausnahmen sind nur zugelassen, wenn der Kunde sich in einem eigenständigen Verfahren gegenüber dem Dienst authentisiert. Zudem muss es nach Ablauf einer Stunde zu einer automatischen Trennung kommen.

Auch gegen die besonders berüchtigten **Dialer**, die sich hinter dem Rücken der Nutzer auf deren PC installieren und für besonders teure Zugangsverbindungen sorgen, ist Abhilfe vorgesehen. Nach der neuen Rechtslage dürfen lediglich solche Dialer tätig werden, die bei der Regulierungsbehörde registriert wurden und definierte Mindestvoraussetzungen erfüllen. Die Regulierungsbehörde hat aufgrund dieser Regelung bereits eine große Zahl von Dialern unschädlich gemacht, indem sie die Registrierung ablehnte. Werden Einwahlverbindungen mithilfe dieser nicht registrierten Dialer vorgenommen, entfällt die Pflicht, die Vergütung zu bezahlen.

Darüber hinaus sind die **Befugnisse der Regulierungsbehörde** gegenüber den Anbietern von Mehrwehrtdiensten erweitert worden. So kann jetzt die Stelle, die im Auftrag des (zunächst unbekannten) Mehrwehrtdienstes dessen Gebühren einzieht, dazu aufgefordert werden, für eine bestimmte Nummer keine Rechnungslegung vorzunehmen, wenn bekannt ist, dass es sich dabei um eine rechtswidrige Nutzung handelt.

Bereits in der Vergangenheit hatten die **Gerichte** den Opfern der unterschiedlichen 0190-Mehrwehrtdienste weitgehend geholfen. In vielen Fällen wurde eine Zahlungspflicht beim Einsatz von Dialern mit unterschiedlichen juristischen Argumenten verneint. Auch wurde eine wettbewerbsrechtliche Mitverantwortlichkeit der Stellen anerkannt, die von der Werbung für bestimmte Dienste profitieren. Mit der sehr zu begrüßenden Rechtsänderung sollte das Unwesen der unkontrollierten Nutzung von Mehrwehrtdiensterufnummern beseitigt worden sein.

7.4 Der elektronische Verwaltungsakt – bald auch von den Kommunen

Der Bund hat die Richtung vorgegeben, Schleswig-Holstein bleibt keine andere Wahl, als auf dem Weg zu folgen: Die Landesregierung hat einen Gesetzentwurf vorgelegt, mit dem die elektronische Kommunikation in das Verwaltungsverfahrensrecht Einzug halten soll. Wichtige Grundsatzfragen sind jedoch noch immer ungelöst und Gefährdungen für die Bürger nicht ausgeschlossen.

Bereits Mitte des Jahres 2002 wurden durch eine Änderung im Verwaltungsverfahrensgesetz die elektronische Kommunikation im Verwaltungsbereich und namentlich der elektronische Verwaltungsakt, signiert mit einer qualifizierten elektronischen Signatur, im Bundesrecht eingeführt (vgl. 25. TB, Tz. 8.2). Das am Anfang 2003 in Kraft getretene neue Recht gilt jedoch nur für die Bundesbehörden. Die überwiegende Zahl der Behörden, die in unmittelbarem Kontakt zu den Bürgern stehen, findet sich allerdings auf der Ebene der Kommunen und des Landes. Grundlage für das Verwaltungsverfahren dieser Stellen ist in **Schleswig-Holstein** das **Landesverwaltungsgesetz**. Gemäß einer Absprache zwischen Bund und Ländern werden die Verwaltungsverfahrensgesetze der Länder die Regelungen des Bundesrechts im Wesentlichen übernehmen.

Ein entsprechender Gesetzentwurf der Landesregierung liegt mittlerweile vor. Wir haben in unserer Stellungnahme auf einige problematische Punkte hingewiesen. Dazu gehört beispielsweise, dass es nach dem Entwurf keiner eindeutigen **Einwilligung des Bürgers** bedarf, um ihm einen elektronisch signierten Verwaltungsakt zuzustellen. Ausreichend ist der „Eindruck“, der Bürger habe den Zugang für diese Art von Kommunikation eröffnet. Zwar stellt die Gesetzesbegründung klar, dass dafür nicht schon ausreichen soll, dass der Bürger beispielsweise eine E-Mail-Adresse angibt. Jedoch wäre es sinnvoll, durch das Gesetz eine eindeutige Einwilligung zu fordern.

Ein anderes Problem, das von uns schon mehrfach thematisiert wurde, ist das der begrenzten **Haltbarkeit von elektronischen Signaturen** (vgl. 24. TB, Tz. 8.1). Aus technischen Gründen nimmt die Beweiskraft von elektronischen Signaturen rapide ab. In wenigen Jahren wird die Rechnerleistung so weit gestiegen sein, dass die heute als sicher angesehenen Verschlüsselungen von jedermann mit haushaltsüblichen Computern geknackt werden können. Dann wird nicht mehr zu unterscheiden sein, ob ein vorgeblich vor acht Jahren von einer bestimmten Behörde ausgestelltes Dokument tatsächlich von dieser stammt oder erst vor wenigen Stunden von einem Unbefugten „nachgebaut“ wurde. Die einzige Lösung bestünde darin, sämtliche Dokumente in regelmäßigen Abständen vor dem „Weichwerden“ der Signaturen **nachzusignieren**. Zu diesem Problem findet sich weder im Gesetzestext noch in der Begründung ein Hinweis.

Mittlerweile haben auch andere Stellen, wie z. B. eine renommierte Unternehmensberatung, den Finger in diese Wunde gelegt. Der unvoreingenommene Beobachter fühlt sich mittlerweile an das Märchen „Des Kaisers neue Kleider“ erinnert. Fast jeder scheint zu wissen, dass es noch ein erhebliches **ungelöstes Problem** gibt, ohne dessen Behebung sich auf die Dauer E-Government nicht

realisieren lässt. Jedoch scheint sich niemand zu trauen, das Problem anzusprechen, möglicherweise in der Befürchtung, dafür verantwortlich gemacht zu werden.

Immerhin hat das Innenministerium des Landes Schleswig-Holstein zugegeben, dass es noch ungelöste technische Probleme bei der Sicherstellung der Überprüfbarkeit elektronischer Signaturen gibt. Zugleich wird deutlich gemacht, in welcher Weise der schleswig-holsteinische Gesetzgeber diesem Defizit zunächst begegnen will. Es soll nämlich gerade bei den Verwaltungsakten, bei denen es besonders auf eine dauerhafte Nachprüfbarkeit ankommt, wie z. B. bei Baugenehmigungen, festgelegt werden, dass sie nicht in elektronischer Form ergehen dürfen. Im Übrigen werde die für die Verwaltung elektronischer Signaturen nötige **Infrastruktur** (so genannte PKI – Public Key Infrastructure) ohnehin nicht vor 2005 einsetzbar sein. Bis dahin werde die technische Entwicklung weiter beobachtet – wohl in der Hoffnung, dass das Problem bis dahin gelöst sein wird. Die durchaus nachvollziehbare Strategie des Landes ist also, zwar den Vorgaben des Bundes nachzukommen, zugleich jedoch die Risiken zu begrenzen.

Allerdings ist nicht zu erwarten, dass das Problem durch zusätzliche Technik gelöst werden kann. Da es sich um eine strukturelle Frage handelt, müsste die Verwaltung verpflichtet werden, als eine Art **neutrales Trustcenter** die in der Vergangenheit den Bürgern gegenüber erlassenen Verwaltungsakte sicher aufzubewahren und zu gegebener Zeit nachzusignieren. Angesichts dieses Problems und weiterer Risiken der mit elektronischer Signatur ausgestellten Verwaltungsakte (vgl. 24. TB, Tz. 8.1) kann den Bürgern derzeit nicht empfohlen werden, sich auf diese Form einzulassen. Sie sollten darauf bestehen, Verwaltungsakte in der klassischen und deutlich besser haltbaren Papierform zu erhalten.

Es finden sich allerdings auch **positive Ansätze** in dem vom Innenministerium vorgelegten Gesetzentwurf. Dazu gehört die Ermächtigung der Landesregierung, durch Rechtsverordnung zu bestimmen, dass ein auf Landesrecht beruhendes Schriftformerfordernis auch durch andere als mit einer qualifizierten elektronischen Signatur versehene elektronische Dokumente gewahrt werden kann. Dahinter steht die bisher noch nicht umgesetzte Idee eines so genannten Single-Sign-on-Verfahrens. Dazu müsste der Bürger einmal bei einer Behörde vorstellig werden, wo ihm ein persönliches Login gegeben würde, nachdem seine Identität geprüft wurde. Damit könnte er alle online angebotenen Behördendienstleistungen abwickeln. Eine elektronische Signatur wäre in diesem Fall nicht erforderlich. Allerdings muss bedacht werden, dass die Einführung eines solchen Verfahrens in einem Flächenland schwierig ist.

Was ist zu tun?
Die Landesregierung sollte auf dem eingeschlagenen Weg weitergehen und die Realisierung von E-Government-Lösungen ohne elektronische Signatur voranbringen.

8 Modellprojekte zum Datenschutz

8.1 EU-Projekt e-Region: Gütesiegel und Audit

Die Europäische Union und das Wirtschaftsministerium des Landes fördern im Rahmen des Programms „e-Region Schleswig-Holstein“ die Verbreitung von Datenschutz-Audits und -Gütesiegeln nach schleswig-holsteinischem Datenschutzrecht. Die Mittel der EU stammen aus den innovativen Maßnahmen des Europäischen Fonds für Regionale Entwicklung (EFRE) der Generaldirektion Regionalpolitik. Das Gütesiegelprojekt ist im EU-Wettbewerb für regionale Innovation in der Kategorie „Informationsgesellschaft“ als einer von drei Finalisten platziert worden.

Gütesiegel

Vierzehn kleine und mittlere Unternehmen wurden im Rahmen des Programms „e-Region Schleswig-Holstein“ bei der Erlangung eines Datenschutz-Gütesiegels finanziell gefördert. Ihre Produkte waren unter anderem nach dem **Innovationspotenzial** hinsichtlich datenschutzfördernder Eigenschaften im Sinne der Datenschutzauditverordnung (DSAVO) ausgewählt worden. Da gemäß dem LDSG öffentliche Stellen in Schleswig-Holstein zertifizierte Produkte bevorzugt einsetzen sollen, achteten wir auch auf die primäre Zielgruppe, die öffentlichen Stellen in Schleswig-Holstein. Die Unternehmen haben einen Zuschuss zu den Gutachterkosten erhalten und selbst einen Eigenanteil von mindestens 50 % der Kosten beigetragen. Wir erbrachten unsere Leistungen im Rahmen des Projektes gebührenfrei. Nachdem bis Ende Oktober 2003 alle Anträge auf Zertifizierung einschließlich der gutachterlichen Stellungnahmen bei uns eingegangen waren, konnten wir bis Redaktionsschluss das **Datenschutz-Gütesiegel** an **zehn Produkte** aus dem e-Region-Programm verleihen. Weitere Verleihungen stehen im ersten Quartal des Jahres 2004 an.


www.datenschutzzentrum.de/guetesiegel/register.htm

Im Einzelnen handelt es sich um folgende Produkte:

1. SQS-Testsuite für SAP HR, ein Beratungsprodukt der Firma SQS GmbH zur Qualitätssicherung (Test) von SAP HR-Anwendungssystemen in der Praxis,
2. E-pacs Speicherdienst der Firma Telepaxx GmbH, eine elektronische externe Archivierung von Röntgenbildern und anderen patientenbezogenen medizinischen Daten,
3. Einfache Einwohnermeldeauskunft per WWW-Zugriff der dataport (vormals: Datenzentrale Schleswig-Holstein), ein Produkt zur Überprüfung der Gültigkeit einer bekannten Adresse oder zur Ermittlung der aktuellen Adresse einer bekannten Person,
4. Opti.List Professional der Firma HSP GmbH, ein Produkt zur Archivierung steuerrechtlich relevanter Drucklisten unter Beachtung der Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) sowie der Abgabenordnung,

5. COMCITY Secured Data Server (SDS) der Firma COMCITY, eine Krypto-Fileserver-Anwendung, die das transparente, verschlüsselte Abspeichern von Daten über einen sicheren Kommunikationskanal über ein Netzwerk für multiple Einsatzbereiche ermöglicht,
6. STEP!basis, ein Produkt der Firma ergo!via GmbH zur Unterrichtungs-, Berufs-, Förder- und Anwesenheitsdokumentation von beruflichen Förderungs- und Qualifizierungsmaßnahmen,
7. Dataport Firewall, ein Produkt zum Schutz der Ressourcen im Netzwerk der dataport (vormals Datenzentrale Schleswig-Holstein) gegen unberechtigte Zugriffe aus dem Internet durch Einschränken der Verbindungen von und zum Internet auf zulässige Dienste,
8. MOBILE-Doctor, ein Produkt der Firma plan business healthcare GmbH, das eine mobile Datenhaltung auf Pocket-PCs in der fachlichen Ausprägung einer mobilen Datenbankanwendung für ärztliche Kernprozesse ermöglicht, bei der eine Synchronisation mit dem originären Datenbankserver erfolgt,
9. DIVA-Pro, ein Produkt der Firma m-privacy GmbH, ein Softwaresystem mit VNC-Server, der unter einem gehärteten Betriebssystem eine rollenbasierte Rechtevergabe zur sicheren und datenschutzgerechten Internet-Anbindung von Verwaltungsarbeitsplätzen ermöglicht,
10. Regionales Digitales Archiv (RDA), ein Produkt der Firma PERmed Gesundheitsprodukte GmbH, ein Verfahren zur Kommunikation und revisionssicheren Langzeitarchivierung von digitalen medizinischen Bildern und Befundberichten.

Dank der finanziellen Förderung der EU konnten wir die Sommerakademie 2003 mit dem Schwerpunkt Datenschutz-Audit und -Gütesiegel mit internationalen Gästen durchführen. Das Wirtschaftsministerium hat unser Projekt „Datenschutz-Gütesiegel“ aus den 14 e-Region-Projekten des Landes ausgewählt und zum **EU-Wettbewerb** für regionale Innovation gemeldet, an dem sich insgesamt 126 Regionen beteiligt haben. Es wurden Preise in drei Kategorien vergeben. Die EU-Kommission traf die Vorauswahl und wählte das ULD-Projekt „Datenschutz-Gütesiegel“ in der Kategorie „Informationsgesellschaft“ unter die ersten drei, zusammen mit je einem Projekt aus der Extremadura (Spanien) und Oberijssel (Niederlande).

Wir haben eine multimediale CD und ein Faltblatt veröffentlicht, auf denen das Audit- und das Gütesiegelverfahren sowie der Verlauf des Projektes „e-Region“ dargestellt werden.

www.datenschutzzentrum.de/download/guetesiegel.exe

Audit

Im Rahmen des Pilotprojektes sollten geförderte Modellprojekte standardmäßig auch ein Datenschutz-Audit durchlaufen. Hierfür mussten zunächst die **Grundlagen** geschaffen werden:

- Beschreibung der Verfahrensabläufe,
- Schaffung technischer Dokumentationsvorlagen,

- Erstellung von Maßnahmen- und Bewertungskatalogen,
- Modellentwicklung von Datenschutzmanagementsystemen und
- Erstellung von Werbebroschüren im Rahmen der Öffentlichkeitsarbeit.

Der **Kreis Segeberg** hat als erste Behörde einen Antrag auf Durchführung eines Datenschutz-Audits für das Projekt „**digitale Bauakte**“ bzw. „**GEO-Informationssystem**“ gestellt. Aufgrund der noch laufenden Entwicklung des Projektes ist mit dem Abschluss des Audits im Laufe des Jahres 2004 zu rechnen. Außerhalb des e-Region-Programms sind weitere Datenschutz-Audits beantragt und durchgeführt worden (vgl. Tz. 9.2). Es konnten hierdurch Erfahrungen bezüglich der Abwicklung von Audits gesammelt werden, die die Arbeiten für das Pilotprojekt unterstützen.

www.datenschutzzentrum.de/audit/

Ein Programm des Ministeriums für Wirtschaft und Arbeit, SH und der Technologiestiftung SH – gefördert von der EU
aus den Innovativen Maßnahmen des Europäischen Fonds für Regionale Entwicklung (EFRE) der Generaldirektion Regionalpolitik

8.2 Das Virtuelle Datenschutzbüro

Das Virtuelle Datenschutzbüro hat sich als stark frequentiertes Portal für Datenschutzexperten und Laien über den deutschsprachigen Raum hinaus etabliert. Im letzten Jahr gab es viele Erweiterungen und ein positives Feedback. Zugleich musste es sich ständig wachsenden Anforderungen stellen – sowohl in technischer und inhaltlicher als auch in finanzieller Hinsicht.

Datenschutzexperten und -interessierten muss das Virtuelle Datenschutzbüro nicht mehr vorgestellt werden. Als gemeinsame Einrichtung fast aller Landesbeauftragten und des Bundesbeauftragten für den Datenschutz in Deutschland sowie weiterer nichtstaatlicher und ausländischer Datenschutzkontrollinstanzen hat es in der **Datenschutzszene** seinen **festen Platz** gefunden. Auch für Datenschutzlaien ist das seit Dezember 2000 online erreichbare Internet-Portal als Einstieg in die Thematik attraktiv.

Die finanzielle Herausforderung gegenüber den vorangegangenen Jahren bestand darin, nach der Ende 2002 ausgelaufenen Förderung durch die „Initiative Informationsgesellschaft Schleswig-Holstein“ auch weiterhin den von den Usern gewohnten Service zu bieten (vgl. 25. TB, Tz. 9.1). Insbesondere den von den meisten Projektpartnern geleisteten **finanziellen Beiträgen** sowie unserer technischen und inhaltlichen Betreuung ist es zu verdanken, dass sich das Projekt nicht nur über Wasser halten konnte, sondern erweitert und verbessert wurde.

Die wichtigste technische Neuerung wurde im Februar 2003 vorgenommen: die Migration auf ein **neues Content-Management-System**. Die Umstellung auf die Open-Source-Software Zope ging mit Kostenersparnissen, Geschwindigkeitsgewinn, Funktionalitätszuwachs und einer größeren Wartungsfreundlichkeit einher; Zope hat sich als flexibler erwiesen als sein kostenpflichtiger Vorgänger Roxen.

Inhaltlich wurde das Angebot stark erweitert. Die bislang bekannten Datenschutzressourcen wie Artikelbeiträge, News, Themenliste, Veranstaltungshinweise, Suchmaschine usw. wurden sowohl für die Nutzer als auch für unsere Projekt- und Kooperationspartner **anwendungsfreundlicher** gestaltet. Die beträchtliche Zunahme an Artikelmeldungen lässt sich beziffern: Bis Redaktionsschluss umfasste der systematisch sortierte Schlagwortbaum 1624 Artikelmeldungen. Im Vergleich zum Jahr 2002 ist dies eine **Steigerung von 53,5 %**. Zudem können sich – insbesondere mit unserem Webportal bereits vertraute – Besucher über den Link „Neueste Artikel“ auf der Startseite einen schnellen Überblick über die 20 zuletzt gemeldeten Artikel verschaffen.

Den Großteil der redaktionellen Arbeit macht die möglichst werktägliche Abfassung **aktueller Newsbeiträge** aus. Die Zahl der Newsmeldungen stieg auf 1135 an; dies ist im Vergleich zum Jahr 2002 eine **Steigerung von etwa 57,5 %**. Das Bedürfnis, in der Öffentlichkeit kontrovers diskutierte Datenschutzfragen thematisch zu bündeln, führte zu einer weiteren Neuerung. Gezielt angelegte **Feature-Seiten** fassen in Form von Dossiers alle auf der Website zu findenden Informationen schwerpunktmäßig zusammen: Jeder Internet-Nutzer, der sich über die US/EU-Flugdatenaffäre, RFID-Chips, die Lkw-Maut oder das US-Programm „Total Information Awareness“ bzw. „MATRIX“ oder andere Schwerpunktthemen informieren möchte, kann dies detailliert und auf einen Blick über den entsprechenden Link auf der Startseite tun. Neben einer kurzen Einführung in die Thematik sind dort alle Artikel- und Newsmeldungen aufgelistet, die sich im Virtuellen Datenschutzbüro zu dem Thema finden.

Die seit Juni 2003 implementierte chronologische Veranstaltungsübersicht einzelner Fortbildungskurse im Bereich Datenschutz und Datensicherheit ist eine weitere inhaltliche Ergänzung. Diese **Veranstaltungsdatenbank** ist zu der bereits existierenden Übersicht über wichtige Veranstaltungen sowie zur allgemeinen Auflistung von Fortbildungsinstitutionen hinzugetreten. Sie wird von den Kooperationspartnern bestückt, die solche Veranstaltungen anbieten. Insgesamt hat das Virtuelle Datenschutzbüro im Berichtszeitraum 20 am Datenschutz interessierte Organisationen und Personen als Kooperationspartner aufgenommen, die mit dazu beitragen, weitere Ressourcen für das Portal bereitzustellen.

Einen weiteren Schwerpunkt stellte die Entwicklung einer datenschutzspezifischen **Literaturdatenbank** dar. Als Nachweissystem für Fundstellen, Publikationen und Gerichtsentscheidungen im Bereich Datenschutz und Datensicherheit konzipiert, soll es thematisch mit dem bestehenden Schlagwortsystem verknüpft werden und das Angebot des Virtuellen Datenschutzbüros optimieren. Nach dem gleichen Muster wie die Artikelmeldungen wird es den Projekt- und Kooperationspartnern möglich sein, Publikationen und Gerichtsentscheidungen samt Fundstelle thematisch einem Schlagwort zuzuweisen und damit den Besuchern des

Portals die Literaturrecherche in diesem Bereich wesentlich zu erleichtern. Zudem wird man anhand einer spezifischen Suchmaske gezielt in dieser Literaturdatenbank suchen können. Längerfristig soll die Datenbank den Partnern des Virtuellen Datenschutzbüros die Möglichkeit bieten, in Form von Rezensionen und Kommentaren Literatur zu bewerten.

Das Virtuelle Datenschutzbüro fand in seiner neuen Aufmachung in der **Öffentlichkeit verstärkt Beachtung**, sei es in Publikumszeitschriften wie c't oder Stern, im Anwaltsblatt oder durch die kostenlose Aufnahme in „Das Web-Adressbuch von Deutschland", das die 6000 wichtigsten Webadressen erfasst. Schließlich kam eine von der Verwaltungshochschule Speyer durchgeführte Studie zum Thema „Datenschutz im Internet – Internet im Datenschutz (Datenschutzbehörden im Internet)" im Frühjahr 2003 zum Fazit: „Wenn es das Virtuelle Datenschutzbüro nicht geben würde, so müsste man es umgehend erfinden."

An Ideen zur **Erweiterung** der Service-Plattform mangelt es weder seitens des Virtuellen Datenschutzbüro-Teams noch seitens der Projekt- und Kooperationspartner. Allerdings ist angesichts der beschränkten finanziellen Mittel, der stetig steigenden Zahl der Artikelmeldungen sowie der aktuellen nationalen und internationalen Entwicklungen im Bereich des Datenschutzes ein weiterer Ausbau der Seite nicht einfach zu leisten. Gleichwohl soll weiterhin versucht werden, diesen wichtigen Service aufrechtzuerhalten.


www.datenschutz.de

Was ist zu tun?
Um in Zukunft das Niveau halten und noch weiter anheben zu können, bedarf es weiterhin der finanziellen Unterstützung durch die Projektpartner. Ebenso unerlässlich ist deren inhaltliche Mitwirkung.

8.3 AN.ON setzt sich durch

Der Dienst AN.ON ermöglicht seit knapp drei Jahren Nutzern das anonyme Websurfen. Im Rahmen eines Strafermittlungsverfahrens erwirkte das Bundeskriminalamt richterliche Beschlüsse des Amtsgerichts Frankfurt, mit denen die Betreiber des Dienstes zur Protokollierung von Zugriffen verpflichtet werden sollten. Sie wurden auf Antrag der AN.ON-Betreiber vom Landgericht Frankfurt alle wieder aufgehoben.

Über das seit Anfang 2001 in Kooperation zwischen der Technischen Universität (TU) Dresden und der Freien Universität (FU) Berlin durchgeführte und vom Bundesministerium für Wirtschaft und Arbeit (BMWA) geförderte **Projekt „AN.ON – Anonymität online"** wurde in den letzten Jahren ausführlich berichtet (vgl. 23. TB, Tz. 9.2; 24. TB, Tz. 9.2; 25. TB, Tz. 9.2). Mithilfe des von der TU Dresden entwickelten Tools **JAP**, das kostenlos aus dem Internet heruntergeladen werden kann, wird die anonyme Nutzung von Diensten im World Wide Web ermöglicht. Im Berichtszeitraum wurde der Dienst weiter ausgebaut.

Von vornherein gehörte es zu unserem Anliegen, auch **Aspekte der Strafverfolgung** mit einzubeziehen. Wir haben uns von Anfang an die Frage gestellt, ob der Dienst zu kriminellen Zwecken missbraucht werden kann. Anfragen bzw. Beschwerden von Strafverfolgungsbehörden und anderen Betroffenen hinsichtlich missbräuchlicher Nutzungen des Dienstes werden von uns im Rahmen unserer juristischen Begleitung des Projektes beantwortet. Bereits in den letzten Tätigkeitsberichten haben wir unsere Erfahrungen mit entsprechenden Anfragen dargestellt (vgl. 24. TB, Tz. 9.2; 25. TB, Tz. 9.2). Im Ergebnis lässt sich sagen, dass die möglicherweise missbräuchlichen Nutzungen des AN.ON-Dienstes nach unseren Auswertungen gegenüber den stetig steigenden Nutzungszahlen nach wie vor einen äußerst geringen Anteil ausmachen. Offenbar erfolgt die überwältigende Anzahl der Nutzungen, entgegen allen Vorurteilen, nicht zu kriminellen Zwecken (vgl. 25. TB, Tz. 9.2). Dieses Ergebnis wird durch unsere aktuelle Auswertung der an uns herangetragenen Missbrauchsfälle bestätigt. So erreichten uns 2003 58 Anfragen, die sich mit Missbrauchsfällen beschäftigten. 22 Anfragen hiervon stammten von Strafverfolgungsbehörden.

? *AN.ON*

Das Ziel des AN.ON-Projekts besteht in der Realisierung von Systemen, mit deren Hilfe jede Nutzerin und jeder Nutzer das Internet auf technisch bestmöglichem Niveau anonym und unbeobachtbar nutzen kann. Das dazu erforderliche, frei verfügbare Programm, das als Java-Applikation auf allen gängigen Betriebssystemen installiert werden kann, ist der JAP. Ergänzend zum JAP, den ein Nutzer auf seinem PC installiert, müssen auch so genannte Mixserver programmiert werden. Diese Mixserver werden von unabhängigen Organisationen betrieben und gewährleisten durch Hintereinanderschaltung mehrerer Mixserver zu so genannten Mixkaskaden die Anonymität auch gegenüber den Betreibern der Mixserver. Unsere Aufgabe besteht darin, das Projekt juristisch und datenschutzpolitisch zu betreuen.

In der Regel erhalten wir Anfragen, die darauf gerichtet sind, einen Nutzer des Anonymisierungsdienstes **für die Vergangenheit** zu **identifizieren**. Derartige personenbezogene Daten sind jedoch nicht vorhanden, da sich der Anonymisierungsdienst streng an das geltende Datenschutzrecht hält. Eine Erhebung und Speicherung personenbezogener Daten über Nutzer des AN.ON-Dienstes ist nach den zwingenden Vorschriften des Teledienstedatenschutzgesetzes (TDDSG) unzulässig.

Im Juli 2003 wurden wir mit einem Ersuchen konfrontiert, die **Überwachung** eines Nutzers **für die Zukunft** zu ermöglichen. Wir erhielten einen richterlichen Beschluss des Amtsgerichts Frankfurt am Main, durch den

? *JAP*

Um anonym und unbeobachtbar im Internet zu surfen, kann man das Programm JAP auf seinem Rechner installieren und verwenden. Es sorgt dafür, dass alle Aktivitäten, die der Nutzer mit seinem Browser im Web ausführt, über den JAP an spezielle Anonymitätsserver, so genannte Mixe, geleitet werden. Die Mixe bringen die im JAP verschlüsselten Datenpakete in eine einheitliche Form, sodass Internet-Provider oder Mixbetreiber nicht mehr sehen können, wer gerade auf welchen Seiten surft. JAP steht kostenlos als Open-Source-Programm auf der Projektwebseite zur Verfügung unter

www.anon-online.de

wir verpflichtet wurden, die Zugriffe auf eine bestimmte IP-Adresse, über die offenbar strafbare Inhalte veröffentlicht wurden, für einen definierten Zeitraum zu speichern und über die gespeicherten Daten Auskunft zu erteilen. Im Rahmen eines konkreten Strafermittlungsverfahrens des Bundeskriminalamtes (BKA) im Zusammenhang mit Kinderpornografie sollten die Zugriffe auf ein bestimmtes im Internet zur Verfügung stehendes Forum überwacht werden.

Gemeinsam mit den Projektpartnern vertreten wir die Auffassung, dass bei Vorliegen aller rechtlichen Voraussetzungen, d. h. eines rechtmäßigen **richterlichen Beschlusses** gemäß §§ 100 a, 100 b Strafprozessordnung (StPO), mit den Strafverfolgungsbehörden im Rahmen der gesetzlichen Notwendigkeiten und technischen Möglichkeiten kooperiert werden muss. Daher wurde in die aktuelle Version der auf den Mixservern eingesetzten Software eine Funktion zur Rückverfolgung eingefügt.

Obwohl das BKA darauf hingewiesen worden war, dass es eines richterlichen Beschlusses gemäß §§ 100 a, 100 b StPO bedürfe, beruhte der Beschluss des **Amtsgerichts Frankfurt** überraschenderweise auf den Regelungen der §§ 100 g, 100 h StPO. Während auf der Grundlage der §§ 100 a, 100 b StPO die künftige **Überwachung** der Telekommunikation angeordnet werden kann, ermöglicht die Anordnung gemäß §§ 100 g, 100 h StPO grundsätzlich nur die nachträgliche **Auskunft** über Telekommunikationsverbindungsdaten, zu denen auch die IP-Adresse gehört. Da nach unserer Auffassung die Anordnung einer **Aufzeichnung** von Nutzungsdaten durch die vom Amtsgericht zugrunde gelegten Rechtsvorschriften nicht gedeckt war, legten wir **Beschwerde** gegen die Anordnung ein. Da der Beschwerde keine aufschiebende Wirkung zukam, d. h. der Inhalt des Beschlusses bis zu einer anders lautenden Gerichtsentscheidung umzusetzen war, protokollierten wir die Zugriffe auf die in der Anordnung angegebene IP-Adresse.

Die Software des Projektes ist **Open Source**. Daher veröffentlichten wir die implementierte Aufzeichnungsfunktion im Quellcode. Für die Nutzer wurde so erkennbar, dass die Mixsoftware eine derartige Überwachung ermöglicht. Bei einer Kooperation der Mixe ist es möglich, die Zugriffe auf eine vorher anzugebende IP-Adresse ausschließlich für die Zukunft mitzuloggen. Die IP-Adresse des Anfragenden sowie das Datum und die Uhrzeit werden mitprotokolliert. Alle anderen Webseiten und alle anderen Nutzer des AN.ON-Dienstes bleiben von der Protokollierungsfunktion unberührt. Es bestand daher zu keiner Zeit die Gefahr einer Überwachung aller Nutzer des Dienstes.

Auf unsere Beschwerde setzte das **Landgericht Frankfurt** am Main bereits im Juli 2003 die Vollziehung des richterlichen Beschlusses des Amtsgerichts Frankfurt am Main aus. Durch ein Versehen des Gerichts erhielten wir diesen Beschluss allerdings erst Ende August 2003 zur Kenntnis. Die Projektpartner deaktivierten die Protokollierung unmittelbar nach Kenntnis des Beschlusses. Bis zu diesem Zeitpunkt war ein einziger Zugriff mitgeloggt worden, dessen Datum zunächst in unserer Obhut blieb. Nach unserer Auffassung sollte erst nach einer endgültigen Entscheidung des Gerichts über dessen Verwendung befunden werden.

Trotz der Aussetzungsentscheidung des Landgerichts erwirkte das **BKA** einen erneuten richterlichen Beschluss beim Amtsgericht Frankfurt am Main. Mit diesem Beschluss wurde die Durchsuchung der Räume des AN.ON-Projektes an der TU Dresden angeordnet, um den in der Obhut des Projektes befindlichen Datensatz aufzufinden. An einem Samstag Ende August 2003 kamen Beamte des BKA nach Dresden und verlangten die Herausgabe des Datensatzes. Um weiteren Schaden (Durchsuchung der Institutsräume, Beschlagnahme von Rechnern) von der TU Dresden und den Projektpartnern abzuwenden, wurde der Datensatz **unter Protest** an die Beamten **herausgegeben**. Gegen den neuen Beschluss wurde ebenfalls Beschwerde eingelegt. Die vorläufig zugunsten von AN.ON ergangene Entscheidung des Landgerichts hätte das BKA nicht unter Berufung auf die allgemeinen Herausgabe- und Beschlagnahmebestimmungen umgehen dürfen.

Mitte September 2003 hob das **Landgericht Frankfurt** am Main den Beschluss des Amtsgerichts auf, mit dem die Auskunftserteilung angeordnet worden war. Das Gericht gab uns nunmehr auch **in der Hauptsache Recht**, indem es feststellte, dass die §§ 100 g, 100 h StPO nur die Fälle regeln, in denen Daten aus anderen Gründen aufgezeichnet und gespeichert worden sind, was aber bei dem Anonymisierungsdienst nicht der Fall ist.

Beispiel Telefonseelsorge

Unter der Überschrift „Anonymität auf beiden Seiten gehört zum Konzept“ schreibt die Telefonseelsorge auf ihrer Webseite (www.telefonseelsorge.de/beratung/ internet.htm):

„(...) Es gibt (...) auch das Konzept der beidseitigen Anonymität, wie es von der Telefonseelsorge im Internet praktiziert wird. Die Mitarbeiter/innen der Telefonseelsorge bleiben – analog zu ihren Grundsätzen am Telefon – bei ihrem Seelsorgekontakt im Internet anonym. Besonders für Menschen mit sehr starken traumatischen Erlebnissen ist es zum Teil etwas leichter, sich an eine anonym arbeitende Einrichtung zu wenden, da die betreffenden Themen und schwerwiegenden Erfahrungen sehr häufig mit großer Scham besetzt sind. (...) So kommt es z. B. vor, dass Rat Suchende zurückmelden, dass ihnen die zweite Mail viel schwerer zu schreiben fiel, weil sie jetzt eine/n konkrete/n Berater/in vor sich haben. Mit diesem Konzept der beidseitigen Anonymität werden also auch Menschen angesprochen, die sich nicht an die telefonische Beratung wenden und die ein Seelsorgeangebot im Internet mit einer persönlichen Beschreibung des Beraters/der Beraterin meiden würden.“

Die Sicherheits- und Datenschutzkriterien der Telefonseelsorge:

www.sewecom.de/telefonseelsorge/sicherheitskonzept/

Dort wird die Nutzung des Anonymisierungsdienstes AN.ON empfohlen.

Anfang November 2003 entschied das Landgericht Frankfurt auch in der dritten und letzten Auseinandersetzung zugunsten von AN.ON. Es stellte die **Rechtswidrigkeit** der vom **BKA** erwirkten **Durchsuchungsanordnung** fest. Das Landgericht folgte unserer Argumentation, dass die Durchsuchungsanordnung eine Umgehung der §§ 100 g, 100 h StPO darstellt.

Nachdem wir mit allen Rechtsmitteln gegen die Ermittlungshandlungen des BKA erfolgreich waren, forderten wir das BKA und auch die Staatsanwaltschaft Frankfurt auf, den fraglichen **Protokolldatensatz** zu löschen. Gleichzeitig haben wir

den zuständigen Bundesbeauftragten für den Datenschutz sowie den Hessischen Landesdatenschutzbeauftragten gebeten, die Löschung der Daten zu überprüfen. Ein Ergebnis lag bei Redaktionsschluss noch nicht vor. Eine ausführliche Dokumentation der geschilderten gerichtlichen Auseinandersetzung befindet sich im Internet unter

www.datenschutzzentrum.de/
projekte/anon/

Wir sehen uns durch die Entscheidungen des Landgerichts Frankfurt in unserem **Kurs bestätigt**, den Nutzern des AN.ON-Dienstes ein technisches Instrument an die Hand zu geben, das sich vollständig auf dem Boden der bestehenden Gesetze bewegt. Inzwischen hat das Bundesministerium für Wirtschaft und Arbeit die Förderung für das AN.ON-Projekt um weitere neun Monate im Jahr 2004 verlängert. Dabei geht es vorrangig um die Klärung von Fragen zur Strafverfolgung und um die Entwicklung einer Bezahlfunktion für den Dienst.

Ein aktuelles Beispiel dafür, dass die Gewährleistung von Anonymität ein wichtiges Anliegen sein kann, ist die **Telefonseelsorge** im Internet. Ein solches Beratungsangebot für biografisch zumeist brisante Situationen ist selbstverständlich darauf angewiesen, ihren Nutzern die aktuell bestmögliche Anonymität zu gewährleisten. Deshalb empfehlen die kirchlichen Stellen die Nutzung von AN.ON.

Seit August 2002 betreiben wir, in administrativer Unabhängigkeit von der TU Dresden, einen **eigenen Mixserver** im Internet. Der Betrieb gestaltete sich bislang problemfrei. Seit Ende Dezember stellen auch das Institut für Wirtschaftsinformatik der Humboldt-Universität Berlin sowie das Institut für Wirtschaftswissenschaften der Universität Regensburg jeweils eigenständige Mixserver zur Verfügung. Die juristische Betreuung erfolgt wie bisher durch uns. Darüber hinaus bestehen Absichtserklärungen zum Betrieb von Mixservern seitens des Instituts für Rechtsinformatik der Universität Wien sowie der People's Solidarity for Participatory Democracy aus Südkorea, einer Organisation für die Durchsetzung von Bürgerrechten in Südkorea.

Weitere Informationen zum Projekt finden sich im Internet unter

www.anon-online.de
www.datenschutzzentrum.de/anon/

Das Projekt „AN.ON – Anonymität online“ wird gefördert durch das

Die Förderung wurde bis September 2004 erneut verlängert.

Was ist zu tun?
Das Recht auf Anonymität ist auch im Internet gegen Angriffe zu verteidigen. Wir werden uns gegen alle Pläne wehren, das Recht auf Anonymität im Internet in eine Pflicht zur Protokollierung für die Provider zu verwandeln.

8.4 P3P – Internet-Datenschutz als Wettbewerbsvorteil

P3P verschafft dem Nutzer mehr Transparenz darüber, was mit seinen Daten geschieht, und ermöglicht ihm so, eine Vertrauensbasis zu dem Betreiber der besuchten Website aufzubauen. Im Rahmen eines vom Wirtschaftsministerium des Landes geförderten Modellprojektes haben wir die Implementierung von P3P verbessert.

„Vertrauen ist der Anfang von allem“ – so warb vor einiger Zeit eine Bank um Kunden. Genauso könnte das Motto von Händlern lauten, die ihre Ware über das Internet absetzen wollen. Kunden besuchen oft die Verkaufswebsites und legen Produkte in den virtuellen Warenkorb. Wenn es aber im nächsten Schritt an die Eingabe personenbezogener Daten geht, die zur Abwicklung des Kaufes erforderlich sind, werden viele Verkaufsvorgänge abgebrochen. **Unsicherheit** über Fragen des Datenschutzes kann sich also konkret **umsatzmindernd** auswirken. Um das Vertrauen des Kunden auch online zu gewinnen, bedarf es anderer Mittel und Wege als in traditionellen Wirtschaftsprozessen. Ein solcher spezieller Weg ist eine Datenschutzerklärung im P3P-Format.

? P3P

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

Um P3P nutzen zu können, benötigt der Internet-Surfer entweder einen P3P-fähigen Browser oder ein passendes Zusatztool. **P3P-Funktionalität** bieten die aktuellen Versionen von Mozilla/Netscape und des Internet Explorers. Sie unterstützen jedoch nur den P3P-basierten Umgang mit Cookies. Dabei wird die Erlaubnis zum Setzen eines Cookies auf dem Nutzerrechner von der elektronischen Datenschutzerklärung des Anbieters abhängig gemacht.

Ein Zusatztool, der **Privacy Bird**, existiert momentan nur als Erweiterung des Internet Explorers. Dieses kleine Softwareprogramm zeigt jedoch, was P3P bereits jetzt zu leisten vermag: Über ein Menü stellt der Nutzer durch einfaches Anklicken ein, bei welcher Datenverarbeitung er vom Programm gewarnt werden möchte. Beim Surfen tritt der Privacy Bird als kleines Symbol in Erscheinung, das abhängig von der Datenverarbeitung der besuchten Seite rot, gelb oder grün aufleuchtet. Der Nutzer erfährt so auf einen Blick, ob seinen Datenschutzvoreinstellungen entsprochen wird oder nicht. Leider existiert bislang weder eine

browserübergreifende noch eine deutsche Sprachversion des Tools, sodass Nutzern anderer Browser diese Funktionalität vorenthalten bleibt.

Eine flächendeckende Unterstützung umfassender P3P-Funktionalität seitens der Softwarehersteller steht bislang noch aus. Für die derzeit existierenden Softwarelösungen haben wir im Rahmen eines P3P-Projekts umfangreiche **Anleitungen veröffentlicht**, die es Nutzern ermöglichen, sicher mit der neuen Technik umzugehen. Dazu werden die P3P-Funktionen der einzelnen Programme anhand von Schritt-für-Schritt-Anleitungen besprochen und die unter Datenschutzgesichtspunkten sinnvollen Einstellungen beschrieben. Mit unserer Unterstützung ist auch in den aktuellen Mozilla-Versionen 1.5 und 1.6 die Übersetzung der ursprünglich englischsprachigen P3P-Einstellungen deutlich verbessert und verständlicher gestaltet worden.

P3P eröffnet den einfachen Weg zur Transparenz in einem Bereich, der sonst schwer vermittelbar ist. Diese **Transparenz** können sich datenschutzkonforme Anbieter als **Wettbewerbsvorteil** zunutze machen. Sie demonstrieren ihre Seriosität in Datenschutzfragen und können so das gewonnene Vertrauen in eine vermehrte Anzahl erfolgreich durchgeführter Geschäfte umsetzen.

? Cookies

Cookies sind kleine Textdateien, die ein Serverbetreiber auf dem Rechner als Datei abspeichern und später wieder abfragen kann. Ursprünglich sollten Cookies das elektronische Einkaufen erleichtern: Ein Benutzer wählt auf einem Server Waren aus, die er kaufen möchte. Der Server speichert die Kennungen dieser Produkte auf dem Rechner des Nutzers und kann auf der Bestellseite diese Informationen wieder abrufen, um die Bestellung automatisch – bequem für den Käufer – auszufüllen. In der Praxis speichern die Server jedoch nicht die gewählten Produkte auf dem Nutzerrechner, sondern nur eine ID-Nummer. Der eigentliche Bestellzettel wird auf dem Server des Anbieters geführt. Ein Server kann Cookies verwenden, um einen Benutzer schon beim Betreten der Startseite eindeutig zu markieren und seine Zugriffe auf Folgeseiten von allen anderen Zugriffen unterscheiden zu können. Hierdurch ist ein detailliertes Abrufprofil möglich, das sogar einer Person zugeordnet werden kann, wenn der Benutzer sich im Rahmen einer Bestellung auch nur ein einziges Mal identifiziert. Der Nutzer weiß nicht, welche Daten auf dem Server über ihn zusammengetragen werden. Heutige Browser sehen verschiedene Einstellungen zum Umgang mit Cookies vor.

Vor einer eventuellen Überprüfung muss der Webanbieter zunächst eine **Datenschutzerklärung im P3P-Format** erstellen. Dies geschieht in einem mehrstufigen Verfahren, in dem zunächst die Datenverarbeitungspraktiken ermittelt und dann am Maßstab des deutschen Datenschutzrechts gemessen werden. Die Ergebnisse werden in einer Datenschutzerklärung ausformuliert. Die Aussagen der Datenschutzerklärung müssen dann in das P3P-Format übertragen werden. Hier bietet sich die Zuhilfenahme so genannter Policy-Editoren an.

Bei den Anbietern von **Policy-Editoren** herrscht bislang ähnliche Zurückhaltung wie bei den Browserherstellern. Die verfügbaren Tools entsprechen noch nicht dem „Look and Feel“ anderer Software für die Webprogrammierung. Neben

Schwächen in der Benutzerfreundlichkeit bereitet es den Webanbietern Schwierigkeiten, die Datenverarbeitungspraxis der eigenen Website den P3P-Grundsätzen entsprechend einzuschätzen. Neben der technischen ist hier eine juristische Bewertung erforderlich. Einen „rechtlich lokalisierten" Policy-Editor, der zumindest die nach deutschem Datenschutzrecht unzulässigen Optionen des P3P-Standards ausschließt und die gesetzlich vorgesehenen Mindestangaben einfordert, gibt es bisher noch nicht. Die Vorgehensweise zur Erstellung einer P3P-Datenschutzerklärung, das grundlegende juristische Rüstzeug sowie **Musterpolicies** für typische Bereiche der Datenverarbeitung im World Wide Web hat das P3P-Projekt jedoch bereitgestellt, sodass der technisch vorgebildete Webanbieter in die Lage versetzt wird, grundsätzlich datenschutzkonforme P3P-Datenschutzerklärungen zu erstellen und anzubieten.

Maßgeblich für die Verwirklichung der mit P3P angestrebten Ziele ist ein flächendeckendes Angebot und die Nutzung von P3P durch Webanbieter und Internet-Nutzer. Um P3P zum **Durchbruch** zu verhelfen, hat das P3P-Projekt technische und rechtliche Voraussetzungen einerseits und das wirtschaftliche und gesellschaftliche Potenzial dieser Technologie andererseits in verschiedenen Kreisen bekannt gemacht. Mit umfangreichen Dokumentationen zum Umgang mit P3P sowohl für Nutzer als auch für Anbieter ist das ULD derzeit führend bei den Bemühungen um die Verbreitung von P3P im deutschsprachigen Raum. Informationen und Präsentationen sind auf der Projektwebseite abrufbar. Nachdem die Möglichkeiten bereitgestellt sind, gilt es nun durch gezielte Ansprache die Vorteile der Anwendung zu verdeutlichen. Außerdem ist ein Herantreten an Softwareentwickler nötig, um P3P in vollem Funktionsumfang in die existierenden Browser zu integrieren. Programme wie Privacy Bird oder IBMs Policy-Editor zeigen bereits, was auf dem Gebiet möglich ist. Insbesondere die Lokalisierung in sprachlicher wie rechtlicher Hinsicht verlangt fundierte Hilfestellung. Hier können wir Unternehmen bei der Integration von Datenschutz in Softwarelösungen unterstützen.

Neben der Praxiseinführung hat das P3P-Projekt auch an der **Weiterentwicklung des P3P-Standards** aktiv teilgenommen. So waren wir gemeinsam mit dem W3C Gastgeber eines Workshops in Kiel zur Entwicklung der Versionen 1.1 und 2.0 des P3P-Standards. Die Teilnahme der Firmen Hewlett Packard, IBM und Microsoft zeigt, dass P3P als zukunftsweisende Technologie gesehen und von den „**Global Players**" der IT-Branche unterstützt wird.

? W3C

Das World Wide Web Consortium (W3C, http://www.w3.org) entwickelt interoperable Technik in Form von Spezifikationen, technischen Richtlinien und Software für das Web. Es wurde im Oktober 1994 gegründet und hat mittlerweile etwa 450 Mitgliedsorganisationen auf der ganzen Welt.

Bei diesem Workshop wurde über die Möglichkeiten einer auf P3P aufbauenden Technologie diskutiert, der so genannten **Enterprise Privacy Authorization Language** (EPAL). EPAL soll die einheitliche Plattform für den Austausch von Datenschutzinformationen in Unternehmens- und Behördennetzwerken werden. Es stellt damit die unternehmensinterne Anbindung an die P3P-Technologie dar.

Eine solche Technologie wird die Möglichkeiten eines unternehmensinternen Datenschutzmanagements nachhaltig beeinflussen und sollte daher bereits frühzeitig unter datenschutzrechtlichen Gesichtspunkten begleitet und erprobt werden.

Zusammenfassend betrachtet stellt sich P3P als **vielversprechende Möglichkeit** dar, den Nutzer in seiner Muttersprache und ohne großen Aufwand über das Datenschutzniveau einer Website zu informieren. Für die IT-Wirtschaft bieten sich die Chancen neuer Dienstleistungsangebote. E-Commerce-Anbietern ermöglicht P3P, nachhaltig um das Vertrauen der Internet-Surfer zu werben und ein Markthemmnis zu beseitigen.

Alle Informationen zu P3P finden sich auf der Projektwebseite unter

www.datenschutzzentrum.de/p3p/

Was ist zu tun?
Softwarehersteller sollten P3P-Applikationen entwickeln oder so verbessern, dass sie den Leistungsumfang dieser Technologie voll ausnutzen. Websiteanbieter sollten prüfen, ob P3P nicht auch ihnen einen nachhaltigen Wettbewerbsvorteil zu relativ geringen Kosten bescheren kann. Internet-Surfer können mit mehr Transparenz durch P3P ihren Selbstdatenschutz verbessern.

8.5 Identitätsmanagement

Das Thema Identitätsmanagement wird zu einem der bestimmenden Themen der nächsten Jahre. Die Verwaltung und insbesondere die Wirtschaft haben das Thema weltweit entdeckt. Wir haben mit einer Studie im Auftrag der EU maßgebliche Grundlagen für die datenschutzrechtliche Beurteilung gelegt. Auch in den nächsten Jahren sind wir als Partner der EU-Projekte PRIME und FIDIS weiterhin an diesem spannenden Zukunftsthema maßgeblich beteiligt.

Für Anonymität und Authentizität in verschiedenen Abstufungen zu sorgen ist Aufgabe von Identitätsmanager-Applikationen (vgl. 23. TB, Tz. 10.6; 24. TB, Tz. 8.5; 25. TB, Tz. 9.6). Es hat sich gezeigt, dass **Identitätsmanagement** vielfältig interpretiert wird: Die Wirtschaft versteht hierunter insbesondere das Managen der Rechtevergabe innerhalb von Firmennetzen an Mitarbeiter und Kunden. Wir haben jedoch vor allem die Nutzer selber im Blick, denen es ermöglicht werden soll, ihre Teilidentitäten bzw. Internet-Accounts im Sinne des Selbstdatenschutzes selbstständig zu verwalten. Erste Applikationen und Systeme wie etwa Microsoft Passport, Liberty Alliance, Yodlee, Novell DigitalMe oder Cookiecooker decken erst kleine Teilbereiche des Identitätsmanagements ab. Bereits in der Entwicklung befindliche Applikationen wie ATUS („A Toolkit for Usable Security“) der Universität Freiburg oder DRIM („Dresden Identity Management“) der TU Dresden zeigen Wege zu einem modernen und intelligenten Identitätsmanagement auf.

Wie im letzten Tätigkeitsbericht angekündigt, haben wir von November 2002 bis September 2003 in Kooperation mit dem Studio Notarile Genghini aus Italien im Auftrag der EU die Studie „**Identity Management Systems (IMS): Identification and Comparison Study**“ erstellt. Die englischsprachige Studie wurde von der Europäischen Union finanziert und von der Gemeinsamen Forschungsstelle der Generaldirektionen der Europäischen Kommission, Institut für technologische Zukunftsforschung (IPTS) Sevilla, begleitet. Das mehr als 300 Seiten umfassende Werk setzt sich ausführlich mit technischen, juristischen und soziologischen Problemstellungen rund um das technisch gestützte Identitätsmanagement auseinander. In acht Kapiteln werden die maßgeblichen Begriffe definiert, die grundsätzlichen Voraussetzungen herausgearbeitet, existierende Applikationen aufgelistet und ausführlich verglichen, das Design für ein umfassendes Identitätsmanagementsystem vorgestellt, die Rolle der EU in diesem Bereich aufgearbeitet und eine mögliche zukünftige Entwicklung erläutert. Ein weiteres zentrales Element der Studie ist die Auswertung einer von uns durchgeführten Befragung unter den derzeit maßgeblichen Entwicklern, Pionieranwendern, Visionären, Forschern und Kritikern von Identitätsmanager-Applikationen.

Durch ihren multidisziplinären Ansatz richtet sich die Studie nicht nur an Entscheidungsträger in Politik und Wirtschaft, sondern kann auch für Entwicklung, Wissenschaft und Anwendung von Nutzen sein. Während der Erstellung der Studie zeigte sich, wie notwendig die Aufarbeitung der vielfältigen Ansätze von Identitätsmanagement war. Nicht zuletzt hat die **Umfrage** ergeben, dass über dieses Thema auch unter Experten unterschiedliche Auffassungen bestehen. Besonderer Wert wurde auf die Betrachtung des nutzergesteuerten Identitätsmanagements gelegt, wobei sich herausstellte, dass alle untersuchten Produkte Mängel aufwiesen. Die Autoren der Studie entdeckten nicht nur bei der Bedienbarkeit, sondern insbesondere bei Datenschutz und Datensicherheit teilweise gravierende Missstände. Dabei zeigt die Studie aber auch, wie ein besseres, datenschutzfreundlicheres bzw. datenschutzgerechteres Identitätsmanagement aussehen könnte.

Eine **Veröffentlichung** der Studie ist für Anfang 2004 geplant. Sie wird zum Download bereitgestellt werden. Hierfür, wie auch für den gesamten Forschungsbereich Identitätsmanagement, wurde 2003 unser Internet-Angebot ausgebaut.

www.datenschutzzentrum.de/idmanage/

Die **Europäische Union** fördert zum Thema Identitätsmanagement ab 2004 das Forschungs- und Entwicklungsprojekt PRIME („Privacy and Identity Management for Europe“) sowie das Projekt FIDIS („Future of Identity in the Information Society“) zum Aufbau eines Expertennetzwerkes. In beiden Projekten sind wir vertreten.

PRIME wird mit insgesamt knapp 10,1 Millionen Euro gefördert. Das Projekt startet im Frühjahr 2004. Ziel ist die Entwicklung von Lösungen, die es dem einzelnen Nutzer ermöglichen, seine Identitäten zu kontrollieren und datenschutzgerechtes Identitätsmanagement zu betreiben. Mitglieder des multidisziplinären Konsortiums sind Firmen wie IBM, Hewlett-Packard, JaTeK, Deutsche Lufthansa, Swisscom und T-Mobile. Daneben sind Universitäten aus Dresden,

Leuven, Tilburg, Mailand, Frankfurt a. M., Aachen, Rotterdam involviert wie auch das Joint Research Centre Ispra, Centre National de la Recherche Scientifique, Chaum LLC, EURECOM und Fondazione Centro San Raffaele des Monte Tabor.

Die Arbeit bei PRIME betrifft nicht nur die Ausarbeitung von Grundlagen. Am Ende soll vielmehr ein erster **Prototyp einer Identitätsmanagement-Applikation** stehen. Um über die Laufzeit von PRIME hinaus eine Nachhaltigkeit der Ergebnisse zu sichern, wurden bereits Kontakte zu **Standardisierungsgruppen** wie W3C, OASIS/WSI, Liberty Alliance, Microsoft/IBM und IETF aufgebaut.

Die Schwerpunkte unserer Arbeit bei PRIME werden insbesondere die datenschutzrechtlichen Aspekte des Identitätsmanagements betreffen, aber umfassen ebenfalls technische und soziologische Themen. Wir sind darüber hinaus für die **Öffentlichkeitsarbeit** zuständig und organisieren die Einbindung von externen Experten in eine Referenzgruppe, die die Meilensteine und Ergebnisse des Projektes kritisch begutachten soll.

Im Gegensatz zu PRIME, das die Entwicklung von anwendungsorientierten Prototypen verfolgt, geht es bei **FIDIS** als interdisziplinärem „Network of Excellence“ vor allem um den Diskurs unter Experten und um die Grundlagenforschung. Wir sind in mehreren der **Workpackages** vertreten. So werden wir mitwirken an der Definition und begrifflichen Ausarbeitung von Identität, Anonymität und Pseudonymität und uns mit Profiling, Identitätsdiebstahl, Datenschutz und Datensicherheit auseinander setzen. Eine leitende Funktion haben wir im Bereich der technischen Ausgestaltung des Identitätsmanagements, was eine Bestandsaufnahme der existierenden Systeme und Applikationen umfasst wie auch Fragen der Biometrie, von Hightech-IDs, der Public Key Infrastructure und des mobilen Identitätsmanagements. Teil dieses Workpackage wird die Organisation eines Workshops sein, der im Zusammenhang mit der Sommerakademie 2004 in Kiel stattfinden soll.

Die Geschäftsführung von FIDIS hat die Johann Wolfgang Goethe-Universität Frankfurt übernommen. Zu den **Projektpartnern** gehören neben dem ULD Universitäten aus Athen, Berlin, Bratislava, Brno (Tschechei), Brüssel, Dresden, Freiburg, Karlstad, Leuven, Reading sowie Tilburg, die Firmen AXSionics AG, Europäisches Microsoft Innovations Center GmbH, IBM sowie SIRRIX AG Security Technologies und die weiteren Forschungsinstitute BUTE-UNESCO Information Society Research Institute, Institute de Recherche Criminelle de la Gendarmerie Nationale, Institut Européen D’Administration des Affaires, Institut für technologische Zukunftsforschung (IPTS) Sevilla, London School of Economics and Political Science, Netherlands Forensic Institute und Virtual Identity and Privacy Research Center.

Was ist zu tun?
Ausgehend von den in der IMS-Studie entwickelten Szenarien sind weitere Einsatzfelder von Identitätsmanagement in den unterschiedlichen Lebensbereichen herauszuarbeiten und datenschutzfreundliche Strategien zu entwickeln. Daraus kann sich die technikgestützte Verwirklichung des Rechts auf informationelle Selbstbestimmung ergeben.

9 Gütesiegel und Audit

9.1 Gütesiegel

9.1.1 Anerkennung von Sachverständigen und Prüfstellen

Sachverständige und Prüfstellen können aufgrund ihrer Fachkunde, Unabhängigkeit und Zuverlässigkeit von uns anerkannt werden und dürfen danach Produkte im Gütesiegelverfahren begutachten.

Wir prüfen IT-Produkte nicht selbst. Diese Aufgabe übernehmen externe Sachverständige und sachverständige Prüfstellen, die wir zuvor in Bezug auf Fachkunde, Unabhängigkeit und Zuverlässigkeit überprüft haben. Wir sprechen auch auf Anfragen interessierter Hersteller und Vertriebsfirmen keine Empfehlungen hinsichtlich einzelner Gutachter aus, sondern führen ein elektronisches **Register der anerkannten Sachverständigen** und **Prüfstellen**, in das diese ihre Spezialgebiete eintragen lassen können. Interessenten entscheiden selbst, wem sie die Begutachtung ihres Produktes anvertrauen.


www.datenschutzzentrum.de/guetesiegel/registga.htm

Anträge auf Anerkennung als Gutachter können fortlaufend gestellt werden. Bis zum Redaktionsschluss sind 14 Gutachter und Prüfstellen anerkannt worden; weitere Anträge sind in der Bearbeitung. Es wurden vier Ablehnungen ausgesprochen, und weitere vier Antragsteller nahmen ihre Anträge nach Beratung zurück. Interessenten können sich – abhängig von der jeweiligen Fachkunde – für die Bereiche Recht und/oder Technik bewerben. Nachzuweisen sind eine adäquate Ausbildung/Fortbildung sowie **entsprechende berufliche Erfahrungen**. Hat der Antragsteller ein einschlägiges Hochschulstudium absolviert, muss er drei Jahre berufliche Erfahrung mit Schwerpunkt „Datenschutzbezogene Sicherheitsprobleme im IT-Sektor“ nachweisen. Eine Anerkennung ist aber nicht nur für Personen möglich, die ein Hochschulstudium absolviert haben. Auch Interessenten, die eine hervorragende anderweitige Aus- und Fortbildung und fünf Jahre einschlägige praktische Erfahrungen nachweisen können, kommen als Sachverständige in Betracht.

Eine Besonderheit besteht darin, dass nicht nur Einzelpersonen als Sachverständige anerkannt werden können, sondern auch Organisationen oder organisatorische Einheiten innerhalb von Organisationen. Die Fachkunde der Leitung bestimmt den Prüfungsscope der Prüfstelle, sodass eine **Prüfstelle** unter einem Leiter mit nachgewiesener Fachkunde Technik keine Rechtsprüfung durchführen darf. Auch die Unabhängigkeit der Sachverständigen und Prüfstellen wird geprüft. Dabei sind sowohl die äußere Unabhängigkeit – gegenüber dem Auftraggeber – als auch die innere Unabhängigkeit – gegenüber dem Arbeitgeber – nachzuweisen.

Sachverständige und Prüfstellen werden unbefristet anerkannt. Gleichwohl handelt es sich bei Fachkunde, Zuverlässigkeit und Unabhängigkeit um Voraussetzungen, die auf Dauer gewährleistet sein müssen. Aus diesem Grund obliegen den

anerkannten Gutachtern und den Prüfstellenleitern diverse Pflichten zur regelmäßigen Beibringung von Unterlagen. Dazu gehören zum Beispiel der Nachweis von besuchten **Fortbildungsveranstaltungen** und die erneute Vorlage von Behördenführungszeugnissen im Abstand von drei Jahren.

Die **Kosten** der Anerkennung richten sich nach einer Gebühren- und Entgeltsatzung und sind entscheidend abhängig von der Qualität und der Vollständigkeit des Antrags. Das Verfahren wird umso günstiger, je weniger Nachforderungen geltend zu machen sind. Die Qualität der Anträge hat sich vor dem Hintergrund dieser Gebührenpolitik deutlich verbessert.

9.1.2 Erfahrungen mit den bisherigen Gutachten

Die Begutachtung verlangt eine enge Verzahnung von Recht und Technik sowie eine sinnvolle Strukturierung. Entscheidend ist dabei die exakte Abgrenzung des Zertifizierungsgegenstandes einschließlich der Definition der Schnittstellen und der Darstellung der Einsatzszenarien.

Mit der Begutachtung von Produkten unter datenschutzrechtlichen und datenschutztechnischen Aspekten haben die meisten der von uns anerkannten Gutachter **Neuland** betreten. Sie können sich nicht auf bereits vorhandene Kriterienkataloge oder Protection Profiles für das jeweilige Produkt stützen, sondern müssen diese erst selbst erarbeiten. Eine Herausforderung ist insbesondere die Verzahnung zwischen Recht und Technik. Die bisherigen Zertifizierungsverfahren haben uns davon überzeugt, dass das Verfahren durch eine weitere Vereinheitlichung und stärkere Strukturierung der Begutachtung gewinnen wird.

Wir haben im Rahmen der kontinuierlichen Ergänzung und Fortschreibung unserer Anforderungskataloge und Verfahren unsere Erkenntnisse aus den abgeschlossenen und laufenden Antragsverfahren aufgearbeitet und in **Regeln** zur **Strukturierung** und **Erarbeitung** von **Gutachten** zusammengefasst. Durch die Umsetzung dieser Regeln werden die Gutachten künftig einheitlich strukturiert sein und die Prüfung und Vergleichbarkeit der Gutachten erleichtern; dies sorgt auch für eine geringere Verfahrensdauer und niedrigere Gebühren. Am Anfang eines jeden Gutachtens steht die umfassende Beschreibung des **Begutachtungsgegenstands** einschließlich aller Schnittstellen sowie der Primär- und Sekundärdaten; dabei ist der Gegenstand der Begutachtung sinnvoll von der Umgebung abzugrenzen.

Profil und Bewertung der einzelnen Anforderungen müssen vollständig vorhanden und voneinander deutlich getrennt sein sowie miteinander korrespondieren. Bewertet werden nur Aspekte, die im **Anforderungsprofil** genannt wurden; alle im Anforderungsprofil genannten Aspekte werden adressiert. Das Gutachten muss aus sich heraus verständlich sein, d. h. relevante Rechts- und Technikfragen sind sämtlich zu erläutern; auch in kooperativer Zusammenarbeit erstellte Teilgutachten (Recht/Technik) müssen aus sich heraus einzeln verständlich sein. Es ist ein **Datenflussmodell** anzufertigen und zu erläutern. Dabei ist insbesondere auf die Identifikation der unterschiedlichen Datenarten zu achten, da die hier gewonnenen Erkenntnisse der Strukturierung des folgenden Gutachtens dienen.

Die Praxis hat gezeigt, dass ein Bedürfnis nach der Begutachtung und Zertifizierung von Produkten mit **multiplen Einsatzbereichen** besteht. Dies ist sowohl mit einem dedizierten Einsatzszenario als auch ohne Benennung eines konkreten Einsatzzieles möglich. Bei allgemein gehaltener Zertifizierung – ohne Einsatzszenario – muss dem Produkt ein Dokumentationsteil beigefügt werden, in dem sowohl aus technischer als auch aus rechtlicher Sicht deutlich dargestellt ist, wie das Produkt datenschutzgerecht eingesetzt werden kann und in welcher Konfiguration/Installation und mit welchen Schnittstellen und Randbedingungen das Produkt zertifiziert wird (Transparenz).

Soweit möglich, müssen darüber hinaus die möglichen Einsatzbereiche des Produktes deutlich dargestellt werden, sodass eine Art „**Einsatzbandbreite**“ des Produktes definiert wird. Die Schnittstellen zu möglichen angeschlossenen Applikationen (Frontends, Backends, anschließende Applikationen) müssen eindeutig definiert sein. Auch bei Produkten mit vielfältigen Einsatzgebieten ist in der Regel eine rechtliche Begutachtung notwendig. Es ist mindestens erforderlich, die auch ohne Betrachtung eines konkreten Einsatzszenarios infrage kommenden rechtlichen Regelungen zu identifizieren und das Produkt an deren Maßstab zu prüfen und zu bewerten. Grundlegende, allgemeine Vorschriften zum Datenschutz sind in jedem Fall zu untersuchen.

Produkte mit vielfachen Einsatzmöglichkeiten erhalten eine Zertifizierung bei eingeschränkter rechtlicher Begutachtung mit **klarem Hinweis** auf ihre besonderen universellen/multiplen Eigenschaften. Dabei muss der genaue Gegenstand der Zertifizierung deutlich gemacht werden. Antrag und Zertifikat müssen sich auch hier entsprechen. Der Hersteller muss auch in der Folge zweifelsfrei kenntlich machen, dass sein Produkt das Gütesiegel ohne konkretes Einsatzgebiet und gegebenenfalls ohne dedizierte Applikation bzw. Frontend erhalten hat.

9.1.3 Fortentwicklung der Produktkriterien

Mit den gewonnenen Erfahrungen aus den durchgeführten Gütesiegelverfahren geht die Weiterentwicklung des Anforderungskataloges einher. Seitens der Gutachter besteht verständlicherweise ein Interesse an einem möglichst exakt gefassten und bei der Begutachtung einfach handhabbaren Kriterienkatalog, andererseits muss der Katalog der Produktkriterien für unterschiedlichste IT-Produkte geeignet sein. Eine reine Prüfcheckliste kommt hierbei nicht in Betracht, da sich die Anforderungen an die zu begutachtenden IT-Produkte unterscheiden.

Zur **CeBIT 2003** haben wir eine aktuelle Version des Anforderungskataloges für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens, Kommentare und Hinweise zum Anforderungskatalog und Anforderungen an die Produktdokumentation als Broschüre und als über das Internet

> ***? Anforderungskatalog***
>
> *Der Anforderungskatalog stellt beispielhaft Datenschutz- und Datensicherheitsanforderungen sowie in ihrem Zusammenhang zu berücksichtigende Fragestellungen nach wichtigen Rechtsnormen dar. Er gibt eine Mustergliederung für das Abarbeiten von Anforderungen jeweils nach Datenart vor (Prüfschema).*

abrufbares Dokument veröffentlicht. In dieser Fortschreibung des Anforderungskataloges wird unter anderem Möglichkeiten der **Modularisierung** und der **Kompatibilität** mit den Common Criteria (CC) nachgegangen. In Kooperation mit anderen Behörden und der Privatwirtschaft, z. B. in Form einer Projektgruppe „Datenschutzaudit“, wird auch weiterhin an der Modularisierung und Kompatibilität mit anderen Zertifizierungswerken gearbeitet. Darüber hinaus wurden in der Neuauflage des Anforderungskataloges die **Anforderungen an die Produktdokumentation** überarbeitet.

www.datenschutzzentrum.de/download/proddoku.pdf

Gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnologie (BSI) hat ein Workshop zu den **Common Criteria** stattgefunden. Hier konnten wir nicht nur von der Erfahrung des BSI mit den Common Criteria profitieren, sondern es soll nunmehr auch geprüft werden, ob und in welchem Umfang die CC für das Datenschutz-Gütesiegel nutzbar gemacht werden können. Für die praktische Durchführung von Gütesiegelverfahren wird es aus den genannten Gründen zwar nicht möglich sein, Checklisten zur Verfügung zu stellen, es ist aber denkbar, Kernteile von Schutzprofilen auszuarbeiten und diese als Module für die Gutachter (z. B. als Modul für Verschlüsselung o. Ä.) zur Verfügung zu stellen. Wir werden dieser Frage weiter nachgehen. Darüber hinaus ist es für die Aussagekraft und Vergleichbarkeit des schleswig-holsteinischen Gütesiegels sinnvoll und wünschenswert, sich an **internationalen Standards** für die Zertifizierung von IT-Produkten zu orientieren.

Wir werden uns weiter aktiv an der **Projektgruppe „Datenschutzaudit“** beteiligen und im ständigen Dialog mit den Gutachtern stehen. Die Abstimmung mit bestehenden und bewährten Zertifizierungswerken zur IT-Sicherheit stellt ein komplexes Feld dar. Die Übertragung dieser Kriterienkataloge auf das Datenschutz-Gütesiegel ist nicht ohne weiteres möglich, da die Anforderungen des Datenschutzes aufgrund der zu berücksichtigenden gesetzlichen Grundlagen an vielen Stellen nicht deckungsgleich mit den Fragen der IT-Sicherheit sind. Ein Modulkonzept könnte auch ein Weg zur Angleichung an internationale Verfahren zur IT-Sicherheit sein. Die Arbeit in den Projektgruppen wie auch die praktische Durchführung von Gütesiegelverfahren werden auch weitere Erkenntnisse für die nächste Version des Anforderungskataloges bringen.

> ***? Projektgruppe Datenschutzauditierung***
>
> *Projektgruppe des Sektorkomitees Security und gemeinsame Initiative von öffentlichen und privaten Stellen Deutschlands, die durch die Entwicklung von Kriterien für die Anerkennung von Gutachtern und Produkt- und Verfahrensprüfung die in der Folge des Bundesdatenschutzauditgesetzes nötigen Prozesse starten und die Realisierung des Audits beschleunigen wollen.*

9.1.4 Rezertifizierung von Produkten

Wir haben Kriterien zur Rezertifizierung von IT-Produkten entwickelt, die für die Dauer von zwei Jahren ein Datenschutz-Gütesiegel erlangt haben. Diese Regelungen enthalten Schwellenwerte, die bei der Entscheidung über die Notwendigkeit einer Rezertifizierung bei Änderungen der Produkte Anwendung finden.

Datenschutz-Gütesiegel werden für die Dauer von zwei Jahren vergeben. Diese **Begrenzung der Laufzeit** schafft den Ausgleich zwischen der Planungssicherheit des Herstellers und der Tatsache, dass sich juristische und technische Rahmenbedingungen im Bereich der Informationstechnologie dynamisch entwickeln. Der Anforderungskatalog für Produkte ist daher ebenfalls nicht statisch, sondern wird ständig fortgeschrieben. In die Fortentwicklung des Kataloges können zukünftig auch **Protection Profiles** einfließen, wie sie zurzeit – etwa im Rahmen des Projektes PETTEP (Privacy Enhancing Technologies – Testing and Evaluation Project) – erarbeitet werden. Wir arbeiten in diesen Fragen auch mit dem Bundesamt für Sicherheit in der Informationstechnik zusammen.

> **? *Protection Profiles – Schutzprofile***
>
> *Schutzprofile ermöglichen es, eine Sicherheitslage anhand von Gefährdungen, Annahmen über die Betriebsumgebung der IT, Sicherheitszielen usw. zu beschreiben. Mithilfe der Anforderungen in den Common Criteria wird dann eine Musterlösung auf angemessen abstrakter Ebene beschrieben.*

Nachdem wir im Dezember 2002 das erste Datenschutz-Gütesiegel vergeben konnten, haben wir in diesem Jahr das Verfahren zur Rezertifizierung entwickelt und zunächst im August 2003 im Rahmen eines Workshops im Kreise der anerkannten Sachverständigen und Prüfstellen vorgestellt und diskutiert. Das Verfahren wurde der Öffentlichkeit zur **CeBIT 2004** in Hannover bekannt gegeben. Dies gibt den Herstellern bereits zertifizierter Produkte ausreichend Vorlauf, sich auf die Rezertifizierung ihres Produktes vorzubereiten. Zukünftig weiß außerdem jeder interessierte Hersteller bereits am Anfang der Entscheidung zu einer Zertifizierung mit dem Datenschutz-Gütesiegel über das Verfahren, die Kosten und die Umstände einer Rezertifizierung Bescheid.

Nach dem Ablauf der zweijährigen Laufzeit für das Datenschutz-Gütesiegel ist eine Rezertifizierung in jedem Fall erforderlich, um auf dem neuesten Stand werben zu können, auch wenn das Produkt nicht verändert wurde. Wurde das Produkt nicht verändert, sondern ist gegenüber dem zertifizierten Prüfmuster „**baugleich**“ geblieben, so beauftragt der Hersteller einen Gutachter oder eine Prüfstelle mit der erneuten Prüfung des Produktes einschließlich der Produktdokumentation. Die Verwendung bestehender Unterlagen, z. B. aus dem ursprünglichen Zertifizierungsverfahren, ist möglich. Der Gutachter bzw. die Prüfstelle prüft und aktualisiert gegebenenfalls das Anforderungsprofil hinsichtlich eventuell erfolgter gesetzlicher Änderungen sowie hinsichtlich des Standes der Technik. Auf dieser Basis ist dann eine Neubewertung des Produktes vorzunehmen. In der Regel ist dieses Verfahren wesentlich einfacher als eine Erstzertifizierung.

Sollte das Produkt gegenüber der zertifizierten Prüfversion verändert worden sein, legt der Hersteller dem von ihm beauftragten Gutachter bzw. der Prüfstelle das **veränderte Produkt**, die aktualisierte Dokumentation sowie zusätzlich eine Aufstellung der Veränderungen (Synopse) vor. Danach prüft der Gutachter/die Prüfstelle die Anforderungsprofile in rechtlicher und technischer Hinsicht und bewertet das Produkt anhand der so gewonnenen aktuellen Profile neu.

Situationen, die eine Rezertifizierung erforderlich machen, können auch schon **während der zweijährigen Laufzeit** eintreten, z. B. wenn das Produkt zwar kaum verändert wird, aber nicht mehr „baugleich“ mit der geprüften Version ist. Wenn Veränderungen die Vorschriften über den Datenschutz und die Datensicherheit tangieren, stellt der Hersteller dies eigenverantwortlich fest und nimmt Kontakt zu den Gutachtern/der Prüfstelle auf. Er legt das veränderte Produkt mit der fortgeschriebenen Dokumentation sowie einer Aufstellung der Veränderungen (Synopse) vor. Der Gutachter/die Prüfstelle stellt das Ausmaß der Veränderung fest und entscheidet, ob die **Erheblichkeitsschwellen** für die Rezertifizierung überschritten werden.

Überschreiten die im Produkt vorgenommenen Veränderungen nach der Einschätzung des Gutachters/der Prüfstelle die definierten Erheblichkeitsschwellen, so ist das **Verfahren zur Rezertifizierung** einzuleiten; das Siegel wird am Ende des Verfahrens erneut für den vollen Zeitraum von zwei Jahren erteilt. Die **Kosten** der Rezertifizierung sind in aller Regel deutlich niedriger als bei einer Erstzertifizierung. Die Frage, an welche Veränderungen die Pflicht zu einer erneuten und vorzeitigen Zertifizierung zu knüpfen ist, ist schwierig eindeutig zu beantworten. Wir haben uns der Definition so genannter Erheblichkeitsschwellen mithilfe von Beispielen angenähert. Veränderungen können in folgenden Bereichen auftreten (Auszug):

- Veränderungen des Produktes: Änderung der Versionsnummer, datenschutzrelevante Funktionsänderungen bzw. -erweiterungen,
- Veränderungen des Einsatzgebietes, die die Heranziehung weiterer/anderer rechtlicher Grundlagen erforderlich machen,
- Veränderung der technischen und/oder rechtlichen Grundlagen.

Weitere Informationen zum Thema Rezertifizierung/Erheblichkeitsschwellen sind zu finden unter

www.datenschutzzentrum.de/download/rezert.pdf

9.1.5 Gütesiegel als Vergabekriterium bei Ausschreibungen

Der mit dem Datenschutz-Gütesiegel angestrebte Wettbewerbsvorteil realisiert sich durch die Bevorzugung gesiegelter Produkte in öffentlichen Ausschreibungen. Wir arbeiten daran, dass die öffentlichen Stellen des Landes bei Beschaffungen das Datenschutz-Gütesiegel als Auswahl- und Bewertungskriterium in Ausschreibungen aufnehmen. Erste Erfolge sind zu verzeichnen.

> ***Im Wortlaut: § 4 Absatz 2 LDSG***
>
> *Produkte, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde, sollen vorrangig eingesetzt werden. Die Landesregierung regelt durch Verordnung Inhalt, Ausgestaltung und die Berechtigung zur Durchführung des Verfahrens.*

Mittel- und langfristig wird das Datenschutz-Gütesiegel erfolgreich sein, wenn die Unternehmen, die finanzielle Mittel in die Zertifizierung investieren, damit auch den erhofften **Wettbewerbsvorteil** realisieren können. Konkret heißt das: Gesiegelte Produkte müssen sich in Ausschreibungen signifikant gegenüber nicht gesiegelten Produkten durchsetzen. Die Regelung des § 4 Absatz 2 LDSG, die öffentlichen Stellen vorschreibt, gesiegelte Produkte bevorzugt zu beschaffen, setzt dieses Ziel rechtlich um. Nachdem wir inzwischen zwölf Gütesiegel vergeben haben, sind wir aktiv geworden, um in den Beschaffungsstellen des Landes Schleswig-Holstein das Bewusstsein für die Aufnahme des Siegels in die Ausschreibungen zu schaffen bzw. zu stärken.

Mit dem **Gebäudemanagement Schleswig-Holstein** haben wir eine Vereinbarung darüber getroffen, in welcher Weise das Datenschutz-Gütesiegel in die Verdingungsunterlagen der Ausschreibungen und die Bewertung der angebotenen Produkte einfließen wird. Das Datenschutz-Gütesiegel wird in Zukunft mit einem Anteil von 30 % bewertet. Wir haben außerdem **Städte**, **Kreise** und **Gemeinden** sowie **dataport** als zentrale Beschaffungsstellen für Behörden angeschrieben. Auch dataport hat zugesichert, bei eigenen Beschaffungen und bei Ausschreibungen von Rahmenverträgen im Hard- und Softwarebereich das Datenschutz-Gütesiegel in die Leistungsbeschreibungen aufzunehmen; dataport wird darüber hinaus im Rahmen der laufenden Geschäftsbeziehungen ihre jeweiligen Partner auf die Vorteile des Datenschutz-Gütesiegels hinweisen. Ein Landkreis entschied sich in einem Beschaffungsvorgang zwar für ein Produkt ohne Gütesiegel, machte die Auftragsvergabe aber vom nachträglichen Erwerb des Gütesiegels abhängig. Es ist auch sinnvoll, das Datenschutz-Gütesiegel als Kriterium in die Ausschreibung aufzunehmen, wenn in einer Produktgruppe noch kein Gütesiegel vergeben wurde. Den Anbietern wird dadurch signalisiert, dass sie in Zukunft mit entsprechenden Qualitätsanforderungen rechnen müssen.

Das Datenschutz-Gütesiegel hat auch das Ziel, die Einhaltung der Datenschutzregeln für die Verwaltungsbehörden einfacher und rationeller zu gestalten. Die nach dem LDSG erforderliche **Vorabkontrolle** vor der Einrichtung oder wesentlichen Änderung automatisierter Verfahren kann z. B. dadurch erheblich erleichtert werden, dass für gesiegelte Produkte ein technisch-organisatorisches Einsatz-

modell einschließlich Hinweisen für Verfahrensbetreuer bereits im Rahmen der Gütesiegelverfahren verlangt wurde, das konkrete Anhaltspunkte für die Praxis geben soll; darüber hinaus wird auch unser **Kontrollaufwand** sowie in der Folge der übliche Erörterungsaufwand **reduziert**.

Einige Hersteller konnten uns bereits einige Wochen bzw. Monate nach der Erlangung des Datenschutz-Gütesiegels durch ihr Produkt von Vertriebserfolgen mithilfe des Gütesiegels berichten.

Was ist zu tun?
Öffentliche Stellen in Schleswig-Holstein müssen bei Beschaffungen von IT-Produkten darauf achten, Datenschutz-Gütesiegel als Kriterium in Ausschreibungen aufzunehmen, damit der Datenschutz von Anfang an in die Technik zum gegenseitigen Vorteil aller Beteiligten eingebaut wird.

9.1.6 PETTEP – Privacy Enhancing Technologies Testing and Evaluation Project

Privacy Enhancing Technologies machen sich auf dem Markt auch heute noch rar. Was sind Kriterien für diese datenschutzfördernde Technik? Wie kann man erkennen, dass ein Produkt wirklich datenschutzfördernd ist? Das Datenschutz-Gütesiegel kann Vorbild für internationale Datenschutzkriterien sein, an denen sich Technik messen lässt.

Parallel zu unseren langjährigen Überlegungen zum Datenschutz-Gütesiegel entwickelten sich ähnliche Gedanken bei Datenschutzkollegen im Ausland. Besonders aktiv war die Datenschutzdienststelle („Information and Privacy Commissioner“) Ontario, Kanada, die im März 2001 damit begann, ein internationales Team aufzubauen, das Kriterien für datenschutzfördernde Technik entwickeln soll. Das Team „**PETTEP – Privacy Enhancing Technologies Testing and Evaluation Project**“ besteht aus Experten aus Verwaltung, Wirtschaft, Wissenschaft und der Datenschutzszene. Mitglieder kommen u. a. von dem Canadian Security Establishment, dem US Department of Defense, von IBM, Microsoft und von Datenschutzbeauftragten, auch aus Kiel.

Zum **PETTEP-Gründungsworkshop** mit internationaler Beteiligung hatten wir im September 2001 nach Kiel eingeladen. Seitdem hat es weitere Workshops in San Francisco, Dresden und nochmals in Kiel (anlässlich der Sommerakademie 2003) gegeben, in denen die nach und nach erarbeiteten Resultate vorgestellt und diskutiert wurden. Aktuell wird versucht, die international anerkannten Datenschutzeckpunkte „**Fair Information Practices**“ in ein Schutzprofil nach den international standardisierten Sicherheitskriterien Common Criteria (vgl. 25. TB, Tz. 10.3.3) zu gießen.


www.cdt.org/privacy/guide/basic/fips.html

Auf unseren Vorschlag wurden die Vorlagen u. a. um Kriterien für **Datensparsamkeit** erweitert, die von den „Fair Information Practices“ nicht explizit genannt werden, denen aber zumindest ansatzweise bereits in den Common Criteria Rech-

nung getragen wird. Zusätzlich wird gesammelt, was an Datenschutzforderungen nicht von den Common Criteria in der jetzigen Fassung abgedeckt wird, um Nachbesserungsvorschläge in die internationale Standardisierung zu tragen. Wir bringen die Erfahrungen mit unserem Datenschutz-Gütesiegel in die PETTEP-Arbeit ein und verfolgen aufmerksam andere Ansätze aus der ganzen Welt. Unsere Motivation für die Mitwirkung an PETTEP ist es, unsere schleswig-holsteinischen Gütesiegelkriterien in die weltweite Fachdiskussion einzubringen.

Was ist zu tun?
Die Idee der Datenschutz-Gütesiegel muss im internationalen Bereich weiter verbreitet werden. Experten sind eingeladen, bei PETTEP mitzuwirken, um die Entwicklung und Standardisierung von Datenschutzkriterien voranzubringen.

9.2 Datenschutz-Audit

9.2.1 Allgemeine Erfahrungen

Das Datenschutz-Audit hat sich in Schleswig-Holstein etabliert. Der Nutzen für die Behörden ist größer als erwartet und rechtfertigt den mit einer sorgfältigen Bestandsaufnahme verbundenen Aufwand. Vor allem aber bewirken die Audits eine deutliche Verbesserung des Datenschutzniveaus. Wir können zwischenzeitlich auf eine zweijährige Erfahrung zurückblicken. Ein erstes Resümee ist daher gerechtfertigt.

Das Datenschutz-Audit erweist sich als **außerordentlich erfolgreich**. Das Interesse der Behörden an diesem Angebot ist weitaus größer, als wir in unseren optimistischsten Planungen angenommen haben. Die zur Verfügung stehenden personellen Kapazitäten sind für die nächsten 18 Monate voll ausgebucht. Es konnten bereits **sieben Audits** erfolgreich **abgeschlossen** werden. An **acht Audits** wird zurzeit in den betreffenden Behörden gearbeitet. Wir begleiten diese Projekte parallel. Mit einer etwa gleich großen Zahl von Behörden stehen wir in Vertragsverhandlungen. Unser Hauptproblem besteht darin, ein Zeitfenster zu finden, in dem wir die auf uns entfallenden Arbeiten abwickeln können.

Die Gründe für die **positive Reaktion** der Behörden auf das Auditangebot sind vielschichtig. Im Wesentlichen werden uns folgende genannt:

- Trotz des durchaus strengen formalen Gerüstes für das Auditverfahren bietet es eine ausreichende **Flexibilität**, um die jeweiligen Besonderheiten in den Behörden und bezüglich des Auditierungsgegenstandes zu berücksichtigen.
- Der erfolgreiche Abschluss eines Audits stellt für die Behörden einen „**Mehrwert**“ dar, da damit in der Regel wesentliche Optimierungen der Verarbeitungsprozesse auch jenseits der Datenschutzfragen verbunden sind.
- Die Behörden können den Anteil der **personellen Unterstützung** durch uns bei der Durchführung des Audits weitgehend selbst festlegen und noch im Verlaufe des Verfahrens verändern.

- **Defizite**, Fehlentwicklungen usw., die im Rahmen des Audits festgestellt und behoben werden, sind nicht Gegenstand von Darstellungen in unserem Tätigkeitsbericht. Es können **Teilbereiche** der Verarbeitungsprozesse in einer Behörde auditiert und deren Ergebnisse auf andere Teilbereiche übertragen werden (Prinzip des „**best practice**“).

Die Vorgaben über die Durchführung des Auditverfahrens in den Anwendungsbestimmungen zum Datenschutz-Audit sind abstrakt und allgemein gehalten. Wir haben daher für die interne Bearbeitung von Auditverfahren ein **Ablaufschema** entwickelt. Darin werden die organisatorischen Abläufe festgehalten und Kriterien für die Beurteilung eines Auditverfahrens vorgegeben. Die einzelnen Schritte des Auditverfahrens, insbesondere Bestandsaufnahme und Datenschutzmanagementsystem, werden in ihren Inhalten genau erläutert. Anhand dieser Darstellung ist eine einheitliche Überprüfung durch uns gewährleistet.

Die **Abwicklung** der Auditierungsverfahren läuft allerdings häufig etwas anders ab, als wir es uns in der Theorie vorgestellt haben. Von den fünf Schritten

- Bestandsaufnahme,
- Festlegung der Datenschutzziele,
- Einrichtung des Datenschutzmanagementsystems,
- Begutachtung und
- Verleihung des Auditzeichens

erfordert die **Bestandsaufnahme** einen zunehmend großen zeitlichen Aufwand. Außerdem dauern viele Audits wesentlich länger als ursprünglich geplant. Die Gründe hierfür sind positiver Natur: Die Praktiker in den Behörden haben schnell erkannt, dass bereits der Prozess einer exakten und umfassenden Bestandsaufnahme unter unserer methodischen und oft auch inhaltlichen Regie quasi automatisch eine Vielzahl von Schwachstellen und Inplausibilitäten zutage treten lässt. In mehreren Fällen hat es dazu geführt, dass das gesamte IT-Konzept „über den Haufen geworfen“, ein neues Konzept entwickelt und das unterbrochene Audit auf der neuen Basis fortgesetzt wurde. Unterbrechungszeiten von mehreren Monaten sind dabei keine Seltenheit. In dieser Zeit reißt der Kontakt zu uns nicht ab. In regelmäßigen Abständen gibt es Zwischenkontrollen, um zu vermeiden, dass durch Einzelfestlegungen die Zielrichtung des Datenschutzmanagementsystems infrage gestellt wird.

In anderen Fällen wurden unsere Mitarbeiter besonders intensiv in die Bestandsaufnahme eingebunden, weil eigenes Personal nicht aus dem Tagesgeschäft abgezogen werden konnte oder weil es ihm schwer fiel, die selbst entwickelten Lösungen infrage zu stellen. Bemerkenswert war in allen Fällen, dass nahezu alle rechtlich bzw. sicherheitstechnisch besonders kritischen Sachverhalte bereits während der Bestandsaufnahme einer Lösung zugeführt werden konnten. Die Formulierung der **Datenschutzziele** und die Ausgestaltung des **Datenschutzmanagementsystems** stellten sich oft nur als eine Auswertung der bereits zu einem früheren Zeitpunkt getroffenen Vorentscheidungen dar. Diese Arbeiten fielen zeitlich kaum noch ins Gewicht.

Grundsätzlich soll der **personelle Aufwand**, den die Unterstützung der Behörden bei der Durchführung des Audits und die Zertifizierung erfordern, durch Gebühren gedeckt werden. Dieses Ziel konnten wir noch nicht voll erreichen (vgl. Tz. 9.1). Das liegt zum einen daran, dass der Umfang unserer Beteiligung an den Audits vorab nur schwer zu schätzen ist. Zum anderen sind die Budgets der Behörden für derartige Projekte sehr schmal. Nachforderungen bei einem erhöhten Aufwand unsererseits sind praktisch nicht durchzusetzen. Die dauerhafte Finanzierung des für die Audits eingesetzten Personals muss daher alsbald sichergestellt werden. Das dürfte auch im Interesse des Landes und der „kommunalen Familie“ liegen.

Das Land hat nämlich ein „gesamtwirtschaftliches“ Interesse daran, dass auch die Kommunen über das **Landesnetz** kommunizieren. Wie kann man aber 237 Verwaltungschefs davon überzeugen, dass ein solcher Anschluss keine negativen Folgen für die eigenen IT-Systeme haben kann? Dies könnte über ein Audit zu bewerkstelligen sein. Auch auf der Ebene der Kreise werden die einzelnen Gemeinden zu einer Vernetzung ihrer Systeme über Kreisnetze nur bereit sein, wenn ein unabhängiger Dritter die Risikolosigkeit dieser Verfahrensweise bescheinigt hat.

Außerdem will der Innenminister die Qualität der **Melderegister** dadurch erhöhen, dass alle Meldebehörden technisch miteinander verknüpft werden, um bei Ummeldungen durch Datenabgleiche Unstimmigkeiten feststellen zu können. Ziel ist sogar eine deutschlandweite Vernetzung. Die dafür erforderlichen **Datendrehscheiben** und Clearing-Stellen bedürfen einer ganz besonders sorgfältigen und allseits akzeptierten Zertifizierung. Schließlich werden die meisten E-Government-Projekte auf Internet-Basis ablaufen. Das damit verbundene „Wurmrisiko“ wird nur über eine zertifizierte Schnittstelle des Landesnetzes gemildert werden können.

> ***? KomFIT***
>
> *Das Kommunale Forum für Informationstechnik ist die gemeinsame Koordinierungs- und Beratungsstelle des Städteverbandes Schleswig-Holstein, des Schleswig-Holsteinischen Landkreistages und des Schleswig-Holsteinischen Gemeindetages für den Bereich der kommunalen Informations- und Kommunikationstechnik. Die Arbeitsergebnisse werden allen Kommunen zur Verfügung gestellt.*

Vor dem Hintergrund, dass das schleswig-holsteinische Datenschutz-Audit in absehbarer Zeit durch ein Bundesauditgesetz und entsprechende Gesetze in anderen Bundesländern „Mitstreiter“ bekommen könnte, wird das im Augenblick zwischen dem KomFIT und uns diskutierte Thema der **Synchronisation** von Zertifikaten bald eine bundesweite Resonanz finden. Deshalb ist es zu begrüßen, dass auf dem letzten KomFIT-Workshop sich eine Arbeitsgruppe speziell mit der Fortentwicklung der Zertifizierung kommunaler Software beschäftigt hat. Endgültige Beschlüsse sind noch nicht gefasst worden. Es gibt aber Anzeichen, dass sich beide Verfahren methodisch aneinander angleichen werden. Das wird ihren Stellenwert im Gesamtgefüge der Zertifikate heben.

In der „**Auditpipeline**“ befinden sich derzeit z. B. das Projekt „Verwaltung 2000“ und das Netz des Kreises Segeberg, das Landesnetz, das Sprachnetz, das Terminal-Server-Konzept, der Stadt Bad Schwartau, das elektronische Handelsregister, die Vertrauensstelle des Krebsregisters und der Internet-Anschluss der Stadt Neumünster.

Alle Kurzgutachten des ULD zu den abgeschlossenen Auditverfahren finden sich im Internet unter


www.datenschutzzentrum.de/audit/register.htm

9.2.2 Datenschutz-Audit für das Personalverwaltungs- und Informationssystem in Norderstedt

Mit der Verleihung des Datenschutzauditzeichens an die Stadt Norderstedt im Rahmen der Sommerakademie 2003 konnten die im Jahre 2001 begonnenen Pilotverfahren zum Datenschutz-Behördenaudit endgültig abgeschlossen werden.

Das Auditverfahren bei der Stadt Norderstedt bezog sich auf die Einführung eines **Personalverwaltungs- und Informationssystems**, das der Wahrnehmung von Personalverwaltungsaufgaben dient. Bei der Einführung des Systems wurden die geltenden Vorschriften zu Datenschutz und Datensicherheit von vornherein berücksichtigt. Bereits vor Beschaffung der Software erstellte die Stadt ein ausführliches Pflichtenheft, in dem die an das System zu stellenden Anforderungen dargelegt wurden. Während des Auditverfahrens wurde dieses Pflichtenheft einer ständigen Bearbeitung und Anpassung im Hinblick auf die datenschutzrechtlichen Vorgaben unterzogen. Geeignete technische Maßnahmen sorgen für deren Einhaltung. Es ist Sorge dafür getragen, dass eine laufende Anpassung an gegebenenfalls geänderte sachliche und rechtliche Anforderungen auch in Zukunft stattfinden wird.

Unsere Begutachtung der von der Stadt Norderstedt vorgelegten Datenschutzerklärung zeigt, dass die Stadt Norderstedt bei der Einführung des Personalverwaltungs- und Informationssystems ein **gutes datenschutzrechtliches Niveau** erreicht hat. Entsprechend den Vorgaben unserer Ausführungsbestimmungen zu den Einzelheiten des Auditverfahrens hat die Stadt Norderstedt ein **Datenschutzmanagementsystem** eingerichtet, das die internen Organisationsregelungen der Stadtverwaltung im Hinblick auf die Erreichung der in der Bestandsaufnahme genannten Datenschutzziele sowie die Einhaltung der datenschutzrechtlichen Vorgaben enthält. Es ist geeignet, eine dauerhafte Aufrechterhaltung des erreichten Datenschutzniveaus zu gewährleisten.

Was ist zu tun?
Das abgeschlossene Verfahren zeigt, dass das Datenschutz-Audit ein Instrument ist, das in der Praxis zu einer tatsächlichen Verbesserung des Datenschutzes beiträgt.

9.2.3 Datenschutz-Audit für den Internet-Anschluss des Kreises Schleswig-Flensburg

Auch wenn zwei Kreisverwaltungen beim Anschluss ihres lokalen Netzwerks sehr unterschiedliche technische Lösungen gewählt haben, sind beide Ergebnisse so gut, dass ihnen ein Auditzeichen verliehen werden konnte. Dies zeugt von der Flexibilität des Verfahrens.

Nachdem bereits vor zwei Jahren der Kreis Ostholstein die Verknüpfung seines lokalen Netzes in der Kreisverwaltung mit dem Internet erfolgreich auditieren ließ (vgl. 24. TB, Tz. 10.6), hat der **Kreis Schleswig-Flensburg** im Jahr 2003 nachgezogen. Zwar ging es auch hier um die Anbindung an das Internet, aber nicht um die gleiche technische Realisierung. Während in Ostholstein der Übergang über dataport realisiert worden ist und man problematische Internet-Seiten über eine so genannte Positivliste blockt, hat man in Schleswig-Flensburg eine **eigene Firewall** installiert und setzt spezielle Softwareprodukte ein, um gegen Angriffe aus dem Internet gewappnet zu sein. So unterschiedlich die Techniken auch sein mögen, sie führen zu vergleichbar guten Ergebnissen. Auch die Gesamtorganisation des Internet-Anschlusses bewegt sich in beiden Verwaltungen auf einem vergleichbaren hohen Niveau. Dazu gehört selbstverständlich die E-Mail-Verschlüsselung sowie die Protokollierung und systematische Auswertung sicherheitsrelevanter Ereignisse. Beide Projekte wurden vom Verwaltungsmanagement initiiert, das die Durchführung konstruktiv begleitete.

Wegen der im Pilotprojekt beim Kreis Ostholstein gewonnenen Erfahrungen und durch eine sehr gute Zusammenarbeit zwischen der IT-Abteilung und den **behördlichen Datenschutzbeauftragten** konnte der Kreis Schleswig-Flensburg die Phasen „Bestandsaufnahme“, „Festlegung der Datenschutzziele“ und „Einrichtung eines Datenschutzmanagementsystems“ weitestgehend ohne unsere Unterstützung abwickeln. Diese idealtypische Konstellation führte dazu, dass nur unwesentliche Kosten für die Begutachtung und Zertifizierung durch uns anfielen.

Was ist zu tun?
Es ist zu hoffen, dass diese beiden Kreise auch Vorreiter bei der Auditierung ihrer Kreisnetze sein werden.

10 Aus dem IT-Labor

10.1 Wireless LAN und Bluetooth

Keine Kabel mehr, über die man stolpern kann, einfach auspacken, anmachen und alles läuft – in der Werbung werden drahtlose Netzwerke (Wireless LAN) als bequem, flexibel und unkompliziert dargestellt. In immer mehr Firmen und Privathaushalten wird daher schon WLAN-Technik eingesetzt. Das freut nicht nur die Hersteller und Händler solcher Produkte, sondern auch Zeitgenossen, die per WLAN Zugriff auf Daten nehmen wollen, die sie nichts angehen.

Seit Herbst 2000 wurden immer wieder neue **Lücken in der Sicherheitsarchitektur** „Wire Equal Privacy“ (WEP) des WLAN-Standards bekannt. Bereits im Sommer 2001 waren alle verwendeten Zugangskontroll- und Verschlüsselungsmechanismen gebrochen. Entsprechende Tools zum Ausnutzen der bekannten Lücken sind kostenlos erhältlich. Alle WLAN-Betreiber sind davon betroffen. Viele namhafte Firmen haben daher eine Policy, die keinen WLAN-Zugang zum unternehmenseigenen Intranet zulässt.

Mit dem **neuen Sicherheitsstandard WPA** soll den bekannten Lücken nun begegnet werden. Allerdings ist WPA erst in Produkten enthalten, die den Standard 802.11i des Institute of Electrical & Electronics Engineers (IEEE) einhalten. Diese sind jedoch noch **nicht** breit **verfügbar**. Zwar besteht die Möglichkeit, auch mit vorhandener WLAN-Infrastruktur eine gesicherte Verbindung durch Einsatz des Protokolls IPsec zu realisieren, dies wird aber die meisten Heimanwender überfordern. Sie müssen beim Einsatz einer WLAN-Verbindung am heimischen DSL-Anschluss damit rechnen, dass auch andere diesen nutzen. Wer dann nicht über eine Flatrate verfügt, kann bei der nächsten Rechnung eine böse Überraschung erleben. Wer außerdem vertrauliche Daten wie E-Mails, Geheimnummern oder Kontoinformationen zum Online Banking auf seinem Rechner speichert, muss sich bewusst sein, dass diese nun auch von Dritten eingesehen werden können. Denn bei den aktuellen Geräten ist meist sogar die schwache WEP-Verschlüsselung im Auslieferungszustand abgeschaltet, und die Datenübertragung erfolgt ungeschützt.

> **? *WLAN & Bluetooth***
>
> *WLAN ist die Abkürzung für Wireless Local Area Network, d. h. kabelloses lokales Netz. Bluetooth („Blauzahn“) ist nach einem dänischen König benannt, der 960 erstmals die skandinavischen Länder zusammenführte. Genauso soll Bluetooth verschiedene Geräte zusammenführen.*
>
> *WLAN und Bluetooth sind beide Standards für Datenübertragung per Funk. Während WLAN zumeist als Ersatz für gängige Netzkabel über mittlere Strecken zum Einsatz kommt, wird Bluetooth in der Regel eher als Ersatz für Peripheriekabel (z. B. zum PDA, Handy oder Drucker) im Nahbereich eingesetzt.*

Neben WLAN ist mit **Bluetooth** ein weiterer Standard für drahtlose Übertragungen auf dem Markt. Er kommt insbesondere zum Einsatz, um Geräte wie Drucker, Handy, Scanner kabellos miteinander zu verbinden, ist aber prinzipiell auch für

eine Rechnervernetzung geeignet. Im Gegensatz zu WLAN unterstützt Bluetooth einen regelmäßigen Frequenzwechsel und erschwert damit sowohl ein Stören wie ein Abhören der Verbindung. Allerdings genügt es, ein Datenpaket abzufangen, um an die Hardwareadresse zu gelangen, die die Frequenzen definiert. Für Bluetooth sind bisher weniger Angriffsmuster bekannt als für WLAN; dies dürfte aber vor allem daran liegen, dass Bluetooth derzeit noch wenig verbreitet ist und nur selten als Basis für ein Netz zum Einsatz kommt. Der in Bluetooth implementierte 128-Bit-Algorithmus „Safer+“ (abgeleitet von DES) kann theoretisch gebrochen werden, wenn es einem Angreifer gelingt, einen ausreichend langen Datenstrom mitzuschneiden. Bluetooth-Kommunikationen sind in der Regel aber von kurzer Dauer. Somit ist ein Abfangen einer ausreichenden Zahl von Datenpaketen unwahrscheinlich, aber eben nicht ausgeschlossen.

Da jedes Bluetooth-Gerät über einen **eindeutigen Identifizierungscode** verfügt, ist es möglich, Personen z. B. anhand ihres Handys mit Bluetooth-Funktion zu identifizieren und zu verfolgen, ohne dass diese dies bemerken. Daher sollten in mobilen Geräten die drahtlosen Komponenten grundsätzlich deaktiviert sein und nur im Bedarfsfall vorübergehend eingeschaltet werden. Auch WLAN-Komponenten besitzen (wie alle Netzkarten) eine weltweit eindeutige Identifikation (MAC-Adresse). Bei einigen Karten lässt sich mit entsprechenden Hilfsprogrammen diese beliebig ändern, was aber keine praktikable Abhilfe ist.

Was ist zu tun?
Sofern der Einsatz eines drahtlosen Netzes nicht unabdingbar ist, sollte derzeit darauf verzichtet werden. Dies gilt insbesondere für die Verarbeitung von sensiblen Daten im Medizin- und Finanzbereich. Kommt man um den Einsatz von WLAN nicht herum, ist auf jeden Fall ein anerkanntes Sicherheitsprotokoll wie IPsec zu verwenden. Nicht benötigte WLAN- oder Bluetooth-Komponenten, etwa in Notebooks oder Handys, sollten auf jeden Fall deaktiviert werden.

10.2 Firewalls im Praxistest

Firewall ist nicht gleich Firewall. Sich für die richtige zu entscheiden, überfordert wegen ihrer Komplexität die meisten IT-Verantwortlichen. Ohne externen Sachverstand geht es in der Regel nicht.

Firewalls im klassischen Sinne haben grundsätzlich eine **Achillesferse**: Unabhängig von der Qualität der Filterung des eingehenden Datenverkehrs (der so genannte Inbound Traffic) können sie den ausgehenden Datenstrom (Outbound Traffic) nur unzureichend analysieren. Soll in einer Behörde beispielsweise das Surfen per Webbrowser möglich sein, so muss jeder Arbeitsplatzrechner mindestens über den Port 80 das http-Protokoll verwenden können. Welche Software dies im Einzelnen tut, kann eine herkömmliche Firewall nicht feststellen. Eine vorgeschaltete Firewall reicht nicht aus, wenn die Client-Rechner keine exakt definierte und unabänderliche Softwareausstattung aufweisen. Die Möglichkeit, Software aus dem Internet zu installieren, bedeutet ein Risiko für eine definierte Softwareumgebung. Findet **fremde Software** den Weg durch eine Firewall hindurch auf einen Client-Rechner, so hat sie dieselben Rechte wie die bereits installierte Software.

Konkret bedeutet das, dass auch Schädlingsprogramme wie Viren und Würmer über dieselben Kanäle wie der Webbrowser nach außen gelangen können, ohne dass eine externe Firewall dies bemerken könnte. Hierzu sind zusätzlich zur Firewall aufwändige Content-Filter notwendig, die den Datenstrom inhaltlich analysieren.

Alternativ können aber auch so genannte **Personal Firewalls** zum Einsatz kommen. Diese Programme, die normalerweise als Firewall-Ersatz bei Privatanwendern dienen, sind in der Lage, bereits auf der Betriebssystemebene festzustellen, welche Applikationen Daten über das Netz senden. Ihr Vorteil liegt in der feineren Granulierung des Netzzugriffs: So kann beispielsweise nur dem installierten Webbrowser erlaubt werden, über Port 80 zu kommunizieren. Anderen Programmen kann derselbe Port verboten werden. Es ist ebenfalls möglich, einzelne IP-Adressen generell oder für bestimmte Applikationen zu sperren.

Besonders gute Personal Firewalls setzen zudem ein **Hash-Verfahren** ein, bei dem die zulässigen Programme mit einem eindeutigen Prüfwert versehen werden. Dadurch wird sichergestellt, dass unzulässige Programme gleichen Dateinamens nicht versehentlich freigegeben werden. Fremdprogramme, die beispielsweise den Dateinamen des freigegebenen Internet-Browsers tragen, werden so von der Personal Firewall anhand der falschen Prüfsumme identifiziert und abgeblockt. Der Vorteil einer Kombination aus Personal Firewall und vorgeschalteter Firewall liegt in der Begrenzung der Zugriffsrechte auf Applikationsebene.

Diese Darstellung zeigt auf, wie intensiv man sich bei der Beurteilung des Wirkungsgrades einer Firewall mit ihrem internen Aufbau und ihrer Positionierung auseinander setzen muss. Die Vielzahl der auf dem Markt angebotenen Produkte macht es allerdings unmöglich, für alle Spezifikationen ein entsprechendes Know-how vorzuhalten. Deshalb haben wir in einer Art **Marktanalyse** festgestellt, welches Produkt in der schleswig-holsteinischen Verwaltung am häufigsten eingesetzt wird. Die in der Praxis gebräuchlichste Standardkonfiguration haben wir in einem im Jahr 2003 gestarteten Projekt in unserem **IT-Labor** nachgebaut, um ihre Stärken und Schwächen zu analysieren und die dabei gewonnenen Erfahrungen im Rahmen von Prüfungen und Beratungen an die Praktiker weiterzugeben.

Kurse
NET, FW

Derartige Installationen sind, wenn „belastbare“ Erkenntnisse gewonnen werden sollen, recht aufwändig. Allein für dieses Projekt waren folgende Komponenten erforderlich: Router, Firewall, Webserver, Mailserver, Sicherheitssoftware für E-Mail-Verkehr, Sicherheitssoftware für Webdienste und Verschlüsselungsserver. Nach dem Projektabschluss soll zu dem Thema „Sicherer Internet-Anschluss“ ein **backUP-Magazin** herausgegeben werden, in dem auch die Konzepte und Erfahrungen der beiden diesbezüglich zertifizierten Kreisverwaltungen (vgl. Tz. 9.2.3) berücksichtigt werden.

Was ist zu tun?
Verwaltungen, die unter den heutigen Gegebenheiten ihr lokales Netzwerk mit dem Internet verbinden wollen, sollten dies nicht ohne professionelle Beratung realisieren. Wegen der schwierigen Auswahl der richtigen Firewallkomponenten sollte eine Auditierung durch uns standardmäßig eingeplant werden. Dies führt zu einem 6-Augen-Prinzip bei der Umsetzung des Sicherheitskonzeptes (Behörde, externer Dienstleister, ULD).

10.3 Der Kampf gegen Spam

Der Versand von Spam-Mails hat in den letzten Jahren erheblich zugenommen. Viele Nutzer klagen über volle Mailboxen, in denen die relevanten Nachrichten kaum zu finden sind. Teilweise werden Nachrichten gar nicht zugestellt, weil das Mailpostfach überfüllt ist. Durch den Einsatz von Spam-Filtern, die die eingehende Mail vom Werbemüll trennen sollen, lassen sich nur teilweise befriedigende Ergebnisse erzielen. Besser ist es, präventive Maßnahmen zu ergreifen.

Besonders wichtig beim Umgang mit elektronischer Post ist es, mit der eigenen **Mailadresse** im Netz sehr vorsichtig umzugehen. Ist die Adresse einmal auf dem Verteiler eines Spam-Versenders gelandet, besteht keine realistische Möglichkeit mehr, der Werbeflut zu entkommen. Die gängigen Hinweise am Ende von Werbemails, mit deren Hilfe man sich von den Verteilern streichen lassen können soll, dienen zumeist nur einem Zweck: zu verifizieren, ob eine Spam-Mail gelesen worden ist. Sollte das der Fall sein (und bei einem Wunsch nach Entfernung vom Verteiler kann man davon ausgehen), gewinnt eine Mailadresse noch an Wert. Sie zählt nun erwiesenermaßen nicht zum Streuverlust, sondern wird tatsächlich gelesen – von einem potenziellen Kunden. Die erste Regel sollte daher sein, **niemals** auf eine Spam-Mail zu **reagieren**, weder durch Klick auf einen darin enthaltenen Link noch durch ein simples Reply. Beides bestätigt dem Absender nur die Mailadresse des Opfers.

Die eigene Mailadresse sollte nur **vertrauenswürdigen Personen** bekannt sein. Sie ist eine Adresse zur Kommunikation mit Kollegen, Geschäftspartnern, Freunden und Familienmitgliedern. Für alle anderen Kommunikationsvorgänge via E-Mail sollte man sich **Alternativen** überlegen. Hierzu gibt es verschiedene Möglichkeiten:

- **Zweitadresse bei einem Gratismailprovider**

Mailadressen sind im Web relativ einfach zu bekommen, und die Einrichtung eines Webmail Accounts ist schnell erledigt. Dabei sollte ein besonderes Augenmerk auf die zur Anmeldung notwendigen Daten gelegt werden. Monatliches Einkommen und Familienstand sind zur Diensterbringung vollkommen unnötig. Es sollten daher Freemail Provider bevorzugt werden, die möglichst wenige Daten für die Anmeldung erheben. Wer sich eine Zweitadresse angelegt hat, kann diese für Online-Shopping, Anmeldungen auf Webseiten und ähnliche Aktivitäten im Internet verwenden. Sollte die Werbepost dann irgendwann überhand nehmen, kann man solch eine Zweitadresse einfach wieder löschen oder, wenn der Mailprovider dies nicht anbietet, verwaisen lassen und einen neuen Account anlegen. Der Vorteil dieser Lösung liegt in der Überschaubarkeit der Mailadressen: eine für Freunde, eine für Spam.

- **Eigene Domain mit Mailboxen**

Wer eine eigene Homepage besitzt, hat häufig mindestens ein Mailpostfach über diese Domain. Hier ist es besonders einfach, sich eine Zweitadresse zu generieren.

Bei Bedarf kann diese dann einfach gelöscht bzw. umbenannt werden. Elegant sind auch so genannte Catch-All-Accounts, die alle eintreffenden Mails zu einer Domain in eine einzige Mailbox schicken, unabhängig vom Text vor dem @-Zeichen. Wer so einen Account von seinem Provider bekommt, kann im Web kurzerhand „personalisierte“ Mailadressen vergeben: In ein Eingabeformular auf einer fremden Webseite wird einfach die Adresse <fremde-Webseite>@<eigene-Domain> eingetragen. Sollte dann irgendwann Spam eintreffen, lässt sich anhand der Adresse erkennen, wer die jeweilige Mailadresse an den Spammer weitergegeben hat. Dann ist es möglich, die spezielle Adresse fortan zu blocken oder einfach umzuleiten – an denjenigen, der die Adresse weitergegeben hat.

- **Webservices für temporäre Adressen**

Ein neuer Trend sind Webseiten, über die der Nutzer kurzfristig temporäre Mailadressen erzeugen kann. Das ist vor allem dann nützlich, wenn eine Adresse nur einmalig zu Verifikationszwecken benötigt wird. Wird beispielsweise für den Download einer Software vom Hersteller eine Mailadresse verlangt, an die der Downloadlink geschickt wird, ist es nicht sinnvoll, dort die eigene Adresse anzugeben. Selbst eine eventuell eingerichtete Zweitadresse ist hierfür zu schade, weil definitiv keine weitere Kommunikation notwendig ist. Eine Lösung stellt z. B. die Webseite www.spam.la dar. E-Mails, die an eine beliebige @spam.la-Adresse geschickt werden, erscheinen umgehend dort auf der Webseite. Wird also beim bereits erwähnten Softwaredownload eine Mailadresse erfragt, so kann der Nutzer beispielsweise die Adresse Software_xy@spam.la angeben. Die Webseite www.spam.la zeigt eine Liste der letzten 20 eingegangenen Mails mit Adresse und Betreffzeile, sodass ein Klick genügt, um die Nachricht und die gewünschte Information zu lesen. Diese Variante hat allerdings einen gravierenden Nachteil: Da jede Mail an spam.la auf der dortigen Webseite veröffentlicht wird, sind die eintreffenden Nachrichten für jedermann lesbar. Deshalb ist dieses System ausschließlich für Adressverifikationen im Netz gedacht. Eine ernsthafte Kommunikation ist darüber nicht sinnvoll. Um jedoch den erwähnten Downloadlink per Mail zu erhalten oder ein Anmeldepasswort für eine Webseite, ist ein Dienst wie spam.la ideal geeignet.

Dienste im Internet, die temporäre Mailadressen vergeben:

- *www.spam.la*
- *www.mailinator.com*
- *www.spamgourmet.com*

Was ist zu tun?
Spam lässt sich nur durch Prävention verhindern. Die eigene Mailadresse sollte sorgfältig eingesetzt werden. Für alle E-Mail-Kontakte, die absehbar nur von kurzer Dauer sind, sollten Zweitadressen zum Einsatz kommen, die leicht gelöscht oder geändert werden können.

10.4 Entwicklungen auf dem Browsermarkt

Nachdem US-Gerichte im Anti-Trust-Prozess gegen Microsoft festgestellt haben, dass der Softwareriese wettbewerbswidrig agiert hat, der angedrohten Firmenzerschlagung jedoch widersprachen, schien es, als würde sich nicht viel ändern auf dem Browsermarkt. Aber die Konkurrenz von Microsoft schläft nicht.

Zeitgleich zum Gerichtsverfahren hatte sich mit dem Mozilla-Projekt eine ernst zu nehmende Alternative zu Microsoft-Produkten entwickelt, die inzwischen immer mehr an Dynamik gewinnt. Über die **Browsersuite Mozilla** wurde bereits in den vergangenen Jahren berichtet (vgl. 25. TB, Tz. 11.3). Inzwischen ist die Browsertechnologie von Mozilla Kernstück diverser Ableger: Neben Netscape gibt es mit Firefox, K-Meleon und Beonex verschiedene Varianten des **Open-Source-Browsers** für alle Einsatzzwecke. Netscape setzt dabei mit seiner Lösung auf ein Komplettpaket, das den ohnehin schon vielfältigen Funktionen der Mozilla-Suite noch einen Instant Messenger sowie einige Multimediaplayer hinzufügt. Firefox als „Nur-Browser"-Version von Mozilla versteht sich hingegen als schlanke Alternative zu Komplettpaketen und verzichtet daher ausdrücklich auf Extras, die mit dem eigentlichen Surfen nichts zu tun haben. Beonex orientiert sich nah am ursprünglichen Mozilla-Paket, enthält also auch ein Mailprogramm. Allerdings wurde hier von den Entwicklern großer Wert auf datenschutzgerechte Voreinstellungen gelegt. So werden Cookies per Default am Sitzungsende gelöscht und kein Referer übertragen. Bei der Anzeige von E-Mails im HTML-Format ignoriert Beonex alle Tags, die nicht zur Textformatierung relevant sind. Auf diese Weise schließen die Entwickler einen Großteil der Gefahren durch HTML-Mails von vornherein aus.

Nach langer Pause wird seit November 2003 auch **K-Meleon** weiterentwickelt. Der ebenfalls auf dem Mozilla-Kern basierende Browser verfolgt einen ähnlichen Ansatz wie Firefox: Ein schlanker, schneller Browser ohne Ballast. Allerdings verfolgt K-Meleon dieses Ziel noch konsequenter als Firefox. K-Meleon bedient sich nur in Teilen des Programmcodes der Mozilla-Entwickler. Insbesondere im Bereich der Konfiguration wird das deutlich, da K-Meleon hier ein durchdachteres Konzept verfolgt. Was die eigentliche Darstellung von Webseiten betrifft, unterscheiden sich die genannten Browser nur unwesentlich, da sie alle dieselbe Darstellungsroutine des Mozilla-Kerns verwenden, die so genannte „Gecko"-Engine. Diese zeichnet sich vor allem durch eine hohe Konformität mit bestehenden Webstandards des W3C aus.

Mitte des Jahres 2003 verkündete Microsoft, dass der aktuelle Internet Explorer (6.0 SP1) der letzte Stand-Alone-Browser von Microsoft sei. Weiterentwicklungen würde es zwar geben, jedoch nur als Bestandteil des kommenden Betriebssystems, das derzeit unter dem Codenamen **Longhorn** entwickelt wird. In Anbetracht der Tatsache, dass Longhorn erst 2005 in den Handel kommen soll (Gerüchte halten 2006 für realistisch), bedeutet das einen Stillstand der Weiterentwicklung für ca. zwei Jahre. Die Hoffnung auf eine umfassende P3P-Implementierung (vgl. Tz. 8.4), eine nutzerfreundliche Konfigurationsoberfläche und vor allem ein Mehr an Sicherheit scheint also vergebens. Patches zum Stopfen

akuter Sicherheitslücken müssen also reichen. Dass diese Patches bisweilen trotz bekannter Sicherheitslücken lange auf sich warten lassen, ist zusätzlich zu bedenken.

Netscape, das einen Großteil der Mozilla-Entwicklung finanziert hatte, entließ im Juli 2003 50 Entwickler und gründete die Mozilla-Foundation, aus deren Mitteln künftig die Weiterentwicklung finanziert werden soll. Befürchtungen, die Entwicklung von Mozilla käme ganz zum Erliegen, haben sich nicht bestätigt. Allerdings lässt sich eine deutliche Verschiebung der Zielsetzung feststellen: Mozilla, ursprünglich als so genannte Browsersuite geplant, wird in seine Einzelteile zerlegt. Die Strategie, ein „Schweizer Taschenmesser" für das Web zu entwickeln (Mozilla enthält neben dem Browser noch Mail- und Newsreader, Adressbuch, Webseiteneditor und Chatprogramm), wird zugunsten von separaten Komponenten aufgegeben. So wird bereits unter dem Namen **Firefox** ein eigenständiger Browser entwickelt; das korrespondierende Mailprogramm nennt sich **Thunderbird**. Die Vorteile separater Programme liegen vor allem in der besseren Optimierbarkeit in Bezug auf die speziellen Einsatzgebiete. Zweckdienliche Oberflächen und ein modulares Erweiterungskonzept sollen die Einzelprogramme in hohem Maße anpassungsfähig machen an besondere Anforderungen der verschiedenen Nutzer. Für den Browser Firefox existieren derzeit über 130 so genannte Extensions, die für Zusatzfunktionen wie dem automatischen Löschen der Surfspuren auf dem eigenen Rechner bis hin zu eigenständigen Programmen wie einem Chatclient viel Spielraum lassen. Dank der durchdachten Schnittstelle integrieren sich die Extensions nahtlos in die jeweiligen Programme, sodass auch spezielle „Datenschutzeditionen" von Firefox denkbar sind, in denen der Browser mit sinnvollen und wichtigen Ergänzungen ausgestattet wird, dabei aber trotzdem als einheitliches Programm erscheint und nicht als Konglomerat von Tools.

Insbesondere im Hinblick auf die bislang sehr knappen **P3P-Implementierungen** der Browser lässt die Entwicklung des Mozilla-Projektes hoffen. Im Rahmen des P3P-Projektes (vgl. Tz. 8.4) haben wir daher mit den Entwicklern des Tools Privacy Bird Kontakt aufgenommen, um eine Portierung auf die Mozilla-Plattform anzuregen. Dieser Schritt würde nicht nur für viele Windows-Anwender eine Lücke schließen, auch Linux-Nutzer könnten davon profitieren, da Mozilla eine plattformunabhängige Software darstellt. Insgesamt ist der Browsermarkt mehr in Bewegung, als dies noch vor einem Jahr abzusehen war. Die Vielfalt an Alternativen zum Internet Explorer hat entgegen ersten Vermutungen sogar zugenommen.

Was ist zu tun?
Angesichts der massiven Sicherheitsprobleme des Internet Explorers sollten die Konkurrenzbrowser im Auge behalten werden. In Handhabung und Leistung stehen sie dem Microsoft-Browser in nichts nach.

10.5 Wie sicher sind Passwörter tatsächlich?

Passwortverfahren als Mittel zur Authentifizierung von Benutzern sind besser als ihr Ruf. Solange die Personalisierungsprobleme beim Einsatz von Chipkarten noch nicht gelöst sind, sind Passwörter das Mittel der Wahl. Für die Sicherheit sind nicht nur die Passwortlängen entscheidend, sondern insbesondere auch die systemtechnischen Rahmenbedingungen.

Eine zentrale Sicherheitskomponente in jedem IT-System ist die korrekte Authentifizierung der Benutzer. Gelingt es z. B. einem Mitarbeiter, dem System vorzugaukeln, er sei nicht die Aushilfe Meier, sondern der Chef Müller, erhält er auch die Zugriffsrechte des Chefs zugewiesen, und in allen Protokollen werden seine (unzulässigen) Aktivitäten so vermerkt, als seien sie zulässigerweise vom Chef vorgenommen worden. Um einen solchen Rollentausch unmöglich zu machen, wird bei der Anmeldung standardmäßig zwischen dem Benutzer und dem Rechnersystem ein Geheimnis in Form eines **Passwortes** ausgetauscht. Dieses ist im Rechner verschlüsselt abgelegt. Das System unterstellt „wer das Passwort von Müller kennt, der ist auch Müller“ und weist die entsprechenden Rechte zu. Von Müller wird erwartet, dass er sich alle Aktivitäten, die aufgrund der Eingabe seines Passwortes vollzogen wurden, zurechnen lässt. Es muss ihm gegenüber also systemseitig gewährleistet werden, dass sich niemand ohne sein Zutun in den Besitz seines Passwortes bringen kann. Über diese Aufgabenstellung und ihre konkrete Bewältigung wird in der IT-Szene seit Jahren heftig diskutiert. Es geht dabei zwar auch um die Grundsatzfrage, ob Passwörter überhaupt sicher genug sind und ob eine ausreichende Sicherheit nicht erst durch Einsatz biometrischer Systeme zu erreichen ist. Im Wesentlichen wird aber über Passwortlängen und Änderungszyklen gestritten.

Auslöser waren im letzten Jahr Messungen darüber, in welcher Zeit man mit einem normalen PC in der Lage ist, ein Passwort durch das Ausprobieren aller Möglichkeiten zu „knacken“. Die Ergebnisse sind in der Tat frappierend. Bei einem Zeichenvorrat, der nur aus Kleinbuchstaben besteht (26 Zeichen), braucht man theoretisch lediglich **48 Sekunden**, um ein 6-stelliges Passwort zu ermitteln. Wohlgemerkt, es wird bei dieser Methode nicht eine Entschlüsselung vorgenommen, sondern es wird schlicht nur geraten und verglichen. Bei Ausnutzung des vollen Zeichenvorrates und längeren Passwörtern liegt man zwar noch im Bereich mehrerer Tage, aber die Verarbeitungsgeschwindigkeiten der PCs steigen nach wie vor so rasant, dass die „Halbwertzeiten“ in diesem Bereich immer kürzer werden.

Aus dieser Erkenntnis sind **mehrere Schlüsse** zu ziehen:

- Auf die Datei der verschlüsselten Passwörter dürfen nur sehr wenige **Administratoren** Zugriff haben.
- Nach spätestens **fünf Fehlversuchen** eines Benutzers bei der Eingabe eines Passwortes ist das Benutzerkonto zu sperren. Eine Wiedereröffnung darf nur durch die Administratoren nach vorheriger Analyse der Gründe für die Sperrung erfolgen.

- Die **Passwortkonventionen** sind so zu gestalten, dass der gesamte Zeichenvorrat genutzt wird, dass Änderungen nach Zeitablauf erzwungen werden und dass eine Mindestlänge von 6 bis 8 Zeichen vorgeschrieben ist.

Die Reihenfolge der Vorgaben entspricht auch ihrer Gewichtung. Als eine besonders gute vertrauensbildende Maßnahme den Benutzern gegenüber ist die automatische Anzeige des **Zeitpunkts der letzten Anmeldung** bei einem erneuten Einloggen anzusehen. Wenn der Benutzer zu dem angegebenen Zeitpunkt nicht an seinem Arbeitsplatz war, kann er mit einiger Wahrscheinlichkeit davon ausgehen, dass ein Unbefugter sich seine Identität angeeignet hat, und die Administration benachrichtigen.

Wie eine solche Kontrollanzeige systemtechnisch zu realisieren ist, haben wir in unserem IT-Labor ausprobiert und auf unserer Homepage unter „System-Nachrichten“ beschrieben (Meldung vom 12.06.2003).

www.datenschutzzentrum.de/systemdatenschutz/meldung/sm26.htm

Was ist zu tun?
Der richtigen Passwortorganisation sollte seitens der Dienststellenleitung, der Administratoren und der Benutzer eine besondere Bedeutung beigemessen werden. Alle Zugriffsrestriktionen verpuffen, wenn ein Identitätsdiebstahl möglich ist.

10.6 Eine ganze Datenbank auf Feuerzeuggröße

Derzeit werden Disketten durch neue und mächtigere Speichermedien ersetzt, etwa durch USB-Speicherkarten. Die Sicherheitsproblematik der „offenen Diskettenlaufwerke“ geht in eine neue Runde, weil sich der Zugriff auf USB-Speichermedien nur schwer einschränken lässt.

Disketten sind immer mehr auf dem Rückzug, so baut die Firma Apple schon seit einigen Jahren keine Diskettenlaufwerke mehr in ihre Computer ein. Der Grund dafür ist, dass die Kapazität von Disketten für den Datenaustausch zwischen heutigen Anwendungen nicht mehr ausreicht. Als Ersatz dienen so genannte **Memory Cards** oder **Memory Sticks**, die sogar im laufenden Betrieb angeschlossen und entfernt werden können und eine Speicherkapazität von 16 MB bis 2 GB haben. Sie werden automatisch durch das Betriebssystem als weitere Laufwerke in die Verzeichnishierarchie eingebunden und erlauben direkte Lese- und Schreibzugriffe. Eine Treiberinstallation ist meist nicht erforderlich (Stichwort „Plug & Play“). Dies gilt für Linux-Systeme, Windows 2000/2003 und Windows XP.

> ***? Universal Serial Bus (USB)***
>
> *USB dient dem Anschluss von Peripheriegeräten aller Art nach einem (neuen) einheitlichen Standard. Jedes USB-Gerät lässt sich während des laufenden Betriebes anschließen und entfernen, weil es von den (neuen) Betriebssystemen automatisch erkannt wird.*

Was so bequem erscheint, ist ein großes Sicherheitsrisiko, wenn Daten unbefugt auf solche bzw. von solchen Speicherkarten kopiert werden. Dies betrifft nämlich beide Richtungen, das unbefugte Kopieren dienstlicher Datenbestände ebenso wie das Aufspielen von privaten Datenbeständen. Daher ist der Zugriff auf USB-Speichermedien auf die Administratoren zu begrenzen. Für die dafür notwendige **Deaktivierung der USB-Schnittstelle** zu Speicherkarten gibt es mehrere Möglichkeiten. Wenn USB-Controller überhaupt nicht gebraucht werden, sollten sie im BIOS des Rechners deaktiviert werden. Neuere Hauptplatinen verfügen über mehrere USB-Controller, von denen nur ein Teil an bestehende externe USB-Buchsen angeschlossen ist. Dennoch sind alle Controller zu deaktivieren. Der Zugriff zum BIOS ist durch ein Administratorpasswort zu schützen. Weiterhin kann man die Verbindung der USB-Anschlüsse am Gehäuse mit der Hauptplatine im Gehäuseinnern unterbrechen.

> ***? Basic Input Output System (BIOS)***
>
> *Es handelt sich um eine Sammlung von Softwareroutinen und Daten, die grundlegende Hardwarefunktionen steuern. Nach dem Einschalten des Computers leitet es z. B. den Hardwareselbsttest ein. Im laufenden Betrieb werden im Wesentlichen die Datenübertragung zwischen den Laufwerken und anderen Geräten gesteuert. Das BIOS darf nur von den Administratoren geändert werden, weil hier die Basis für alle Sicherheitseinstellungen gelegt wird.*

Bei Windows-Systemen kann der (bzw. können die) USB-Controller durch den Administrator auch im Gerätemanager mithilfe von Hardwareprofilen deaktiviert werden. Eleganter ist es, lediglich die **Verwendung** von USB-Massenspeichermedien zu **unterbinden**, etwa wenn die USB-Ports für Tastaturen oder Drucker aktiviert bleiben müssen. Unter Linux-Systemen ist dazu das Kernel-Modul „usb-storage“ zu deaktivieren. Für Windows-Systeme gibt es kommerzielle Produkte, die das bewerkstelligen.

Ein Anschluss von USB-Speichermedien wird anders als etwa Zugriffe auf das Diskettenlaufwerk in der Systemprotokolldatei erfasst und kann daher nicht unbemerkt vorgenommen werden. Auf jeden Fall ist also die **Systemprotokolldatei** auf unbefugte Nutzungen von Wechselmedien hin zu überprüfen. Auf die entsprechenden Softwareprodukte und Skripte wird auf unserer Homepage unter „System-Nachrichten“ (Meldung vom 15.04.2003) hingewiesen.

www.datenschutzzentrum.de/systemdatenschutz/meldungen/sm22.htm

Was ist zu tun?
Die Nutzung von USB-Speichermedien ist an „normalen“ Arbeitsplätzen auszuschließen. Werden sie zum Datenträgeraustausch benötigt, sind die Protokolle über ihre Nutzung genau zu überprüfen.

10.7 Warum ist der Terminal-Server-Betrieb so verpönt?

Technische Entwicklungen haben oft eine Eigendynamik, der mit Logik schwer beizukommen ist. Schwierig zu handhabende Computersysteme werden über Jahre am Leben erhalten. Sichere und wirtschaftlichere Lösungen setzen sich dagegen nur sehr schwer durch.

Seit Jahren wird von mehreren Anbietern, u. a. auch von der Firma Microsoft, eine technische Lösung für lokale Netzwerke angeboten, die nicht nur den Datenschützern, sondern wahrscheinlich auch den Rechnungsprüfern das Herz vor Vergnügen höher schlagen lässt, weil sie offenbar trotz geringerer Kosten ein Mehr an Datensicherheit gegenüber den gängigen Client-Server-Lösungen bietet.

> **? *Client-Server-Konzept***
>
> *Es handelt sich um eine in lokalen Netzwerken eingesetzte technische Anordnung, bei der sowohl die Server als auch die Arbeitsstationen „intelligente", programmierbare Geräte darstellen. Bei der Client-Komponente handelt es sich um einen PC mit eigenem, selbstständig zu administrierenden Betriebssystem, der den Benutzern das volle Leistungsspektrum zur Verfügung stellt.*

Gleichwohl fristet die **Thin-Client-Architektur**, wie ein Terminal-Server-Betrieb auch genannt wird, im Gesamtgefüge der IT-Landschaft ein Schattendasein. Die Gründe hierfür sind schwer zu ermitteln. So konnte von unserer Seite nie ganz geklärt werden, warum der landesweite IKOTECH III-Standard die Benutzung von aufwändig zu administrierenden PC-Arbeitsplätzen nach dem Client-Server-Konzept zwingend vorschreibt.

> **? *Terminal-Server-Architektur***
>
> *Bei diesem Netzwerkkonzept werden die Arbeitsplatzsysteme lediglich als Ein- und Ausgabemedien benutzt. Die Verarbeitungsprozesse finden ausschließlich auf den Servern statt. Die Terminals brauchen nicht gesondert administriert zu werden und sind deshalb häufig als Thin-Clients gestaltet. Bei ihnen entfällt das Abschottungsproblem zwischen der Nutzerebene und der Administrationsebene und die Überwachung der Datenbestände auf den lokalen Platten. Dementsprechend sind die Verarbeitungs- und Speicherkapazitäten auf den Servern größer ausgelegt.*

Diese einseitige Ausrichtung der Rechnerarchitektur wird allerdings in jüngster Zeit mehr und mehr aufgebrochen. Dataport bietet zwei Lösungen auf der Basis von Terminal-Servern an, wovon eine allerdings datenschutzrechtlich und sicherheitstechnisch problematisch ist (vgl. Tz. 6.7.3). Eine andere Lösung ist bei mehreren Kommunen im Einsatz und wird zurzeit bei der Stadt Bad Schwartau einem Audit unterzogen. Auch bundesweit entscheiden sich immer mehr Behörden für **Terminal-Server-Systeme**.

Eine Anfang 2004 veröffentlichte Analyse eines Marktforschungsunternehmens bei sechs großen Organisationen enthält nahezu nur positive Aussagen. Die Finanzverwaltung im Land Nordrhein-Westfalen hat z. B. insgesamt 17.000 Arbeitsplätze auf diese Weise eingerichtet und berichtet über eine wesentliche Entlastung der Administratoren, ihre organisatorische Konzentration auf

wenige Dienststellen, eine höhere Flexibilität und einen besseren Know-how-Austausch. Alle befragten Firmen und Behörden äußerten sich positiv hinsichtlich der gestiegenen Datensicherheit. Ohne Disketten- oder andere Speicherlaufwerke könnten die Thin-Clients nicht für das Herunterladen sensibler Daten missbraucht werden. Zudem ermögliche es die **serverbasierte Architektur**, die Zugriffe auf Informationen besser zu überwachen und zu dokumentieren und Verfahren zu implementieren, mit denen sich Back-ups erstellen und Datensicherheitsprozesse in Gang setzen lassen. Auf diese Weise ließen sich auch die den Datenschutz betreffenden gesetzlichen Vorgaben wesentlich einfacher erfüllen. Als wesentliches Negativum wurde lediglich die Tatsache bezeichnet, dass IT-Spezialisten, die sich mit der neuen Architektur auskennen, spärlich gesät und deshalb relativ teuer seien.

Diese Gegebenheiten haben wir zum Anlass genommen, in unserem **IT-Labor** ein praxisnahes **Terminal-Server-System** aufzubauen und es hinsichtlich des erzielbaren Sicherheitsgewinns systematisch zu analysieren. Hierin fließen auch die Erkenntnisse aus dem oben angeführten Datenschutz-Behördenaudit ein. Wenn die Arbeiten im Laufe des Jahres 2004 abgeschlossen sind, beabsichtigen wir, die Ergebnisse in einem backUP-Magazin zusammenzufassen und Konfigurationsvorschläge zu machen.

Was ist zu tun?
Spätestens bei der anstehenden Fortschreibung des IKOTECH III-Standards sollte das Land sich mit dem Nutzen der Terminal-Server-Architektur auseinander setzen. Es sollte ermittelt werden, warum eine Lösung, die dem Land Nordrhein-Westfalen offensichtlich Vorteile bringt, z. B. für die schleswig-holsteinische Steuerverwaltung, die Polizei und die Justizverwaltung weniger geeignet ist.

10.8 Kooperation mit CASES zum Selbstdatenschutz

Mit der International School of New Media (ISNM) Lübeck haben wir eine Reihe von Kooperationen vereinbart. Ziel der Zusammenarbeit wird die deutsche Vertretung des europäischen CASES-Projekts sein.

Die „Cyberworld Awareness and Security Enhancing Structure“ (CASES) stellt ein europäisches Netzwerk zur Schärfung des Sicherheitsbewusstseins der Nutzer dar. Dabei sollen in Datenbanken Informationen über Sicherheitsrisiken und -probleme zusammengefasst und Anwendern Tipps und Hinweise gegeben werden, wie bestimmte Risiken minimiert werden können. Das CASES-Netzwerk richtet sich an **Privatnutzer** sowie **kleine und mittelständische Unternehmen**, die in der Regel keine eigenen Sicherheitsexperten beschäftigen. Die einzelnen europäischen CASES-Vertretungen (auch Nodes genannt, deutsch: Knoten) besitzen dabei jeweils spezifische Schwerpunkte, woraus sich durch Vernetzung der verschiedenen nationalen Knoten entsprechende Synergieeffekte ergeben. Der CASES-Node Deutschland wird, nicht zuletzt durch unsere Kompetenz, einen besonderen Schwerpunkt auf Privacy und Selbstdatenschutz legen. In der Anfangsphase wird sich CASES Deutschland vor allem auf Jugendliche konzentrieren und diese Zielgruppe sensibilisieren. Insofern haben wir mit der Erstellung

einer Schul-CD (vgl. 25. TB, Tz. 9.3) bereits Erfahrungen gesammelt, die in die Zusammenarbeit mit CASES einfließen können.

Zusammen mit der ISNM Lübeck wird neben CASES Deutschland auch das **Cyber Prevention and Awareness Laboratory** (CyPAL) entstehen. Dort werden ins CASES-Netzwerk einzuspeisende Informationen erarbeitet und verifiziert. Auf diese Weise entsteht mit CASES ein umfassender Informationsdienst und mit CyPAL eine komplementäre Forschungseinrichtung. Auch hier können wir mit unserem IT-Labor bereits umfassende Erfahrungen vorweisen.

11 Internationales

11.1 Flugdatenaffäre: Überzogene Datenwünsche der USA

Seit März 2003 haben US-Behörden Zugriff auf die Buchungsdatenbanken europäischer Airlines bei transatlantischen Flügen, obwohl dies im Widerspruch zu europäischen und nationalen Datenschutzbestimmungen steht. Während die Europäische Kommission in Verhandlungen mit den USA den Grundstein für dieses zweifelhafte Vorgehen gelegt hatte, bemühen sich das Europäische Parlament und andere Gremien um eine datenschutzgerechte Lösung, die aber zurzeit noch nicht in Sicht ist.

Unter dem Eindruck der Terroranschläge vom 11. September 2001 ist in den USA ein Gesetz verabschiedet worden, welches allen ausländischen Fluglinien für Flüge in bzw. aus den USA vorschreibt, ihre Buchungssysteme für die US-Zollbehörden zu öffnen. Bis zu diesem Zeitpunkt erhielten US-Behörden von jedem Flug aus einem EU-Land in die Vereinigten Staaten lediglich die Passagierlisten nach Abschluss des Checkin. Bereits vor dem In-Kraft-Treten des Gesetzes gab es eine Absprache zwischen den USA und der Europäischen Kommission, in welcher die Einzelheiten des Datenzugriffs der USA festgelegt wurden. Die Öffentlichkeit erfuhr erst im Nachhinein von dieser Vereinbarung. Allem Anschein nach wurden die Vorschriften der **EG-Datenschutzrichtlinie** 95/46/EG, die bei Datentransfers in Länder außerhalb der EU hohe Voraussetzungen vorschreiben, beim Abschluss dieser Vereinbarung nicht beachtet. Einige europäische Fluggesellschaften haben trotzdem ihre Buchungssysteme für den Zugriff durch den US-Zoll geöffnet. Die Passagiere werden allenfalls über den Umstand informiert, dass etwa 40 Einzelinformationen von Personen durch den US-Zoll abgerufen werden; sie können die Übermittlung jedoch nicht beeinflussen oder gar untersagen.

Die Übermittlung ist aus folgenden Gründen nicht mit den geltenden europäischen und nationalen Datenschutzbestimmungen vereinbar:

- **Pull-Verfahren statt Push-Verfahren**

  Momentan „ziehen“ US-Zollbehörden im Wege eines Vollzugriffs etwa 40 Daten je Fluggast (so genanntes „Pull-System“) aus den IT-Systemen der Airlines. Dieser uneingeschränkte Vollzugriff auf die Buchungsdatenbanken müsste zumindest durch ein „Push-Verfahren“ ersetzt werden: Dies hätte zur Folge, dass nur diejenigen Datenfelder pro Passagier von den Fluggesellschaften bereitgestellt werden, die Europa liefern will bzw. muss. Das technische Konzept für ein entsprechendes Verfahren wurde bereits entwickelt und sowohl von der Artikel 29-Gruppe als auch von den betroffenen europäischen Fluglinien begrüßt.

- **Fehlende Einhaltung des Zweckbindungsprinzips**

  Da sich die US-Zollbehörden ausdrücklich vorbehalten haben, auch sensible Daten der Passagiere an andere US-Sicherheitsbehörden weiterzugeben, und es in den Vereinigten Staaten keine Datenschutzvorschriften nach europäischem Standard gibt, ist die Einhaltung der Zweckbindung äußerst fraglich. Zwar wurde vom US-Department of Homeland Security versichert, dass kommer-

zielle Datenfirmen keinen Zugriff auf die personenbezogenen Passagierdaten erhalten würden. Nichtsdestotrotz wurden die Daten bereits für das Data-Mining-Programm CAPPS II verwendet. Auch räumte die US-Airline JetBlue die zweckentfremdete Weitergabe von Passagierdaten an eine US-Rüstungsfirma ein. Eine Beschwerdeinstanz für Unionsbürger fehlt bei den verantwortlichen US-Behörden, sodass sie gegen eine Weitergabe sensibler Daten machtlos sind.

- **Unverhältnismäßigkeit der Datensammlung, insbesondere der Datenmenge und Speicherfrist**

  Zudem behalten sich die US-Behörden vor, die Liste der übertragungspflichtigen Daten von derzeit etwa 40 Angaben beliebig zu erweitern. Während die Kommission die Verkürzung der ursprünglichen Speicherfrist von 50 (!) Jahren auf sieben Jahre als Fortschritt in den Verhandlungen mit den USA verbucht, fordert das Europäische Parlament die Beschränkung der Speicherfrist auf die Aufenthaltsdauer des jeweiligen Passagiers in den USA. Dass die praktizierte Übermittlung nicht dem Verhältnismäßigkeitsgrundsatz genügte, wird auch von der Europäischen Kommission nicht infrage gestellt.

Die **Internationale Konferenz der Datenschutzbeauftragten** in Sydney hat die Flugdatenaffäre aufgegriffen. In einer Entschließung vom September 2003 wurde bekräftigt, dass regelmäßige internationale Transfers von Passagierdaten nur innerhalb eines bestimmten datenschutzrechtlichen Rahmens erfolgen dürfen. Dieser könnte z. B. in einem internationalen Abkommen festgelegt werden, das den Zweck der Übermittlung klar definieren sowie die Verhältnismäßigkeit und zeitliche Begrenzung der Datenverarbeitung, die Gewährleistung der Rechte betroffener Passagiere und eine unabhängige Aufsicht gewährleisten müsse.

Die Europäische Kommission räumt ein, dass die mit den USA getroffene Abmachung keine Rechtsgrundlage für Datenübermittlungen darstellt. Sie geht aber davon aus, dass die europäischen Airlines auf Anfrage der US-Behörden ihre Buchungsdatenbanken ohnehin geöffnet hätten. Die USA hatten in Aussicht gestellt, im Falle der Verweigerung der Datenübermittlung den europäischen Fluggesellschaften die **Landerechte** zu **entziehen**. Dass dieses Argument nicht wirklich durchgreift, zeigt sich nicht zuletzt daran, dass kleinere Fluggesellschaften wie Austrian Airlines und Alitalia bis zuletzt beharrlich die Übermittlung der geforderten Daten verweigerten – ohne negative Konsequenzen. Zumindest muss sich die EU-Kommission vorhalten lassen, dass sie mit der Abmachung die Datenweitergabe vereinfacht hat – auf Kosten der Freiheitsrechte der Unionsbürger.

Nachdem bekannt wurde, dass die US-Zollbehörden tatsächlich einen Zugriff auf die Reservierungsdatenbanken europäischer Airlines haben, regte sich Widerstand von verschiedenen Seiten. Bereits im März 2003 übte die **Artikel 29-Datenschutzgruppe** der EU deutliche **Kritik** an der vereinbarten Weitergabe der Passagierdaten und forderte, die Umsetzung der Vereinbarung aufzuschieben, bis eine den Rechten der Betroffenen angemessene, rechtlich sichere Lösung gefunden ist. Das **Europäische Parlament** hat sich ebenfalls gegen die Datenübermittlung in der von der Kommission und der USA vereinbarten Art und Weise

ausgesprochen. Im Oktober 2003 hat es in einem mit breiter Mehrheit angenommenen Entschließungsantrag die Kommission aufgefordert, innerhalb von zwei Monaten die Abmachungen mit den US-Behörden zur Flugdatenweitergabe an das geltende EU-Datenschutzrecht anzupassen. Andernfalls hat das Europäische Parlament die Anstrengung eines Vertragsverletzungsverfahrens gegen die Europäische Kommission gemäß Artikel 232 EGV vor dem Europäischen Gerichtshof (EuGH) in Aussicht gestellt.

Rechtzeitig zum Fristablauf legte EU-Kommissar Frits Bolkestein im Dezember 2003 eine mit den USA erzielte Einigung vor. Dabei handelt es sich um ein so genanntes sektorübergreifendes Konzept, welches einen zeitlich auf dreieinhalb Jahre befristeten Rechtsrahmen für die Übermittlung der Passagierdaten an die USA beinhaltet. Dafür wurde die **Angemessenheit des Datenschutzstandards** in den USA durch ein bilaterales Abkommen als gegeben unterstellt.

? Artikel 29-Gruppe

Die Datenschutzgruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie ist das unabhängige Beratungsgremium der Europäischen Union in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 14 der Richtlinie 97/66/EG festgelegt.

Die in den Verhandlungen mit dem US-Heimatschutzministerium von der EU-Kommission gesetzte „clear deadline“ bewirkte, dass die US-Seite ihre starre Haltung aufgab und zu Zugeständnissen bereit war: Die Frist für die Speicherung der Passagierdaten soll nunmehr dreieinhalb Jahre betragen; die Zahl der übertragungspflichtigen Dateneinheiten wurde auf 34 reduziert. Diese sollen zukünftig nach einem Push-Verfahren übermittelt werden. Die Flugdaten sollen nicht zur allgemeinen innerstaatlichen Verbrechensbekämpfung, sondern ausschließlich zu Zwecken der Terrorismusbekämpfung und gegen organisierte Kriminalität verwendet werden. Die amerikanische Zoll- und Grenzschutzbehörde hat sich zudem bereit erklärt, sich an einer jährlichen **Überprüfung der Umsetzung** der festgelegten Verpflichtungen durch die EU-Kommission zu beteiligen.

Im Virtuellen Datenschutzbüro ist die US/EU-Flugdatenaffäre dokumentiert. Die Informationen sind in einem Dossier zusammengetragen unter

www.datenschutz.de/feature/flugdaten

11.2 Trusted Computing

Hersteller von EDV-Produkten kämpfen auf dem Markt zunehmend mit Viren, Würmern und Sicherheitslöchern in Betriebssystemen und Internet-Programmen. „Trusted Computing“ soll insofern für mehr Sicherheit sorgen. Hinterfragt man die Konzepte, stellt sich aber die Frage, wer hier vor wem geschützt wird.

Der Begriff „Trusted Computing“ wurde von der **Trusted Computing Platform Alliance** (TCPA) kreiert. Dabei handelte es sich um einen Zusammenschluss von EDV-Firmen, in dem Spezifikationen standardisiert werden, um eine Interoperabilität von vertrauenswürdigen Systemen verschiedener Hersteller zu gewährleisten. Gegründet wurde die TCPA im Jahre 2002 von den Firmen Compaq, Hewlett-Packard, Intel, IBM und Microsoft. Die TCPA hat derzeit ca. 200 Mitglieder. Im Sommer 2003 übernahm die Trusted Computing Group (TCG) die Weiterentwicklung der Spezifikationen und trat die Nachfolge der TCPA an. Ein „trusted“ System im Sinne der TCG ist im Vergleich zu einem herkömmlichen System um ein so genanntes Trusted Platform Module (TPM) erweitert. Dabei ist der Einsatzbereich eines TPM nicht auf Personal Computer beschränkt, sondern z. B. auch für Mobiltelefone geplant.

> **? *Trusted Computing (TC)***
>
> *bezeichnet das Konzept, mithilfe spezieller Hard- und Softwarekomponenten die Manipulierbarkeit einzuschränken, um so die Sicherheit bzw. Verlässlichkeit solcher Systeme zu erhöhen. „Trust“ kann dabei mit Vertrauen oder Zuverlässigkeit übersetzt werden.*

> **? *TPM***
>
> *Eine Trusted Platform ist ein System, welches seine eigene Integrität (Unversehrtheit) dem lokalen Anwender und/oder einer beliebigen entfernten Instanz durch kryptographische Verfahren nachweist. Damit soll u. a. ein Schutz vor Viren, Trojanischen Pferden oder Dialern möglich sein.*

Microsoft beabsichtigt, in die zukünftigen Versionen seines Betriebssystems Windows ein darüber hinausgehendes Sicherheitskonzept (NGSCB) zu integrieren, und benutzt hierfür den Begriff **Trustworthy Computing** (als TC abgekürzt; deutsch: vertrauenswürdige Datenverarbeitung). Kritiker interpretieren das Kürzel TC dagegen mit **Treacherous Computing** (engl: heimtückische Datenverarbeitung), um auf das von dieser Technologie ausgehende Gefahrenpotenzial hinzuweisen.

Ein System, das über ein TPM verfügt, kann als so genannte Trusted Platform agieren. Im Unterschied zu vielen Veröffentlichungen, insbesondere aus der Anfangsphase der TC-Diskussion, handelt es sich beim TPM nicht um eine Komponente, die aktiv bestimmte Aktionen des Nutzers einfordert oder verhindert. Ein TPM kann lediglich das Betriebssystem bei kryptographischen Funktionen unterstützen, einen **abgesicherten Speicherbereich** für kryptographische Schlüssel zur Verfügung stellen und den Betriebszustand eines Rechners messen sowie Ände-

rungen des Zustandes feststellen. Damit wäre eine Trusted Platform unanfällig gegen Manipulationsversuche, da eine Modifikation des Systems bzw. seiner Komponenten mithilfe des TPM vom Betriebssystem erkannt und gegebenenfalls blockiert werden kann.

Eine solche Technologie kann durchaus datenschutzgerecht gestaltet und eingesetzt werden. Wir stehen daher in Kontakt mit der TCG, um frühzeitig von neuen Entwicklungen zu erfahren und gegebenenfalls beratend tätig zu sein. In der Ende 2003 verabschiedeten TPM-Spezifikation 1.2 ist mit „**Direct Anonymous Attestation**“ (DAA) nun ein Mechanismus in den Standard eingeflossen, der es Trusted Platforms erlaubt, sich gegenseitig verlässlich ihre Integrität zu bestätigen, ohne dafür eine so genannte Trusted Third Party (deutsch: zuverlässige dritte Partei) in Anspruch nehmen zu müssen. Dies hat den deutlichen Vorteil, dass damit keine Datenspuren über die Kommunikation zwischen den beiden Systemen an einer zentralen Stelle anfallen.

Die Einführung von DAA ist ein **Schritt in die richtige Richtung**; allerdings leistet auch die neue Spezifikation noch immer nicht, dass der Eigentümer eines Systems die vollständige Kontrolle über sämtliche in einem TPM enthaltenen kryptographischen Schlüssel erhält. Da das grundlegende Schlüsselpaar eines TPM, der so genannte Endorsement Key (deutsch: Bestätigungsschlüssel), im Herstellerwerk erzeugt wird, kann dort theoretisch auch ein „Nachschlüssel“ gespeichert werden. Hier ist eine Weiterentwicklung seitens der TCG noch dringend erforderlich.

Die Firma Microsoft plant, in der nächsten Version von Windows (Arbeitstitel „Longhorn“) Trustworthy Computing intensiv zu nutzen, um zum einen die Sicherheit der Systeme zu erhöhen und zum anderen die Grundlage für ein umfangreiches **Digital Rights Management** (deutsch: digitale Rechteverwaltung) zu bieten (vgl. Tz. 11.3). Dieses Projekt wurde unter dem Namen **Palladium** bekannt und von Microsoft inzwischen in **Next Generation Secure Computing Base** (NGSCB) umbenannt.

Um die genannten Ziele zu erreichen, sollen **mittelfristig** die TC-Funktionen eines TPM in entsprechende CPUs integriert (z. B. Intel LaGrande CPU) und seitens der Hardware getrennte Speicherbereiche für Programmcode und Arbeitsdaten zur Verfügung gestellt werden. Damit soll sichergestellt werden, dass Prozesse und deren Daten voneinander abgeschottet sind, sodass eine gegenseitige Beeinträchtigung ausgeschlossen wird. Durch den Einsatz von Kryptographie soll weiterhin gesichert werden, dass nur entsprechend autorisierte Applikationen bestimmte Daten lesen oder schreiben können.

Während der Einsatz von TC durchaus geeignet sein kann, datenschutzgerechte Systeme zu erstellen, kann man mit dieser Technologie auch sehr eingriffsintensive Systeme gestalten. In den TPM-Spezifikationen sowie den Veröffentlichungen zu NGSCB ist deutlich zu erkennen, dass die Entwicklung vor allem den Interessen großer Unternehmen entspricht, während **Privatanwender** nicht zu Unrecht fürchten, die Hoheit über ihre Daten und Systeme an die Hersteller von Hard- und Software zu verlieren.

Ein „trusted“ System schützt nicht mehr den Besitzer vor Angriffen von außen, sondern in erster Linie das System vor dem Besitzer, der nicht mehr allein entscheidet, was wie auf seinem System geschieht.

Dies hat gleichermaßen Auswirkungen auf öffentliche wie nichtöffentliche Daten verarbeitende Stellen, die die **Verantwortung für die Datenverarbeitung** nur dann wirklich wahrnehmen können, wenn eine Kontrolle ihres Systems nicht von außen stattfindet (vgl. Tz. 6.4).

Was ist zu tun?
Die Entwicklung und Ausgestaltung von TC-Technologien ist so weiterzuführen, dass die Eigentümer die vollständige Kontrolle über sämtliche Daten auf ihren Systemen wahrnehmen können. Ansonsten wäre fraglich, ob ein rechtskonformer Einsatz von TC-Systemen in Daten verarbeitenden Stellen überhaupt möglich ist.

11.3 Digital Rights Management

Digital Rights Management (DRM) ermöglicht es, vor der Übertragung von Daten festzulegen, was der Empfänger mit diesen anstellen darf. So kann beispielsweise festgelegt werden, dass ein Film nur innerhalb eines bestimmten Zeitraumes abgespielt werden kann oder dass ein Musikstück sich nicht auf CD brennen lässt. Um die Einhaltung dieser Restriktionen zu sichern, nehmen viele dieser DRM-Mechanismen per Internet Kontakt mit einem zentralen Server auf. Dass dort dabei aussagekräftige personenbezogene Daten anfallen, ist den Nutzern meist nicht bewusst.

Musik- und Filmindustrie jammern über schwindende Umsätze. Schuld daran seien nicht mangelnde Originalität oder zu hohe Preise ihrer Produkte, sondern vielmehr die Massen unberechtigt angefertigter Kopien. Durch Einsaz von **Digital Rights Management** (digitale Rechteverwaltung) soll hier Abhilfe geschaffen werden, denn dann entscheidet nicht mehr der Eigentümer bzw. Nutzer eines Rechners, was mit eingehenden Daten geschehen soll, sondern diejenigen, die die Daten bereitstellen, können festlegen, welche Art der Verarbeitung erlaubt und welche verboten ist. Das Gleiche gilt für Software, die dann „selbst entscheidet“, ob sie ihre Funktion ausführt oder nicht.

Damit wird es möglich, Beschränkungen für die Nutzung von Software und Daten auch dann technisch durchzusetzen, wenn dies auf juristischem Wege nicht durchsetzbar wäre. Exemplarisch sind hier zunächst die **Lizenzbedingungen** anzuführen, denen man bei der Installation von Software oft per Mausklick zustimmen muss. Während diese in Deutschland oftmals keine rechtliche Bindung des Nutzers bewirken, können die darin enthaltenen Bestimmungen mittels DRM dennoch **durchgesetzt** werden. Festgesetzt werden kann unter anderem, dass die zum Abspielen eines Musikstückes eingesetzte Software vor der Wiedergabe einen Server per Internet kontaktiert, um zu prüfen, ob die entsprechende Berechtigung noch gültig ist. Dabei fallen auf dem kontaktierten Server zwangsläufig Daten an, die zur Bildung eines Nutzungs- und Interessenprofils geeignet sind.

Bereits seit einiger Zeit enthalten viele Mediaplayer Funktionen, um auch bei nicht DRM-beschränkten Medieninhalten die **Konsumgewohnheiten** der Nutzer **auszuforschen** und an einen zentralen Server zu melden. Wenn man Glück hat, findet sich in den Tiefen der Konfigurationsdialoge eine entsprechende Option oder irgendwo im Internet ein Hilfsprogramm eines Drittanbieters, um der Software das Spionieren zu verbieten. Dazu muss man aber zunächst um diese Funktionen und die entsprechende Abhilfe wissen. Positiv fallen einige Open-Source-Player auf – den Datensammelteil sucht man bei ihnen vergeblich.

In Verbindung mit spezieller Hardware, die ein System vor Manipulationsversuchen schützt (vgl. Tz. 11.2), können Datensammler zukünftig ihre **Interessen durchsetzen** – selbst wenn sie dabei gegen Datenschutzbestimmungen verstoßen. Ein Nutzer, der gegebenenfalls vor der Wahl steht, einen bereits bezahlten Film nicht sehen zu können oder mit einem Mausklick doch seine „freiwillige" Einwilligung in unüberprüfbare Datenübermittlungen und -speicherungen zu geben, hat nicht mehr die Möglichkeit, ohne Preisgabe seiner Privatsphäre zu seinem Recht zu kommen.

Es lassen sich prinzipiell alle Daten per DRM in ihrer Verwendung einschränken. Für neuere Versionen von Office-Paketen ist die Einführung bereits angekündigt, um so den Schutz eigener Dokumente zu ermöglichen. Man darf sich allerdings nicht wundern, wenn man demnächst von seinen Textverarbeitungsprogrammen freundlich darauf hingewiesen wird, dass man zwar im Besitz guter und ausgereifter Software sei, die Lizenz aber abgelaufen und nun ein **kostenpflichtiges Update** erforderlich sei, ohne das man leider auch keinen weiteren Zugriff auf die eigenen Dokumente mehr habe. Auch mit DRM ist bisher allerdings eine Lizenzbestimmung nicht durchsetzbar, die unlängst in einem neuen E-Book-Shop die potenziellen Käufer verwunderte: Neben dem Drucken, Kopieren und Verleihen des E-Books war dort explizit auch das laute Vorlesen verboten.

Durch den Einsatz von DRM werden zahlreiche datenschutzrechtliche Fragen aufgeworfen. Gesetzlich sind die aktuellen Bestrebungen, das DRM zum Schutz urheberrechtlich geschützter Werke im digitalen Kontext auch technisch zu gewährleisten, auf die EU-Richtlinie 2001/29/EG zurückzuführen. Deren Umsetzung in nationales Recht innerhalb der Umsetzungsfrist zur „Harmonisierung bestimmter Aspekte des Urheberrechts" wurde zunächst von nahezu allen Mitgliedstaaten versäumt. Inzwischen ist mit Gesetz vom 15. September 2003 in Deutschland zumindest das **neue Urheberrecht** in Kraft getreten und damit auch der neue § 95 a UrhG, der sich mit der Zulässigkeit des DRM und dem Verbot der Umgehung entsprechender Schutzvorrichtungen befasst.

Im Wortlaut: § 95 a Abs. 1 UrhG

Wirksame technische Maßnahmen zum Schutz eines nach diesem Gesetz geschützten Werkes oder eines anderen nach diesem Gesetz geschützten Schutzgegenstandes dürfen ohne Zustimmung des Rechtsinhabers nicht umgangen werden, soweit dem Handelnden bekannt ist oder den Umständen nach bekannt sein muss, dass die Umgehung erfolgt, um den Zugang zu einem solchen Werk oder Schutzgegenstand oder dessen Nutzung zu ermöglichen.

Aus Datenschutzsicht besonders interessant ist, ob unter die „technischen Maßnahmen zum Schutz eines [...] geschützten Werkes“ auch technische Verfahren zur **Registrierung des Nutzerverhaltens** fallen. Es zeichnet sich ab, dass hier zu differenzieren ist. Ist eine Maßnahme in erster Linie für die Durchsetzung der Urheberrechte notwendig, so dürfte sie zulässig sein. Zielt sie hingegen auf Direktmarketing ab, und ist der Schutz vor Urheberverletzungen nur von zweitrangiger Bedeutung, so sind unter Umständen die Datenschutzrechte der Nutzer verletzt.

Aber auch ganz **allgemeine datenschutzrechtliche Fragen** stellen sich je nach Ausgestaltung des Digital Rights Managements. Wird der Nutzer rechtzeitig vor der Erhebung von Daten über dessen genauen Inhalt und Zweck aufgeklärt? Hat er noch die freie Möglichkeit, seine Einwilligung zur Verarbeitung der Daten zu verweigern oder später zurückzuziehen? Werden die Daten tatsächlich nur zur Durchsetzung des Urheberrechts benutzt, oder besteht die Gefahr, dass andere Ziele (wie z. B. Direktmarketing) (mit-)verfolgt werden? Wird auf die Grundsätze der **Datenvermeidung** und der **Datensparsamkeit** Rücksicht genommen, sodass auch z. B. die Nutzung des urheberrechtlich geschützten Werkes anonym bzw. pseudonym möglich ist? Wird bei den Speicherfristen je nach Dienst und Zweck (Abrechnungsdaten, Nutzungsdaten, HGB-Aufbewahrungsfristen usw.) differenziert? Werden sie eingehalten?

Das durchaus berechtigte Interesse von Herstellern und Vertreibern von urheberrechtlich geschützten Werken am Schutz ihrer Rechte darf nicht dazu **missbraucht** werden, personenbezogene Daten bzw. das **Nutzungsverhalten des Kunden auszuspionieren**. Die Verlockung hierzu bei der Industrie dürfte jedoch groß sein. Die Anwendung unterschiedlicher Rechtssysteme im Bereich des Datenschutzes (z. B. USA – EU) erschwert die Transparenz bei der Datenverarbeitung für Kunden wie auch Datenschutzbehörden.

Was ist zu tun?
Das Digital Rights Management ist darauf zu untersuchen, ob es sich im Rahmen der geltenden Gesetze bewegt. Das Sammeln nicht erforderlicher Daten und die Bildung von Nutzerprofilen ist zu unterbinden.

11.4 RFID und allgegenwärtiges Computing

In fast jedem Alltagsgegenstand steckt bald ein kleiner Chip. Nicht immer wird man ihn sehen können, aber stets ist es möglich, mit ihm per Funk zu kommunizieren. Neuere Chipgenerationen reden nicht mehr nur mit speziellen Lesegeräten, sondern auch miteinander.

Radio Frequency Identification (RFID, deutsch: Identifizierung per Funk) dient dem **kontaktlosen** Speichern und Auslesen von Daten. Die Daten werden auf so genannten RFID-Tags (kleine Etiketten) gespeichert, die nahezu überall befestigt werden können. Diese Systeme sollen die heute üblichen Barcodes ablösen, die zwar ebenfalls maschinenlesbar sind, dazu aber eine Sichtverbindung benötigen, während RFID-Tags je nach Modell Distanzen von wenigen Zentimetern bis ca. 30 Metern überbrücken können.

Ein Barcode identifiziert in der Regel ein Objekt lediglich als zu einer bestimmten Kategorie gehörend – RFID-Tags hingegen können jedes Objekt mit einer **eindeutigen Kennung** versehen, anhand derer sich Informationen zu diesem Gegenstand mit einer Datenbank abgleichen lassen. Dies bietet im Logistikbereich viele Vorteile, ist aber nicht ohne **Folgen für die Privatsphäre**: Da für das Lesen der Kennung kein Sichtkontakt erforderlich ist, ist es für eine Person nicht bemerkbar, wenn ein RFID-Tag gescannt wird, von dem man vielleicht gar nicht weiß, dass man ihn mit sich führt.

Sind solche **RFID-Tags** zum Beispiel in Schuhsohlen eingegossen, kann man davon ausgehen, dass jedes Mal, wenn die eindeutige Kennung irgendwo ausgelesen wird, sich die gleiche Person dort befindet, denn der Tausch von Schuhen mit anderen Personen ist äußerst ungewöhnlich. RFID-Tags werden schon heute für Zugangskontrollen, Wegfahrsperren, Lagerverwaltung, Tierkennzeichnung oder Mautsysteme eingesetzt. Diskutiert wird derzeit auch der Einsatz in Euro-Banknoten. Es handelt sich nicht um eine Zukunftsvision, sondern um eine ausgereifte und allgemein verfügbare Technologie.

Die zunehmende Verbreitung von RFID-Tags birgt z. B. das Risiko der Erstellung **personalisierter Einkaufs- und Nutzungsprofile**. In Verbindung mit Informationen aus anderen Datenbanken, geographischen Ortungssystemen oder mit Lokalisationsdaten etwa aus dem Mobilfunk kann sich dies leicht vom allgegenwärtigen Computing zu einer allgegenwärtigen Überwachung ausdehnen.

Es läuft der **informationellen Selbstbestimmung** zuwider, wenn nicht erkennbar ist, wo RFID-Tags sind und wann und welche Daten sie an wen übertragen. Die Betroffenen können sich kaum gegen eine **versteckte Datenerhebung** schützen. Die Internationale Konferenz der Datenschutzbeauftragten hielt 2003 in einer von uns mitgestalteten Resolution fest, dass personenbezogene Daten aus RFID-Tags nur in einer offenen und transparenten Weise erhoben werden dürfen, um einen ungerechtfertigten Eingriff in die Privatsphäre zu verhindern.

Auch andernorts äußert man sich skeptisch: Das US-amerikanische Auto-ID Center des MIT fordert „the right to know whether a product contains an EPC (Electronic Product Code) tag, and whether a public place is using public readers“, Wissenschaftler der RSAlabs entwarfen einen **RFID-Blocker**, der den Datenaustausch zwischen Etikett und Lesegerät behindert, und der deutsche Verein zur Förderung des bewegten und unbewegten Datenverkehrs (FoeBuD) arbeitet zur verbesserten Wahrnehmung und Sensibilisierung an der Entwicklung eines Warnsensors, der u. a. akustisch meldet, wenn sich RFID-Tags oder Lesegeräte in der Nähe befinden.

Aufgrund der Datenschutzvorbehalte gegen den RFID-Einsatz seitens der **Verbraucher** sehen die Spezifikationen inzwischen auch Mechanismen vor, um RFID-Tags unbrauchbar zu machen, indem z. B. der Speicherinhalt gelöscht oder durch ein spezielles Kommando eine Sicherung im Tag durchgebrannt wird. Um hier einen Missbrauch zu verhindern, bedarf es allerdings der Implementierung geeigneter Protokolle zur Authentisierung.

Damit nicht genug: Die Beratende Gruppe für Technologie der Informationsgesellschaft (ISTAG) der EU zeichnet mit „**Ambient Intelligence Landscape**“ eine Welt vor, in der alle möglichen Alltagsgegenstände miteinander kommunizieren und auf die Anwesenheit von bestimmten Personen mit spezifischen Verhaltensweisen reagieren. Dies wird in den entsprechenden Aufsätzen als bequem und komfortabel dargestellt, beinhaltet aber das Risiko, dass Dritte sich die leicht erfassbaren Verhaltensmuster einer Person zugänglich machen und die informationelle Selbstbestimmung ausgehebelt wird.

Smart Dust ist eine weitere Anwendung für allgegenwärtige Datenverarbeitung. Es handelt sich dabei um winzige Chips, die in großen Mengen eingesetzt werden, sich miteinander vernetzen, ihre Umgebung überwachen und die dabei anfallenden Daten an eine Basisstation übermitteln. Für diese extrem unauffällige Überwachung gibt es zahlreiche zivile und militärische Einsatzszenarien. Die Privatsphäre der Menschen kann dabei allerdings auf der Strecke bleiben. Wir empfehlen daher den regelmäßigen und gründlichen Hausputz.

Was ist zu tun?
Die Entwicklung von mobilen kommunizierenden Minichips muss dem Recht auf informationelle Selbstbestimmung Rechnung tragen. Es müssen Mechanismen geschaffen werden, die sicherstellen, dass kein Mensch unbemerkt oder gegen seinen Willen elektronisch gescannt und überwacht wird.

12 Informationsfreiheit

12.1 Überblick

Auch im vierten Jahr nach In-Kraft-Treten sind die Auswirkungen des Informationsfreiheitsgesetzes Schleswig-Holstein (IFG-SH) nach wie vor positiv. Unsere Erfahrungen zeigen, dass das Informationsrecht der Bürgerinnen und Bürger gegenüber Behörden in der Praxis gut umgesetzt werden kann.

Die Behörden stehen dem Informationsinteresse der Bürgerinnen und Bürger überwiegend aufgeschlossen gegenüber. Die meisten Zweifelsfälle, die an uns im Rahmen von Eingaben, Anfragen von Bürgern oder Behörden sowie bei Fortbildungsveranstaltungen herangetragen werden, können im Sinne der Informationsfreiheit gelöst werden. Häufig genügt es, das Informationsinteresse zu ermitteln und pauschale Informationsansprüche präziser zu formulieren. Nur in wenigen Fällen sperrten sich Behörden gegen **berechtigte Informationsansprüche** der Bürgerinnen und Bürger. Gelegentlich bleibt es auch nach einer Vermittlung durch uns bei verhärteten Standpunkten. In solchen Fällen müssen die Gerichte entscheiden.

Unser Informationsangebot zur Informationsfreiheit unter

www.datenschutzzentrum.de/informationsfreiheit/

wird kontinuierlich ausgebaut.

12.2 Interessante Einzelfälle

- **Auskunft über den Verkauf der Stadtwerke verweigert**

Der geplante **Verkauf** von Teilen der **Stadtwerke** an ein Energieversorgungsunternehmen stieß bei vielen Bürgerinnen und Bürgern einer Stadt auf Unverständnis. Da sie an der Wirtschaftlichkeit dieser Maßnahme zweifelten, begehrten sie Einsicht in Unterlagen über den Verkauf. Von besonderem Interesse war in diesem Zusammenhang ein Unternehmenswertgutachten, das der Bildung des Kaufpreises zugrunde lag. Die Stadt lehnte die begehrte Einsichtnahme ab und begründete ihre Entscheidung u. a. damit, dass es sich um Unterlagen über **fiskalisches Handeln** einer Behörde handele, auf die das IFG-SH nicht anwendbar sei. Wegen des Verweises auf den Behördenbegriff des Landesverwaltungsgesetzes im IFG-SH beschränke sich dieses Gesetz ebenso wie das Landesverwaltungsgesetz auf öffentlich-rechtliche Handlungsformen.

Eine solche Einschränkung des Anwendungsbereichs ist mit den Zielen des Gesetzes nicht vereinbar und findet im Gesetz keine Stütze (vgl. 25. TB, Tz. 13.2; 24. TB, Tz. 13.1). Die Intention des Gesetzgebers, durch Informationsrechte der Bürger mehr Transparenz in das Verwaltungshandeln zu bringen und dadurch das **Vertrauen der Bevölkerung** in behördliche Entscheidungen zu stärken, würde

nur unzulänglich erreicht, wollte man den Zugang auf Informationen über hoheitliches Handeln beschränken. Denn gerade in Bereichen, in denen Behörden in privatrechtlicher Form handeln, ist Transparenz besonders wichtig. Hier geht es, wie der Fall der Stadtwerke eindrucksvoll belegt, oft um Angelegenheiten, die die öffentlichen Haushalte belasten und für die Allgemeinheit von großem Interesse sind. Die Bürger interessiert zu Recht, ob dabei alles mit rechten Dingen zugegangen ist.

Die Vorenthaltung des Wertgutachtens und anderer Informationen über den Verkauf der Stadtwerke haben wir gegenüber der Stadt als Verstoß gegen das IFG-SH **förmlich beanstandet**. Das Innenministerium als Kommunalaufsichtsbehörde hat sich allerdings der Argumentation der Stadt zur Verweigerung des Informationszuganges angeschlossen. Abgeordnete des Landtages überlegen nun, das Gesetz in unserem Sinne klarzustellen.

- **Einsicht in Planungsunterlagen für die Startbahnverlängerung des Flughafens Kiel**

Angesichts der Planungen für die Verlängerung der Startbahn des Flughafens Kiel begehrte eine Bürgerinitiative Einsicht in Vorgänge, die den Bau des Flughafens und dessen geplante Erweiterung betrafen. Einen entsprechenden Antrag stellte die Bürgerinitiative beim Wirtschaftsministerium und bei der Stadt Kiel. Ein Teil der Akten wurde der Bürgerinitiative daraufhin zugänglich gemacht. Hinsichtlich der Akten, in die keine Einsicht gewährt werden sollte, wandte sich die Bürgerinitiative an uns. Hierzu ist inzwischen eine Klage der Bürgerinitiative gegen das Land und die Stadt beim Verwaltungsgericht anhängig. Dabei wird die Frage zu klären sein, inwieweit das IFG-SH auch auf **Regierungshandeln** anwendbar ist. Das Ministerium verneint diese Frage. Seine Tätigkeit im Rahmen der Flughafenerweiterung habe sich auf die Vorbereitung der politischen Grundsatzentscheidungen der Landesregierung beschränkt. Es handele sich bei einem solchen Vorgang nicht um öffentlich-rechtliches Verwaltungshandeln, was jedoch Voraussetzung für die Anwendbarkeit des IFG-SH sei.

- **Keine Auskunft über vom Eichamt festgestellte Mogeleien?**

Die Statistiken der Eichämter über Füllmengenkontrollen weisen immer wieder Fälle von Unregelmäßigkeiten bei der Abfüllung von Fertigpackungen aus. Verbraucherschützer sind deshalb alarmiert. Der Statistik der Eichämter sind jedoch die jeweiligen Produkte und die verantwortlichen Betriebe nicht zu entnehmen. Um diese in Erfahrung zu bringen, wandte sich eine Verbraucherschutzorganisation an das Eichamt und bat unter Berufung auf die Vorschriften des IFG-SH um Auskunft über die konkreten Beanstandungsfälle in Schleswig-Holstein. Das zuständige Ministerium lehnte die Auskunftserteilung ab mit der Begründung, in **Bußgeldverfahren** sei das **IFG-SH nicht anwendbar**. Daraufhin erhob die Verbraucherorganisation Klage beim Schleswig-Holsteinischen Verwaltungsgericht und bat uns parallel dazu um eine rechtliche Bewertung des Sachverhalts. Wir haben mitgeteilt, dass wir die Auffassung des Ministeriums grundsätzlich teilen, soweit das Eichamt durch die Ahndung von Ordnungswidrigkeiten als strafverfolgende Behörde tätig wird. In dieser Funktion ist das Eichamt vom Anwendungsbereich des IFG-SH ausgenommen.

Soweit darüber hinaus beim Eichamt Unterlagen über Füllkontrollen vorhanden sind, die nicht Gegenstand eines Bußgeldverfahrens sind, unterfallen diese vollständig dem IFG-SH. Bei der Offenlegung dieser Informationen sind allerdings zwei Dinge zu berücksichtigen: Zum einen könnten Interessen Dritter betroffen sein, wenn die Unterlagen **personenbezogene Daten** über natürliche Personen enthalten. Hier würde es sich anbieten, die Unterlagen anonymisiert zugänglich zu machen. Zum anderen könnten **Betriebs- und Geschäftsgeheimnisse** der kontrollierten Unternehmen einer Offenbarung der Informationen entgegenstehen. Das Vorliegen eines Betriebs- und Geschäftsgeheimnisses und das Interesse der Allgemeinheit an der Offenbarung der Informationen müssten in jedem Einzelfall gegeneinander abgewogen werden.

- **Informationszugang zur Vorbereitung eines Gerichtsverfahrens**

Eine Petentin benötigte wegen eines unmittelbar bevorstehenden Gerichtstermins dringend Informationen aus einer Gewerbeakte. Es ging darum, in Erfahrung zu bringen, wann genau die Gewerbeuntersagungsverfügung gegen ihren Prozessgegner erlassen worden war. Wir teilten ihr mit, dass auch zu Prozesszwecken Informationen nachgefragt werden können. Sind jedoch personenbezogene Daten Dritter im Spiel, muss der Antragsteller bei der Behörde schlüssig darlegen, dass die Kenntnis dieser Informationen für die Wahrnehmung seiner **rechtlichen Interessen** vor Gericht notwendig ist.

- **Einsicht in die Bauakte bei Lärmbelästigungen**

Kann ein Nachbar Einsicht in die Bauakte eines Lebensmittelhändlers nehmen? Mit dieser Frage wandte sich ein Petent an uns, der sich durch den Betrieb eines Lebensmittelladens in einer umgebauten Garage gestört fühlte. Insbesondere ging es um von dem Laden ausgehenden **Lärm**. Wir haben den Petenten bei der Akteneinsicht unterstützt. Bei den in Bauakten enthaltenen Informationen handelt es sich zwar durchweg um personenbezogene Daten. Eine Offenbarung derartiger Informationen kommt also nur dann in Betracht, wenn der Antragsteller ein rechtliches Interesse geltend machen kann und keine überwiegenden schutzwürdigen Belange des Betroffenen, um dessen Daten es geht, entgegenstehen.

Das rechtliche Interesse bestand hier aber zweifelsfrei wegen der nachbarrechtlichen Situation. Ein **überwiegendes schutzwürdiges Interesse** des Lebensmittelbetreibers war nicht zu erkennen. Im Gegenteil: Es handelte sich – wie sich im weiteren Verlauf des Verfahrens herausstellte – um einen Betrieb, für den keine Genehmigung vorlag. Schutzwürdige Belange sind dann nicht anzunehmen, wenn ein Verhalten nicht im Einklang mit der geltenden Rechtsordnung steht. Das Gleiche galt für die Einsichtnahme in die beim Kreis vorliegenden **Lärmschutzprotokolle**. Auch hier war – allerdings gemessen an den etwas weniger strengen Anforderungen des Umweltinformationsgesetzes des Bundes – Einsicht zu gewähren.

- **Einsicht in Bauplanungsunterlagen**

Gegen die Planung eines Neubaugebietes in einer Gemeinde regte sich in der Bevölkerung Widerstand. Eine Bürgerinitiative begehrte Einsicht in sämtliche bei der Gemeinde vorhandenen Unterlagen zu dem **Bebauungsplanverfahren**, z. B. in die Planungsunterlagen, Landschaftspläne und Flächennutzungspläne. Den Antrag auf Einsichtnahme lehnte die Gemeinde rigoros ab. Sie vertrat dabei die Ansicht, dass sich das Informationsbegehren der Bürgerinitiative ausschließlich nach dem **Baugesetzbuch** (BauGB) richte, das aufgrund der Kollisionsnorm des Art. 31 Grundgesetz (**„Bundesrecht bricht Landesrecht**“) gegenüber dem IFG-SH vorrangig sei. Eine Einsichtnahme in ein laufendes Bebauungsplanverfahren sei nach dem Baugesetzbuch nicht möglich.

Tatsächlich enthält auch das BauGB Vorschriften über die Auslegung von Planentwürfen in der Öffentlichkeit. Allein der Umstand, dass es sich bei diesen Vorschriften um Bundesrecht handelt, führt jedoch nicht dazu, dass in Bauleitplanverfahren das IFG-SH keine Anwendung findet. Wegen ihrer **unterschiedlichen Ausrichtung** kommen die Vorschriften des IFG-SH und des BauGB nebeneinander zur Anwendung. Das BauGB regelt lediglich die Frage, welche Unterlagen im Bauleitplanverfahren durch die Gemeinde öffentlich auszulegen sind. Der **individuelle Informationszugang** einzelner Bürger nach dem IFG-SH wird hierdurch **nicht berührt**. Auch nach Darlegung unserer Rechtsauffassung weigerte sich die Gemeinde weiterhin, der Bürgerinitiative die Unterlagen zugänglich zu machen, sodass wir eine förmliche **Beanstandung** ausgesprochen haben. Gleichzeitig haben wir die Kommunalaufsicht benachrichtigt, die in dieser Frage jedoch ausdrücklich keine Stellung bezogen und die Antragsteller auf den Gerichtsweg verwiesen hat.

- **Einsicht in die Unterlagen über die Standortprüfung für eine Abfallverbrennungsanlage**

Im Zuge der Planung einer Abfallverbrennungsanlage prüfte eine Stadt mehrere Standorte. Als sie sich schließlich auf einen Standort mitten im Stadtgebiet festlegte, regte sich in der Bevölkerung Protest. Eine Bürgerinitiative wurde gegründet und ein Antrag auf Durchführung eines Bürgerentscheides gestellt. Eine zentrale Rolle spielten für dieses Verfahren **Prüfungen von alternativen Standorten** für die Anlage. Die Bürgerinitiative wandte sich an die Stadtwerke, die die alternativen Standortüberprüfungen durchgeführt hatten, und bat um Einsicht in die entsprechenden Unterlagen. Diese wurde der Bürgerinitiative verweigert. Auch eine Aufforderung der Ratsversammlung an die Stadtwerke, die alternativen Standortüberprüfungen zu veröffentlichen, hatte nicht den gewünschten Erfolg. Die Bürgerinitiative wandte sich schließlich an uns. Unsere Anfrage bei der Stadt zeigte Wirkung. Sämtliche Unterlagen, die die Bürgerinitiative hatte einsehen wollen, wurden **im Internet veröffentlicht**.

Was ist zu tun?
Bürgerinnen und Bürger sollten auch weiterhin ihre gesetzlichen Informationsansprüche wahrnehmen. Behörden sollten die Anliegen der Bürger ernst nehmen und die Herausgabe von Informationen als Serviceangebot verstehen.

12.3 AGID – Jahr der Informationsfreiheit 2003

Transparente Verwaltungsverfahren, E-Government und größere Partizipation der Bürgerinnen und Bürger am staatlichen Handeln sind Kernthemen der Modernisierungsdiskussion in der öffentlichen Verwaltung. Um die Informationsfreiheit auch in Deutschland stärker in den Mittelpunkt der öffentlichen Wahrnehmung zu rücken, hatte die Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands (AGID) 2003 als *Jahr der Informationsfreiheit* ausgerufen.

In Düsseldorf, Berlin, Potsdam und Kiel wurde in öffentlichen Veranstaltungen für die Idee der Informationsfreiheit geworben. Ihre Bedeutung in einer lebendigen und funktionsfähigen Demokratie war Gegenstand des Sommersymposiums „Informationsfreiheit“ in **Düsseldorf**. Bei dieser Auftaktveranstaltung wurde die Vielschichtigkeit der Thematik deutlich. Der Bogen spann sich von den historischen Wurzeln bis zu den Bezügen der Informationsfreiheit zum aktuellen Verfassungsrecht. Auch der Aspekt „Informationsfreiheit als mögliches Mittel zur Korruptionsbekämpfung“ nahm auf der Veranstaltung einen besonderen Platz ein.

Dass Informationsfreiheit eine technische Komponente hat, wurde auf der im Rahmen der Internationalen Funkausstellung in **Berlin** durchgeführten Veranstaltung „Informationsfreiheit und Datenschutz im Internet“ deutlich. Neben der grundsätzlichen Frage, wie die Zielvorgaben von Datenschutz und Informationsfreiheit im Zeitalter der **elektronischen Informationsvermittlung** miteinander harmonisiert werden können, berichteten internationale Referenten über ihre Erfahrungen bei der Umsetzung von Informationsfreiheitsgesetzen. Einen wesentlichen Beitrag leisteten die Vereinigten Staaten, deren Informationsfreiheitsrecht aus Bürgerbewegungen hervorgegangen ist.

Wir stehen vor dem Beitritt der mittel- und osteuropäischen Staaten zur Europäischen Union. Sowohl in den bisherigen als auch in den neuen Mitgliedsländern wird die Beziehung zwischen Staat und Bürgerinnen und Bürgern zunehmend auf eine elektronische Basis gestellt. Wie sieht unter diesen Bedingungen die Praxis des Persönlichkeitsschutzes und der Informationsfreiheit aus? Mit dieser Frage beschäftigte sich das internationale Symposium „Informationsfreiheit und Datenschutz – Transparenz und E-Government in Mittel- und Osteuropa“ in **Potsdam**. Es wurde deutlich, dass E-Government, um bei Bürgerinnen und Bürgern Akzeptanz zu finden, den Informationszugang für jedermann voraussetzt und dabei zugleich den datenschutzrechtlichen Anforderungen genügen muss. Beiträge von Referenten aus der Türkei, der Ukraine, aus Estland und Slowenien zeigten, dass auf dem Weg zu einem elektronischen Behörden- und Informationsdienst überall ähnliche Hindernisse auftreten, die es zu überwinden gilt.

Die Veranstaltungsreihe fand Ende des Jahres in Kiel ihren Abschluss in dem mit dem Schleswig-Holsteinischen Landtag durchgeführten Symposium **„Informationsfreiheit – vom Norden lernen“**. Vertreter aus den skandinavischen Staaten berichteten von deren zum Teil jahrhundertealter Tradition der Informationsfrei-

heit. Ein Referent aus Thailand referierte über die wichtige Funktion der Informationsfreiheit beim dortigen Demokratisierungsprozess und ihre Bedeutung für die Korruptionsbekämpfung in seinem Land. Daneben gaben die Initiatoren des schleswig-holsteinischen Gesetzes Einblick in dessen Entstehung. Ein weiterer Schwerpunkt lag auf der Umsetzung des Gesetzes und den dabei von uns gemachten – durchweg positiven – Erfahrungen. Abgeschlossen wurde die Veranstaltung durch eine Diskussionsrunde, bestehend aus Vertretern der öffentlichen Verwaltung und Antragstellern, die aus ihrer jeweiligen Sichtweise von Erfahrungen beim Umgang mit dem IFG-SH berichteten. Auch in dieser Veranstaltung wurde der Ruf nach einem Bundesinformationsfreiheitsgesetz laut. Die Referenten zeigten deutliches Unverständnis für die Untätigkeit des Bundesgesetzgebers und forderten, die für das Funktionieren der Demokratie wesentliche Initiative endlich angemessen voranzubringen (vgl. Tz. 12.4).

12.4 Bundesinformationsfreiheitsgesetz

Für die laufende Legislaturperiode sieht der Koalitionsvertrag erneut die Schaffung eines Informationsfreiheitsgesetzes des Bundes vor. Von ihm könnte ein Signal auch für die anderen Bundesländer ausgehen, die noch über kein derartiges Gesetz verfügen. Soll die Vereinbarung nicht erneut nur auf dem Papier stehen, ist die Bundesregierung jetzt aufgefordert zu handeln.

Die Absicht zur Schaffung eines Bundesinformationsfreiheitsgesetzes ist nicht neu. Bereits im vorangegangenen Koalitionsvertrag war eine entsprechende Vereinbarung enthalten, die allerdings nicht in die Tat umgesetzt wurde. Zu groß waren die **Bedenken aus der Verwaltung**. Angesichts der Erfahrungen, die in Schleswig-Holstein mit dem Informationsfreiheitsgesetz gemacht worden sind, ist dies allerdings nicht nachzuvollziehen (vgl. 25. TB, Tz. 13, sowie Tz. 12.1 dieses Berichtes). Sie zeigen, dass gravierende Probleme bei der Umsetzung des Informationsfreiheitsgesetzes praktisch nicht aufgetreten sind. Warum sollte dies auf Bundesebene anders sein?

Die Bundesregierung wäre gut beraten, aus dem Misslingen der letzten **Initiative** zu lernen. Bedenken aus einigen Fachressorts sollte nicht vorschnell nachgegeben werden. Ein Informationsfreiheitsgesetz, das den Namen nicht verdient, weil die gesetzlichen Ausnahmen vom **Grundsatz der Aktenöffentlichkeit** nichts mehr übrig lassen, hilft nicht weiter. Dabei kommt es nicht auf ein kompliziertes Gesetzeswerk an. Ein gutes Gesetz kommt auch mit wenigen Tatbeständen aus. Gibt es Gründe, den Informationszugang im Einzelfall nicht zu gewähren, bedeutet dies nicht, gleich den gesamten Verwaltungszweig aus dem Anwendungsbereich des Gesetzes herauszunehmen.

Und noch eine Frage stellt sich: Warum macht sich die Bundesregierung eigentlich nicht die vorhandenen **internationalen Erfahrungen** zunutze? Erfahrungen mit der Informationsfreiheit gibt es in ganz Europa zur Genüge. Da nimmt sich Deutschland wie ein weißer Fleck auf der Landkarte aus. Außer Luxemburg haben alle Länder der EU ein Informationsfreiheitsgesetz. Mit einer entsprechenden Gesetzesvorlage würde die Bundesregierung auch einen weiteren Vorteil

erlangen: Mehr **Transparenz** und eine stärkere **Partizipation der Bürgerinnen und Bürger** am gesellschaftlichen und kulturellen Leben würden dazu beitragen, das Vertrauen in die Politik zu stärken.

Was ist zu tun?
Die Bundesregierung sollte endlich handeln und einen Gesetzentwurf einbringen, um das Informationsfreiheitsgesetz noch in dieser Legislaturperiode zu verabschieden.

13 Was es sonst noch zu berichten gibt

13.1 Vorabkontrolle deckt Mängel beim HKR auf

Durch die Novelle des Landesdatenschutzgesetzes im Jahre 2000 wurde das Instrument der Vorabkontrolle eingeführt. Diese geht zurück auf eine Vorgabe in der Europäischen Datenschutzrichtlinie und hat unter anderem dann zu erfolgen, wenn ein automatisiertes Verfahren eingerichtet oder wesentlich geändert wird, in dem besonders sensible Daten verarbeitet werden. Solche Daten liegen bei Verfahren im Bereich **Haushalt-, Kassen- und Rechnungswesen** (HKR) vor, da dort unter anderem Steuerdaten und durch die Kreise oft auch Daten aus Sozialleistungsangelegenheiten verarbeitet werden. Die erforderliche Vorabkontrolle ist eine Aufgabe der behördlichen Datenschutzbeauftragten. Beim **Kreis Schleswig-Flensburg** wie auch bei der **Stadt Flensburg** wurde mustergültig aufgezeigt, welchen Wert eine vom behördlichen Datenschutzbeauftragten durchgeführte Vorabkontrolle für die Verbesserung des Datenschutzniveaus haben kann. Die Datenschutzbeauftragten beider Behörden konnten bei der Überprüfung eines weit verbreiteten HKR-Verfahrens einen Mangel feststellen, der zu erheblichen datenschutzrechtlichen Risiken führte. Unter Nutzung der Funktion der Haushaltsüberwachungsliste war es bei dieser Software möglich, auch Zahlungsvorgänge außerhalb des jeweiligen Zuständigkeitsbereiches des betreffenden Sachbearbeiters angezeigt zu bekommen. Damit konnte z. B. bei der Stadt Flensburg jeder mit Zahlungsvorgängen befasste Mitarbeiter auf einzelne Beihilfevorgänge, Steuerdaten oder Zahlungsrückläufe aus der Sozialhilfe zugreifen. Die Datenschutzbeauftragte des Kreises Schleswig-Flensburg informierte die Herstellerfirma des Produktes, die bereits nach wenigen Wochen einen speziellen Patch zur Behebung des Fehlers bereitstellte. Die Vorabkontrolle führte in diesem konkreten Fall nicht nur zum Nachweis der Datenschutzverträglichkeit des eingesetzten Verfahrens, sondern hatte positive Auswirkungen für eine Vielzahl anderer Kommunen, die das Verfahren ebenfalls einsetzen.

13.2 Müssen Vereine einen betrieblichen Datenschutzbeauftragten bestellen?

Von Vereinen und Verbänden wurde mehrfach die Frage an uns herangetragen, ob sie zur Bestellung eines Datenschutzbeauftragten verpflichtet seien. Grundsätzlich gelten für Vereine und Verbände die gleichen Datenschutzvorschriften wie für Wirtschaftsunternehmen. Für die Bestellung eines Datenschutzbeauftragten ist es in der Regel erforderlich, dass mindestens **fünf Arbeitnehmer** mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden. Wenn eine Vereinigung professionelle Strukturen hat, insbesondere selbst Arbeitgeber ist, muss auch sie die Verpflichtung zur Bestellung eines Datenschutzbeauftragten erfüllen.

13.3 Arbeitsgruppe FISCUS liegt auf Eis

Mit großen Erwartungen ist eine Arbeitsgruppe ans Werk gegangen, die die Entwicklung des bundeseinheitlichen automatisierten Besteuerungsverfahrens

FISCUS begleiten wollte (vgl. 24. TB, Tz. 4.10.2). Auch das für die Entwicklung von FISCUS gegründete Softwarehaus versprach sich einiges von dieser Zusammenarbeit, weil verabredet war, bereits auf Konzeptebene einen datenschutzrechtlichen und sicherheitstechnischen Abstimmungsprozess zu realisieren. Leider konnte dies nur für ein einziges Projekt und auch nur für dessen Pilotversion durchgeführt werden. Offenbar hat die FISCUS GmbH von ihrem Auftraggeber, dem Bundesfinanzministerium, kein Mandat für weitere Gespräche und die Übergabe von Konzeptunterlagen bekommen. Die Arbeitsgruppe besteht derzeit praktisch nur auf dem Papier. Mit dem automatisierten Besteuerungsverfahren werden sich die Datenschutzbeauftragten wohl erst wieder befassen können, wenn die Einzelmodule in den Ländern in Pilotverfahren getestet werden. Die Behebung von Mängeln und die Berücksichtigung datenschutzrechtlicher und sicherheitstechnischer Verbesserung werden dadurch nicht eben einfacher.

13.4 Arbeitsgruppe AOK-SAM effizient

Eine Arbeitsgruppe der Datenschutzbeauftragten begleitet das automatisierte Verfahren **AOK-SAM**. Hierbei handelt es sich um ein Mammutprojekt des Bundesverbandes der Allgemeinen Ortskrankenkassen in Zusammenarbeit mit dem AOK-Systemhaus und der Firma SAP, das über mehrere Jahre angelegt ist. Die Vertreter der Krankenkassen haben offenbar den Wert sehr frühzeitiger datenschutzrechtlicher Klärungen erkannt. Sie legen bereits ihre Konzepte offen, demonstrieren ihre Prototypen für die so genannte Masterversion und ermöglichen die Analyse von Pilotverfahren. Dies ist für beide Seiten sehr arbeitsintensiv, erleichtert den Datenschutzbeauftragten aber beim späteren Einsatz der Module das Ermitteln und Bewerten kassenspezifischer Besonderheiten. Deshalb werden die Erkenntnisse, die in der Arbeitsgruppe gewonnen werden, über die Arbeitskreise „Gesundheit und Soziales“ und „Technik“ bereits jetzt den Kollegen in denjenigen Bundesländern bekannt gegeben, die nicht in der Arbeitsgruppe vertreten sind. Welche unmittelbaren Konsequenzen die Projektverantwortlichen der Krankenkassenseite aus den manchmal durchaus kontroversen Erörterungen ziehen, lässt sich nicht genau abschätzen. Eine Reihe von problematischen Absichten werden aber offenbar nicht mehr weiterverfolgt, weil man erkannt hat, dass diesbezüglich ein Konsens mit den Datenschützern nicht herstellbar sein wird. Nicht zuletzt auch wegen der außergewöhnlich guten kollegialen Atmosphäre dürfte diese Arbeitsgruppe auch künftig sehr effizient arbeiten können.

13.5 Weitergabe der Mängel an Hauswasseranschlüssen an private Firmen

Eine Gemeinde hatte gemeinsam mit dem zuständigen Wasserbeschaffungsverband die in der Gemeinde vorhandenen Hauswasseranschlüsse überprüft. Dabei wurden Mängel festgestellt, die von den Eigentümern der Hausanschlussleitungen zu beseitigen waren. Noch bevor die Betroffenen überhaupt über die festgestellten Mängel unterrichtet wurden, hatte die Gemeinde zwei **örtliche Fachfirmen** aufgefordert, Kostenvoranschläge für die Mängelbeseitigung abzugeben. Das jeweils günstigste Angebot wurde den Eigentümern zusammen mit der Aufforderung zur Mängelbeseitigung zur Verfügung gestellt. Die Gemeinde wollte dieses Verfahren als selbstverständliche Serviceleistung gegenüber den Betroffenen verstanden

wissen; unseres Erachtens hätte ein wirklicher Service zuvor eine Abstimmung mit den Betroffenen erfordert. Die Datenübermittlung war deshalb als Verstoß gegen geltendes Datenschutzrecht zu beanstanden.

13.6 Prüfung von Wahlunterstützungsunterschriften

Das Verfahren für die Behandlung von Wahlvorschlägen ist im Gemeinde- und Kreiswahlrecht geregelt. Danach sind Wahlvorschlägen zwingend auch die erforderlichen Unterstützungsunterschriften nebst Bescheinigung des Wahlrechts der Unterzeichnerinnen und Unterzeichner beizufügen. Eine Partei begehrte die Zulassung zur Kreistagswahl. Die Wahlunterlagen enthielten zwar eine ausreichende Zahl von **Unterstützungsunterschriften**, allerdings fehlte die für jeden Einzelfall vorgesehene Wahlrechtsbescheinigung des Unterstützers. Die Zulassung der Partei wurde deshalb abgelehnt. Auf Wunsch der Partei sind wir der Frage nachgegangen, ob die Einholung der Wahlrechtsbescheinigung durch die sich bewerbende Partei den datenschutzrechtlichen Grundsätzen entspricht. Das Verfahren war im Hinblick auf die Persönlichkeitsrechte der Unterschriftsleistenden **nicht zu beanstanden**. Entsprechend dem geprüften Vordruck erklärt sich der Unterstützer damit einverstanden, dass für ihn eine Bescheinigung des Wahlrechts eingeholt wird. Sollte er dies nicht wollen, kann er den Zusatz auch streichen, die Bescheinigung selbst einholen und sie erst dann der Partei zuleiten. In diesem Fall wäre sichergestellt, dass Dritte von einer möglichen Versagung der Bescheinigung keine Kenntnis erlangen.

13.7 Datenschutz zum Schmunzeln

Einen sehr spezifischen „technischen“ Fortschritt bei der Altaktenvernichtung konnten wir bei der Prüfung einer Kommunalverwaltung registrieren. In den 70er-Jahren erfolgte die Vernichtung noch im Handbetrieb. Man vergrub die Altakten auf einem gemeindeeigenen Grundstück. In den 80er-Jahren wurde das Papier in einem mechanischen Schredder zerkleinert und die Schnipsel dem örtlichen Bestattungsunternehmer zur **Auspolsterung von Särgen** übergeben. Als in den 90er-Jahren das Altpapier überhand nahm und das Bestattungsunternehmen auf andere Materialien zur Sargpolsterung auswich, beauftragte man einen professionellen Altaktenversorger, der die ordnungsgemäße Entsorgung mit modernen Systemen schriftlich bestätigte. Keine der drei Methoden bot einen Grund zu Beanstandungen, aber die Technik schreitet eben unaufhaltsam voran!

14 Rückblick

14.1 Nutzung der Steuernummern ohne Beanstandung

Viele Bürger fürchteten um das Steuergeheimnis, als die bis dahin quasi vertraulich behandelten Steuernummern von den Steuerpflichtigen auf Rechnungen und dergleichen vermerkt werden mussten. Sie wurden damit öffentlich wie Kontonummern. Dem Versprechen der Steuerverwaltung, keine Auskünfte zu erteilen, wenn nur die Steuernummer als Identifizierungsmerkmal genannt wurde, vertraute man nicht (vgl. 25. TB, Tz. 4.10.4). Nach nunmehr fast zweijähriger Erfahrung kann man sagen, dass die Finanzämter wohl tatsächlich „dichthalten". Man bezweifelt seitens der Steuerpflichtigen zwar nach wie vor die Sinnhaftigkeit der Verpflichtung, immer und immer wieder die Steuernummer anzugeben, Beschwerden über unzureichende Identitätsprüfungen bei Auskünften durch die Finanzämter oder über sonstige Missbrauchsversuche mit Steuernummern sind uns jedoch nicht auf den Tisch gekommen.

14.2 Firewall endlich korrigiert und ausreichend dokumentiert

Kurs FW

Die Überprüfung einer Firewall, die von uns bereits im Januar 2002 durchgeführt wurde, konnte erst Ende 2003 zum Abschluss gebracht werden, weil es nahezu zwei Jahre dauerte, um von dem betreffenden Anbieter prüffähige Unterlagen zu erhalten (vgl. 25. TB, Tz. 7.4.2). Es zeigte sich, dass die Amtsverwaltung, die die Firewall einsetzt, ohne unsere Hilfe wohl nie in den Besitz der vollständigen Dokumentation gekommen wäre. Dabei ging es nicht nur um die Durchsetzung eines formalen Anspruches. Als wir Anfang 2003 die ersten Unterlagen erhielten, stellte sich schnell heraus, dass seitens des Anbieters eine Reihe von Schwachstellen und Inplausibilitäten zu bereinigen waren. Unsere Beharrlichkeit hatte also einen guten Grund.

14.3 Was lange währt, wird nicht zwangsläufig gut!

Jahrelang hatten wir gefordert, die Sicherheitsüberprüfungen im Lande auf eine gesetzliche Grundlage zu stellen. Seit Februar 2001 lag der Entwurf eines Landessicherheitsüberprüfungsgesetzes vor, den das Parlament inzwischen verabschiedet hat. Zeit genug eigentlich, um auch datenschutzrechtlichen Aspekten ausreichend Rechnung tragen zu können. Im Ergebnis lässt sich zwar feststellen, dass der Gesetzestext insgesamt ein akzeptables Datenschutzniveau aufweist. Einige grundsätzliche datenschutzrechtliche Mängel konnten jedoch im Gesetzgebungsverfahren leider nicht beseitigt werden. Dazu gehört insbesondere die Abschaffung der aus datenschutzrechtlicher Sicht wünschenswerten Funktion des Sicherheitsbeauftragten des Landes sowie die Festlegung der sicherheitsempfindlichen Stellen bestimmter lebens- oder verteidigungswichtiger Einrichtungen durch eine Verordnung der Landesregierung (vgl. 23., 24. und 25. TB, Tz. 4.4). Daraus entstehen vermeidbare Risiken beim Umgang mit den besonders sensiblen Daten aus Sicherheitsüberprüfungsverfahren.

14.4 Angaben über Mieter in der Zweitwohnungssteuererklärung

In den letzten Jahren hat es immer wieder Beschwerden über die Neugierde der Kommunen bei der Erhebung von Daten für die Festsetzung der Zweitwohnungssteuer gegeben (vgl. 24. TB, Tz. 4.10.3). Die entsprechenden Vordrucke einer Reihe von Gemeinden mussten aufgrund unserer Beanstandungen neu gestaltet werden. Dies ist offenbar in der Zwischenzeit geschehen. Die Anzahl der uns erreichenden Beschwerden jedenfalls ist sehr rückläufig. Es fällt zwar immer noch unangenehm auf, dass oft die Namen von Mietern erfragt werden. Da jedoch keine Angaben über die Anschrift zu machen sind, ist ein konkreter Personenbezug nicht gegeben und die Begründung, dass die Namen nur zu Plausibilitätszwecken gebraucht würden, nicht zu widerlegen.

14.5 Steuerverwaltung reklamiert für sich nach wie vor Sonderrechte

Die Abgabenordnung ist eines von vielen Verwaltungsverfahrensgesetzen. Sie hat den gleichen Rang wie z. B. das Sozialgesetzbuch X, das Baugesetzbuch, das Verwaltungsverfahrensgesetz des Bundes und die Strafprozessordnung. Soweit diese Gesetze keine ausreichenden Regelungen zur Gewährleistung des informationellen Selbstbestimmungsrechts der Bürger enthalten, gelten die Datenschutzgesetze. Das wird in allen Verwaltungsbereichen anerkannt, nur die Steuerverwaltung reklamiert für sich seit Jahren Sonderrechte (vgl. 25. TB, Tz. 4.10.5). Sie ist zwar schnell bei der Hand, wenn es darum geht, den Gesetzgeber zum Aufbau großer Informationssysteme zu bewegen (vgl. Tz. 4.9.1). Die Anpassung der AO an das Niveau der EU-Datenschutzrichtlinie steht jedoch nach wie vor noch aus. Gleichzeitig wird aber eine Anwendung des allgemeinen Datenschutzrechts abgelehnt mit der Begründung, in der AO sei der Datenschutz abschließend und ausreichend geregelt.

14.6 Steuerfahnder in der Grauzone

Wenn Steuerfahnder ermitteln, sind sie Diener zweier Herren. Einerseits erhalten sie Weisungen von ihren Vorgesetzten im Finanzamt. Andererseits erteilen ihnen auch die Staatsanwaltschaften Aufträge. Welche Behörde für welche Aktivitäten die Verantwortung trägt, ist oft nicht leicht zu erkennen, insbesondere wenn mal etwas schief läuft (vgl. 25. TB, Tz. 4.10.7). Trotz offenkundiger Defizite in diesem Bereich hat sich die Steuerverwaltung bisher nicht veranlasst gesehen, für klare Regelungen zu sorgen. Es bedarf offensichtlich erst noch weiterer Konfliktfälle.

14.7 Zu hohe Anforderungen an Systemadministratoren

Selbst Fulltimesystemadministratoren raufen sich immer häufiger die Haare. Die Betriebssysteme und Hardwarekomponenten werden immer komplexer, ohne Vernetzung aller Arbeitsplätze mit der ganzen Internet-Welt droht der Zusammenbruch der Verwaltung, und alle Anforderungen des Managements müssen abends erfüllt sein, selbst wenn sie morgens noch so ungenau formuliert worden

sind (vgl. 25. TB, Tz. 7.1). Das Verwaltungsmanagement betrachtet die Systemadministratoren gleichwohl mehr und mehr als einen Kostenfaktor. Ein entscheidendes Umdenken in Richtung auf eine verbesserte organisatorische Anbindung und eine fundierte Ausbildung dieses Bereiches ist in der Praxis nicht zu erkennen. Allerdings ist im kommunalen Bereich eine verstärkte behördenübergreifende Zusammenarbeit bei der Betreuung von IT-Systemen zu erkennen. Dies ist immerhin ein Hoffnungsschimmer.

14.8 Werbung, die die Verbraucher nicht wollen

Im 25. Tätigkeitsbericht (vgl. Tz. 6.1) hatten wir berichtet, dass die Bürgerinnen und Bürger Schleswig-Holsteins laut einer Verbraucherumfrage mit unverlangten Werbezuschriften nicht einverstanden sind. Hierüber hat sich der Deutsche Direktmarketing Verband (DDV) beim Ministerium für Wirtschaft, Technologie und Verkehr sowie beim Innenministerium des Landes Schleswig-Holstein beschwert. Das Innenministerium wies die Beschwerde des DDV in der Sache zurück, während das Ministerium für Wirtschaft, Technologie und Verkehr seine Zuständigkeit verneinte. Die Stellungnahmen sind veröffentlicht unter

www.datenschutzzentrum.de/material/themen/wirtscha/ddvumfra.htm

14.9 Ergebnisse von Kontrollen der schleswig-holsteinischen Wirtschaftsauskunfteien

Wiederholt (vgl. zuletzt 25. TB, Tz. 6.2.1) hatten wir nach der Kontrolle von Auskunfteien beanstandet, dass diese Informationen auch dann weitergeben, wenn das berechtigte Interesse an dem Datenerhalt nur vage begründet ist. Um bundeseinheitlich eine datenschutzkonforme Verfahrensweise herbeizuführen, haben wir dem „Düsseldorfer Kreis“ der obersten Datenschutzaufsichtsbehörden die Beanstandung der beiden nichts sagenden Anfragegründe „Bonitätsprüfung“ und „Geschäftsanbahnung“ mitgeteilt. Der Düsseldorfer Kreis hat den Verband deutscher Wirtschaftsauskunfteien zu einer Stellungnahme aufgefordert. Ein greifbares Ergebnis der Verhandlungen steht noch aus.

14.10 Flucht aus dem Informationsfreiheitsgesetz

Im 24. und 25. Tätigkeitsbericht hatten wir über die Gesetzesauslegung (vgl. dort Tz. 13.1 und Tz. 13.2) einiger Kommunen berichtet, wonach das Informationsfreiheitsgesetz keine Anwendung auf fiskalisches Handeln einer Behörde finden soll. Nach wie vor finden sich keine nachvollziehbaren Argumente für diese Lesart. Im Gegenteil: Weitere Einsichtsersuchen, die uns im Rahmen von Eingaben bekannt geworden sind, belegen, dass bei Bürgerinnen und Bürgern Interesse an der Öffentlichmachung von Vorgängen aus diesem Bereich besteht. Im Zuge der Beratungen des 25. Tätigkeitsberichtes im Landtag kündigten einige Abgeordnete die Prüfung einer Änderung des Informationsfreiheitsgesetzes mit dem Ziel an, dieses Schlupfloch zu schließen.

14.11 Heimliche Vaterschaftstests

Im 24. Tätigkeitsbericht (Tz. 4.8.10) berichteten wir über heimliche genetische Vaterschaftstests und brachten die Hoffnung zum Ausdruck, dass der Bundesgesetzgeber hierzu ein klares Verbot ausspricht. Leider müssen wir feststellen, dass sich die Praxis der heimlichen genetischen Abstammungsuntersuchungen immer noch weiter ausbreitet. Der Gesetzgeber ist untätig geblieben. Nicht nur das: Das Landgericht München entschied in einem Wettbewerbsverfahren, dass gegen das Angebot solcher Gentests nichts einzuwenden sei. In einer Urteilsanmerkung haben wir zum Ausdruck gebracht, dass dieses Urteil aus Datenschutzsicht verfehlt ist:

www.datenschutzzentrum.de/medizin/genom/vaterschtest.htm

Inzwischen hat das Oberlandesgericht Celle in einem Vaterschaftsanfechtungsverfahren entschieden, dass die heimlich eingeholten Vaterschaftsnachweise das Recht auf informationelle Selbstbestimmung der betroffenen Kinder verletzen und die Ergebnisse der Gentests nicht verwertet werden dürfen.

15 Beispiele dafür, was die Bürgerinnen und Bürger von unserer Tätigkeit haben

1. *In einem Bürgerbüro konnten Gespräche, die an einem Besucherarbeitsplatz geführt wurden, auch an anderen Besucherarbeitsplätzen und im Wartebereich auf dem Flur problemlos mit angehört werden. Auf diese Weise erhielten Unbefugte Kenntnis von sensiblen Daten der Besucher. Auf unsere Anregung hin wurde die Akustikabtrennung zwischen den Besucherarbeitsplätzen sowie gegenüber dem Wartebereich wesentlich verbessert.*

2. *Bei der Festsetzung von Straßenausbaubeiträgen sollten die Bemessungsgrundlagen sowie die Höhe des zu zahlenden Beitrages einzelfallbezogen allen Beitragspflichtigen gegenüber bekannt gegeben werden. Für einen effektiven Rechtsschutz der Betroffenen war dies nicht erforderlich. Auf unseren Vorschlag hin wurden nur solche Daten weitergegeben, die zwar eine Kontrolle der Festsetzung der Ausbaubeiträge zuließen, jedoch keine Rückschlüsse auf die beteiligten Grundstückseigentümer ermöglichten.*

3. *Auf der Seite www.schleswig-holstein.de, die auch das offizielle Internet-Angebot des Landes beinhaltet, wurden langfristige Cookies verwendet, im Rahmen einer so genannten Mit-Mach-Börse unzulässig Daten erhoben und ein Webmaildienst angeboten, der für den Nutzer zunächst unerkennbar die vollständigen Personendaten den von ihm abgesendeten Mails beifügte. Nach unserer Intervention gegenüber dem Anbieter konnten diese Probleme behoben werden.*

4. *Das Landesbesoldungsamt Schleswig-Holstein verweigerte geschiedenen Ehefrauen ehemaliger Landesbeamten die Erteilung von Auskünften aus deren Personalakten zur Verfolgung von Unterhaltsansprüchen. Auf Bitten des Petitionsausschusses des Schleswig-Holsteinischen Landtages haben wir dem Landesbesoldungsamt einen rechtlich zulässigen Weg zur Weitergabe der gewünschten Informationen aufgezeigt.*

5. *Einer Grundstückseigentümerin war im Rahmen eines Neubauvorhabens des Nachbarn von der zuständigen Bauaufsichtsbehörde die Einsicht in dessen Bauakte unter Hinweis auf den „Datenschutz“ versagt worden. Unsere Prüfung ergab, dass die Grundstückseigentümerin nach der Landesbauordnung einen Anspruch darauf hatte, Lageplan, Bauzeichnungen und Baubeschreibung des Nachbarn einzusehen, da die Baumaßnahme ihre Belange berühren konnte.*

6. *Gelegentlich fordern Banken Ärzte im Rahmen der Überprüfung der Kreditwürdigkeit auf, ihre Debitorenliste vorzulegen. Auf diesem Wege könnten Patientendaten an die Banken gelangen. Unsere Intervention führte zu einer Änderung dieser Verfahrensweise.*

7. *Bei der Übermittlung von Blutbefunden an die Polizei wurden Informationen über Abbauprodukte auch dann bekannt gegeben, wenn gar keine Trunkenheit im Straßenverkehr vorlag. Nach unserem Tätigwerden wird sich die Datenübermittlung künftig strikt an die Vorgaben der Straßenverkehrsgesetze halten.*

8. *Das Landgericht Kiel betreibt einen Schulungsraum, der mit dem restlichen Netz des Gerichts verbunden ist. Aufgrund einer unzureichenden Absicherung bestand die Gefahr, dass von dort Angriffe auf Datenbestände der Justiz unternommen werden konnten. Mit Vertretern des Ministeriums und des Landgerichts haben wir ein Konzept erarbeitet, mit dem die Sicherheit im Schulungsraum ohne großen finanziellen und systemadministrativen Aufwand gewährleistet werden kann.*

9. *Auf der Grundlage schwer zu durchschauender Lizenzvereinbarungen versuchte die Firma Microsoft, von Kunden unbemerkt Änderungen an den Betriebssystemen online vornehmen zu können. Angepriesen wurde diese Methode mit dem Angebot, fehlerberichtigende Software (Patches) zum frühestmöglichen Zeitpunkt einzuspielen. Nicht erwähnt wurde, dass Microsoft damit die volle Verfügungsgewalt über das Betriebssystem erlangt hätte und auch die Datenbestände hätte ausspähen können. Nach dem von uns initiierten Protest der Datenschutzbeauftragten des Bundes und der Länder bietet Microsoft nunmehr ein datenschutzrechtlich und sicherheitstechnisch besseres Verfahren an.*

10. *In schleswig-holsteinischen Justizvollzugsanstalten wurden medizinische Gutachten mit intimen Angaben auch über Opfer von Straftätern so vorgehalten, dass weit mehr Personen Zugriff darauf hatten, als dies für die Aufgabenerfüllung erforderlich war. Durch unser Tätigwerden konnte erreicht werden, dass diese sensiblen Informationen künftig getrennt von der Gefangenenpersonalakte so aufbewahrt werden, dass nur ein kontrollierter Zugriff möglich ist.*

11. *Pressewirksam wurde wiederholt die Forderung erhoben, Bewährungshelfer müssten Daten ihrer Probanden freizügig an die Polizei übermitteln dürfen. Neben einer Störung des Vertrauensverhältnisses zwischen Bewährungshelfer und Proband hätte dies zu überflüssigen Datenübermittlungen geführt. Nunmehr hat das Justizministerium unsere Auffassung bekräftig, dass die Einschaltung der Polizei nur dann in Betracht kommt, wenn konkrete Anhaltspunkte für neue Straftaten vorliegen.*

12. *Detekteien und Sicherheitsunternehmen verarbeiten in erheblichem Umfang personenbezogene Daten und greifen in die Privatsphäre ihrer „Zielpersonen“ ein. Vor allem die systematische Observation des Privatlebens darf nur unter strikt rechtlichen Bedingungen erfolgen. Nach unseren Beanstandungen stellte ein geprüftes Sicherheitsunternehmen seine bedenkliche Observationspraxis komplett ein.*

13. *Bei der Zweitwohnungssteuer wurden in den vergangenen Jahren regelmäßig mehr Daten erhoben als zulässig. Auf diesem Weg erhielten die Kommunen vor allem persönliche Daten über Übernachtungs- und Kurgäste. Nach unserer Intervention schränkten die kritisierten Kommunen ihre Vordrucke entsprechend ein.*

14. *Ein Unternehmen plante die Einführung einer Revisionssoftware, die sämtliche Vorgänge an seinen Kassen erfassen und auswerten sollte. Die Kassenmitarbeiter wären bei einer ungeregelten Nutzung der Software einer lückenlosen Überwachung durch den Arbeitgeber ausgesetzt gewesen. Wir haben die Software begutachtet und die Bedingungen für einen rechtmäßigen Einsatz formuliert. Unsere rechtlichen Wertungen sind in eine Gesamtbetriebsvereinbarung umgesetzt worden, in der sowohl eine effektive Revision als auch der Schutz der Arbeitnehmer gewährleistet ist.*

15. *In bestimmten Ausnahmefällen darf mit personenbezogenen Krebsregisterdaten geforscht werden. Damit ohne sein Wissen kein „Gesamtbild" eines Krebskranken entstehen kann, sind die Forschungsprojekte gegeneinander abzuschotten. Nach einer Prüfung des Krebsregisters sind die Maßnahmen zur Trennung der Datenbestände so verbessert worden, dass die Gefahr unzulässiger Verknüpfungen praktisch nicht mehr gegeben ist.*

16. *Viele Benutzer von Arbeitsplatzrechnern haben Zweifel, ob die von den Systemadministratoren vorgegebenen Sicherheitsmaßnahmen tatsächlich ausreichend sind. Da ihnen zumeist nicht bekannt ist, welcher Sicherheitsstandard möglich ist, haben sie keine Möglichkeit zu kritischen Fragen. Unser neues backUP-Magazin versetzt sie in die Lage, die erforderliche Sicherheit am Arbeitsplatz einzufordern. Nutznießer sind die Bürgerinnen und Bürger, deren Daten verarbeitet werden. Auf diese Weise wird insbesondere die Vertraulichkeit der Datenverarbeitungsprozesse verbessert.*

17. *Unsere Hinweise auf die erforderlichen (Mindest-)Sicherheitsmaßnahmen und die verbleibenden Restrisiken der in der Verwaltung eingesetzten Betriebssysteme der Firma Microsoft gehören in der Zwischenzeit zur Standardliteratur von Systemadministratoren. Selbst die Firma Microsoft empfiehlt die Einhaltung unserer Empfehlungen. Man kann wegen der weiten Verbreitung der backUP-Magazine davon ausgehen, dass durch sie das Sicherheitsniveau der IT-Systeme verbessert wird.*

18. *Bei einer Versicherung war es im Rahmen der engen Zusammenarbeit mit Sparkassen „üblich", medizinische Daten aus den Unterlagen über Lebensversicherungen an die örtliche Sparkassenfiliale zu schicken. Auf unser Betreiben hin hat die Versicherungsgesellschaft ihr Verfahren geändert und zugesagt, künftig derartige Unterlagen mit medizinischen Einzelheiten nur noch an den Betroffenen selbst zu übersenden.*

19. *Die Telefonseelsorge im Internet ist als Beratungsangebot für manche Menschen in brisanten Situationen der letzte Ausweg. Wesensmerkmal der Telefonseelsorge ist, dass sie auf Wunsch anonym erfolgt. Kirchliche Stellen empfehlen die Nutzung unseres Anonymitätsdienstes AN.ON.*

20. Die chinesische Regierung betreibt eine rigide Zensur des Internet-Verkehrs von Nutzern in China, sodass zahlreiche Internet-Angebote gesperrt werden. Dies betrifft auch deutsche Firmen, die in China tätig sind. Mittels AN.ON ist es ihnen möglich, diese Zensur zu umgehen und auch auf von der Regierung nicht überwachte Internet-Angebote zuzugreifen.

21. In der Ärzteschaft, der Zahnärzteschaft und bei den Patientinnen und Patienten besteht oft Unsicherheit, welche Ansprüche und welche Pflichten aus Datenschutzsicht bestehen. Folge dieser Unsicherheit ist, dass aufgrund falscher Befürchtungen wichtige Informationen vorenthalten werden oder aber ohne rechtliche Grundlage das Patientengeheimnis und damit die Vertrauensbeziehung zwischen Arzt und Patient verletzt wird. Gemeinsam mit den Kammern der Ärzte und der Zahnärzte haben wir auch im Berichtsjahr mit unserer Aktion „Datenschutz in meiner Arztpraxis" allen Betroffenen Informationen und Hilfen für die typischen Problemlagen gegeben.

22. Über Jahre hinweg bestand ein Konflikt zwischen Krankenhäusern und Krankenkassen hinsichtlich der Kostenabrechnung: Unter der Androhung, anderenfalls die Kosten nicht zu tragen, erreichten die Krankenkassen, dass ihnen auch sensibelste Arztunterlagen übergeben wurden, auf die sie keinen Anspruch hatten. Im Rahmen eines Schiedsverfahrens machten wir einen von allen Seiten akzeptierten und nunmehr landesweiten praktizierten Vorschlag, der den Krankenkassen eine Plausibilitätskontrolle von Abrechnungen ermöglicht, ohne dass dabei ein Übermaß an Patientendaten an die Kassen gelangt.

16 DATENSCHUTZAKADEMIE Schleswig-Holstein

16.1 10 Jahre DATENSCHUTZAKADEMIE Schleswig-Holstein

Die DATENSCHUTZAKADEMIE geht mit dem Programm 2004 in das elfte Jahr ihres Bestehens. Sie wurde am 30. August 1993 in der Heimvolkshochschule Leck (jetzt: Nordsee Akademie Leck) eröffnet. Die DATENSCHUTZAKADEMIE dient dem Zweck, Kenntnisse auf dem Gebiet des Datenschutzes, der Datensicherheit und des Datenverarbeitungsrechts praxisgerecht zu vermitteln. Die angebotenen Kurse verfolgen das Ziel, den Teilnehmern eine systematische Fortbildung zu ermöglichen, an deren Ende sie in der Lage sind, Fragen des Datenschutzes an ihrem Arbeitsplatz zu bewältigen.

Die DATENSCHUTZAKADEMIE ist ein Kooperationsprojekt. Sie wird vom Deutschen Grenzverein, der Nordsee Akademie Leck und dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) gemeinsam betrieben. Der Grenzverein steuert seine Erfahrungen bei der Durchführung von Bildungsveranstaltungen und seine Verwaltungskapazität für die Abwicklung der Kurse bei. Der Nordsee Akademie Leck obliegt in erster Linie die organisatorische Betreuung der einzelnen Veranstaltungen. Das ULD übernimmt vor allem die inhaltliche Konzeption des Fortbildungsangebotes unter datenschutzrechtlichen Aspekten, die Erstellung des Jahresprogramms, die Außendarstellung der DATENSCHUTZAKADEMIE und die Gewinnung von Referenten für die Fortbildungskurse.

Das Angebot der DATENSCHUTZAKADEMIE richtete sich zunächst an Mitarbeiterinnen und Mitarbeiter in Behörden Schleswig-Holsteins und wurde 2000 mit der Übernahme der Kontrolle des Datenschutzes in der Wirtschaft auf die Privatwirtschaft ausgedehnt. Allerdings konnte bis heute aufgrund der knappen personellen Ressourcen in diesem Bereich noch kein so umfangreiches Fortbildungsangebot entwickelt werden, wie es wünschenswert wäre. In den letzten Jahren begann sich der Datenschutz in Schleswig-Holstein verstärkt als Serviceeinrichtung für die Bürger zu verstehen. So ist das Angebot der DATENSCHUTZAKADEMIE auch für Bürgerinnen und Bürger geöffnet worden.

Einige Kurse werden in Zusammenarbeit mit anderen Trägern der Bildungsarbeit durchgeführt. Es sind dies: Institut für Qualitätsentwicklung an Schulen Schleswig-Holstein, Verwaltungsakademie Bordesholm, Polizeischule in Kiebitzhörn, Verwaltungsfachhochschule Altenholz. Mehrtageskurse finden in der Regel in der Nordsee Akademie Leck statt, die seit 2001 über einen modern eingerichteten Computerschulungsraum verfügt. Die Gebäude der Nordsee Akademie liegen in einer parkähnlichen Anlage und sind im Jahr 2000 grundlegend modernisiert worden. Große und kleine Seminarräume ermöglichen mit den vorhandenen pädagogischen Medien intensive Arbeit im Plenum und in Gruppen. Eine komfortable Unterbringung in Einzelzimmern und eine hervorragende Küche runden das Bild ab.

Auch beim ULD steht seit 2002 ein Schulungsraum mit 12 vernetzten PC-Arbeitsplätzen zur Verfügung und wird vorwiegend für eintägige IT-Schulungsveranstaltungen genutzt. Weitere Veranstaltungen werden in Kiel in Hotels durchgeführt. In den letzten Jahren steigend ist die Anzahl von Inhouse-Schulungen, bei denen unsere Referenten vor Ort Veranstaltungen durchführen.

Die DATENSCHUTZAKADEMIE Schleswig-Holstein hat es sich von Anfang an zur Aufgabe gemacht, ihr Programm nach den aktuellen technischen und gesellschaftlichen Entwicklungen fortzuentwickeln. Sie wertet seit Beginn auch die Wünsche ihrer Teilnehmerinnen und Teilnehmer sowie die Anregungen aus Wirtschaft und Verwaltung in Schleswig-Holstein aus und setzt diese um, wo es möglich ist.

Die DATENSCHUTZAKADEMIE Schleswig-Holstein kommt ohne eigenen Verwaltungsapparat und ohne eigene Haushaltsmittel aus. Die Kursgebühren sind deshalb so angelegt, dass sie die Kosten für Referenten, Unterrichtsmaterial, Unterkunft und Verpflegung sowie die anfallenden Verwaltungskosten decken.

Neuorganisation der DATENSCHUTZAKADEMIE Schleswig-Holstein

Die DATENSCHUTZAKADEMIE Schleswig-Holstein war zunächst eine Art Arbeitsgemeinschaft des Landesbeauftragten für den Datenschutz und des Deutschen Grenzvereins. Die ersten neun Jahre wurde sie von einem Kuratorium begleitet und gefördert. Ihm gehörten folgende Personen an:

Prof. Dr. Ralf Bernd Abel
ehem. stv. Vorstandsvorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V., Bonn (bis 1996)

MDgt. a. D. Ernst Eugen Becker
ehem. Datenschutzbeauftragter von Schleswig-Holstein

Dr. Hartmut Borchert
Geschäftsführer des Schleswig-Holsteinischen Gemeindetages

Prof. Dr. jur. Alfred Büllesbach
Konzernbeauftragter für Datenschutz der DaimlerChrysler AG, Stuttgart, ehem. Bremer Datenschutzbeauftragter

Prof. Dr. Hans Peter Bull
Universität Hamburg, Seminar für Verwaltungslehre, ehem. Innenminister des Landes Schleswig-Holstein, ehem. Bundesbeauftragter für den Datenschutz

Dr. Carl-August Conrad
Geschäftsführer des Schleswig-Holsteinischen Landkreistages (bis 1996)

Jan-Christian Erps
Geschäftsführendes Mitglied des Schleswig-Holsteinischen Landkreistages (ab 1997)

Bernd Hentschel
Vorstandsvorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V., Bonn

Dr.-Ing. Gert Lang-Lendorff
ehem. Vorstandsvorsitzender der Datenzentrale Schleswig-Holstein

Prof. Dr. Bernd Lutterbeck
Technische Universität Berlin, Institut für angewandte Informatik

Prof. Dr. Albert von Mutius
Geschäftsführender Vorstand des Lorenz-von-Stein-Instituts für Verwaltungswissenschaften an der Christian-Albrechts-Universität zu Kiel, Vorsitzender des Kuratoriums

Prof. Dr. Andreas Pfitzmann
Technische Universität Dresden, Institut für Theoretische Informatik

Harald Rentsch
Geschäftsführendes Vorstandsmitglied des Städteverbandes Schleswig-Holstein

Karl-Ludwig Schmiing
Geschäftsführer des Städtetages Schleswig-Holstein (bis 1996)

Prof. Dr. Dr. h. c. Spiros Simitis
Forschungsstelle für Datenschutz der Johann Wolfgang Goethe-Universität Frankfurt, ehem. Hessischer Datenschutzbeauftragter

Dr. Otto Ulrich
Bundesamt für Sicherheit in der Informationstechnik, Bonn (ab 1996)

Prof. Dr. Joseph Weizenbaum
Massachusetts Institute of Technology, Cambridge, USA

Nach der Neugliederung der DATENSCHUTZAKADEMIE Schleswig-Holstein hatte auch das Kuratorium seine Funktion erfüllt. Seine Aufgaben wurden teilweise vom neu gebildeten Gemeinsamen Ausschuss der DATENSCHUTZAKADEMIE Schleswig-Holstein übernommen. Den Kuratoriumsmitgliedern wurde für ihr Engagement und ihre Ideen und Anregungen, die maßgeblich zum Aufbau der DATENSCHUTZAKADEMIE Schleswig-Holstein beigetragen haben, gedankt.

Durch die Änderung des Landesdatenschutzgesetzes 2000 hat die DATENSCHUTZAKADEMIE Schleswig-Holstein eine gesteigerte Bedeutung erhalten. Die Vermittlung von Medienkompetenz gehört nunmehr zu den gesetzlichen Aufgaben des Unabhängigen Landeszentrums für Datenschutz. Da sich der Ansatz der DATENSCHUTZAKADEMIE Schleswig-Holstein als dauerhaft erfolgreich herausgestellt hat, war es notwendig geworden, die vertraglichen Grundlagen zu verbessern, zu präzisieren und auf eine längere Dauer hin auszulegen.

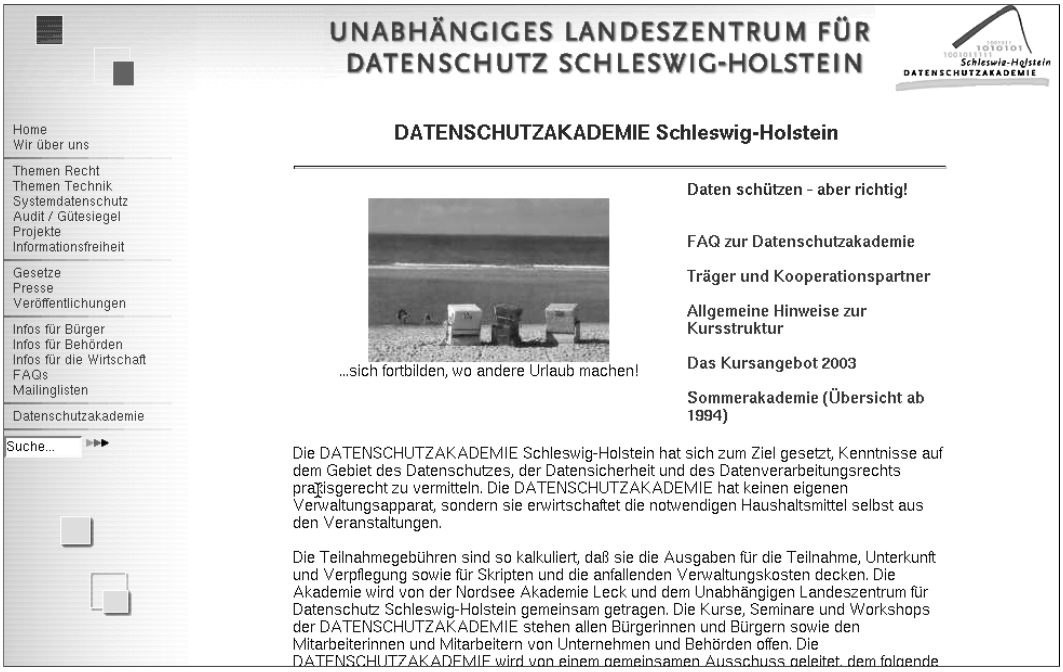
Das Unabhängige Landeszentrum für Datenschutz und der Deutsche Grenzverein entschlossen sich, die Zusammenarbeit auch in Zukunft fortzusetzen, zumal die Nordsee Akademie Leck, eine Einrichtung des Deutschen Grenzvereins, in den letzten Jahren ein deutliches Profil im Bereich der Vermittlung von Medienkompetenz gewonnen hat. Der neue Vertrag sieht eine Präzisierung der Arbeitsteilung zwischen dem Deutschen Grenzverein und dem Unabhängigen Landeszentrum für Datenschutz vor. Über strittige Fragen entscheidet ein Gemeinsamer Ausschuss, der außerdem noch den Wirtschaftsplan beschließt und die Jahresrechnung feststellt.

Der Vertrag wurde am 28. August 2002 in der Nordsee Akademie Leck vom Vorsitzenden des Deutschen Grenzvereins und dem Leiter des Unabhängigen Landeszentrums für Datenschutz in Anwesenheit des geschäftsführenden Vorstandsmitgliedes des Grenzvereins, der Leiterin der Nordsee Akademie Leck, des Vorsitzenden des ehemaligen Kuratoriums der DATENSCHUTZAKADEMIE und des stellvertretenden Datenschutzbeauftragten von Schleswig-Holstein unterzeichnet.

Internet-Präsenz

Unter www.datenschutzzentrum.de/akademie/ veröffentlicht die DATENSCHUTZAKADEMIE Schleswig-Holstein ihr umfangreiches Internet-Angebot. Dort werden neben einer allgemeinen Beschreibung das jeweils aktuelle Fortbildungsprogramm, die Teilnahmebedingungen und das Formular zur Anmeldung bereitgehalten.


www.datenschutzzentrum.de/akademie/



Entwicklung des Kursangebots
Fortbildungskurse der DATENSCHUTZAKADEMIE Schleswig-Holstein

Das Fortbildungsprogramm der DATENSCHUTZAKADEMIE spricht behördliche und betriebliche Datenschutzbeauftragte, Systemadministratoren, Führungskräfte und Mitarbeiter von Verwaltung und Wirtschaft sowie Bürgerinnen und Bürger an. Zu 58 Themen wurden in den letzten Jahren und werden weiterhin reguläre Fortbildungsveranstaltungen im Rahmen des Jahresprogramms der DATENSCHUTZAKADEMIE angeboten:

- Beauftragte für Sozialdatenschutz
- Behördliche Datenschutzbeauftragte nach Landesdatenschutzgesetz 2000
- Bundesdatenschutzgesetz (Aufbaukurs)
- Bundesdatenschutzgesetz (Grundkurs)
- Datenschutz am PC-Arbeitsplatz
- Datenschutz an der Schule
- Datenschutz bei der Internet-Nutzung
- Datenschutz bei der Justiz
- Datenschutz für Bürger
- Datenschutz für den Medizinischen Dienst
- Datenschutz für Kommunalpolitiker
- Datenschutz für Mitarbeiter von Ausländerbehörden (Einführungskurs)
- Datenschutz für Mitarbeiter von Verkehrsbehörden (Einführungskurs)
- Datenschutz im Bauamt
- Datenschutz im Krankenhaus
- Datenschutz im Ordnungsamt
- Datenschutz im Schulsekretariat (Einführung)
- Datenschutz im Sozialamt
- Datenschutz in der Arztpraxis

- Datenschutz in der Umweltverwaltung
- Datenschutz in der Wirtschaft – Schwerpunkte der Datenschutzaufsicht in Schleswig-Holstein
- Datenschutzrecht für behördliche Datenschutzbeauftragte
- Datenschutzverordnung des Landes Schleswig-Holstein
- Datensicherheitsrecht, Prüfung und Bewertung von Sicherheitsmaßnahmen durch behördliche
- Datenverarbeitungsrecht für Führungskräfte der Verwaltung
- E-Government
- Einführung in das Internet
- Einstieg in das Datenschutzrecht
- Entwicklung eines Sicherheitskonzepts für ein Krankenhaus
- Führung von Personalakten
- Informationsfreiheitsgesetz Schleswig-Holstein
- IT-Revision
- Landesdatenschutzrecht Schleswig-Holstein
- Modernisierung der Verwaltung
- Multimedia – Rechte der Nutzer / Pflichten der Anbieter
- Neue Entwicklungen auf dem Gebiet der Datensicherheit im Anschluss an die CeBIT
- Personaldatenverarbeitung im Rahmen des Mitbestimmungsrechts
- Personalrat und Einführung von IT-Systemen
- Prüfung zum Systemadministrator mit Datenschutzzertifikat
- Revisionsfähigkeit der automatisierten Datenverarbeitung
- Safer Surfen im Internet
- Schutz von Personaldaten
- Seminar für Gütesiegel-Sachverständige
- SGB-Änderungsgesetz
- Sozialdatenschutz
- Systemdatenschutz nach Landesdatenschutzgesetz Schleswig-Holstein
- Technik und Recht von Firewalls
- Technischer Datenschutz an Schulen
- Technischer Datenschutz/Systemdatenschutz nach Bundesdatenschutzgesetz
- Verschlüsselung und digitale Signatur
- Windows 2000/2003 Sicherheit
- Windows NT Sicherheit (Grund- und Aufbaukurs)
- Workshop Datenschutz im Schulsekretariat
- Workshop für behördliche Datenschutzbeauftragte
- Workshop für betriebliche Datenschutzbeauftragte
- Workshop für Sozialdatenschutzbeauftragte
- Workshop zur Datensicherheit

Zusätzlich können zu allen datenschutzrelevanten Themen Sonderkurse auch vor Ort durchgeführt werden. Dabei können spezielle Fragestellungen in den Kurs integriert werden.

Kurszahlen und Teilnehmerzahlen 1993-2003

Jahr	reguläre Kurse im Programm der DATENSCHUTZAKADEMIE	Teilnehmer	Sonderkurse vor Ort	Teilnehmer
1993	3	60	--	--
1994	6	116	--	--
1995	22	511	--	--
1996	27	598	6	102
1997	25	508	8	192
1998	23	402	8	240
1999	30	600	21	469
2000	37	577	16	313
2001	52	768	30	536
2002	28	422	15	250
2003	31	413	13	255
Summe	269	4870	112	2183

Gesamtzahl an Kursen: **381**
Gesamtzahl an Teilnehmern: **7053**

Kursunterlagen

Von Anfang an wurden die Kurse der DATENSCHUTZAKADEMIE durch **schriftliche Unterlagen** unterstützt, in denen die Referenten ihre Themen praxisnah darstellen. Nach anfänglicher „Textverarbeitung zu Fuß“ und der Präsentation als Loseblattsammlung wurde das Layout der Kursunterlagen Mitte 1995 umgestellt. Nun präsentieren sich die Kursunterlagen als Nachschlagewerke in gebundener Form mit kompaktem und umfassendem Datenschutzinhalt.

Die Kursunterlagen sind **modular aufgebaut**, sodass für verschiedene Kurse vorhandene und spezielle Module zusammengestellt werden können. Insgesamt sind in der DATENSCHUTZAKADEMIE 205 Datenschutzthemen als Module aufbereitet, von denen 124 Module im Jahr 2003 verwendet wurden. Die Module werden jeweils unmittelbar vor Beginn der Kurse von den Referenten aktualisiert.

Sommerakademie

Jährlich Ende August veranstaltet die DATENSCHUTZAKADEMIE eine Sommerakademie zu einem speziellen Datenschutzthema. Die Sommerakademie hat sich zu einem Kongress von bundesweitem und sogar internationalem Charakter entwickelt. Sie dient neben der Information des ULD über seine Arbeit auch der Diskussion von aktuellen Datenschutzthemen und dem fachlichen Austausch unter den Teilnehmern. Die Sommerakademie wird inzwischen von durchschnittlich 300 Teilnehmern besucht. Die Kosten der Sommerakademie werden aus den Überschüssen der Kurseinnahmen der DATENSCHUTZAKADEMIE bezahlt.

Folgende Themen wurden in den vergangenen Jahren behandelt:

Jahr	Thema
1994	Datenschutz in Europa
1995	Wahrung der Grundrechte in der modernisierten Verwaltung
1996	Datenschutz durch Technik – Technik im Dienste der Grundrechte
1997	Computermedizin und Patientengeheimnis
1998	Der neue Datenschutz – Datenschutz in der Informationsgesellschaft von morgen
1999	Polizei und Datenschutz
2000	E-Privacy – Datenschutz im Internet
2001	Datenschutz als Wettbewerbsvorteil
2002	Unser Recht auf Anonymität
2003	Datenschutz mit Brief und Siegel – Kontrolle ist gut, Vertrauen ist besser

16.2 Jahresprogramm 2004 der DATENSCHUTZAKADEMIE

Das Jahresprogramm 2004 knüpft an das bisherige Kursangebot an und nimmt folgende Kurse im Programm auf:

- Workshop zum Datenschutz im Krankenhaus
- Datenschutz für Inhaltsanbieter im WWW
- Datenschutz in Anwaltskanzleien
- Datenschutz im Sozialamt
- Sozialdatenschutzrecht
- Datenschutz in der Schule
- Technischer Datenschutz an Schulen
- Datenschutz bei der Internet-Nutzung durch Schulen
- Einführung in datenschutzgerechtes Linux
- Datenschutzgerechte Firewalls unter Linux

Veranstaltungsübersicht 2004 für die Kurse der DATENSCHUTZAKADEMIE Schleswig-Holstein			
Januar:	Windows 2000/2003 Sicherheit I	WIN-I 5	27. - 30.01.2004
März:	Datenschutz in der Schule	L 32	09.03.2004
	Informationsfreiheitsgesetz Schleswig-Holstein	IFG 9	16.03.2004
	Behördliche Datenschutzbeauftragte Recht	DR 7	22. - 23.03.2004
	Datensicherheitsrecht, Prüfung und Bewertung von Sicherheitsmaßnahmen durch behördliche Datenschutzbeauftragte	DT 7	24. - 26.03.2004
	Datenschutz am PC-Arbeitsplatz	DPC 5	31.03.2004
	Datenschutz im Krankenhaus	DK 2	24.03.2004

April:	Datenschutz für Inhaltsanbieter im WWW	IP 1	20.04.2004
	IT-Revision	ITR 5	27.04.2004
	Grundkurs Bundesdatenschutzgesetz	BDSG-I 3	28.04.2004
	Technischer Datenschutz/ Systemdatenschutz nach BDSG	SIB 6	29.04.2004
Mai:	Windows 2000/2003 Sicherheit I	WIN-I 6	04. - 07.05.2004
	Datenschutz in der Arztpraxis Grundkurs	AR-I 3	05.05.2004
	Landesdatenschutzrecht Schleswig-Holstein	R 15	05.05.2004
	Systemdatenschutz nach LDSG	T 15	06.05.2004
	Datenschutz in der Arztpraxis Aufbaukurs	AR-II 3	12.05.2004
	Safer Surfen	SURF 3	06.05.2004 13.05.2004
	Einführung Datenschutz im Schulsekretariat	ES 15	12.05.2004
	Datenschutz für Kommunalpolitiker	EK 10	13.05.2004
	Bundesdatenschutzgesetz Aufbaukurs	BDSG-II 3	25.05.2004
	Workshop zum Datenschutz im Krankenhaus	DKW 1	26.05.2004
Juni:	E-Government	EG 2	01.06.2004
	Datenschutz in Anwaltskanzleien	ANW 1	01.06.2004
	Datenschutz im Sozialamt	SOZ 4	02.06.2004
	Einstieg in das Datenschutzrecht	E 16	03.06.2004
	Datenschutz für Bürger	DB 3	03.06.2004 10.06.2004
	Einführung in datenschutzgerechtes Linux	LIN-I 1	08.06.2004
	Schutz von Personaldaten	P 12	09. - 10.06.2004
August:	IT-Revision	ITR 6	17.08.2004
	Grundkurs Bundesdatenschutzgesetz	BDSG-I 4	18.08.2004
	Technischer Datenschutz/ Systemdatenschutz nach BDSG	SIB 7	19.08.2004
September:	Windows 2000/2003 Sicherheit I	WIN-I 6	07. - 10.09.2004
	Datenschutz in der Arztpraxis Gesamtkurs	AR 5	08.09.2004
	Datenschutz in der Schule	L 33	09.09.2003
	Behördliche Datenschutzbeauftragte Recht	DR 8	20. - 21.08.2004
	Datensicherheitsrecht, Prüfung und Bewertung von Sicherheitsmaßnahmen durch behördliche Datenschutzbeauftragte	DT 8	22. - 24.08.2004
	Datenschutz im Krankenhaus	DK 3	21.09.2004
	Bundesdatenschutzgesetz Aufbaukurs	BDSG-II 4	22.09.2004
	Datenschutz am PC-Arbeitsplatz	DPC 6	29.09.2004
Oktober:	Datenschutz bei der Internet-Nutzung	NET 7	05. - 06.10.2004
	Technik und Recht von Firewalls	FW 10	07.10.2004
	Führung von Personalakten	PA 12	25. - 26.10.2004
	Sozialdatenschutzrecht	S 10	26. - 28.10.2004

November:	Safer Surfen	SURF 4	02.11.2004 09.11.2004
	Einführung Datenschutz im Schulsekretariat	ES 16	03.11.2004
	Workshop für behördliche Datenschutzbeauftragte	DW 9	04.11.2004
	Technischer Datenschutz an Schulen	LT 8	04.11.2004
	Workshop für betriebliche Datenschutzbeauftragte	DWBT 3	09.11.2004
	Informationsfreiheitsgesetz Schleswig-Holstein	IFG 10	10.11.2004
	Personaldatenverarbeitung im Rahmen des Mitbestimmungsrechts	PR 8	11.11.2004
	Datenschutz für Bürger	DB 4	18.11.2004 25.11.2004
	Datenschutzgerechte Firewalls unter Linux	LIN-FW 1	23.11.2004
	Datenschutz bei der Internet-Nutzung durch Schulen	L-INT 1	24.11.2004
	Prüfung zum Systemadministrator mit Datenschutzzertifikat	SDZ 2	30.11.2004

16.3 Sommerakademie 2004

Am 30. August 2004 veranstaltet die DATENSCHUTZAKADEMIE in Kiel wieder eine Sommerakademie.

Der Datenschutz der Zukunft
– Informationelle Selbstbestimmung durch Identitätsmanagement –

Viele reden darüber, jeder meint etwas anderes: Identitätsmanagement ist ein Modewort in Industrie und Verwaltung geworden. Für Datenschützer steht Identitätsmanagement im Interesse der Nutzer im Vordergrund. Es beschreibt die Vision, informationelle Selbstbestimmung der Menschen technisch zu gewährleisten oder zumindest zu unterstützen – **Identitätsmanagement als Datenschutz in Nutzerhand**. Bereits jetzt werden die Weichen für „Privacy Next Generation“ gestellt, bei dem das Identitätsmanagement eine wesentliche Rolle spielen wird.

Auf der Sommerakademie 2004 geht es nicht allein um künftige **Perspektiven für den Datenschutz**, sondern um ganz konkrete Schritte, wie man sein Recht auf Datenschutz in der von Technik geprägten Informationsgesellschaft wahrnehmen kann. Experten werden interdisziplinär über die Gestaltung von Identitätsmanagementsystemen im Dienste der Menschen diskutieren: Welche Systeme sind heute auf dem Markt? Was passiert diesbezüglich in den Forschungslaboren von Industrie und Universitäten? Welche Trends erwarten uns? Die Sommerakademie soll Forum für die Initiativen rund um das Identitätsmanagement sowie für Datenschutzpraktiker sein. Die Teilnahme ist kostenlos.


www.datenschutzzentrum.de/somak/somak04/somak04.htm

Wenn Sie gern eine Einladung zu dieser Veranstaltung haben möchten und noch nicht in unserem Versandverteiler sind, können Sie sich gern vormerken lassen unter:

DATENSCHUTZAKADEMIE Schleswig-Holstein
beim Unabhängigen Landeszentrum für Datenschutz
Tel: 0431/988-1209 oder -1210, Fax: 0431/988-1223
E-Mail: akademie@datenschutzzentrum.de

16.4 Datenschutzzertifikate für Systemadministratoren

Im Verlaufe des 10-jährigen Bestehens der DATENSCHUTZAKADEMIE Schleswig-Holstein ist das Angebot stets den entsprechenden Bedürfnissen der Kunden (den Behörden) im Lande erweitert worden. So veränderten sich die Schwerpunkte der Kurse, in denen rechtliches Wissen vermittelt wird, vom allgemeinen Datenschutz hin zu bereichsspezifischen Fragestellungen.

Im sicherheitstechnischen Bereich war es neben der Berücksichtigung immer neuerer Betriebssysteme erforderlich, mehr und mehr von der reinen Theorievermittlung auf ein Praxistraining in IT-Labors umzuschwenken. Dies wird nunmehr seit vier Jahren erfolgreich durchgeführt. In der Nordsee Akademie Leck und in unserer Dienststelle in Kiel stehen für diesen Zweck unterschiedlich konfigurierbare Lehrsysteme zur Verfügung.

Der logisch nächste Schritt bestand in dem Angebot, dass sich die Teilnehmer an Kursen der DATENSCHUTZAKADEMIE ihren Wissensstand nach einer entsprechenden Prüfung zertifizieren lassen können.

Zur Erlangung des Zertifikats müssen sie Kenntnisse in folgenden Bereichen nachweisen:

- Grundkenntnisse im Datenschutzrecht (LDSG und DSVO), z. B. über Systemdatenschutz bzw. Datensicherheit, Dokumentation automatisierter Verfahren, Überwachung des ordnungsgemäßen Einsatzes der Hard- und Software,
- Kenntnisse im Bereich der technischen Umsetzung von Sicherheitsmaßnahmen, z. B. sichere Administration von Windows 2000-Betriebssystemen (Gruppenrichtlinien, Benutzerprofile, NTFS- und Freigaberecht, Verschlüsselung, Überwachungsrichtlinien, Passwortrichtlinien, Sicherheitskonfiguration und -analyse, Datensicherung und -wiederherstellung), Systemdokumentation,
- Kenntnisse im Bereich der IT-Revision, z. B. methodische Vorgehensweise bei der IT-Revision, Aufbau und Begutachtung von IT- und Sicherheitskonzepten, Einsatz von technischen Revisionswerkzeugen,
- Kenntnisse in Bezug auf eine datenschutzgerechte Anbindung an das Internet, z. B. konzeptionelle Umsetzung, Problematik beim Einsatz der Internet-Dienste E-Mail und WWW, mögliche Sicherheitsmaßnahmen und Schwachstellen.

Kurse
DT, WIN-I,
ITR, FW, T

Als Vorbereitung auf die Prüfung empfehlen wir die Teilnahme an den Kursen T oder DT oder WIN-I, ITR und FW. In diesen Kursen werden alle prüfungsrelevanten Themen behandelt. Die Prüfung gliedert sich in eine theoretische und eine praktische Einheit und wird an einem Tag abgenommen und bewertet.

Die ersten Zertifikate sind im November 2003 an Systemadministratoren übergeben worden. Das Niveau der Prüfung ist als durchaus anspruchsvoll zu bezeichnen, denn die Behördenleitungen müssen sich darauf verlassen können, dass der Aufwand für die Schulung und Zertifizierung ihrer Mitarbeiter durch eine entsprechende Qualifikation gerechtfertigt ist.

www.datenschutzzentrum.de/akademie/programm/info_sdz.htm

Beim **ULD SH** erhältliche Publikationen:

Neues Datenschutzrecht in Schleswig-Holstein
Text des Landesdatenschutzgesetzes, der Datenschutzverordnung, des Informationsfreiheitsgesetzes, der Regelungen zum Datenschutz-Audit und Datenschutz-Gütesiegel und des Bundesdatenschutzgesetzes

Tätigkeitsbericht
des letzten Jahres als Landtagsdrucksache

Faltblätter
Datenschutz ist auch nicht mehr das, was es einmal war
(Dienstleistungsangebot des ULD)
Safer Surfen!:
Clever verschlüsselt mailen, Selbst sicher(n)!, Ich bin drin! ... Und meine Daten?, Sicherheit durch Anonymität im Internet, P3P – ich hab's gecheckt und den Rest macht mein PC
Ihre Daten sind auch bei der Polizei geschützt
Patientenfaltblatt „Datenschutz in meiner Arztpraxis"
Virtuelles Datenschutzbüro – Virtual Privacy Office
Das Informationsfreiheitsgesetz Schleswig-Holstein
Broschüre und Faltblätter zum Datenschutz-Audit und Datenschutz-Gütesiegel

Broschüren
99 +1 Beispiel zum Schutz Ihrer Daten nach dem Bundesdatenschutzgesetz
Datenschutztagebuch – Datenschutz im Alltag für jedermann
Sicherheit durch Anonymität im Internet (Hintergründe zum Projekt AN.ON)
backUP-Magazine 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, Virtuelles Datenschutzbüro,
Aufkleber zum Thema E-Mail-Verschlüsselung, Rote Karte für Internet-Schnüffler

---

DATENSCHUTZAKADEMIE Schleswig-Holstein
Jahresprogramm 2004

Schleswig-holsteinische Datenschutzinformationen im Internet
Alle Datenschutzinformationen aus Schleswig-Holstein finden Sie natürlich auch auf der Homepage des ULD unter: **http://www.datenschutzzentrum.de**. Auf der umfangreichen Website finden Sie neben den Publikationen des Unabhängigen Landeszentrums für Datenschutz weitere umfangreiche Informationen zum Thema Datenschutz und das Fortbildungsangebot der DATENSCHUTZAKADEMIE Schleswig-Holstein. Weiterhin ist dort der öffentliche Schlüssel des Unabhängigen Landeszentrums für Datenschutz zur Verschlüsselung von E-Mails an das ULD 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 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