Tätigkeitsbericht 2005

des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

Berichtszeitraum: 2004, Redaktionsschluss: 01.03.2005
Landtagsdrucksache 16/50

(27. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz)

Dr. Thilo Weichert
Leiter des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein, Kiel

Inhaltsverzeichnis **Seite**

1 Situation des Datenschutzes in Schleswig-Holstein – zwischen Konsolidierung und Aufbruch

Das Unabhängige Landeszentrum für Datenschutz (ULD) befindet sich in einer spannenden Situation: Angesichts bedeutender personeller Veränderungen wäre dringend eine Konsolidierung der bisherigen Arbeit notwendig. Zugleich aber wird das ULD mit immer **neuen Herausforderungen** konfrontiert, die angenommen werden müssen, wenn der Datenschutz keinen Schaden nehmen soll.

Die gravierendste personelle Veränderung ist die Verabschiedung von Dr. Helmut Bäumler in den Ruhestand. Nach zwei Wahlperioden konnte er nicht wiedergewählt werden. Mit seinem Weggang verliert das Land Schleswig-Holstein einen seiner innovativsten Beamten, der den Datenschutz für das Land zu einem Markenzeichen und einem Standortvorteil gestaltet hat. Die DATENSCHUTZAKADEMIE, das ULD als Anstalt des öffentlichen Rechts und Dienstleistungszentrum, das Datenschutz-Gütesiegel und das Datenschutz-Audit sowie das Innovationszentrum ULD-i sind einige wichtige von vielen Innovationen, für die Dr. Helmut Bäumler verantwortlich ist. In den 15 Jahren seiner Tätigkeit als Datenschützer in Kiel, davon 12 als Landesbeauftragter, hat er sich weit über die Grenzen des Landes hinaus einen Namen gemacht. Und dieser gute Name war immer mit dem Datenschutz in Schleswig-Holstein verknüpft. Daher, aber auch wegen seiner angenehmen und sachlichen Art im Umgang mit Freunden, Partnern und auch Gegenspielern in Datenschutzkonflikten, fiel Ende August 2004 den zahlreichen Gästen bei der Amtsübergabe der Abschied sichtlich schwer, so unabwendbar dieser Abschied auch war. Freunde von Dr. Helmut Bäumler haben ihm als ein Zeichen des Dankes ein Buch als Freundesgabe gewidmet, das beim ULD bestellt werden kann:

Innovativer Datenschutz 1992-2004 – Wünsche, Wege, Wirklichkeit – für Helmut Bäumler, Kiel 2004, 367 S.

Der Fortgang des bisherigen Leiters war nicht der einzige **personelle Aderlass** für das ULD. Es gab weitere Veränderungen. Viele Kolleginnen und Kollegen verließen – teilweise nur vorübergehend – die Dienststelle, weil ihnen wegen ihrer erfolgreichen Tätigkeit beim ULD attraktivere Angebote unterbreitet wurden. Sie arbeiten heute z. B. als Referentin in einem Bundesministerium, als Richterin im Verwaltungsgericht, als wissenschaftlicher Mitarbeiter beim Bundesverfassungsgericht, bei einer anderen Datenschutzdienststelle, beim Landeskriminalamt, als Datenschutzkoordinator der Europäischen Union in Litauen oder als Manager bei einem großen EDV-Dienstleister im Land.

Angesichts dieser Fluktuation ist die **Konsolidierung** der Arbeit eine zentrale Aufgabe für die ULD-Führung. Eine gute Grundlage hierfür ist, dass der bisherige langjährige Stellvertreter des Landesbeauftragten die Leitungsposition übernommen hat und an dessen bisherige Stelle mit Johann Bizer ein Datenschützer nachgerückt ist, der sich in Wissenschaft, Wirtschaft und Verwaltung bundesweit einen

Namen gemacht hat. Das altbewährte Team und neue Mitarbeiterinnen und Mitarbeiter tun alles dafür, dass die personellen Veränderungen zu keinen Qualitätseinbußen führen.

Die **Rahmenbedingungen** für einen guten Datenschutz in Schleswig-Holstein sind gegeben: Der Landtag unterstützt das Anliegen des ULD. Mit den Ministerien findet eine enge, partnerschaftliche Zusammenarbeit statt. Die Behörden, insbesondere auch die Kommunen, haben erkannt, dass Datenschutz und Datensicherheit Qualitätsmerkmale einer guten Verwaltung sind. Und die Wirtschaft begegnet dem ULD in den meisten Fällen nicht mit Misstrauen und Abwehr, sondern mit Interesse. Dieses Interesse beruht auf der Erkenntnis, dass aus der Not, die Datenschutzgesetze beachten zu müssen, eine Tugend gemacht werden kann, die sich gegenüber Kunden und Beschäftigten bezahlt macht – durch Kundenvertrauen und zufriedene Mitarbeiter. Natürlich herrscht bei der Tätigkeit als Datenschutzaufsicht für das ULD nicht immer eitel Sonnenschein. Angesichts von Interessenkonflikten, aber auch wenn die Einsicht in den Sinn des Grundrechts auf informationelle Selbstbestimmung fehlt, müssen Kontroversen offen ausgetragen werden. Dies war im letzten Jahr aber die Ausnahme und nicht die Regel.

Das ULD kann sich aber keine ruhige Phase leisten. Die Gründe hierfür liegen zum einen in bundesweiten, europäischen, ja teilweise globalen politischen Entwicklungen (Tz. 2). Sie liegen aber auch im **technischen Fortschritt**, der eine Datenschutzkontrollinstanz dauernd zu neuen Anstrengungen zwingt: Telekommunikationsüberwachung, Digital Rights Management, Radio Frequency Identification, Identitätsmanagement – jeder dieser Begriffe steht für technisch und rechtlich noch nicht gelöste Aufgaben zur Wahrung der Privatsphäre.

Mit dem neu geschaffenen Innovationszentrum ULD-i verfügen wir über ein Instrument, um durch Beratung datenschutzfreundliche Innovationen zu fördern. Im Vordergrund steht nicht die Änderung von Gesetzen, sondern die **Gestaltung technisch-organisatorischer Lösungen**, um grundrechtsfreundliche Antworten auf die neuen Gefahren zu finden. Wir sorgen uns außerdem darum, dass diese Lösungen nicht in Gutachten, Projektberichten und Doktorarbeiten vergilben, sondern dass sie in die IT-Produkte von morgen Eingang finden. Deshalb bekommen die Instrumente des Datenschutz-Gütesiegels und des Datenschutz-Audits als Ausweis von Qualität in Zukunft eine noch stärkere Bedeutung.

Bisher konnte sich das ULD einer Herausforderung nur eingeschränkt widmen: der Kontrolle des Einsatzes der **Informationstechnik in der Wirtschaft**. Für die Datenschutzaufsicht in den Unternehmen im Land ist das ULD seit dem Jahr 2000 verantwortlich. Doch es zeigt sich, dass seine Reaktionsmöglichkeiten zum Schutz der Persönlichkeitsrechte auf technische und organisatorische Neuerungen in den Unternehmen unzureichend bleiben. Die Einführung von Data Warehouses, großen „Warenhäusern“ voller Kundendaten, von Data-Mining-Auswertungswerkzeugen, von Menschen bewertenden Scoringverfahren, von Skilldatenbanken über Arbeitnehmer, von Überwachungstechnik in vielen Betrieben macht es uns angesichts unserer begrenzten personellen Kapazitäten fast unmöglich, auch nur ansatzweise adäquat zu reagieren. Dabei ist die Situation in Schleswig-Holstein

nicht schlechter als andernorts. Es muss generell konstatiert werden, dass das Vollzugsdefizit beim Datenschutz in der Wirtschaft von vielen als Dauernormalzustand hingenommen wird. Dies kann nicht das letzte Wort in einer Informationsgesellschaft sein, die den Anspruch verfolgt, dass Technik vorrangig dem Menschen dienen soll und daher freiheitsfördernd, nicht freiheitsbeschränkend, demokratisch und nicht manipulierend, rechtswahrend und nicht rechtsgefährdend wirken muss.

2 Datenschutz in Deutschland

Die positive **Bilanz** für den Datenschutz in Schleswig-Holstein lässt sich leider nicht auf Gesamtdeutschland übertragen. In vielen Ländern, aber auch im Bund sind die Weichen zwar in Richtung Informationsgesellschaft gestellt, doch wird dabei dem Datenschutz oft nur ein zu geringer Stellenwert beigemessen. Diese Entwicklung ist fatal, weil die Gestaltung der Informationsgesellschaft auf die Akzeptanz der Bürgerinnen und Bürger angewiesen ist. Ohne die informationelle Selbstbestimmung gibt es keine Handlungsfreiheit, und ohne diese gerät die Entwicklungsdynamik der privaten, geschäftlichen, aber auch der sozialen und politischen Kommunikation ins Stocken. Wer die Zukunft von Wirtschaft, Verwaltung und Gesellschaft in der Entwicklung einer zivilen Informationsgesellschaft sieht, ist gut beraten, den Datenschutz als einen zentralen Konstruktionspfeiler zu beachten und zu fördern.

Insbesondere auf Bundesebene ist eine **Überwachungsneigung** festzustellen, die aus Grundrechtssicht beängstigend ist. Kaum ein Ressort zeichnet sich durch ein ausgeprägtes Datenschutzbewusstsein aus, schon gar nicht das für Verfassungsfragen und für den Datenschutz allgemein zuständige Bundesinnenministerium. Es scheint weniger böser Wille als mangelndes Problembewusstsein zu sein, dass in den Ministerien informationstechnische Blütenträume wachsen und gedeihen, bei denen die Grundrechte zu kurz kommen. Diese Träume auf den Boden unseres Grundgesetzes zu vererden ist die Aufgabe der Datenschutzbeauftragten des Bundes und der Länder. Unterstützung erhalten sie von Fall zu Fall durch das Bundesverfassungsgericht und die öffentlichen Medien.

2.1 Das Lauschurteil des Bundesverfassungsgerichts

Das am 15. Dezember 1983 am Vorabend des Orwell-Jahres 1984 gefällte Volkszählungsurteil des Bundesverfassungsgerichts hat die Bedeutung einer Bergpredigt des Datenschutzes gewonnen. In vielen weiteren Entscheidungen hat das höchste deutsche Gericht inzwischen den Schutz des Grundrechts auf informationelle Selbstbestimmung konkretisiert und vertieft. Immer wieder hat es der Politik bescheinigt, dass die von ihr verabschiedeten Überwachungsgesetze über das hinausgehen, was unser Grundgesetz erlaubt. Am 3. März 2004 fällte das Bundesverfassungsgericht zwei weitere grundlegende Entscheidungen, in denen es gravierend in die informationellen Freiheitsrechte eingreifende Gesetze aufhob und fundamentale Aussagen zu den Verfassungsanforderungen an präventive Telekommunikationsüberwachung sowie zum heimlichen Belauschen des privaten Wohnraums traf.

Insbesondere das so genannte **Lauschurteil** lässt die Herzen der Verteidiger unserer bürgerrechtlichen Freiheiten höher schlagen: Es stellt fest, dass die private Wohnung zur Schutzsphäre des grundsätzlich unantastbaren Kernbereichs privater Lebensgestaltung gehört und als „letztes Refugium“ zur Wahrung der Menschenwürde fungiert. Der Schutz dieses Kernbereichs darf nicht mit Argumenten zur „Effektivität der Strafrechtspflege“ relativiert werden. Zum Höchstpersönlichen

gehören die Familie und die Sexualität, aber auch Gespräche mit Pastoren, Ärzten und Rechtsanwälten, zu denen aus beruflichen Gründen ein besonderes Vertrauensverhältnis besteht. Ebenso wie das Volkszählungsurteil beschränkt sich das Lauschurteil nicht auf grundsätzliche Erwägungen, sondern konkretisiert den Grundrechtsschutz durch Anforderungen an die Rechtskontrolle durch unabhängige Richter, an Löschfristen, an Evaluierungspflichten, an Beweisverwertungsverbote, an die Befristung von Maßnahmen sowie an Kennzeichnungs- und nachträgliche Benachrichtigungspflichten (Tz. 4.3.1).

Verblüffend war die geringe Überzeugungskraft, die dieses Urteil bei vielen Verantwortlichen entfaltete. Als kurz nach dem Urteil in Madrid ein schrecklicher terroristischer Anschlag verübt worden war, standen auf der politischen Agenda Überwachungsmaßnahmen, die offensichtlich nicht mit den Ausführungen zum Lauschurteil in Einklang zu bringen waren, sei es der Spähangriff in Wohnungen, die Vorratsspeicherung von Telekommunikationsverkehrsdaten oder die Zulassung weiterer geheimer Vorfeldermittlungsmaßnahmen. Häufig wurde gar nicht erst versucht, sich mit den Argumenten des Bundesverfassungsgerichtes auseinander zu setzen. Vielmehr wurden diese ignoriert; die Freiheitsrechte wurden einer **einfachen Sicherheitsdogmatik** unterworfen. Dass bislang nur wenige Forderungen im Namen der Sicherheit umgesetzt wurden, ist vielen Menschen in unserer Gesellschaft zu verdanken, die die Messlatte der Verfassung als Maßstab ihres politischen Handelns begreifen.

2.2 Die Neigung zur Vorratsdatenverarbeitung

Verfassungsrechtliche Vorgaben gelten nicht nur für geheime Ermittlungsmaßnahmen der Sicherheitsbehörden, sondern für jede Form staatlicher Datenverarbeitung. Das abgelaufene Jahr wurde durch einen besonderen Trend gekennzeichnet: die Neigung zur Vorratsdatenverarbeitung. Im Volkszählungsurteil hat das Bundesverfassungsgericht die Vorratsdatenverarbeitung **zu unbestimmten Zwecken** als verfassungswidrig verworfen. Dabei handelt es sich um eine Umsetzung des Erforderlichkeitsgrundsatzes für komplexe Gesamtverfahren. Mit dem Verbot der Sammlung auf Vorrat soll verhindert werden, dass Daten „einfach darauf los“, „ins Blaue hinein“ oder „für alle Fälle“ gespeichert werden.

Im Wortlaut:
Verbot der Vorratsdatenspeicherung

„Ein Zwang zur Angabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren. Auch werden sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken müssen.“ (BVerfGE 65, 46)

Es gilt – wie in anderen Bereichen auch – der Grundsatz der **Datensparsamkeit**. Dieser scheint bei manchem Projekt der Bundesregierung in Vergessenheit geraten zu sein. Dies zeigt die Datenerhebung sämtlicher Kfz-Kennzeichen im Rahmen der Erhebung der Autobahnmaut (Tz. 4.5.1) oder der Zugriff von Finanzbehörden auf sämtliche Kontostammdaten bei Banken (Tz. 4.9). Aber nicht nur im Verkehrs- und im Finanzressort werden akribisch umfassende Datensammlungen zwecks späterer Selektion im eventuellen Bedarfsfall angelegt. Auch in anderen Bereichen und auf anderen Ebenen findet diese Idee Anhänger.

Ein klassisches Beispiel für eine verfassungswidrige Vorratsdatenspeicherung ist die **Speicherung von Telekommunikationsdaten** für andere als Kommunikationszwecke. Es gab und gibt keinen vernünftigen Grund die Anbieter zu verpflichten, beim Verkauf von Prepaid-Handys die Identifikationsdaten der Kunden zu erfassen, nur auf den vagen Verdacht hin, die Angaben könnten künftig für Zwecke einer heimlichen Telefonüberwachung durch Sicherheitsbehörden von Nutzen sein (25. TB, Tz. 8.4). Nicht erfolgreich war der Versuch, sämtliche Telekommunikationsanbieter zu verpflichten, langfristig die Verkehrsdaten sämtlicher Kommunikationsverbindungen zu speichern (25. TB, Tz. 8.5; 26. TB, Tz. 7.1). Nachdem die Befürworter gegen die verfassungsrechtlichen Argumente auf nationaler Ebene nicht durchgedrungen sind, haben sie allerdings auf die europäische Karte gesetzt. Der EU-Ministerrat versucht nun schon in mehreren Anläufen, Provider für Internet und für sonstige Telekommunikation zu einer ein- bis dreijährigen Vorratsspeicherung sämtlicher Verbindungs- und Standortdaten zu verpflichten. Doch auch diese Initiativen stoßen auf Widerstand, nicht nur bei Datenschützern und Bürgerrechtlern. Nationale Parlamente wie der Deutsche Bundestag, das Europäische Parlament und die EU-Kommission widersetzten sich bisher hartnäckig und erfolgreich den Bestrebungen aus dem Ministerrat.

2.3 Das JobCard-Verfahren – der zentrale Einkommensdatenpool

Mit dem JobCard-Verfahren sollen in einer zentralen Speicherstelle alle Arbeits- und Einkommensdaten der gesamten abhängig beschäftigten Bevölkerung in Deutschland gespeichert werden.

Erklärter Zweck des Verfahrens ist die Entlastung der Arbeitgeber von der **Ausstellung von Entgeltbescheinigungen**, die man Sozialleistungsträgern z. B. bei der Beantragung von Arbeitslosengeld, Wohngeld, Kindergeld oder BAföG vorlegen muss. Alle öffentlichen und privaten Arbeitgeber sollen zu diesem Zweck monatlich sämtliche relevanten Einkommensdaten elektronisch an eine Speicherstelle (ZSS) schicken, in der sie dann für die Sozialleistungsträger zum Abruf bereitstehen. Die Mitarbeiter der Sozialbehörden sollen zum Abruf der Daten nur befugt sein, wenn die Antragsteller ihre Erlaubnis gegeben haben. Hierzu sollen alle abhängig Beschäftigten eine signaturgesetzkonforme Chipkarte, die so genannte JobCard, erhalten. Das Verfahren wird derzeit – noch nicht im Realbetrieb – mit einigen Arbeitgebern und Sozialbehörden erprobt.

Als die Landesbeauftragten zum ersten Mal über dieses Verfahren informiert wurden, waren die wesentlichen technischen Modalitäten schon festgelegt. Alle Forderungen nach grundlegenden Verfahrensänderungen zur Wahrung der informationellen Selbstbestimmung wurden von den für die Projektdurchführung Verantwortlichen bisher zurückgewiesen. Unsere zentrale Forderung besteht darin, dass die Einkommensdaten der Beschäftigten mit deren öffentlichem Schlüssel direkt bei den Arbeitgebern verschlüsselt und so an die ZSS zur Speicherung versandt werden. Auf diese Weise könnten die Daten ausschließlich mit dem privaten Schlüssel der Betroffenen entschlüsselt und genutzt werden, wenn diese ihn den jeweiligen Sozialbehörden für den Abruf der Daten zur Verfügung stellen. Durch diese **Ende-zu-Ende-Verschlüsselung** hätten ausschließlich die Betroffenen selbst die Verfügungsbefugnis über ihre eigenen Daten.

Nach dem bisherigen Konzept soll die Verfügungsgewalt über diesen sensiblen Datenpool bei der ZSS liegen. Damit stehen die zentral elektronisch gespeicherten Daten grundsätzlich auch für sonstige Zwecke zur Verfügung. Zwar hat offiziell bisher niemand bestätigt, dass Nutzungen zu anderen Zwecken geplant sind, doch wurde von den dafür zuständigen Stellen bereits öffentlich darüber nachgedacht, die zwangsweise bei den Arbeitgebern erhobenen Daten z. B. zur Bekämpfung der Schwarzarbeit zu verwenden. Selbstverständlich wäre der Datenpool auch von größtem Interesse für die Finanzbehörden, die Polizei, die Staatsanwaltschaften und viele andere „Bedarfsträger“. Es genügt eine kleine Gesetzesänderung, um deren Zugriff zu ermöglichen. Das Resultat wäre der „**gläserne Arbeitnehmer**“. Die Arbeits- und Kostenentlastung der Unternehmen mag ein wichtiges Ziel sein. Es auf einem datenschutzfreundlichen Weg zu erreichen sollte eine Selbstverständlichkeit sein. Stattdessen ist geplant, nicht nur die Arbeitsentgelte zu speichern, sondern auch Entgeltersatzzahlungen wie z. B. Kranken- oder Arbeitslosengeld.

Bisher wurden vom Bundeswirtschaftsministerium trotz entsprechender Aufforderung durch die Datenschutzbeauftragten keine Zahlen vorgelegt, in welchem Umfang die Daten zur Ausstellung von Bescheinigungen wirklich benötigt werden. Es hat z. B. keinen Sinn, kindergeldrelevante Daten von kinderlosen Arbeitnehmern zu sammeln. Tatsächlich dürften weit über 90 % der monatlich neu angehäuften Daten nie genutzt werden. Für die Entwicklung der gewaltigen Infrastruktur der Einkommensüberwachung wurden schon große öffentliche Ausgaben getätigt, ohne dass die Vereinbarkeit mit der Verfassung von neutraler Stelle geprüft worden wäre. Tatsächlich handelt es sich bei dem JobCard-Verfahren um eine **verfassungswidrige Vorratsdatenspeicherung** mit einem gewaltigen Missbrauchsrisiko. Eine gesetzliche Grundlage für das Verfahren gibt es bisher nicht. Auch eine öffentliche parlamentarische Debatte hierüber wurde bislang nicht geführt.

Es drängt sich der Eindruck auf, als verfolge man mit dem JobCard-Verfahren noch andere Zwecke als die Entlastung der Arbeitgeber beim Ausstellen von Bescheinigungen. Wir wollen nicht unterstellen, dass die damit ermöglichte Einkommenskontrolle das wahre Motiv für die Durchsetzung dieses Verfahrens ist. Sicherlich brächte das Verfahren für die IT-Wirtschaft große Aufträge – finanziert aus Steuermitteln. Wahrscheinlich verspricht man sich durch die

flächendeckende Ausgabe von digitalen Signaturkarten den Durchbruch dieser Technologie auf dem Massenmarkt. Aber selbst für diese **wirtschaftlichen Nebeneffekte** wurden bisher keine aussagekräftigen Untersuchungen vorgelegt.

Was ist zu tun?
Das JobCard-Verfahren sollte ad acta gelegt werden. Alternativ muss eine technisch-organisatorische Lösung realisiert werden, bei der die Betroffenen die ausschließliche Verfügung über ihre Arbeits- und Einkommensdaten behalten.

3 Datenschutz im Landtag

3.1 Zutrittsberechtigungssystem im Schleswig-Holsteinischen Landtag

Für ein datenschutzgerechtes Zutrittsberechtigungssystem wurde der Schleswig-Holsteinische Landtag mit einem Datenschutz-Audit ausgezeichnet.

Mit den Plänen für ein chipkartenbasiertes Zutrittsberechtigungssystem im Gebäude des Landeshauses und im Bürogebäude des Landtags im Karolinenweg hat sich die Landtagsverwaltung auf politisches Glatteis begeben: Die Einrichtung von gesicherten Türen, die nur mit individuellen Chipkarten geöffnet werden können, ermöglicht es, detaillierte **Bewegungsprofile** über die Karteninhaber zu erstellen. Es könnte also festgestellt werden, welche Journalisten, Abgeordneten oder auch Bürgerinnen und Bürger sich zu welcher Zeit in welchem Teil des Gebäudes aufgehalten, z. B. auch welche Politiker sich wann mit welchen Personen getroffen haben.

Eine solche Kontrollmöglichkeit wollte der Landtag in jedem Fall verhindern, ohne aber auf den Sicherheitsgewinn einer elektronischen Zutrittskontrolle zu verzichten. Ein entsprechendes Sicherheitskonzept wurde auf Initiative des Datenschutzgremiums des Schleswig-Holsteinischen Landtags im Auftrag der für die Baumaßnahmen verantwortlichen Gebäudemanagement Schleswig-Holstein (GMSH) durch uns einem förmlichen **Audit** unterzogen. Dabei stellten wir fest, dass das Zutrittsberechtigungssystem den Anforderungen an Datenschutz und Datensicherheit genügt.

Zutritt zum Landeshaus, zum Bürogebäude Karolinenweg sowie zu den durch elektronisch schließbare Türen gesicherten Bereichen innerhalb der Gebäude erhält grundsätzlich nur der, der sich mit einer besonderen Transponder-Chipkarte als Berechtigter ausweist. Die beim Einsatz der Chipkarten anfallenden Nutzungsdaten werden nicht gespeichert, sodass im Nachhinein nicht nachvollziehbar ist, welche Person zu welchem Zeitpunkt welche Räumlichkeiten betreten hat. Die Chipkarte wird lediglich dazu verwendet, die **Berechtigung einer Person zu überprüfen** und daraufhin den Zutritt zu gewähren oder zu verweigern.

Von diesem Prinzip wird aus Sicherheitsgründen lediglich eine Ausnahme für die **IT-Server-Räume** des Landtags gemacht. Zur Gewährleistung der Sicherheit der sensiblen Daten von Landtag und Fraktionen werden dort alle gewährten und abgewiesenen Zutritte für die Dauer von einem Monat protokolliert.

Durch die Einrichtung eines **Datenschutzmanagementsystems** trägt die Landtagsverwaltung dafür Sorge, dass das definierte Datenschutzniveau auch in Zukunft eingehalten wird. Für die Funktionsfähigkeit eines demokratischen Parlamentsbetriebs ist es unabdingbar, dass Politiker und Bürger unbeobachtet sich treffen und austauschen können. Das Datenschutz-Audit zeigt, dass Sicherheit und Datenschutz kein Widerspruch sein müssen.

Das Kurzgutachten zum Datenschutz-Audit ist abrufbar unter

www.datenschutzzentrum.de/audit/

Was ist zu tun?
Das auditierte Konzept zur Regelung der Zutrittsberechtigungen im Landtag kann als Vorbild und Prüfmuster für ähnliche Systeme genutzt werden.

3.2 Die nicht ganz ungefährliche Petition

Wenn Petenten sich an den Landtag wenden, dürfen sie deswegen keine Nachteile erleiden. Doch ist es nötig, zur Aufklärung des Sachverhaltes Stellungnahmen einzuholen. Dabei muss sich die Verwaltung auf die relevanten Sachverhaltsfragen beschränken.

Der Petitionsausschuss des Landtags informierte uns über eine Eingabe einer Lehrerin und bat uns eine Datenweitergabe zwischen dem Kultusministerium und einer Schule zu bewerten: Die Lehrerin hatte sich mit dem **Vorwurf des Mobbings** an ihrer Schule an den Ausschuss gewandt, der das Ministerium zur Stellungnahme aufforderte. Da dieses hierfür eine Darstellung der Schule benötigte, kopierte das Ministerium die Petition und gab sie an die Schulleitung weiter. Die Darstellung der Petentin enthielt subjektive Vorwürfe wegen sexueller Belästigung und gesundheitsgefährdenden Verhaltens sowie einen **ärztlichen Befundbericht**. Umgehend erhielt der Petitionsausschuss ein Schreiben des Anwaltes des Schulleiters, in dem dieser strafrechtliche Schritte gegen die Petentin wegen beleidigender Falschbehauptungen androhte.

Der Petitionsausschuss beanstandete, dass das Kultusministerium die Weitergabe der Petitionsunterlagen an die Schule nicht auf die zur Stellungnahme erforderlichen Unterlagen beschränkt hatte. Wir haben dem Ausschuss beigepflichtet: Ohne den ärztlichen Befundbericht konnte das Ministerium die Petition nicht beurteilen, nicht erforderlich aber war seine Weitergabe an den Schulleiter. Diese Übermittlung war somit unzulässig. Aus dem verfassungsmäßigen Recht, sich an den Landtag wenden zu können, ist auch der Anspruch abzuleiten, wegen der Inanspruchnahme dieses Rechtes **keine Nachteile** zu erleiden. Daher muss das zur Stellungnahme aufgeforderte Ministerium prüfen, ob durch die Weitergabe von Informationen aus der Petition schutzwürdige Interessen des Petenten verletzt werden. Nicht sachdienliche Ausführungen eines Petenten dürfen nicht weitergegeben werden. Doch geht die Fürsorge gegenüber Petenten nicht so weit, dass in einer Eingabe ungeprüft Falschbehauptungen übernommen werden müssten oder dürften.

Hinsichtlich der Weitergabe der Kopie der Eingabe meinte das Ministerium, im Interesse der **Wahrung der Rechte seiner Beschäftigten** korrekt gehandelt zu haben. Angesichts der schwer wiegenden Vorwürfe gegen die Schulleitung habe diese auch die subjektiven Bewertungen der Petentin kennen dürfen, um angemessene Möglichkeiten zur Äußerung und zur Gegendarstellung zu haben. Künftig

wolle man aber verstärkt bei der Weitergabe von Petitionen eine Erforderlichkeits- und Angemessenheitsprüfung durchführen.

Was ist zu tun?
Vor der Weitergabe der Kopie einer Landtagspetition vom zuständigen Ministerium an den nachgeordneten Bereich muss eine Erforderlichkeits- und Angemessenheitsprüfung durchgeführt werden. Im Zweifelsfall sollte der Petent darüber informiert werden, dass Dritte zum Zweck der Bearbeitung über seine Eingabe informiert werden müssen. Vor der Weitergabe ist der Betroffene um seine Einwilligung zu bitten.

4 Datenschutz in der Verwaltung

4.1 Kommunalbereich

4.1.1 Neues Landesmeldegesetz in Kraft

Im Juni 2004 trat im Land ein neues Melderecht in Kraft. Dieses bringt für Bürgerinnen und Bürger sowie für die Verwaltungen spürbare Veränderungen mit sich, die eine umfassende Aufklärung erfordern.

Die Änderungen des Landesmeldegesetzes werden zum großen Teil durch das Melderechtsrahmengesetz des Bundes vorgegeben, das manchen Vorstellungen von einem bürgerfreundlichen Melderecht nicht entspricht. Doch können folgende Verbesserungen für **Bürgerfreundlichkeit**, **Datensicherheit** und **Datensparsamkeit** verbucht werden:

- Bei Umzügen im Inland ist die Pflicht zur Abmeldung entfallen.
- Meldebehörden dürfen künftig bei der Anmeldung die Daten der Betroffenen online bei der Wegzugsbehörde abrufen. In diesen Fällen braucht der Bürger keinen Anmeldevordruck mehr auszufüllen. Übertragungsfehler werden auf diese Weise ausgeschlossen.
- Alle öffentlichen Stellen dürfen bundesweit Meldedaten online abrufen, soweit dies zu ihrer rechtmäßigen Aufgabenerfüllung erforderlich ist. Die Meldebehörden werden dadurch erheblich entlastet. Durch sorgfältige Identitätsprüfungen der anfragenden Stelle sowie der angefragten Person und durch eine umfassende Protokollierung der Abfragen werden die Persönlichkeitsrechte der Betroffenen ausreichend geschützt.
- Auch private Stellen können online über das Internet einfache Melderegisterauskünfte erhalten. In diesen Fällen muss die anfragende Stelle den gesuchten Einwohner eindeutig identifizieren, bevor sie eine Auskunft erhält. Die Meldepflichtigen haben das Recht, dieser Form der Auskunftserteilung zu widersprechen.
- Meldepflichtige können sich künftig unter Verwendung ihrer Signatur online bei der Meldebehörde anmelden. Eine persönliche Vorsprache ist in diesen Fällen nicht mehr notwendig. Um dies zu ermöglichen, wird auf die Vorlage einer Vermieterbescheinigung verzichtet. Zum Ausgleich der Interessen der Vermieter haben diese nun das Recht, Auskünfte über die in ihren Wohnungen gemeldeten Personen zu erhalten.
- Es können erstmalig Wohnungslose melderechtlich erfasst werden, was diesem Personenkreis die gesellschaftliche Wiedereingliederung erleichtert.

Folgende Erweiterungen des Melderegisters haben bei uns **keine Begeisterung** ausgelöst: Die Speicherung

- der Seriennummer des Personalausweises und Reisepasses,
- der waffenrechtlichen Erlaubnisse und
- des neu einzuführenden steuerlichen Personenkennzeichens für alle Bürger (26. TB, Tz. 4.1.8).

Die weit reichenden Gesetzesänderungen erforderten, einen Schwerpunkt unserer Arbeit auf die **Service- und Beratungsebene** zu verlagern. In Zusammenarbeit mit der Verwaltungsakademie Bordesholm haben wir für die Mitarbeiterinnen und Mitarbeiter der Meldeämter landesweit zehn Sonderkurse der DATENSCHUTZ-AKADEMIE Schleswig-Holstein abgehalten, in denen die Gesetzesänderungen eingehend erläutert und diskutiert wurden. In der Reihe „Datenschutz leicht gemacht“ haben wir überarbeitete „Erläuterungen und Praxistipps zum neuen Landesmeldegesetz“ vorgelegt. Diese Hinweise sind bei den Meldebehörden sehr begehrt. Nachdem die Verwaltungsvorschriften des Innenministeriums aufgehoben wurden, sind unsere Hinweise die einzigen „offiziellen“ Auslegungshilfen. Die Erläuterungen sind im Internet abrufbar unter


www.datenschutzzentrum.de/material/recht/dsleicht/hinwlmg.htm

4.1.2 Ermittlung der Hundehalter zur Erhebung der „Kampfhundesteuer“

Daten der Ordnungsämter aus dem Vollzug der Gefahrhundeverordnung können nur dann für Zwecke der Steuerveranlagung genutzt werden, soweit eine Ermächtigungsgrundlage im Satzungsrecht besteht.

Die Hundesteuersatzung einer Stadt sah vor, für gefährliche Hunde eine so genannte „Kampfhundesteuer“ zu erheben. Die Besitzer gefährlicher Hunde waren vom Ordnungsamt auf der Grundlage der Gefahrhundeverordnung festgestellt und gespeichert worden. Um nun die **Besteuerung** durchführen zu können, lag die Weitergabe der zur Steuerfestsetzung erforderlichen Daten vom Ordnungsamt an das Steueramt nahe.

Eine solche zweckändernde Nutzung personenbezogener Daten ist zulässig, wenn eine Rechtsvorschrift als Befugnisgrundlage besteht. Rechtsvorschrift in diesem Sinne kann auch eine **kommunale Satzung** sein, soweit der Bereich der Selbstverwaltungsangelegenheiten der Kommunen nicht überschritten wird und kein Widerspruch zu höherrangigem Recht besteht. Wir haben der Stadt eine Ergänzung der Hundesteuersatzung vorgeschlagen, wonach Namen und Anschriften von Hundehaltern, die im Rahmen eines Verfahrens nach der Gefahrhundeverordnung

von der Stadt erhoben wurden, zum Zwecke der Steuerveranlagung weiterverarbeitet werden dürfen.

Was ist zu tun?
In den Kommunen sollte für den Fall der Erhebung von einer Kampfhundesteuer geprüft werden, ob für die Übermittlung der Daten von Gefahrhundehaltern ausreichende Befugnisgrundlagen vorhanden sind.

4.1.3 Einbruchsbekämpfung mit zentraler Schließanlage

Die Speicherung von Zutrittsdaten in elektronischen Schließanlagen in Behörden ist datenschutzrechtlich zulässig, soweit sie nur für Zwecke der Gefahrenabwehr erfolgt. Technische und organisatorische Datensicherheitsmaßnahmen müssen die rechtmäßige Verwendung der Daten gewährleisten.

Nach mehreren Einbrüchen wurde im Rathaus der Landeshauptstadt Kiel eine neue elektronische Schließanlage montiert. Sie ermöglicht es, die Nutzung des Schlosses und damit das Betreten der Räume durch bestimmte Personen zu **protokollieren** und zu **kontrollieren**. Bei den einzelnen Zimmertüren erfolgt eine Datenspeicherung nur innerhalb des jeweiligen Schlosses. Um an den Haupteingangstüren außerhalb der Dienstzeiten ein unbefugtes Betreten zu verhindern und das befugte Betreten zu ermöglichen, werden die Daten der Zutrittsberechtigten in einem separaten Rechner gespeichert. Für uns war bei der Beurteilung des Systems von zentraler Bedeutung, dass

- die Datenverarbeitung nur zum Zwecke der Brandbekämpfung und des Einbruchsschutzes erfolgt,
- die Datenspeicherung zeitlich eng begrenzt ist,
- nur sehr wenige Mitarbeiter, abgesichert durch das Vieraugenprinzip, Zugriff auf die gespeicherten Daten haben und
- eventuelle Auswertungen schriftlich und damit revisionsfähig dokumentiert werden.

Eine Nutzung der Daten zur **Überwachung der Mitarbeiter** ist ausdrücklich ausgeschlossen worden. Unter den genannten Voraussetzungen bestanden aus unserer Sicht keine Bedenken gegen die vorgesehene Speicherung der Zugangsdaten.

Was ist zu tun?
Bei der Installation elektronischer Zutrittskontrollsysteme ist darauf zu achten, dass nur ein Minimum an Daten verarbeitet wird, eindeutige Verwendungsregelungen für die gespeicherten Daten getroffen werden und deren Einhaltung revisionsfähig geprüft wird.

4.1.4 Vertrauliche Versendung von Gehaltsnachrichten

Die Verwendung von Fensterbriefumschlägen kann aus datenschutzrechtlicher Sicht sehr problematisch sein.

Uns wurde der Umschlag mit einer Gehaltsabrechnung zur Prüfung vorgelegt, bei dem durch leichtes Anheben des **Adressfensters** die Vergütungsgruppe wie auch die Altersstufe des Adressaten in Erfahrung gebracht werden konnten. Diese Angaben sind vertrauliche Personalaktendaten, die durch geeignete technische und organisatorische Datensicherheitsmaßnahmen vor unbefugter Einsicht zu schützen sind. Wir haben der Personalverwaltung empfohlen, Gehaltsabrechnungen künftig so zu falten, dass die Personalaktendaten nur im mittleren oder letzten Teil des gefalteten Blattes enthalten sind und dadurch Neugierigen Erkenntnisse bei Manipulation des Sichtfensters vorenthalten bleiben. Gegebenenfalls sollte die Formatierung des Briefes dem Fenster angepasst werden.

Aus Datenschutzsicht kann es zudem sinnvoll sein, **neutrale Umschläge** zu nutzen, um auszuschließen, dass einzelne Briefe gezielt unbefugt geöffnet und gelesen werden.

4.1.5 Unverschlossene Umschläge zwecks Kostenersparnis

Beim Sparen lassen sich Kommunen einiges einfallen. So werden zwecks Reduzierung von Portokosten Briefe per Infopost verschickt, d. h., die Umschläge werden wegen der Gebührenstruktur der Post nicht verschlossen.

Eine Behörde schrieb im Rahmen der Vorbereitung einer neuen Abwassersatzung sämtliche Grundstückseigentümer des betroffenen Gebietes an, um die künftigen Kosten und Gebühren zu ermitteln. Dem Anschreiben war ein Fragebogen beigefügt, der nicht nur die Adresse, sondern auch Daten über die Gemarkung, Flur und Flurstück enthielt. Beigelegt war auch eine Karte, auf der das jeweilige Grundstück gekennzeichnet war. Das alles steckte in **unverschlossenen Umschlägen**.

Zum vertraulichen Umgang mit personenbezogenen Daten gehört auch, dass **Unbefugten der Zugang** zu persönlichen Unterlagen **verwehrt** wird. Wegen der Zuordnung der Eigentümer zu ihren Grundstücken handelte es sich um personenbezogene Daten. Die Behörde hätte durch geeignete Maßnahmen sicherstellen müssen, dass nicht etwa im Haushalt beschäftigte Personen die Schreiben lesen können. Dazu hätten die Umschläge verschlossen werden müssen. Möglich wäre auch gewesen, bei der Versendung auf die **Angabe personenbezogener Daten zu verzichten**. Die Daten über ihr Grundstück dürften den Grundstückseigentümern ja ohnehin bekannt sein.

Was ist zu tun?
Behörden müssen bei der Zustellung von Schriftstücken mit personenbezogenen Daten grundsätzlich verschlossene Briefumschläge verwenden.

4.1.6 Wer erhält die Protokolle nichtöffentlicher Gemeindevertretersitzungen?

Personenbezogene Sitzungsunterlagen für nichtöffentliche Sitzungen sind kommunalen Mandatsträgern nur im Rahmen ihrer Zuständigkeit zu übersenden.

Ein bürgerliches Ausschussmitglied einer Gemeindevertretung hatte offensichtlich unseren letzten Tätigkeitsbericht sorgfältig gelesen, in dem wir uns ausführlich zu Auskünften an politische Mandatsträger geäußert haben (26. TB, Tz. 4.1.3). Er wies uns darauf hin, dass er – im Widerspruch zu unserer Darstellung – regelmäßig auch die **Protokolle über den nichtöffentlichen Teil** der Sitzungen der Gemeindevertretung erhielt.

Die Verwaltung bestätigte uns, man habe die Veröffentlichung in einer kommunalpolitischen Zeitschrift in der Weise missverstanden, dass auch die bürgerlichen Ausschussmitglieder, die nicht der Gemeindevertretung angehören, in den Besitz aller vollständigen Unterlagen gelangen müssten. Das Verfahren zur Verteilung von **nichtöffentlichen Sitzungsunterlagen** wurde auf unsere Anregung wie folgt neu geregelt:

- Einladungen mit Anlagen zur Sitzung eines bestimmten **Ausschusses** werden an den Bürgermeister und die Mitglieder dieses Gremiums versandt. Alle anderen Funktionsträger bekommen nur die Einladung zur Information ohne die Anlagen.
- Mit den Anlagen werden die Einladungen zu Sitzungen der **Gemeindevertretung** nur den Mitgliedern der Gemeindevertretung zugesandt.
- **Protokolle** der Ausschusssitzungen einschließlich Anlagen – auch des nichtöffentlichen Teils – gehen den jeweiligen bürgerlichen Ausschussmitgliedern und den Gemeindevertreterinnen und Gemeindevertretern zur Vorbereitung für ihre nächste Gemeindevertretersitzung zu, soweit dort eine abschließende Beratung erfolgen soll.

Diese Verfahrensweise gewährleistet, dass kommunale Funktionsträger personenbezogene Daten nur **im Rahmen ihrer Zuständigkeit** erhalten.

Was ist zu tun?
Kommunen sollten ihre Praxis bei der Versendung von Sitzungsunterlagen unter Beachtung der vorstehenden Maßstäbe überprüfen.

4.1.7 Zusendung von Werbung an Wahlhelfer

Bei Wahlen werden Wahlhelfer eingesetzt, über die bei den Gemeinden bestimmte Angaben, z. B. Name und Telefonnummer, vorgehalten werden. Ein Missbrauch dieser Daten ist nicht ausgeschlossen.

Ein Wahlhelfer bei der Europawahl im Juni 2004 hatte einige Tage nach der Wahl einen Brief von seinem Wahlleiter erhalten, in dem dieser ihm für seine Tätigkeit als Wahlhelfer dankte. Zugleich warb er in seinem Schreiben für ein Nahrungsergänzungsmittel und für Verdienstmöglichkeiten bei dessen Vertrieb. Der Wahlleiter hatte den Namen aus einer ihm offiziell zugänglichen **Wahlhelferliste** entnommen; die Anschrift stammte aus dem örtlichen Telefonbuch. Der Wahlhelfer war erstaunt und verärgert. Er hatte während der Durchführung der Wahl kein Interesse an einer derartigen Geschäftsverbindung oder an einem solchen Produkt gezeigt; er war auch nicht darauf angesprochen worden.

Die Nutzung der Liste **für eigene Geschäftszwecke** – z. B. Werbung – verstößt gegen Datenschutzvorschriften. Eine solche Nutzung wäre erlaubt, wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte. Dies gilt aber nicht, wenn das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung gegenüber dem berechtigten Interesse der verarbeitenden Stelle überwiegt.

Die Adressdaten des Wahlhelfers waren zwar allgemein zugängliche Daten, da sie im Telefonbuch veröffentlicht sind, es widersprach jedoch dem schutzwürdigen Interesse des Wahlhelfers, dass ihm **Werbung im Zusammenhang mit seiner Wahlhelfertätigkeit** zugesandt wurde. Die Zusendung des Schreibens war daher unzulässig. Wir stellten einen weiteren formellen Rechtsverstoß fest: Der Werbende hätte den Wahlhelfer bei der Werbeansprache darauf hinweisen müssen, dass ihm ein Widerspruchsrecht gegen die Datennutzung zusteht.

Was ist zu tun?
Wahlleiter sind über ihre datenschutzrechtlichen Pflichten zu belehren.

4.1.8 Personalkostenbudgetierung in Landesverwaltung verbessert

Eine neue Software ermöglicht den Personal verwaltenden Dienststellen des Landes einen Online-Abruf von Personalkostendaten beim Landesbesoldungsamt zum Zwecke der Budgetierung. Datenschutzrechtliche Vorgaben wurden vorbildlich umgesetzt.

In der Landesverwaltung ist seit einigen Jahren die Personalkostenbudgetierung eingeführt: Die Personal verwaltenden Stellen müssen nicht nur ihre Stellenpläne einhalten, sondern auch darauf achten, dass die tatsächlich zugewiesenen Mittel nicht überschritten werden. Hierfür müssen im laufenden Haushaltsjahr **regelmäßig Hochrechnungen der Personalkosten** vorgenommen werden, bei denen die tatsächlich zu erwartenden Personalkosten zu berücksichtigen sind. Entspre-

chende Daten und Berechnungsgrundlagen waren bisher nur beim Landesbesoldungsamt vorhanden. Von den Personal verwaltenden Stellen wurde nun der dringende Wunsch geäußert, einen **Online-Zugang zu den Besoldungsdaten** ihrer Mitarbeiter zu erhalten.

Diesem Wunsch hatte sich unter unserer Beteiligung das Finanzministerium angenommen. Gemeinsam mit dem Landesbesoldungsamt konnten **Standards** erarbeitet werden, unter denen ein rechtmäßiger Online-Abruf von Besoldungsdaten stattfinden kann, die inzwischen vorbildlich umgesetzt worden sind. Zu den datenschutzrechtlichen Anforderungen gehörte insbesondere, dass

- Mitarbeiter der Personal verwaltenden Stellen nur so weit Zugriffsrechte erhalten dürfen, wie sie für entsprechende Personalverwaltungsaufgaben zuständig sind, und
- bei jedem Datenabruf protokolliert wird, wer zu welchem genauen Zeitpunkt auf welchen Personalfall und auf welche Daten des Falles zugegriffen hat.

4.1.9 Medizinische Daten eines Polizeibeamten – keine offene Weitergabe

Medizinische Daten eines Polizeibeamten müssen nicht sämtlichen Dienstvorgesetzten und deren Geschäftsstellen zur Kenntnis gelangen.

Nach einem Dienstunfall hatte sich ein Polizeibeamter ärztlich untersuchen lassen. Die Untersuchungsergebnisse – einschließlich Laborergebnisse – wurden über den Geschäftsstellenbeamten verschiedenen Dienstvorgesetzten mitgeteilt. Diesen kommen nach dem Landesbeamtengesetz **Fürsorgepflichten** zu. Eine Kenntnisgabe von sensiblen Gesundheitsdaten darf aber nur so weit erfolgen, wie dies für den konkreten gesetzlichen Zweck erforderlich ist.

Hier hatte der Dienstunfall keine dienstliche Beeinträchtigung zur Folge. Gibt ein Befund **keinen Anlass für eine Personalentscheidung** über die dienstliche Einsatzfähigkeit des Beamten wegen gesundheitlicher Bedenken oder für eine versorgungsrechtliche Beurteilung, so genügt es, wenn den unmittelbaren Dienstvorgesetzten genau dies mitgeteilt wird, aber auch nicht mehr.

Was ist zu tun?
Bei der Weitergabe medizinischer Daten an Dienstvorgesetzte ist der Erforderlichkeitsgrundsatz streng zu beachten.

4.1.10 Beratung durch den privaten Landesverband für Standesbeamte

Für die Rechtsberatung durch einen privatrechtlich organisierten Berufsverband gilt hinsichtlich der Übermittlung personenbezogener Daten das Erforderlichkeitsprinzip. Anfragen sind so weit wie möglich zu anonymisieren.

Die Standesbeamtin einer Amtsverwaltung hatte Zweifel an der Rechtmäßigkeit einer Urkunde über eine Namensänderung. Vor der Beischreibung der Änderung

im Familienbuch wandte sie sich deshalb an den Landesverband für Standesbeamte – ein privatrechtlich organisierter Berufsverband – und bat dort um eine rechtliche Begutachtung zu dem Problem. Der Anfrage beigefügt war eine Fotokopie des Familienbuches des Betroffenen mit Angaben auch über die Ehefrau. Die Beratung durch den Landesverband wäre auch in anonymer Form möglich gewesen. Die **personenbezogenen Angaben** hätten problemlos **geschwärzt** werden können. Für die Zukunft sagte die Standesbeamtin zu, Beratungsersuchen an Dritte nur noch in anonymisierter Form zu stellen.

Was ist zu tun?
Behörden sollten vor einer Beratung oder Begutachtung durch Dritte sorgfältig prüfen, ob dafür tatsächlich die Kenntnis personenbezogener Daten erforderlich ist. Im Regelfall müssen die personenbezogenen Daten in den zu übersendenden Unterlagen vor ihrer Übersendung geschwärzt werden.

4.1.11 Prüfung gaststättenrechtlicher Erlaubnisverfahren

Die Prüfung gaststättenrechtlicher Erlaubnisverfahren bei einer kreisfreien Stadt führte zu einer Beanstandung. In der Folge wurde das Verwaltungsverfahren vereinfacht und entbürokratisiert.

Bei der Prüfung gaststättenrechtlicher Erlaubnisverfahren bei einer kreisfreien Stadt ergaben sich eine Reihe von **Abweichungen von den Vorschriften** der sehr detaillierten Gaststättenverordnung. Nach Diskussion der vorgefundenen Mängel versprach die Stadt, ihre Verwaltungspraxis umzustellen.

- Im Konzessionsverfahren wurden **Regelanfragen** sowohl bei der für den Wohnsitz des Antragstellers wie auch bei der für die Gaststätte zuständigen Polizeistation vorgenommen, obwohl keine der beiden Stellen über für das Konzessionsverfahren geeignete Datensammlungen verfügt. In der Regel war der Antragsteller bei der örtlich für die Gaststätte zuständigen Polizeistation nicht einmal bekannt. Die Anhörungspraxis erzeugte damit nur unnötigen Verwaltungsaufwand.
- Obwohl die von den Betroffenen im Antragsverfahren vorzulegenden Unterlagen in der Gaststättenverordnung abschließend aufgezählt sind, wurde von den Antragstellern die Vorlage eines vollständigen Miet- oder Überlassungsvertrages gefordert. Diese Unterlagen enthielten eine Vielzahl sensibler, für das Konzessionsverfahren nicht erforderlicher Daten.
- Nach Erteilung der Gaststättenkonzession erhielten die für die Gaststätte zuständige Polizeistation, das Landesamt für Gesundheit und Arbeitssicherheit, die Lebensmittelüberwachungsbehörde sowie das Bauordnungsamt jeweils eine Durchschrift des **vollständigen Erlaubnisbescheides** zur Kenntnis. Erlaubt ist nur eine formlose Unterrichtung, soweit die jeweilige Stelle zuvor im Verfahren angehört worden ist.

Was ist zu tun?
Die Konzessionsbehörden sollten ihre Verwaltungspraxis unter Berücksichtigung der Gaststättenverordnung auf Erforderlichkeit hin überprüfen.

4.2 Polizeibereich

4.2.1 Innenminister für Erweiterung der DNA-Datei

Die Ständige Konferenz der Innenminister der Länder hat unter dem Vorsitz des schleswig-holsteinischen Innenministers in Kiel eine Erweiterung der DNA-Datei vorgeschlagen.

Unbestreitbar ist die DNA-Analyse ein wichtiges Instrument zur Aufklärung schwerer Straftaten. Eine dauerhafte Speicherung der Analysedaten im Bereich einfacher oder mittlerer Kriminalität ist jedoch **unverhältnismäßig**. Die umfassende Speicherung der DNA-Merkmale von Sexualstraftätern hat der Bundesgesetzgeber bereits zugelassen, sodass inzwischen von der zentralen DNA-Datei weitere Deliktsbereiche erfasst werden (siehe Kasten). Die Erforderlichkeit einer noch weitergehenden Erfassung wurde von der Konferenz nicht überzeugend begründet. So konnte der spektakuläre Mord an Moshammer aufgrund der geltenden Vorschriften aufgeklärt werden.

Die Innenminister meinen die DNA-Analyse im nicht codierenden Bereich mit sonstigen erkennungsdienstlichen Maßnahmen – z. B. Fingerabdruck, Lichtbild – gleichsetzen zu können. Dies hätte zur Folge, dass die Polizei künftig bei jeder **erkennungsdienstlichen Behandlung** genetische Merkmale der Bürgerinnen und Bürger erfassen würde. Auch aus dem so genannten nicht codierenden Bereich der DNA lassen sich sensible Informationen, z. B. über die Ethnie des Betroffenen, seine Verwandtschaftsverhältisse, seine Erbkrankheiten oder andere persönliche Merkmale ableiten.

Anlasstaten für Aufnahme in DNA-Datei nach geltender Rechtslage:

1. *Straftat von erheblicher Bedeutung, insbesondere: Verbrechen, gefährliche Körperverletzung, Diebstahl in besonders schwerem Fall oder Erpressung*
2. *Straftat gegen die sexuelle Selbstbestimmung (§§ 174 bis 184f des Strafgesetzbuches)*

Dabei muss in beiden Fällen Grund zu der Annahme bestehen, dass wegen der Art oder Ausführung der Tat, der Persönlichkeit des Beschuldigten oder sonstiger Erkenntnisse, gegen ihn künftig Strafverfahren wegen einer Straftat von erheblicher Bedeutung zu führen sind.

Was ist zu tun?
Die bisherigen Möglichkeiten zur Speicherung in der DNA-Datei sind zur Strafverfolgung ausreichend. Die DNA-Analyse als Standardmaßnahme zur Identifizierung von einer Straftat Verdächtigen ist abzulehnen.

4.2.2 Grenzen einer Terroristendatei von Polizei und Verfassungsschutz

Eine gemeinsame Datei von Nachrichtendiensten und Polizei über islamistische Terroristen ist nur unter engen Voraussetzungen verfassungsrechtlich vertretbar.

Aufgrund der verfassungsrechtlich vorgegebenen Trennung der Aufgaben von Polizeibehörden und Nachrichtendiensten sind die Möglichkeiten, gemeinsame Dateien einzurichten, begrenzt. Entscheidend ist, dass die Polizeibehörden nur Zugriff auf solche Daten erhalten, die sie mit den ihnen zur Verfügung stehenden rechtlichen Eingriffsinstrumentarien selbst hätten erheben dürfen. Für die Beobachtung des islamischen **Extremismus** ist nicht die Polizei, sondern ausschließlich der Verfassungsschutz zuständig.

In der Regel muss bereits ein **konkreter Anfangsverdacht** einer erheblichen Straftat – z. B. der Mitgliedschaft in einer terroristischen Vereinigung – bestehen, um der Polizei geheimdienstliche Daten verfügbar zu machen. Diese Voraussetzungen müssen geprüft werden, bevor Daten von einem Nachrichtendienst an die Polizei übermittelt werden. Deshalb muss sich eine gemeinsame Informationsbasis auf eine **Hinweisdatei** beschränken. Die beteiligten Behörden erhalten durch eine solche Datei die Information, dass über eine bestimmte verdächtige Person bereits ein Vorgang bei einer anderen Behörde geführt wird. Eine darüber hinausgehende Datenübermittlung kann aufgrund dieser Information **im Einzelfall** geprüft werden. Gemeinsame Informationsbestände von Polizei- und Verfassungsschutzbehörden darf es nicht geben.

Aus Gründen der Verhältnismäßigkeit dürfen die aus einer gemeinsamen Datei stammenden Informationen **streng zweckgebunden** nur zur Bekämpfung des Terrorismus weitergegeben werden. Eine effektive Kontrolle durch die zuständigen Datenschutzbeauftragten und die Protokollierung der Daten sind sicherzustellen. Eine zeitliche Begrenzung und Evaluation der Datei ist ebenso notwendig.

Was ist zu tun?
Eine gemeinsame Datei von Nachrichtendiensten und Polizei darf nur als Hinweisdatei ausgestaltet werden. Aufgrund der Sensibilität des Datenbestandes unterliegt sie restriktiven Verwendungsbeschränkungen.

4.2.3 Bekämpfung der Internetkriminalität – „quick freeze“

Alle Versuche, eine Vorratsspeicherung von Verkehrsdaten bei der Telekommunikation einzuführen, sind bislang gescheitert. Als Alternative kommt eine kurzfristige Speicherungsanordnung in besonders begründeten Verdachtsfällen – das so genannte „quick freeze“ – in Betracht.

Bei der Telekommunikation fallen Daten über Verbindungen und Verbindungsversuche – die so genannten Verkehrsdaten – an. Für die Strafverfolgung sind diese von Interesse, wenn z. B. der Inhaber einer Zielrufnummer oder die

IP-Adresse eines Internetnutzers ermittelt werden soll. Über diese IP-Adresse kann festgestellt werden, von welchem Anschluss auf eine bestimmte Internetseite zugegriffen wurde (Tz. 7.4).

Voraussetzung einer solchen Maßnahme ist ein richterlicher Beschluss. Was aber, wenn die Daten bereits gelöscht sind, bevor der richterliche Beschluss vorliegt? Hier kann ein gesetzlich geregeltes „quick freeze“ den Strafverfolgern helfen. Dabei ordnen in einem ersten Schritt die Ermittlungsbehörden an, dass bei Vorliegen eines konkreten Tatverdachtes die routinemäßige Löschung der Daten durch den Diensteanbieter blockiert – „eingefroren“ – wird (so genannte „**Speicheranordnung**“ bzw. „anlassbezogene Speicherung“). In einem zweiten Schritt können die Daten durch eine nachträgliche richterliche Anordnung „aufgetaut“ und den Ermittlungsbehörden zur Verfügung gestellt werden.

Eine solche Anordnungsbefugnis für Polizei und Staatsanwaltschaft kann eine sinnvolle Ergänzung des bisherigen Ermittlungsinstrumentariums sein. Sie wäre eine weniger eingriffsintensive Alternative bzw. ein **milderes Mittel** zur verfassungswidrigen Vorratsdatenspeicherung. Allerdings sollte der Gesetzgeber nicht voreilig handeln. Es fehlt bislang an einer verlässlichen Datenbasis über die Zahl und den Erfolg der derzeit schon zulässigen Herausgabeanordnungen von Verkehrsdaten. Mit einer „quick-freeze-Anordnung“ wird in das Fernmeldegeheimnis nicht nur des Betroffenen, sondern auch seiner Kommunikationspartner eingegriffen. Denn auch diese geraten bei einem solchen Verfahren in das Fadenkreuz der Fahnder.

Was ist zu tun?
„quick freeze“ ist ein denkbares milderes Mittel gegenüber der verfassungswidrigen Vorratsdatenspeicherung. Verfahrensrechtlich ist sicherzustellen, dass die Herausgabe von Telekommunikationsverkehrsdaten nur durch richterlichen Beschluss erfolgt.

4.2.4 INPOL-SH

INPOL-SH ist das Zugangssystem des Landes zu INPOL-Zentral, dem beim Bundeskriminalamt geführten Informationssystem der Polizeien des Bundes und der Länder. Zugleich ist INPOL-SH als Folgeverfahren der alten PED (Polizeiliche Erkenntnisdatei) das zentrale Informationssystem der Landespolizei. In Sachen Sicherheit und Rechtmäßigkeit besteht noch Klärungsbedarf.

Die beim Bundeskriminalamt (BKA) betriebenen Altsysteme von dem seit 1970 in Betrieb befindlichen INPOL wurden mit der Einführung und der Aufnahme des Wirkbetriebs von INPOL-Zentral im Jahr 2003 sukzessive abgeschaltet. Für Schleswig-Holstein hatte dies zur Folge, dass mit den alten Landesverfahren nicht mehr auf die neuen Systeme des Bundes hätte zugegriffen werden können. Um die direkte **Anbindung an die Verfahren von INPOL** beim BKA weiterhin zu gewährleisten, wurde INPOL-SH implementiert.

Die gesetzlich vorgeschriebene Vorabkontrolle hatte im Juni 2003 einen Stand erreicht, der uns eine abschließende Bewertung nicht ermöglichte. Die notwendigen Unterlagen konnten vom Innenministerium nicht zeitgerecht zur Verfügung gestellt werden. Dies wurde uns mit der Komplexität des Vorhabens und internen Problemen, insbesondere der Abhängigkeit von der Entwicklung von INPOL-neu (jetzt: INPOL-Zentral) des Bundes begründet.

Wir wiesen in einer vorläufigen Bewertung bereits im Dezember 2003 darauf hin, dass auf der Basis der vorgelegten Unterlagen über die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung eine im Ergebnis positive Vorabkontrolle nicht möglich sei. Das Innenministerium signalisierte in seiner auch auf inhaltliche Aspekte eingehenden

Im Wortlaut: § 9 Abs. 1 LDSG

Vor der Einrichtung oder wesentlichen Änderung

1. *eines Verfahrens nach § 8 Abs. 1 oder*
2. *eines automatisierten Verfahrens, in dem Daten im Sinne des § 11 Abs. 3 verarbeitet werden,*

ist der oder dem behördlichen Datenschutzbeauftragten oder, wenn eine solche oder ein solcher nicht bestellt ist, dem Unabhängigen Landeszentrum für Datenschutz Gelegenheit zur Prüfung innerhalb einer angemessenen Frist zu geben, ob die Datenverarbeitung zulässig ist und die vorgesehenen Maßnahmen nach den §§ 5 und 6 ausreichend sind (Vorabkontrolle).

? Errichtungsanordnungen

sind Verwaltungsvorschriften, in denen Festlegungen bezüglich der Rechtsgrundlage des Verfahrens, des Datenumfangs, der Zugriffsberechtigten, der Übermittlungsregelungen, der Speicherfristen und der zu ergreifenden technisch- organisatorischen Maßnahmen zu treffen sind. Sie sind Organisationsmaßnahmen, die Verletzungen des Persönlichkeitsrechts vermeiden sollen. Solche Maßnahmen werden vom Bundesverfassungsgericht für eine rechtmäßige Datenverarbeitung ausdrücklich gefordert.

Stellungnahme vom April 2004 das Interesse an einem **positiven Votum des ULD**, auch wenn dies nicht gesetzliche Voraussetzung für die Freigabe des Verfahrens sei.

Nachdem INPOL-SH in Wirkbetrieb gegangen ist, macht die Fortsetzung der begonnenen „Vorab"-Kontrolle wenig Sinn. Das Landesverwaltungsgesetz schreibt neben der Vorabkontrolle eine **Errichtungsanordnung** vor. Deshalb regten wir an, die zunächst noch ausstehende Errichtungsanordnung kurzfristig zu erstellen, und haben dem Innenministerium hierfür unsere Unterstützung und Beratung – auch in der Konzeptphase – angeboten. Der uns vorgelegte Text einer Errichtungsanordnung erwies sich als verbesserungsbedürftig.

Was ist zu tun?
INPOL-SH muss auf rechtlich einwandfreie Füße gestellt werden. Die bisher vorgelegten Unterlagen sind ein erster Schritt, um einen datenschutzkonformen Zustand zu erarbeiten.

4.2.5 Die Datei @rtus der schleswig-holsteinischen Polizei

@rtus steht für den Aufbruch der Polizei des Landes in eine neue Welt der Informationsverarbeitung. Das Verfahren ist mit erheblichen datenschutzrechtlichen Defiziten in den Wirkbetrieb gegangen.

Mit „@rtus" steht der Landespolizei ein Datenverarbeitungssystem zur Verfügung, mit dem sie **sämtliche Vorgänge** bearbeitet und speichert – von der einfachen Strafanzeige bis zum Großverfahren, vom Entstehen eines Vorgangs bis zum Ende seiner Archivierung. Gespeichert werden Daten über Täter, Opfer, Zeugen, Hinweisgeber und andere Personen sowie zahlreiche Einzelheiten der bearbeiteten Fälle. @rtus ist also ein Verfahren, das der Polizei die **Vorgangsbearbeitung „aus einer Hand"** ermöglicht.

In Betrieb befindet sich derzeit eine **Basisversion** mit noch sehr eingeschränkten Recherchemöglichkeiten. Nach dem weiteren Ausbau des Verfahrens können die Informationen multifunktional ausgewertet werden. Dadurch gewinnt @rtus besondere Brisanz: In dem Verfahren werden neben Daten aus Ordnungswidrigkeitenverfahren und dem Bereich der Gefahrenabwehr auch solche aus strafrechtlichen Ermittlungsverfahren verarbeitet. Nach den Vorstellungen der Polizei sollen in der Zukunft all diese Informationen, die in einer Datenbank abgelegt sind, nach polizeilichen Bedürfnissen miteinander verknüpft und ausgewertet werden können. Konkrete Angaben über diese **Auswertungstools** liegen aber noch nicht vor.

Bei unserer rechtlichen Bewertung liegt ein besonderes Augenmerk auf dem Einsatz von Auswertetools. Der über diese Werkzeuge erschlossene Datenbestand umfasst nicht nur ein konkretes Verfahren, sondern künftig sämtliche in Schleswig-Holstein bei der Polizei erfassten Vorgänge. Über sie erfolgt eine Auswertung **zu anderen Zwecken und in anderem Kontext**. Dabei entstehen

neue – logische – Dateien, für die Regularien erst noch erarbeitet werden müssen. Beachtlich ist dabei die Regelung des Landesverwaltungsgesetzes, wonach erforderlich ist, dass Verdachtsdaten für die Verhütung einer künftigen Wiederholungstat benötigt werden. Zudem legt das Gesetz klare Prüffristen für die weitere Speicherung fest.

Da die Daten aus strafrechtlichen Ermittlungsverfahren gemeinsam mit Daten aus der Gefahrenabwehr in einer Datei gespeichert werden, handelt es sich um eine so genannte **Mischdatei**. Für Mischdateien gelten – so die Strafprozessordnung – die landesrechtlichen Vorschriften, also das Landesverwaltungsgesetz. Eine logische und damit auch eine rechtliche Trennung nach bestimmten Zwecken ist bisher nicht vorgesehen.

Bevor über weitere „intelligente“ Nutzungen und Auswertungen nachgedacht wird, muss Klarheit über die rechtlichen Grundlagen des bereits bestehenden Datenbestands hergestellt werden, auch soweit dieser noch nicht komplexen Recherchen unterworfen ist. Dem dient die Errichtungsanordnung, die uns **erst nach Aufnahme des Wirkbetriebs** zugeleitet wurde. Dies ist eine für die Polizistinnen und Polizisten verbindliche Verwaltungsvorschrift (Tz. 4.2.4). @rtus ist bereits seit einigen Monaten bei verschiedenen Polizeidienststellen in Schleswig-Holstein in Betrieb und wird sukzessive flächendeckend eingeführt. Die verspätete Errichtungsanordnung haben wir gegenüber dem Innenministerium beanstanden müssen. Wir formulierten zahlreiche Kritikpunkte zu der uns nunmehr vorliegenden Errichtungsanordnung. Diese werden wir nun in einem Dialog mit dem Innenministerium erörtern.

Was ist zu tun?
Im weiteren Dialog mit dem Innenministerium müssen die offenen Fragen zügig geklärt werden.

4.2.6 Arbeitsdatei PIOS Innere Sicherheit (APIS)

APIS ist eine „Staatsschutz“-Datei beim Bundeskriminalamt, die auch mit Daten aus den Ländern gespeist wird. Der Versuch des Bundesministeriums des Innern, die Errichtungsanordnung für APIS an andere Errichtungsanordnungen „anzupassen“, brachte datenschutzrechtlich eher Flurschaden als Verbesserungen. Dies hinderte das Landesinnenministerium nicht, der Errichtungsanordnung zuzustimmen.

? PIOS

***PIOS**-Dateien sollen die Zusammenhänge zwischen „**P**ersonen, **I**nstitutionen, **O**bjekten und **S**achen“ klären. In ihnen werden Inhalte aus Ermittlungsakten gespeichert. Sie dienen nicht unmittelbar der Aufklärung einzelner Straftaten, sondern der Beobachtung eines gesamten Kriminalitätsbereichs. Neben Beschuldigten und Verdächtigen werden auch „andere Personen“ erfasst.*

Die Errichtungsanordnung APIS wurde als Verschlusssache eingestuft. Daher können wir an dieser Stelle nur einen Punkt aus einer längeren Mängelliste

hervorheben: „Aus technischen Gründen“ erfolgt keine automatische **Protokollierung von Anfragen** an die Datei oder von Übermittlungen aus der Datei. Diese datenschutzrechtliche Selbstverständlichkeit soll erst mit der Einführung von INPOL-neu realisiert werden. Ein genauer Zeitpunkt wird nicht genannt. Vorläufig wird offenbar nur die **Änderung** von Datensätzen protokolliert.

Eine solche **Protokollierungspraxis** erlaubt keine effektive Datenschutzkontrolle. Im Nachhinein kann nicht festgestellt werden, wer Informationen abgerufen hat und bei welchen Stellen diese letztlich verblieben sind. Weder der Weg noch der Verbleib der hochsensiblen Staatsschutzdaten kann rekonstruiert werden. Selbst stichprobenartige Kontrollen sind nicht möglich. Dieser Verzicht ist nicht nur ein Datenschutz-, sondern auch ein **Sicherheitsproblem**. Eine effektive Kontrollmöglichkeit durch unabhängige Datenschutzbeauftragte ist für die verfassungskonforme Datenverarbeitung unabdingbar. Diese setzt eine vollständige Aufzeichnung der Abrufe, die regelmäßige Auswertung der Protokolldaten sowie deren Bindung auf Zwecke der Datenschutzkontrolle voraus. Leider teilte das Innenministerium unsere Bedenken nicht, sondern signalisierte seine Zustimmung zur Errichtungsanordnung.

Was ist zu tun?
APIS ist unverzüglich an die gesetzlichen Anforderungen anzupassen. Die lückenlose Protokollierung aller Transaktionen muss für Zwecke der Datenschutzkontrolle gewährleistet sein.

4.2.7 Einsatzleitstellensystem Lübeck – Ende gut, alles gut?

Die Mängel des polizeilichen Einsatzleitstellensystems sind behoben worden, nachdem die für die Überarbeitung der Software notwendigen Haushaltsmittel bereitgestellt wurden.

Wir berichteten über datenschutzrechtliche Mängel des Einsatzleitstellensystems der Polizeidirektion Lübeck (26. TB, Tz. 4.2.3.), insbesondere über zu weit gehende **Recherchemöglichkeiten**. Inzwischen wurden technische Tools eingerichtet, die dafür sorgen, dass in dem Verfahren eine Recherche zu Opfern von Straftaten oder zu Zeugen nicht mehr möglich ist.

Die Polizei hat uns die fachliche Notwendigkeit dargelegt, dass **personengebundene Hinweise** zur Eigensicherung der eingesetzten Polizeibeamten im Einsatzleitstellensystem erforderlich sind. Es ist auch aus unserer Sicht in Ordnung, dass die Einsatzleitstelle die Polizeibeamten im Einsatz – etwa vor bewaffneten Personen – warnt. Die Polizei muss aber die Datensätze in kurzen Zeitabständen überprüfen, ob sie im Einzelfall auf einen hinreichend aktuellen Sachverhalt gestützt werden können. Die Hinweise dürfen auch nur für den Zweck der Eigensicherung verwendet werden.

Was ist zu tun?
Das Einsatzleitstellensystem Lübeck hat nun auch die datenschutzrechtlichen Hürden genommen. Künftig sollte ein finanzieller Mehraufwand durch unsere rechtzeitige Beteiligung vermieden werden.

4.2.8 Hafensicherheitsgesetz – Wer kontrolliert die Mitarbeiter?

Mit einem „Gesetz zur Verbesserung der Sicherheit in den schleswig-holsteinischen Hafenanlagen“ soll internationalen Anforderungen zur Terrorismusabwehr in internationalen Häfen genügt werden. Zuverlässigkeitsprüfungen bei Mitarbeitern stellen das Trennungsgebot zwischen Verfassungsschutz und Polizei infrage.

Hafensicherheit ist für Schleswig-Holstein ein wichtiges Thema. Unbestreitbar kann hierfür die Überprüfung der Zuverlässigkeit eines begrenzten Kreises von Mitarbeitern in Hafenanlagen ein Beitrag sein. Doch sollten hierbei bewährte Aufgabenzuweisungen nicht infrage gestellt werden: Nach den Vorschlägen des Innenministeriums wird für die Durchführung der Zuverlässigkeitsüberprüfungen die **Wasserschutzpolizei zuständig** sein. Hierbei soll sie auf zahlreiche zentrale Dateien – auch solche des Verfassungsschutzes – zugreifen können.

Damit erhält eine Polizeibehörde, die zugleich Strafverfolgungsbehörde ist, Zugriff auf Daten von Nachrichtendiensten. Diese Daten wurden möglicherweise mit geheimdienstlichen Methoden erlangt. Das **Trennungsgebot zwischen Polizei und Nachrichtendiensten** soll aber gerade eine solche Aufgabenvermischung ausschließen. Sicher ist die Polizei nicht weniger zuverlässig im Umgang mit personenbezogenen Daten als andere Behörden. Hier handelt es sich aber um einen Fall verfassungsrechtlicher Inkompatibilität.

Daher haben wir vorgeschlagen, abweichend von den sonstigen Zuständigkeiten im Hafensicherheitsgesetz die Durchführung der Zuverlässigkeitsprüfung nicht einer Polizeibehörde, sondern z. B. dem Verkehrsministerium oder dem Landesamt für Straßenbau und Verkehr zu übertragen. Dies führt nicht zu einem „bürokratischen Monstrum“ – wie das Innenministerium behauptet. Weitaus umfänglichere Sicherheitsüberprüfungen nach dem Atomrecht und nach dem Luftverkehrsrecht werden bereits seit langem von **Verkehrsbehörden** durchgeführt. Dies hat sich als praxisnahe Lösung bewährt.

Was ist zu tun?
Die Zuständigkeit für die Durchführung der Zuverlässigkeitsprüfung sollte auf ein Ministerium oder das Landesamt für Straßenbau und Verkehr übertragen werden.

4.2.9 Löschung und Auskunft aus Verbunddateien

Bei Verbunddateien sind nach Ablauf der Speicherfrist des eingebenden Landeskriminalamtes die Daten des Betroffenen auch vom Bundeskriminalamt zu löschen.

Zu einem Petenten waren Daten direkt bei der Landespolizei und in einer Verbunddatei des Bundeskriminalamtes (BKA) auf Veranlassung der schleswig-holsteinischen Polizei gespeichert. Nach Ablauf der Speicherfrist bat der Petent um Prüfung, ob die Daten auch tatsächlich **gelöscht** worden sind. In den Dateien der Landespolizei war dies der Fall. Nicht gelöscht waren aber, wie der Bundesbeauftragte für den Datenschutz feststellte, die Daten beim BKA. Die **Auskunft** des Landeskriminalamtes (LKA), wonach keine Daten über den Petenten durch die Landespolizei gespeichert seien, erwies sich deshalb als falsch.

Uns wurde vom LKA zugesagt, dass zukünftig umfassend Auskunft erteilt wird, auch über Daten, die in Verbunddateien eingestellt wurden sowie über solche, die zum Zeitpunkt der Anfrage gespeichert waren und im Zuge der Bearbeitung der Anfrage gelöscht werden sollen. Das BKA muss sicherstellen, dass die von den Ländern angelieferten Datensätze nach deren Vorgaben gelöscht werden.

Was ist zu tun?
Das BKA muss die Verantwortlichkeit der Länder respektieren, die ihre Daten in Verbunddateien eingestellt haben.

4.3 Justizverwaltung

4.3.1 „Großer Lauschangriff" – Urteil des Bundesverfassungsgerichts

Mit dem Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung vom 3. März 2004 wurden verfassungsrechtliche Maßstäbe für zahlreiche heimliche Ermittlungsmaßnahmen im Strafprozess- und Polizeirecht gesetzt. Die bestehenden gesetzlichen Vorschriften schützen die Betroffenen nicht ausreichend vor Eingriffen in den Kernbereich privater Lebensgestaltung.

Im Wortlaut:
Art. 1 Abs. 1 Grundgesetz

„Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt."

Das Urteil des Bundesverfassungsgerichts beschränkt sich nicht auf Aussagen zum in Art. 13 GG garantierten Grundrecht auf „Unverletzlichkeit der Wohnung". Vielmehr wurden bei der Überprüfung des „Großen Lauschangriffs" **zentrale Maßstäbe des Grundgesetzes** angelegt, an denen sämtliche heimlichen Ermittlungsmaßnahmen gemessen werden müssen, die sich aus der Menschenwürdegarantie, dem damit verbundenen allgemeinen Persönlichkeitsrecht sowie dem Verhältnismäßigkeitsprinzip ableiten.

Das Persönlichkeitsrecht verbietet dem Staat zwar nicht sämtliche heimlichen Beobachtungen, es ist jedoch stets ein unantastbarer **Kernbereich privater Lebensgestaltung** zu wahren. Dringt der Staat in diesen Kernbereich ein, so verletzt dies die jedem Menschen unantastbar gewährte Freiheit zur Entfaltung in den ihn betreffenden höchst persönlichen Angelegenheiten. Dieser Kernbereich ist nicht relativierbar. Das heißt: Auch überwiegende Interessen der Allgemeinheit können einen Eingriff nicht rechtfertigen. Der Kernbereich ist in der Regel berührt, wenn eine Person mit **engsten persönlichen Vertrauten** in einer geschützten Gesprächssituation – z. B. in einer Privatwohnung – kommuniziert.

Der Schutz des Kernbereichs bedingt ein gesetzliches Verbot, in diesen Bereich eindringende Gespräche zu erfassen oder aufzuzeichnen (**Erhebungsverbot**). Falls die Gespräche erfasst werden, dürfen die Inhalte im betreffenden Verfahren und auch in weiteren Zusammenhängen nicht verwendet werden. Auch dürfen die ermittelten Tatsachen nicht als Anknüpfungspunkte für weitere Ermittlungen dienen (**erweitertes Verwertungsverbot**).

Neben dem Schutz des Kernbereichs privater Lebensgestaltung spricht das Bundesverfassungsgericht **konkrete Verhältnismäßigkeitsanforderungen** und notwendige verfahrensrechtliche Absicherungen an. Das Gericht hat die Eingriffsschwelle für Lauschaktionen erhöht. Diese dürfen in Zukunft nur noch zur Verfolgung von Straftaten erfolgen, die im Mindestmaß mit einer Freiheitsstrafe von mehr als fünf Jahren belegt werden.

www.datenschutzzentrum.de/material/themen/lausch/bvg_lauschangriff.htm

Was ist zu tun?
Die Vorschriften der Strafprozessordnung und der Polizeigesetze müssen Erhebungs- und Verwertungsverbote zum Schutz des Kernbereichs privater Lebensgestaltung erhalten.

4.3.2 Referentenentwürfe zum „Großen Lauschangriff“

Nach dem Urteil zum „Großen Lauschangriff“ hat die Bundesjustizministerin zwei Referentenentwürfe vorgelegt. Statt sich auf eine Umsetzung der Vorgaben des Bundesverfassungsgerichts zu beschränken und auch andere Überwachungsmaßnahmen in die Neuregelung einzubeziehen, wollte die Bundesjustizministerin mit dem ersten Entwurf sogar das Abhören der Kommunikation mit Berufsgeheimnisträgern ermöglichen.

Nach scharfen Protesten u. a. von Berufsverbänden und Datenschützern und auch nach kritischen Stimmen aus der Politik – so etwa der Justizministerin des Landes Schleswig-Holstein – wurde dieser erste Entwurf **zurückgenommen**.

Der Schutz der **Vertrauensverhältnisse** ist **Grundbedingung** einer freiheitlichen und rechtsstaatlichen Gesellschaft. Jeder kann in eine schwierige Lebenslage kommen, in der er in einem vertraulichen Gespräch über intime Sachverhalte

Expertenrat zu medizinischen, seelischen oder rechtlichen Fragen einholen muss. Es ist nicht zumutbar, solche Gespräche in dem Bewusstsein führen zu müssen, dass Dritte später anhand des aufgezeichneten Inhalts entscheiden, ob und zu welchen strafprozessualen Zwecken die Informationen verwertet werden können.

In einem zweiten vorgelegten Entwurf sind diese Abhörbefugnisse nun nicht mehr vorgesehen. Aber der Entwurf bezieht lediglich die akustische Wohnraumüberwachung ein und beschränkt sich auf das zur Umsetzung des Verfassungsgerichtsurteils **absolut Notwendige**.

Durch das Urteil ist der verfassungsrechtliche Spielraum für den „Großen Lauschangriff“ gering geworden. Zudem sind die bisherigen Erfolge bei diesem Grundrechtseingriff mager. Die Praktikabilität der in den Referentenentwürfen vorgesehenen Regelungen ist zweifelhaft. Auf den „Großen Lauschangriff“ – der unter allen heimlichen Ermittlungsmaßnahmen den empfindlichsten Rechtseingriff darstellt – sollte daher unseres Erachtens **gänzlich verzichtet** werden.

? Berufsgeheimnisträger

Nicht alle, die aufgrund ihres Berufs zum Schweigen verpflichtet sind (§ 203 StGB), dürfen im Prozess die Zeugenaussage verweigern. Dies dürfen z. B. im Strafprozess grundsätzlich nur diejenigen, die in § 53 StPO aufgezählt sind. Hierzu zählen Ärzte, Zahnärzte, Rechtsanwälte, Steuerberater, Psychotherapeuten, Geistliche, Suchtberater, Schwangerschaftsberater und Journalisten. Zum Schutz vor Überwachungsmaßnahmen bestehen keine einheitlichen Regelungen. Im Rahmen der Telefonüberwachung sind z. B. nur Gespräche mit Strafverteidigern (nicht: Rechtsanwälten im Allgemeinen!) geschützt.

www.datenschutzzentrum.de/material/themen/lausch/lsch_st4

Was ist zu tun?
Der Schutz der Kommunikation mit zeugnisverweigerungsberechtigten Berufsgeheimnisträgern darf nicht ohne Not – und schon gar nicht ohne plausible Begründung – eingeschränkt werden. Die Landesregierung kann im Bundesrat auf einen einheitlichen Schutz dieser Vertrauensverhältnisse bei allen Überwachungsmaßnahmen hinwirken.

4.3.3 Die Überwachung der Telekommunikation nach dem Urteil

Auf Bundesebene wird derzeit eine Novelle der Überwachung der Telekommunikation diskutiert. Auch hier sind die Grundsätze des Urteils des Bundesverfassungsgerichts zum „Großen Lauschangriff“ zu beachten. Die Ergebnisse der Evaluierung der bisherigen Telekommunikationsüberwachung zeigen gewaltige Defizite beim Grundrechtsschutz.

Intime Gespräche – z. B. zwischen Eheleuten – können nicht nur in der Ehewohnung abgehört werden, sondern auch während einer gemeinsamen Autofahrt oder in einem Telefongespräch. **Sämtliche heimlichen Ermittlungsmethoden**, egal ob in der Strafprozessordnung oder im Polizeirecht geregelt, können den absolut geschützten Bereich des Persönlichkeitsrechts verletzen.

Das Bundesverfassungsgericht hat festgestellt, dass die Schutzbedürftigkeit der Kommunikation sich aus dem **Inhalt der Gespräche** ergibt. Ort und Mittel der Kommunikation sind nicht die einzigen Aspekte bei der Feststellung der Eingriffsstufe. Daraus ergibt sich unzweifelhaft, dass alle Formen der Kommunikation kernbereichsrelevant sein können und dementsprechend zu schützen sind.

Dies gilt in besonderem Maße für die Überwachung der **Telekommunikation**, zu der ebenfalls Erhebungs- und Verwertungsverbote zum Schutz des Kernbereichs der persönlich vertraulichen Kommunikation geschaffen werden müssen. Wegen der übergreifenden Zielsetzung ist es wünschenswert, wenn für alle Formen des heimlichen Abhörens einheitliche, „vor die Klammer“ gezogene Erhebungs- und Verwertungsverbote geschaffen würden.

Die vom Bundesverfassungsgericht thematisierten verfahrensrechtlichen Absicherungen, wie die Pflicht zur Begründung der Überwachungsanordnung und die zur Benachrichtigung der betroffenen Personen, wurden – wie eine **Evaluierung** der Praxis der Telekommunikationsüberwachung aufgezeigt hat (26. TB, Tz. 4.2.5) – in der Vergangenheit nicht eingehalten. Von der Einhaltung der genannten verfahrensrechtlichen Vorkehrungen ist aber die Verfassungsmäßigkeit der Telekommunikationsüberwachung abhängig. Auch in Zukunft wird auf die Einhaltung der verfassungsrechtlichen Anforderungen besonderes Augenmerk zu legen sein.

Was ist zu tun?
Die Vorgaben des Bundesverfassungsgerichts zum „Großen Lauschangriff“ müssen für sämtliche heimlichen Ermittlungsmaßnahmen umgesetzt werden. Vorzuziehen sind „vor die Klammer“ gezogene einheitliche Erhebungs- und Verwertungsverbote.

4.3.4 Das ULD bei der Staatsanwaltschaft – Kontrollbefugnis

Nach Diskussionen zwischen ULD und Generalstaatsanwaltschaft besteht nunmehr Einvernehmen, dass das ULD in Ermittlungsakten Einsicht nehmen kann.

Das Landesdatenschutzgesetz verpflichtet alle öffentlichen Stellen, das ULD bei Datenschutzkontrollen zu unterstützen. Dabei muss dem ULD Einsicht in Unterlagen und Dateien gewährt werden, um eine effektive Datenschutzkontrolle zu ermöglichen. Ausnahmen bestehen nur für den Landesrechnungshof und die Gerichte, soweit diese in **richterlicher Unabhängigkeit** tätig werden, nicht aber für andere Justizbehörden und die gerichtliche Tätigkeit, die außerhalb der richterlichen Unabhängigkeit liegt. Dies gilt auch für den Bereich der Staatsanwaltschaften, da für diese im LDSG keine Ausnahme vorgesehen ist. Von unserer Bewertung nicht erfasst werden rein strafprozessuale Ermittlungsentscheidungen der Staatsanwaltschaft ohne Datenschutzbezug.

Die Generalstaatsanwaltschaft hat dies zunächst für ihren Bereich in Zweifel gestellt und in Einzelfällen die Herausgabe staatsanwaltschaftlicher Akten an das ULD verweigert. Seit dem Volkszählungsurteil sollte geklärt sein, dass die staatliche Verarbeitung personenbezogener Daten durch eine flankierende **Beteiligung unabhängiger Stellen** kontrolliert werden muss. Dabei geht es nicht nur um die Möglichkeit einer gerichtlichen Überprüfung. Vielmehr fordert das Bundesverfassungsgericht zusätzlich eine unabhängige Stelle, die die Datenschutzaufsicht auch **aus eigener Initiative** wahrnehmen kann. Durch eine solche Kontrollmöglichkeit wird der Grundrechtseingriff abgefedert und erhält eine zusätzliche verfassungsrechtliche Legitimation.

Was ist zu tun?
Die Kontroverse um die Einsicht in Ermittlungsakten zur Datenschutzkontrolle ist beigelegt. Einer guten praktischen Handhabung steht aus Sicht des ULD nichts mehr im Wege.

4.3.5 Löschung von Telefonüberwachungsprotokollen bei Parallelverfahren

Nach der Strafprozessordnung müssen die Aufzeichnungen und Niederschriften aus einer Telefonüberwachung unverzüglich vernichtet bzw. gelöscht werden, sobald sie für die Strafverfolgung nicht mehr benötigt werden.

Dies haben wir in einem Einzelfall anhand der Haupt- sowie der Sonderbände bei einem Vorgang geprüft. Die formalen Voraussetzungen der Telefonüberwachung waren dokumentiert. Der Nachweis über die Vernichtung bzw. Löschung der Unterlagen war in den Akten ebenfalls ordentlich dokumentiert. Wir fanden eine entsprechende Niederschrift, die den Anforderungen der Strafprozessordnung entsprach. Die Unterlagen waren allerdings erst knapp ein Jahr nach Verfahrensabschluss vernichtet worden. Dieses wurde damit begründet, dass nicht absehbar

gewesen sei, ob diese in – im Einzelnen bezeichneten und an andere Stellen abgegebenen – Parallelverfahren noch benötigt würden. Diese Frage hätte **anlässlich der Abgabe des Vorgangs** durch Anfrage bei den beteiligten Stellen **geklärt** werden können. Die betroffene Staatsanwaltschaft hat hierauf reagiert und in einer Hausverfügung entsprechende Anfragen vorgesehen.

Was ist zu tun?
Bevor Unterlagen für ein Parallelverfahren aufbewahrt werden, sollte bei Abgabe des Vorgangs an eine andere Stelle die Frage geklärt werden, ob diese hierfür weiter aufbewahrt werden müssen.

4.3.6 Schöffenwahl

Nach dem Gerichtsverfassungsgesetz obliegt es den Gemeinden, in jedem vierten Jahr eine Vorschlagsliste für die Schöffenwahl aufzustellen. Bei Beratung und Veröffentlichung der Vorschlagsliste ist der Datenschutz zu beachten.

Die Vorschlagsliste für die Wahl der Schöffen muss in einer Sitzung der Gemeindevertretung beraten werden. Diese Beratung darf nichtöffentlich erfolgen. Für eine Veröffentlichung der personenbezogenen Daten im Rahmen der Erörterung gibt es keine Rechtsgrundlage. In der Beratung kommen zum Teil **sensible persönliche und sachliche Verhältnisse** der auf der Vorschlagsliste aufgeführten Personen zur Sprache. Vor Aufnahme in die Liste werden Alter, Beruf und soziale Stellung ermittelt, da die Gemeinde alle Gruppen der Bevölkerung gleichmäßig berücksichtigen soll. Zudem erörtert der Gemeinderat Ablehnungs- bzw. Ausschlussgründe, die einer Aufnahme in die Liste entgegenstehen. Dabei geht es etwa um Vermögensverhältnisse oder gar um die Fähigkeit zur Bekleidung öffentlicher Ämter oder gesundheitliche Bedenken. Es ist nicht ausgeschlossen, dass das Gremium im Einzelfall eventuell kontrovers die charakterliche Eignung einer Person für das Amt des Schöffen in der Gemeindevertretung bespricht und für die Auswahl der vorzuschlagenden Kandidaten eine Bewertung der in Rede stehenden Personen im Verhältnis zueinander vornimmt. Erst die endgültig beschlossene Vorschlagsliste darf nach dem Gerichtsverfassungsgesetz veröffentlicht werden.

? *Vorschlagsliste*

Insbesondere in der Straf- und Verwaltungsgerichtsbarkeit sind an der Rechtsprechung auch Laienrichter (Schöffen) beteiligt. Diese werden in einem besonderen Wahlverfahren aus einer Vorschlagsliste gewählt. Diese wird durch die Gemeinden erstellt, damit ein möglichst breiter Querschnitt der Bevölkerung an der Rechtsprechung beteiligt wird. Betroffen sein kann grundsätzlich jede Bürgerin und jeder Bürger.

Was ist zu tun?
Die Beratung der Vorschlagsliste für die Schöffenwahl muss im nichtöffentlichen Teil der Sitzung der Gemeindevertretung erfolgen. Die dabei zur Vorbereitung notwendigen Unterlagen sind entsprechend zu kennzeichnen und ebenfalls als nichtöffentlich zu behandeln.

4.3.7 Ermittlungsakten für die Täter-Opfer-Ausgleichsstelle

Ein Strafverfahren kann häufig durch einen Täter-Opfer-Ausgleich abgeschlossen werden. Hierzu informiert die Staatsanwaltschaft eine Ausgleichsstelle, die an die Beteiligten herantritt und zu vermitteln versucht. Welche Daten dürfen dabei von der Staatsanwaltschaft an die Ausgleichsstelle übermittelt werden?

Die Datenübermittlung ist in der Strafprozessordnung ausdrücklich erlaubt. Hierfür muss noch nicht endgültig feststehen, ob die Sache für einen Täter-Opfer-Ausgleich geeignet ist. Es genügt, dass die Ausgleichsstelle dies näher feststellen soll, etwa im Hinblick darauf, ob bei den Beteiligten hierzu eine Bereitschaft besteht. Die Staatsanwaltschaft darf aber nur Daten übermitteln, wenn dies **für die Durchführung des Ausgleichs** erforderlich ist. Viele Ermittlungsdaten, z. B. die persönlichen Angaben zu Zeugen, dürfen nicht weitergegeben werden.

Daraus folgt, dass in der Regel keine vollständigen Ermittlungsakten weitergegeben werden dürfen. Eine Ausnahme hiervon ist möglich, wenn es einen **unverhältnismäßigen Aufwand** bedeuten würde, die erforderlichen Angaben „auszusortieren“. Dies ist aber die Ausnahme, wenn etwa eine Vielzahl von Personen beteiligt ist oder der Vorgang mehrere Aktenbände umfasst.

Was ist zu tun?
Die Staatsanwaltschaft darf an die Täter-Opfer-Ausgleichsstelle Aktenauszüge oder Sachverhaltsschilderungen weitergeben. Die Weitergabe vollständiger Akten ist nur möglich, wenn dies bei äußerst komplexen Aktenvorgängen erforderlich ist, um den Täter-Opfer-Ausgleich durchzuführen.

4.3.8 Datenerhebung durch Betreuungsbehörden

In Betreuungssachen haben die Gerichte den Sachverhalt aufzuklären. Hierzu können sie sich der Hilfe durch die Betreuungsbehörden bedienen. Es kann streitig sein, in welchem Umfang die Betreuungsbehörde dabei selbstständig vorgehen darf.

Bei der Datenerhebung handelt die Behörde **eigenständig** und unabhängig vom Gericht. Sie hat sich im Rahmen der für sie geltenden Rechtsvorschriften zu bewegen; dies sind mangels spezialgesetzlicher Regeln die des Landesdatenschutzgesetzes. Danach darf die Betreuungsbehörde zunächst **die betroffene Person selbst** nach ihrer persönlichen Situation befragen. Dieser steht es frei, sich zu offenbaren. Hierüber ist sie vor dem Gespräch zu informieren, ebenso über den Zweck des Gesprächs. Soweit besonders geschützte Daten aus den Gesprächen festgehalten werden sollen, also etwa Angaben über die körperliche oder psychische Gesundheit, und keine besonderen Umstände dem entgegenstehen, ist eine schriftliche Einwilligung erforderlich.

Nur dann, wenn der oder die Betroffene eingewilligt hat, können auch **Dritte** in die Sachverhaltsaufklärung durch die Betreuungsbehörde einbezogen werden. Willigt die betroffene Person nicht ein, so kann die Betreuungsbehörde die Daten in der Regel nicht selbst erheben; dann ist das Gericht gefragt.

Ist die betroffene Person **nicht einwilligungsfähig**, ist die Befragung der nächsten Angehörigen im Rahmen des mutmaßlichen Interesses des Betroffenen möglich. In Ausnahmefällen kommt auch eine Datenerhebung bei sonstigen Dritten in Betracht, etwa bei Gefahren für die Gesundheit der betroffenen Person oder wenn eine entsprechende Patientenverfügung vorliegt.

Damit stehen der Betreuungsbehörde im Ergebnis Befugnisse zur Datenerhebung zur Verfügung, die häufig ausreichend sein dürften. Sofern die Behörde an der Datenerhebung rechtlich gehindert ist, obliegt es dem **Vormundschaftsgericht** tätig zu werden. Mit dieser Aufgabenverteilung soll verhindert werden, dass die „Ermittlungen“ der Betreuungsbehörde die Stellung der betroffenen Person im gerichtlichen Verfahren beeinträchtigen.

Was ist zu tun?
Die Betreuungsbehörden können Daten in der Regel nur bei den Betroffenen selbst erheben. Die Erhebung bei Dritten oder soweit es um Gesundheitsdaten geht, bedarf grundsätzlich der Einwilligung. Ist die Datenerhebung durch die Betreuungsbehörde so nicht möglich, muss sie durch das Gericht erfolgen.

4.4 Ausländerverwaltung

Auch im vierten Jahr nach den Anschlägen am 11. September 2001 hat sich an der Fixierung auf die unverhältnismäßige Überwachung von Ausländerinnen und Ausländern nichts geändert. Im Gegenteil: Nach dem In-Kraft-Treten des Zuwanderungsgesetzes hat sich die Kontrolle weiter verschärft.

Im Hinblick auf die Kontrolle der Ausländer verdient das Zuwanderungsgesetz nicht seinen Namen. Ebenso wie das Terrorismusbekämpfungsgesetz (24. TB, Tz. 4.5.2) ist das Anfang 2005 nach einigen politischen und rechtlichen Wirren in Kraft getretene Zuwanderungsgesetz darauf ausgerichtet, durch möglichst lückenlose Kontrollen Deutschland und Europa von Zuwanderern abzuschotten. Dem dienen zum einen der Ausbau bestehender Datenverarbeitungsstrukturen. So wird das **Ausländerzentralregister** (AZR) mit seiner Hauptdatei und seiner Visadatei ausgebaut. Verantwortlich ist für das weiterhin beim Bundesverwaltungsamt geführte AZR künftig das Bundesamt für Migration und Flüchtlinge. Das als Sicherheitsdatei konzipierte AZR erhält mit dem Anschluss der Sozialbehörden zusätzliche soziale Kontrollfunktionen. Im AZR bleiben weiterhin Staatsangehörige anderer EU-Mitgliedstaaten erfasst, obwohl das Verwaltungsgericht Köln schon Ende 2002 feststellte, dass die AZR-Speicherung von Unionsbürgern, die ein Recht auf Aufenthalt im Bundesgebiet haben, gegen das europarechtliche Diskriminierungsverbot verstößt.

Im **Aufenthaltsgesetz**, welches seit Anfang 2005 das Ausländergesetz ablöst, erfolgten weitere Regelungen, die gegen europäische Vorgaben verstoßen. So wird der europarechtlich vorgesehene Schutz von besonders sensiblen Daten per nationalem Gesetz faktisch aufgehoben. Entgegen dem ausdrücklichen Wortlaut der EU-Datenschutzrichtlinie soll es zudem im Ausländerrecht kein Recht der Betroffenen auf Widerspruch gegen Datenverarbeitungen geben. Beibehalten wurden alle Vorschriften, in denen Menschen nur deshalb ausländerrechtlichen Sicherheitsüberprüfungen unterworfen werden, weil sie – ohne jemals mit der Polizei in Konflikt gekommen zu sein – einer definierten Gruppe von Ausländern angehören. Damit nicht genug. Noch bevor das neue Gesetz Anfang 2005 in Kraft getreten war, hatte die Bundesregierung schon die ersten Änderungen vorgeschlagen, die auf eine weitere Intensivierung der Kontrolle hinauslaufen: weitere Datenbanken und Ausweitung des AZR auf die Arbeitsverwaltung.

Was ist zu tun?
Die Regelungen über die Erfassung von Ausländern müssen einer Generalrevision unterworfen werden. Zu überprüfen ist dabei nicht nur die Vereinbarkeit mit dem auch Nichtdeutschen zustehenden Grundrecht auf Datenschutz, sondern auch die Sinnhaftigkeit der ganze Ausländergruppen undifferenziert treffenden Kontrollregelungen sowie die Verletzung europarechtlicher Diskriminierungsverbote.

4.4.1 Die Europäisierung der Ausländerüberwachung

Große Teile des Aufenthalts- und Flüchtlingsrechts wurden inzwischen in die erste Säule der Europäischen Union integriert. Dies hat den Auf- und Ausbau von Datenbanken zur Folge, mit denen so genannte Drittausländer erfasst werden.

Drittausländer werden die Menschen genannt, die keine Staatsbürgerschaft eines EU-Mitgliedstaates haben. Deren **Erfassung in Datenbanken** findet mit der Europäisierung der Visa- und der Flüchtlingspolitik verstärkt auf europäischer Ebene statt. Dies gilt für das Schengener Informationssystem, in dem ausgewiesene, zurückgewiesene oder abgeschobene Drittausländer zur Fahndung ausgeschrieben sind, sowie für die Fingerabdruckdatenbank Eurodac, über die festgestellt werden kann, ob ein Flüchtling schon in einem anderen EU-Staat Zuflucht gesucht hat.

Der aktuellste Plan besteht im Aufbau eines **Visa-Informationssystems** (VIS), in dem die Erteilung von kurzfristigen Einreisesichtvermerken durch sämtliche EU-Mitgliedstaaten zusammengeführt wird. Ergänzt wird diese Datenbank durch einen regelmäßigen Datenaustausch zwischen den Mitgliedstaaten über Kurzzeitvisa. Mit VIS wird auf europäischer Ebene eine Datenspeicherung vorgesehen, die es bisher noch nicht einmal auf nationaler Ebene gab: Neben Angaben über die Beantragung, Ausstellung oder Verweigerung von Sichtvermerken sollen auch biometrische Daten, Gesichtsbilder und Fingerabdrücke, erhoben und zum Abgleich bereitgehalten werden. Die Daten sollen für Zwecke der Grenzkontrollen

automatisiert abgerufen werden können. Als Speicherfrist für Antragsdatensätze sind fünf Jahre vorgesehen. Anders als etwa die nationale AFIS-Datenbank wird die Nutzung der Daten ausschließlich auf aufenthaltsrechtliche Zwecke beschränkt. Dies ändert aber nichts an dem Umstand, dass gegenüber dem Eurodac eine Ausweitung hinsichtlich Datenumfang und Verwendungszusammenhängen erfolgt.

Diese europäischen Planungen gehen manchen Ländern im Bundesrat noch nicht weit genug. Diese forderten, dass VIS umfassend den Ausländerbehörden und den Sicherheitsbehörden zur Verfügung stehen soll. Wir haben den Vertretern des Landes Schleswig-Holstein dringend geraten, die **Ausweitung der Zwecke** von VIS, die Zulassung von direkten Abrufmöglichkeiten durch viele weitere Behörden und die Verlängerung der Speicherfrist auf zehn Jahre abzulehnen.

Was ist zu tun?
Bei dem Ausbau ausländerrechtlicher Datenbanken auf europäischer Ebene ist darauf zu achten, dass hierüber keine Diskriminierung von Angehörigen bestimmter Nationalitäten und Gruppen erfolgt, so wie dies auf nationaler Ebene der Fall ist. Die Zweckbindung der Daten ist zu beachten.

4.4.2 Ausländerrechtliche Rasterfahndung im Klassenzimmer

Nach der Feststellung, dass drei Schülerinnen und Schüler, die in städtischen Schulen unterrichtet wurden, keine Aufenthaltsgenehmigung in Deutschland hatten, forderte eine Ausländerbehörde von allen städtischen Schulen Klassenlisten an, um festzustellen, ob dies nur die Spitze eines Eisbergs sei.

Die Ausländerbehörde wollte die kompletten Klassenlisten nach ausländischen Kindern durchsuchen. Fast alle Schulen lieferten diese Listen prompt, ohne sich Gedanken über die Rechtmäßigkeit der Nachfrage zu machen. Wenige Schulen teilten „nur“ die Namen und Adressdaten ihrer ausländischen Kinder mit. Das anzuwendende Ausländergesetz erlaubt **Datenerhebungen ohne Kenntnis der Betroffenen** nur im Falle einer konkreten ausländerrechtlichen Maßnahme. Dies setzt jedoch voraus, dass die Daten der Betroffenen der Ausländerbehörde bereits bekannt sind. Die von der Stadt praktizierte Vorgehensweise, die an eine Rasterfahndung erinnert, sieht selbst das wenig datenschutzfreundliche Ausländerrecht nicht vor. Da mit den Klassenlisten auch die Daten der sich legal in Deutschland aufhaltenden ausländischen Kinder sowie aller deutschen Staatsangehörigen mit übermittelt wurden, wurde zudem gegen den **Erforderlichkeitsgrundsatz** verstoßen. Daher haben wir sowohl die Anfrage der Ausländerbehörde als auch die Datenübermittlungen der Schulen beanstandet. Die Stadt hat den Fehler eingeräumt und zugesagt, solche Datenerhebungen zukünftig nicht mehr vorzunehmen.

4.5 Verkehr

4.5.1 Begehrlichkeiten an den Autobahnmautdaten

Das Autobahnmautgesetz sieht die Erhebung von streckenbezogenen Gebühren für die Benutzung von Bundesautobahnen mit schweren Nutzfahrzeugen vor. Trotz eindeutiger Zweckbestimmungsregelungen sucht die Polizei nach Hintertüren, um an die Daten zu gelangen.

Das Autobahnmautgesetz legte unmissverständlich fest, dass die erhobenen Daten ausschließlich für die Abrechnung der Autobahnmaut verarbeitet und genutzt werden dürfen. Dies hinderte Strafverfolger nicht daran, die Mautdaten für eigene Zwecke zu beanspruchen (26. TB, Tz. 4.5.1). Um auch die letzten öffentlichen Zweifel zu beseitigen, hat der Bundestag über eine Gesetzesänderung die **Zweckbindung** unmissverständlich bekräftigt. Dies ändert aber nichts daran, dass die Begehrlichkeiten nach den technisch einmal erhobenen Daten, insbesondere nach den erfassten Kfz-Kennzeichen, weiter bestehen. Schon heute werden zunächst auch sämtliche Pkws videografiert, bevor diese Daten mangels Mautpflichtigkeit wieder gelöscht werden.

In einigen Ländern wurden inzwischen die Polizeigesetze um eine Regelung zur **Kennzeichenerfassung** ergänzt; in anderen Ländern stehen entsprechende Vorschläge zur Diskussion. Damit sollen nicht nur Lastkraftwagen, sondern sämtliche Fahrzeuge, die per Suchmeldung in polizeilichen Fahndungsbeständen gespeichert sind, ausfindig gemacht werden. Sobald dieses neue Instrument im Polizeirecht etabliert ist, ist es nur noch eine Frage der Zeit, wann die Zweckbindung des Mautgesetzes zugunsten der Polizei aufgehoben wird. Diese kann vortragen, dass es wirtschaftlich unsinnig ist, eine polizeiliche Überwachungsinfrastruktur auf Autobahnen aufzubauen, wenn eine solche für Mautzwecke von TollCollect schon vorgehalten wird.

Gegen die Kfz-Kennzeichenerfassung bestehen schwer wiegende Datenschutzbedenken: Mit ihr wäre die **Anonymität der Nutzung von Autobahnen** aufgehoben. Auch nur eine kurze Speicherung der Kennzeichendaten für Zwecke des Datenabgleichs hat zur Folge, dass sämtliche Kraftfahrzeuge zum Gegenstand polizeilicher Ermittlungen gemacht werden. Dieser informationelle Eingriff zeigt handfeste Auswirkungen, wenn – aus welchen Gründen auch immer – automatisch ein „Treffer“ gemeldet wird, der zwangsläufig zu einer polizeilichen Maßnahme, zumindest zu einer Halterüberprüfung führt. Die Eignung dieser Methode zur Bekämpfung schwerer Kriminalität ist dagegen gering: In Kenntnis der neuen Maßnahmen können sich gezielt vorgehende Straftäter z. B. durch Kennzeichenfälschung den Ermittlungen einfach entziehen.

4.5.2 A7 Richtung Norden – videoüberwacht

Vielen Autofahrern werden die mit Videokameras bestückten Masten entlang der Autobahn A7 Richtung Norden von der Landesgrenze Hamburg bis zum Autobahndreieck Bordesholm bereits aufgefallen sein.

Besorgte Bürgerinnen und Bürger haben sich deswegen an uns gewandt. Die Videokameras dienen der **Kontrolle des Standstreifens**. Dieser wird bei starkem Fahrzeugverkehr als dritte Fahrspur freigegeben und muss vor der Freigabe auf Hindernisfreiheit überprüft werden. Für andere Zwecke, insbesondere zur Verfolgung von Verkehrsordnungswidrigkeiten oder gar Straftaten, dürfen die Videobilder nicht verwendet werden. Wir haben uns vergewissert, dass die Auflösung der Kameras so gering ist, dass einzelne Kfz-Kennzeichen oder Fahrzeugführer während der Vorbeifahrt an den Kameras nicht erkannt werden können.

4.6 Schutz von Sozialdaten

4.6.1 Hartz IV und kein Ende

Zum Jahresbeginn 2005 trat das Sozialgesetzbuch Teil II (SGB II) in Kraft. An die Stelle von Arbeitslosen- und Sozialhilfe tritt teilweise das neue Arbeitslosengeld II. Alleine in Schleswig-Holstein sind hiervon ungefähr 200.000 Menschen betroffen. Bei der Zusammenlegung von Arbeitslosen- und Sozialhilfe spielte das Sozialgeheimnis leider oft keine Rolle.

Im Sommer 2004 verschickte die Bundesagentur für Arbeit (BA) bundesweit an über 2,2 Millionen Empfänger von Arbeitslosenhilfe **16-seitige Antragsvordrucke** zum Arbeitslosengeld II (ALG II). Schon wenige Tage später gingen unzählige Beschwerden und Fragen von verunsicherten Betroffenen bei uns ein. Tatsächlich enthält der Antragsvordruck viele Fragen, die aus Datenschutzgründen nicht gestellt werden dürfen. Gemeinsam mit der Bürgerbeauftragten für soziale Angelegenheiten haben wir Anfang August Ausfüllhinweise zu diesem Antragsvordruck veröffentlicht. Die bundesweite Nachfrage hiernach war groß. Die BA hat unsere Kritik angenommen und reagiert. Mitte September 2004 veröffentlichte die BA eigene Ausfüllhinweise und sagte eine Überarbeitung des Vordruckes zu. Bis Anfang März 2005 lagen jedoch noch keine Entwürfe vor. Die Zeit drängt jedoch, müssen doch schon im Juni 2005 hunderttausende Weiterbewilligungsanträge stellen.

www.datenschutzzentrum.de/allgemein/alg2.htm
www.arbeitsagentur.de

Auch die besten Ausfüllhinweise konnten nicht verhindern, dass durch die fehlerhaften Antragsvordrucke Daten beschafft wurden, die nicht erhoben werden

dürfen. Gemeinsam mit der Landeshauptstadt Kiel wurde ein „**vereinfachtes Antragsverfahren**“ entwickelt: Sozialhilfeempfänger in Kiel hatten die Wahl zwischen dem 16-seitigen Vordruck der BA oder einem einseitigen Antragsvordruck der Landeshauptstadt Kiel.

www.datenschutzzentrum.de/material/themen/presse/20040924-alg2.htm

Weiter kritisierten wir die mangelnde **Einweisung der Sachbearbeiter** durch die BA. Noch Wochen, nachdem die BA ihre Ausfüllhinweise veröffentlicht hatte, wurden vor Ort unzulässige Fragen gestellt. Frühzeitig forderten wir die BA auf, unzulässig erhobene Daten zu löschen, was von der Bundesregierung in einer Pressemitteilung auch zugesagt worden war.

In Schleswig-Holstein wird das ALG II seit Januar 2005 in den Kreisen und kreisfreien Städten von den **Arbeitsgemeinschaften** ausgezahlt. Lediglich die Kreise Nordfriesland und Schleswig-Flensburg haben von einer Optionsmöglichkeit Gebrauch gemacht und übernehmen diese Aufgabe in alleiniger Verantwortung. Zuständig für die Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften bei den **optierenden Kommunen** sind die Landesbeauftragten für den Datenschutz. Das Gleiche gilt für die Arbeitsgemeinschaften, die nach dem Willen des Gesetzgebers als Sozialleistungsträger tätig werden und in eigenem Namen Leistungsbescheide erlassen dürfen. Arbeitsgemeinschaften sind eigenverantwortlich Daten verarbeitende Stellen.

Der bundesweite Antragsvordruck war für uns nur der Einstieg in eine umfassende Prüf- und Beratungstätigkeit. Aus der gesamten Bundesrepublik wurden wir nach der Veröffentlichung unserer Hinweise mit Anfragen überhäuft. Wir erhielten von einzelnen Agenturen vor Ort in „Eigenregie“ entwickelte, noch umfangreichere Vordrucke mit der Bitte um Prüfung. Gemeinsam mit dem Bundesbeauftragten für Datenschutz (BfD) haben wir die BA aufgefordert, nur **autorisierte Vordrucke** zu verwenden. Wie sonst soll ein Antragsteller erkennen können, welcher Vordruck wirklich auszufüllen ist?

Als Nächstes erarbeiteten wir einen Katalog „**Offene datenschutzrechtliche Fragen zum SGB II**“. Über dessen Internetveröffentlichung sowie durch eine Unterrichtung der betroffenen Kommunen und Ministerien in Schleswig-Holstein versuchten wir, einen einheitlichen Informationsstand und ein erhöhtes Problembewusstsein herzustellen.

www.datenschutzzentrum.de/sozialdatenschutz/sgb2_fragen.htm

Viele der offenen Fragen lassen sich auf unschlüssige oder fehlende Regelungen im SGB II zurückführen. So ist z. B. die Zusammenarbeit der Arbeitsgemeinschaften untereinander bzw. mit der BA nicht ausreichend geregelt.

In der ARGE wird zur Leistungsberechnung das elektronische Verfahren A2LL eingesetzt. Bereits früh mussten wir feststellen, dass dieses Verfahren einen **bundesweiten Personenabgleich** ermöglicht. Jeder Mitarbeiter, der mit A2LL

arbeitet – vom Postboten bis zum Geschäftsführer –, hat die Möglichkeit, sich sämtliche Daten aller ALG-II-Bezieher jeder ARGE anzuschauen. Eine Protokollierung der Zugriffe und deren Kontrolle waren nicht vorgesehen. Über eine Schnittstelle zu einem weiteren Verfahren der BA (zPDV) bestand die Möglichkeit unkontrollierter Einsicht in Sozialdaten von Personen, die andere Leistungen bei der BA beziehen. Jeder Mitarbeiter erhielt also – im übertragenen Sinn – nicht nur den Generalschlüssel für das eigene Rathaus, sondern gleich die Schlüssel für alle Rathäuser und Arbeitsagenturen in der gesamten Bundesrepublik. Wir unterrichteten den BfD. Dieser beanstandete Ende 2004 gegenüber der BA formell das fehlende Zugriffs- und Berechtigungskonzept sowie die fehlende Protokollierung. Hätte man uns doch nur vorher gefragt!

Dadurch, dass die ARGE weitere Verfahren der BA einsetzt, verschärft sich die Situation erheblich. So sind z. B. im BA-Verfahren „coArb“ sensibelste Daten der Betroffenen über so genannte Vermittlungshemmnisse gespeichert. Jeder Mitarbeiter jeder ARGE erhält hierüber Kenntnisse über Suchtprobleme, gesundheitliche Einschränkungen, Ehe- oder Familienprobleme oder die Schuldensituation der Leistungsempfänger von Arbeitslosengeld.

Es stellen sich derzeit noch eine Vielzahl weiterer Fragen. Strittig ist z. B., in welchem Umfang die ARGE auf alte Datenbestände der Sozialämter oder der BA zugreifen darf. Durch ein „**Profiling**“ soll die ARGE die Stärken und Schwächen der Arbeit Suchenden feststellen. Es bedarf jedoch konkreter Vorgaben, in welchem Umfang hierfür Daten erhoben werden dürfen. Die ARGE schließt mit den Arbeit Suchenden eine „Eingliederungsvereinbarung“ ab, welche die Verpflichtung zum Besuch einer Schuldner-, Sucht- oder Familienberatungsstelle beinhalten kann. Dabei darf sie jedoch nicht Kenntnis von den sensiblen Gesprächsinhalten zwischen Arbeit Suchenden und Berater erhalten.

Um Hartz IV auch weiterhin datenschutzrechtlich zu begleiten, wurde auf Bundesebene eine Arbeitsgruppe eingesetzt, der u. a. auch ein Vertreter des ULD angehört.

Was ist zu tun?
Das Sozialgeheimnis ist auch bei der Zusammenlegung von Arbeitslosen- und Sozialhilfe zu wahren.

4.6.2 Drum prüfe, wer sich ewig bindet, ob er dabei den Datenschutz nicht vergisst

Wenn Menschen heiraten, ist das zumeist schön und sinnvoll. Wenn öffentliche Stellen fusionieren, mag dies ähnlich sein. Der Datenschutz darf hierbei nicht unberücksichtigt bleiben.

Die Statistischen Landesämter, die Datenzentralen und die Eichbehörden von Schleswig-Holstein und der Freien und Hansestadt Hamburg haben **fusioniert**. Der Medizinische Dienst der Krankenversicherungen Schleswig-Holstein (MDK) und der MDK Hamburg wollen es bis spätestens 2006 tun. Die AOK Schleswig-

Holstein hat es noch eiliger und möchte gerne mit der AOK Westfalen-Lippe gemeinsame Sache machen, die Innungskrankenkasse (IKK) des Landes ebenso mit der von Mecklenburg-Vorpommern. Und die Landesversicherungsanstalt (LVA) Schleswig-Holstein soll mit der LVA Hamburg und der LVA Mecklenburg-Vorpommern zusammengelegt werden.

Fusionen haben unbestritten manchen Vorteil, nicht nur finanzieller Art. Sie sollten aber wohl durchdacht und geplant werden, auch im Hinblick auf den Datenschutz. Die Krankenkassen, die LVA und der MDK verarbeiten überwiegend äußerst sensible medizinische Personendaten. Während und nach einer Fusion gilt es, die Verantwortlichkeiten für die Datenverarbeitung zu klären. Unter wessen Aufsicht soll die neue Daten verarbeitende Stelle liegen? Für die Stellen in Schleswig-Holstein ist derzeit das ULD zuständig. Wie ist dies aber nach der Fusion? Die AOK Schleswig-Holstein z. B. hat in den vergangenen Jahren nicht zuletzt aufgrund unserer **Kontrollen** einen hohen Datenschutzstandard für ihre Versicherten aufgebaut, der auch bei einer Fusion gehalten werden sollte. Wir favorisieren daher Lösungen, die die Zuständigkeit des ULD nicht vollständig aufheben.

Was ist zu tun?
Wenn Sozialleistungsträger fusionieren, sind die Fragen der Datenschutzkontrolle und des internen zukünftigen Datenschutzmanagements vertraglich verbindlich zu regeln.

4.6.3 Anzeige bei Verdacht auf Kindesmisshandlung an Krankenkasse, Polizei, Jugendamt und ...

Seit Anfang 2004 besteht für Ärzte die Pflicht zur Mitteilung von Krankheitsursachen und drittverursachten Gesundheitsschäden an die Krankenkassen. Mitteilungspflichtig sind Angaben über Berufskrankheiten, Arbeitsunfälle, sonstige Unfälle, Körperverletzungen, Impfschäden oder sonstige drittverursachte Gesundheitsschäden einschließlich Ursachen und mögliche Verursacher.

Die Änderung im Rahmen des Gesundheitsmodernisierungsgesetzes wurde im Vorfeld nicht öffentlich diskutiert. Welche heiklen Konflikte dadurch entstehen können, zeigt folgender praktischer Fall: Ein mehrfach körperlich und geistig behindertes Kind hatte sich beim Spielen verletzt. Die Eltern suchten umgehend den Arzt auf. Sie verstanden die Welt nicht mehr, als sie einige Zeit später Besuch von der Polizei bekamen und von den Beamten in Uniform vernommen wurden. Man habe **von der Krankenkasse** den **Hinweis** auf eine mögliche Kindesmisshandlung erhalten. Bei den Eltern kamen Zweifel an der Verschwiegenheit und der Vertrauenswürdigkeit ihres Arztes auf.

Was war geschehen? Der Arzt hatte die Krankenkasse – entsprechend der gesetzlichen Mitteilungspflicht – über den Unfall des Kindes informiert. Bei einem Unfall prüft die Krankenkasse, ob die ärztliche Behandlung aufgrund des Fehlver-

haltens eines Dritten erforderlich wurde, um gegebenenfalls Kostenersatz geltend machen zu können. Allein der Verdacht reicht hierfür nicht; der Verursacher muss beweissicher festgestellt werden. Dies ist bei Straftaten Aufgabe der Polizei. Daher **unterrichtete die Krankenkasse die Polizei** über eine mögliche Kindesmisshandlung zwecks Aufnahme von Ermittlungen. So kam es zu dem Besuch der Polizei.

Selbstverständlich muss alles unternommen werden, um Kindesmisshandlungen oder Kindesmissbrauch zu verhindern bzw. aufzuklären. Neben dem finanziellen Interesse der Krankenkassen und den strafprozessualen Interessen der Polizei müssen aber auch andere Interessen beachtet werden, so das Patientengeheimnis als Grundlage des Vertrauensverhältnisses zwischen Arzt und Patient. Die **Angst vor einer Strafverfolgung** darf nicht dazu führen, dass misshandelten Kindern die medizinische Behandlung vorenthalten wird.

Der **Arzt** selbst **muss entscheiden** können, wann die Polizei eingeschaltet wird. In bestimmten Fällen mag es genügen, das Jugendamt zu informieren. So gilt es, die familiäre Situation zu berücksichtigen. Krankenkassen haben grundsätzlich Abrechnungsaufgaben, wofür sie nur begrenzt Daten benötigen. Die wenigen vom Arzt erhaltenen Informationen reichen in der Regel nicht aus, um diese verantwortungsvolle Entscheidung treffen zu können.

Die AOK Schleswig-Holstein als betroffene Krankenkasse hat die Problematik erkannt. Gemeinsam konnte eine **interne Arbeitsrichtlinie** erarbeitet werden, die den Arzt in den Mittelpunkt des Verfahrens stellt. Erklärt ein Arzt, dass eine Einschaltung der Polizei nicht erforderlich oder kontraproduktiv ist, sind die Mitarbeiterinnen und Mitarbeiter der AOK Schleswig-Holstein an diese Entscheidung grundsätzlich gebunden. Die AOK zeigt damit, dass sie ihre Aufgaben verantwortungsbewusst wahrnimmt. Die Arbeitsrichtlinie ist veröffentlicht unter

www.datenschutzzentrum.de/medizin/arztprax/verdacht-kindesmissbrauch.htm

Was ist zu tun?
Ärzte und Krankenkassen sind aufgefordert, bei der Beachtung der Mitteilungspflicht von drittverursachten Gesundheitsschäden das Patientengeheimnis zu beachten.

4.6.4 Keiner zu Hause? Das Sozialamt schaut sich trotzdem die Wohnung an!

Aufgeregt schilderte uns eine Frau, dass Mitarbeiter des örtlichen Sozialamtes in ihrer Abwesenheit ihre Wohnung besichtigt hätten, obwohl sie weder Sozialhilfe beantragt habe noch beziehe. Der Untermieter, der Sozialhilfe beantragt hatte, habe die Beamten in die Wohnung gelassen.

Das Sozialamt bestätigte, dass nicht nur die Räume des Untermieters, sondern auch die Räume der Vermieterin geprüft worden sind. Man habe feststellen wollen, ob der Untermieter mit seiner Vermieterin in einer **eheähnlichen**

Gemeinschaft lebt. Bewusst habe man für diese Prüfung einen Zeitpunkt gewählt, zu dem die Vermieterin nicht zu Hause war.

Hausbesuche sind in Sozialhilfeverfahren nicht grundsätzlich unzulässig. Aufgrund des für den Betroffenen äußerst belastenden Charakters müssen diese jedoch das letzte Mittel sein, das nur dann eingesetzt wird, soweit es **zwingend erforderlich** ist. Stets ist zu prüfen, ob nicht andere, weniger belastende Mittel der Sachverhaltsfeststellung bestehen (23. TB, Tz. 4.7.3).

Im konkreten Fall deuteten bereits vor Durchführung des Hausbesuches **viele Indizien** auf eine eheähnliche Gemeinschaft zwischen Untermieter und Vermieterin hin. So war u. a. bekannt, dass die Hauptmiete vom Konto des Untermieters überwiesen wurde. Die Vermieterin bezahlte nach eigenen Angaben die Medikamente für den Untermieter und bezeichnete diesen gegenüber dem Amtsgericht als ihren Lebensgefährten. Diese Informationen hätten für die Annahme einer eheähnlichen Gemeinschaft genügt. Aus dem Protokoll des Hausbesuches ergab sich, dass zunächst die Räume des Untermieters besichtigt wurden. Hierbei wurde festgestellt, dass dieser über kein eigenes Bett verfügte. Gegenüber den Sozialamtsmitarbeitern erklärte der Untermieter, dass er im Schlafzimmer der Vermieterin schlafe und dort auch seine Kleidung aufbewahre. Spätestens zu diesem Zeitpunkt hätte das Sozialamt von einer eheähnlichen Gemeinschaft zwischen dem Untermieter und seiner Vermieterin ausgehen können. Eine Besichtigung der Räume der Vermieterin ohne deren Kenntnis und Einverständnis war nicht mehr erforderlich und wurde von uns beanstandet.

Was ist zu tun?
Hausbesuche dürfen nur in dem Umfang durchgeführt werden, wie dies erforderlich ist und keine anderen Möglichkeiten der Datenerhebung bestehen.

4.6.5 Wie eine Jugendhilfemaßnahme im Ausland das Jugendamt einholte

Nett und freundlich war der Brief aus Portugal: Eine Studentin, die ihr Auslandssemester an der Algarve absolvierte, bat das Jugendamt im kühlen Schleswig-Holstein um Mithilfe. Sie habe vom Instituto Algarve Projecto Unterlagen von Jugendlichen erhalten, die dort im Zeitraum von 1993 bis 2003 betreut wurden, um ein Forschungsvorhaben durchzuführen. Sie bat um das Ausfüllen eines dreiseitigen Fragebogens über den Werdegang eines dieser Jugendlichen.

Für diesen Jugendlichen war das Jugendamt in Schleswig-Holstein Kostenträger der Maßnahme gewesen. Das Jugendamt konnte und wollte nicht behilflich sein. Die Unterlagen über den Jugendlichen waren bereits gelöscht. Warum aber verfügte das Institut in Portugal noch über Unterlagen? Durften diese Unterlagen an eine Studentin weitergegeben werden? War der Betroffene unterrichtet, und hatte er zugestimmt? Dem Jugendamt stellte sich insbesondere die Frage, inwieweit es als Kostenträger die **Verantwortung für die Daten** bei dem Institut trägt.

Die Übermittlung von Sozialdaten ins Ausland ist an strenge Voraussetzungen geknüpft. Bei Mitgliedstaaten der Europäischen Union wird davon ausgegangen, dass ein dem deutschen Recht vergleichbares Datenschutzniveau gewährleistet ist. Die übermittelnde Stelle steht aber dennoch in der Pflicht, den Schutz der Sozialdaten bei der empfangenden Stelle sicherzustellen. So muss bereits bei der Übermittlung darauf hingewiesen werden, zu welchem Zweck die Übermittlung erfolgt und dass die Sozialdaten nur zu diesem Zweck verwendet werden dürfen. Durch **vertragliche Regelungen** sollte sichergestellt werden, dass die im Sozialdatenschutz geltenden Rechte der Betroffenen, zu denen auch der Löschungsanspruch gehört, beachtet werden. Aufbewahrungsfristen sind zu definieren. Das konkrete Forschungsvorhaben durfte nur mit Wissen und Einverständnis des Betroffenen durchgeführt werden.

Was ist zu tun?
Will sich ein Jugendamt bei der Erfüllung seiner Aufgaben der Hilfe einer anderen Einrichtung bedienen, so hat es durch eindeutige vertragliche Regelungen sicherzustellen, dass die Vorschriften zum Sozialdatenschutz beachtet werden. Dies gilt natürlich auch, wenn sich die andere Einrichtung im Ausland befindet.

4.6.6 Erhalten Taxifahrer eine Kopie der Patientenakte?

Die Gesundheitsreform hat manche Aufregung ausgelöst. Eine betraf die Einführung neuer Vordrucke für die Verordnung einer Krankenbeförderung. Damit die Krankenkasse die Kosten des Transports übernimmt, wurde der Arzt verpflichtet, auf dem Taxiformular auch die Diagnose des Patienten zu notieren. So können Patienten Risiken und Nebenwirkungen der Gesundheitsreform auch mit dem Taxifahrer besprechen.

Wenn sich ein Patient in stationäre oder ambulante Behandlung begeben muss und es aus gesundheitlichen Gründen nicht möglich ist, öffentliche Verkehrsmittel oder ein privates Fahrzeug zu benutzen, wird durch den behandelnden Arzt eine Krankenfahrt mit einem Mietwagen oder Taxi verordnet. Seit Anfang 2004 muss ein solcher Transport zuvor von der Krankenkasse genehmigt werden. Dies war bislang datenschutzrechtlich kein Problem, da der Taxifahrer nur einen Transportschein ohne sensible medizinische Daten erhielt. Mitte des Jahres wurde jedoch ein **neu gefasster Vordruck** für die Verordnung einer Krankenbeförderung eingeführt, auf dem auch die Diagnose einzutragen ist.

Nach Übermittlung des Formblatts an die Krankenkasse und deren Genehmigung muss der Patient die Verordnung – inklusive **Diagnose** – dem Taxifahrer aushändigen, der diese für seine Abrechnung bei der Krankenkasse einreicht. „Somit weiß auch der Taxifahrer, wenn ich einen Patienten mit chronischem Rektalulkus zum regelmäßigen Verbandswechsel an einen Chirurgen überweise“, empörte sich zu Recht ein Arzt über den Zwang zur Offenlegung medizinischer Geheimnisse.

Der gemeinsame Bundesausschuss von Ärzten und Krankenkassen kündigte nach der einstimmig von Datenschützern und Ärzten vorgetragenen Kritik eine daten-

schutzgerechte Neugestaltung der Bescheinigungen an, jedoch frühestens für Anfang 2005. Bis dahin galt es, eine **Übergangslösung** zu finden. Wir machten den Vorschlag, einen „Beförderungsgutschein“ zu erstellen, den die Krankenkasse nach Genehmigung anstelle der Verordnung dem Patienten aushändigt. Dieser Gutschein sollte keine medizinischen Angaben enthalten.

Die Spitzenverbände der Krankenkassen und die Kassenärztliche Bundesvereinigung einigten sich leider nur auf eine **Minimallösung** für eine Übergangszeit. Auf die Angabe der Diagnose wird bei einer Dauergenehmigung der Krankenkasse oder bei nicht planbaren Fahrten zu einer ambulanten Behandlung verzichtet. „Im Regelfall“ sind jedoch weiterhin Diagnosen anzugeben.

Sowohl die AOK als auch die IKK des Landes sowie Kassen anderer Bundesländer haben **datenschutzgerecht reagiert**. In Anlehnung an unseren Vorschlag händigt die Krankenkasse dem Patienten nach Genehmigung einer Krankenfahrt ein Genehmigungsschreiben aus, welches lediglich Name, Anschrift, Krankenversicherungsnummer und Angaben zu den genehmigten Fahrten (Abfahrt- und Zielort, eventuell Zuzahlung) enthält. Die ärztliche Verordnung verbleibt bei der Krankenkasse.

Der zuständige Bundesbeauftragte für den Datenschutz wurde durch die Kassenärztliche Bundesvereinigung und die Spitzenverbände der Krankenkassen im Zusammenhang mit der bis Anfang 2005 angekündigten Überarbeitung des Verordnungsvordruckes bisher nicht beteiligt. Wir favorisieren die Umsetzung eines „**Durchschreibeverfahrens**“. Der Vordruck sollte einen Durchschlag enthalten, auf dem nur die für die Abrechnung durch den Taxifahrer notwendigen Daten erkenntlich sind, nicht jedoch die Diagnose. Lediglich diesen Durchschlag würde der Patient zwecks Aushändigung an den Taxifahrer erhalten.

Was ist zu tun?
Die Kassenärztliche Bundesvereinigung und die Spitzenverbände der Krankenkassen sind angehalten, schnellstmöglich ein datenschutzkonformes Formular für die Verordnung einer Krankenbeförderung zu entwickeln.

4.7 Schutz des Patientengeheimnisses

4.7.1 Die elektronische Gesundheitskarte kommt

Mit der Gesundheitskarte Schleswig-Holstein wird in Flensburg das derzeit wohl am weitesten fortgeschrittene Pilotprojekt zur bundesweiten Einführung der elektronischen Gesundheitskarte durchgeführt. Die Beteiligten sind bei ihren rechtlichen, technischen und organisatorischen Lösungen bestrebt, nicht nur die elektronische Kommunikation mit Patientendaten zu erleichtern, sondern zugleich das Patientengeheimnis zu wahren.

Als Ende 2003 die Einführung der elektronischen Gesundheitskarte vom Bundesgesetzgeber beschlossen wurde, gingen noch alle Beteiligten davon aus, dass Anfang 2006 diese Karte bundesweit eingeführt werden könnte. Inzwischen zeigt

sich, dass dieser Zeitplan zu ehrgeizig war. Statt aber, wie bei anderen informationstechnischen Großprojekten, die Realisierung zu überstürzen und zu erzwingen, ist den Verantwortlichen klar, dass bei diesem **Mammutprojekt** strukturiert vorgegangen werden muss. Verantwortlich sind hier viele: nicht nur das Bundesgesundheitsministerium, sondern alle Beteiligten im Gesundheitswesen, von Arztpraxissoftwareherstellern über die Krankenkassen und die Verbände der verschiedenen Heilberufe bis hin zu den Krankenhäusern, ambulanten Ärzten und Apotheken. Alle diese Beteiligten sollen über eine Telematikinfrastruktur miteinander verknüpft werden, um hochsensible Patientendaten auszutauschen.

Dies darf und soll – insofern bestehen klare gesetzliche Vorgaben – nur unter Wahrung der ärztlichen Schweigepflicht und der Wahlfreiheit der Patienten geschehen. Lediglich das elektronische Rezept wird als medizinische Applikation verpflichtend eingeführt. Trotz dieser Gesetzeslage ist das Misstrauen in der Ärzte- wie in der Patientenschaft groß. Beide Gruppen befürchten, dass sie ihre Bestimmungsmöglichkeiten nicht nur über die Behandlungsdaten, sondern über den gesamten Behandlungsprozess verlieren könnten, wenn die Daten unkontrolliert in die Hände der Krankenkassen, der Pharmaunternehmen und der Gesundheitspolitik geraten. Ganz unbegründet sind diese Befürchtungen nicht angesichts der immer wieder neuen im Gesundheitswesen eingeführten Kontrollmechanismen. Doch haben Politiker, Gesundheitsfunktionäre wie auch die IT-Wirtschaft erkannt, dass ohne die Akzeptanz von Ärzten und Patienten die elektronische Gesundheitskarte nicht eingeführt werden kann. Eine der Voraussetzungen für diese Akzeptanz ist die Wahrung des Patientengeheimnisses.

Um das Patientengeheimnis beim elektronischen Datenaustausch zu wahren, bedarf es intelligenter technischer Lösungen. Der Schlüssel für die Souveränität des Patienten über seine Daten ist, dass er die Datenverschlüsselung mit seiner Karte selbst in der Hand behält. Daher legen wir Wert darauf, dass die Speicherung der elektronischen Rezepte auf Servern so erfolgt, dass ein Abruf nur in Kombination eines Arztschlüssels auf einem ärztlichen Berufsausweis, der Health Professional Card, mit dem individuellen Patientenschlüssel möglich ist. Eine solche **Ende-zu-Ende-Verschlüsselung** gewährleistet, dass weder die Krankenkassen noch neugierige Ärzte, geschweige denn sonstige interessierte Dritte ohne den Patienten auf die Daten zugreifen können.

Zwar befindet sich das Pilotprojekt der **Gesundheitskarte Schleswig-Holstein** mit nur wenig über 100 ausgegebenen Karten noch in einem frühen Stadium, doch ist das Projekt in Flensburg das wohl bundesweit technologisch am weitesten fortgeschrittene. Dies liegt zum einen an der Kartenstruktur, mit der die elektronischen Rezepte oder auch sonstige sensible Patientendaten mithilfe der Ende-zu-Ende-Verschlüsselung in einem sicheren elektronischen Postfach abgelegt werden. Dies liegt aber auch daran, dass dieses Projekt von langer Hand geplant und kooperativ mit allen Beteiligten realisiert wird. Nur so ist es möglich, dass keine wichtigen Interessen unter den Tisch fallen. Im Interesse der Wahrung der Patien-

teninteressen waren wir von einem frühen Stadium an beteiligt, bei der Ausgestaltung der Einwilligungserklärung ebenso wie bei der technischen Realisierung der Kommunikationsstrukturen. Der längste Weg bis zur flächendeckenden Einführung steht aber noch bevor: Nur durch eine umfassende Information und begleitende Unterstützung von Ärzte- und Patientenschaft ist es möglich, die für die Wahrnehmung informationeller Selbstbestimmung notwendige Kompetenz und damit die nötige Akzeptanz zu erreichen.

Was ist zu tun?
Bei der Einführung der elektronischen Gesundheitskarte muss behutsam vorgegangen werden. Um Wahlfreiheit und Patientengeheimnis sicherzustellen, sind die dauernde Begleitung durch Datenschutzbeauftragte und Patientenvertreter, demokratische Transparenz in jedem Planungsstadium und die Vermittlung von Medienkompetenz für die Anwender dringende Voraussetzungen.

4.7.2 Aktion „Datenschutz in meiner Arztpraxis“

Die Aktion „Datenschutz in meiner Arztpraxis“, die wir zusammen mit der Ärztekammer und der Zahnärztekammer 2001 ins Leben gerufen haben, geht in ein weiteres Jahr. Neben dem ambulanten Bereich setzen wir einen Schwerpunkt im stationären Bereich.

Im Rahmen der Fortsetzung der Aktion (24. TB, Tz. 4.8.8; 25. TB, Tz. 4.8.9; 26. TB, Tz. 4.7.2) erfolgten in Kooperation mit den Berufsschulen Schleswig-Holsteins erneut zahlreiche Präsentationen für **Auszubildende zum Beruf der Arzthelferin/Zahnmedizinische Fachangestellte**. Die Rückmeldungen der Auszubildenden über die Datenschutzpraxis in den Arztpraxen sind ermutigend. Bei Umfragen, die selbstverständlich für uns anonym bleiben, zeigt sich, dass gängige Fehler weniger werden, etwa das offene, für jedermann einsehbare Auslegen von Patientenkarten auf dem Empfangstresen. Wir werten dies als einen Erfolg unserer Aktion.

Die **bundesweite Nachfrage** nach unserem auch in diesem Jahr ausgeweiteten Informationsmaterial ist anhaltend groß. Unsere Beiträge sind nun auch Bestandteil des „Gesundheitsportals Schleswig-Holstein“ sowie von „Medfindex“ und werden hierüber erschlossen. Niedersachsen hat die Idee unserer Aktion übernommen und macht nun ebenfalls Ärzte für den Datenschutz mobil.

Wie angekündigt (26. TB, Tz. 4.7.3) weiteten wir unsere Aktion auf den **stationären Bereich** aus. Seitdem erreichen uns viele Beratungsersuchen von Krankenhäusern, die zu Hilfestellungen z. B. bei der Gestaltung von Aufnahmeverträgen, Schweigepflichtentbindungserklärungen, Archivregelungen usw. führen.

Über die DATENSCHUTZAKADEMIE Schleswig-Holstein bieten wir Ärzten und Mitarbeitern ein Ausbildungsangebot in Sachen Datenschutz. In speziell auf Ärzte zugeschnittenen **Fortbildungsseminaren** werden die grundlegenden Anforderungen des Datenschutzes vermittelt und aufgezeigt, mit welchen Mitteln das Patientengeheimnis in der Praxis gewahrt werden kann.

4.7.3 Krankenhaus ohne Behandlungsverträge

Behandlungs- oder Aufnahmeverträge sind in den Krankenhäusern nicht immer datenschutzgerecht. Dass ein großes Krankenhaus in Schleswig-Holstein gar keine schriftlichen Behandlungsverträge mit den Patienten abschloss, war selbst uns neu.

Eigentlich sollten wir nur die Frage beantworten, unter welchen Voraussetzungen ein Krankenhaus die Mikroverfilmung von Patientenakten durch eine externe private Firma durchführen lassen darf. Wir rieten dazu, den Behandlungsvertrag um eine entsprechende Erklärung der Patienten zur Entbindung von der Schweigepflicht zu ergänzen. Da es aber keinen Behandlungsvertrag gab, konnte auch keine Ergänzung vorgenommen werden. Nach kurzem Zögern und wohl auch aufgrund unseres nachdrücklichen Beratungsangebotes entschloss sich die Leitung des Krankenhauses, einen **datenschutzgerechten Behandlungsvertrag** zu entwerfen, der die datenschutzrechtlichen Vorschriften berücksichtigt. Ein erster Entwurf enthielt Hinweise über die gesetzlich vorgesehene Datenverarbeitung bei gesetzlich versicherten Patienten. Weiter wurden inhaltlich bestimmte und damit wirksame Erklärungen zur Entbindung von der Schweigepflicht aufgenommen, soweit Patientendaten, z. B. zum Zwecke der Mikroverfilmung oder Archivierung, an externe private Unternehmen übermittelt werden sollen.

Datenschutzgerecht gestaltete Behandlungsverträge sind eine unabdingbare Grundlage für die Wahrung der Datenschutzrechte der Patienten wie auch für eine rechtlich zulässige und effizient gestaltete Datenverarbeitung innerhalb des Krankenhauses. Bei Redaktionsschluss lag die endgültige Version des Behandlungsvertrages leider noch nicht vor. Wir planen eine datenschutzgerecht gestaltete Version eines **Musterbehandlungsvertrages** zu veröffentlichen unter

www.datenschutzzentrum.de/medizin/

Was ist zu tun?
Die Beachtung der ärztlichen Schweigepflicht beginnt in einem Krankenhaus mit datenschutzgerechten Behandlungsverträgen. Hierfür muss die Krankenhausleitung die Verantwortung übernehmen.

4.7.4 Wenn Krankenhaus und Radiologische Praxis (zu gut) zusammenarbeiten

Eine Klinik an der Westküste beherbergt in den eigenen Räumen eine selbstständige Radiologische Praxis. Werden Röntgenaufnahmen benötigt, können die Patienten des Krankenhauses an diese Praxis überwiesen werden. Den Patienten werden lange Wege erspart. Dies legitimiert aber noch nicht die pauschale Übermittlung sämtlicher Patientenstammdaten.

Im Rahmen der zweifellos sinnvollen Kooperation übermittelte das Krankenhaus pauschal die Stammdaten aller neuen Patienten an die Radiologische Praxis, unabhängig davon, ob für einen Patienten überhaupt eine Röntgenaufnahme benötigt wurde. Wenn mehrere Ärzte gleichzeitig oder nacheinander denselben Patienten untersuchen oder behandeln, so sind sie untereinander **von der Schweigepflicht** insoweit **befreit**, als das Einverständnis des Patienten vorliegt oder anzunehmen ist. So steht es in der Berufsordnung der Ärztekammer Schleswig-Holstein.

Liegt keine ausdrückliche Einwilligung des Patienten vor, wird dieser aber darüber unterrichtet, welche Ärzte ihn aus welchem Grund (weiter)behandeln werden, so liegt eine **Einwilligung durch schlüssiges Verhalten** vor, sofern der Patient der Überweisung an den weiterbehandelnden Arzt (hier die Radiologische Praxis) nicht widerspricht. Dann ist auch die Übermittlung der Patientendaten zulässig.

Am Tag der Aufnahme steht – zumindest für den Patienten – nicht fest, ob zukünftig eine Röntgenaufnahme benötigt wird. Es kann nicht davon ausgegangen werden, dass der Patient mit der Übermittlung seiner Daten an eine ihm unbekannte Röntgenpraxis einverstanden ist. Für eine Übermittlung von Patientendaten unabhängig von der aktuellen Behandlung bedürfte es einer **ausdrücklichen Einwilligung**, was z. B. auch für die Weitergabe an ein externes Labor gilt.

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

Das Krankenhaus veranlasste zwischenzeitlich die Löschung der Daten, die ohne die Einwilligung der Patienten an die Radiologische Praxis übermittelt wurden. Gemeinsam mit dem ULD wurde ein neuer **Aufnahmeantrag** entwickelt. Dieser bittet bereits bei der Aufnahme im Krankenhaus um Einverständnis zur Weitergabe der Stammdaten an die Radiologische Praxis. Ohne diese ausdrückliche Einwilligung werden fortan keine Daten übermittelt.

Was ist zu tun?
Die Vorschriften zur ärztlichen Schweigepflicht sind auch von Ärzten untereinander zu beachten. Bevor Daten von Patienten an dritte Stellen – dies können auch andere Ärzte sein – übermittelt werden, muss man sich der Einwilligung des Patienten versichern.

4.7.5 Säumige Privatpatienten sind kein Fall für das Sozialamt

Eine ältere Dame wurde stationär in einem Krankenhaus behandelt. Da sie privat versichert war, erhielt sie selbst die Rechnung. Groß war der Schreck, als sie zwei Monate später vom Sozialamt die Aufforderung erhielt, an einem der nächsten Tage im Amt mit Nachweisen über ihr Einkommen und Vermögen vorzusprechen. Man habe erfahren, dass sie die Behandlungskosten nicht beglichen habe.

Die völlig verunsicherte Dame fragte ihren Sohn: „Was hat das Sozialamt mit der Krankenhausrechnung zu tun?“ Dieser bat das ULD um Rat. Das Krankenhaus schaltete generell das Sozialamt ein, wenn ein privat versicherter Patient seine Rechnung nicht fristgerecht beglich. Die **Wahlleistungsvereinbarung** enthielt folgende Passage:

„Für den Fall, dass ich eine Selbstzahlerrechnung nicht fristgerecht begleiche, erkläre ich hiermit mein Einverständnis zur Weitergabe meiner erforderlichen personenbezogenen Daten gemäß § 3 Bundesdatenschutzgesetz an ein mit der Einziehung der Forderung beauftragtes Anwalts- oder Inkassobüro.“

Um unnötige Kosten für alle Beteiligten zu sparen, glaubte das Krankenhaus zur Unterrichtung des Sozialamtes berechtigt zu sein. Doch enthält das Bundessozialhilfegesetz hierfür keine **Offenbarungsbefugnis**. Eine Einwilligung zur Offenbarung ihrer Behandlungsdaten an das Sozialamt hatte die Patientin auch nicht erteilt. Auch wenn das Krankenhaus vermeintlich in guter Absicht handelte, hätte es zuvor die Patientin fragen müssen.

Auch eine Übermittlung an ein privates Inkassobüro darf nur dann erfolgen, wenn hierfür eine konkrete Übermittlungsbefugnis z. B. in Form einer wirksamen Einwilligung vorliegt. Die in der Wahlleistungsvereinbarung des Krankenhauses enthaltene Erklärung entfaltet jedoch trotz Unterschrift des Patienten keine rechtliche Wirkung, da die für eine **Schweigepflichtentbindungserklärung** bestehenden Anforderungen nicht erfüllt sind. Ein Patient kann anhand dieser Erklärung nicht erkennen, welche Daten konkret an welches Inkassobüro übermittelt werden. Zudem enthält die Erklärung keinen Hinweis zur Freiwilligkeit und Widerrufbarkeit.

Zuletzt: Der Verweis auf § 3 BDSG, der Begriffsbestimmungen regelt, ging völlig fehl. Hingegen ist ein Arzt berechtigt, ohne Einwilligung des Patienten mit der Geltendmachung einer offenen streitigen Forderung einen **Rechtsanwalt** zu **beauftragen** und hierfür die erforderlichen Daten zu übermitteln. Das Krankenhaus hat zwischenzeitlich die Erklärung zur Entbindung von der Schweigepflicht entsprechend unserer Vorgaben überarbeitet. Ein Muster für eine solche Erklärung findet sich unter

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

Was ist zu tun?
Eine Übermittlung von Daten säumiger Patienten an ein Sozialamt oder ein Inkassobüro ist ohne wirksame Einwilligung der betroffenen Patienten nicht zulässig. Bei der Abfassung einer Schweigepflichtentbindungserklärung sind datenschutzrechtliche Vorgaben zu beachten.

4.7.6 Zwei Arztpraxen, ein Aktenkeller, und der Sohn des Hausmeisters räumt auf

Die Meldung der *Lübecker Nachrichten* „Patientendaten in Müllcontainer" machte neugierig. Der Umweltdienst der Lübecker Polizei habe kistenweise Patientendaten und Röntgenbilder sichergestellt.

Was war geschehen? In einem Ärztehaus in der Lübecker Innenstadt residieren mehrere Arztpraxen. Zwei Arztpraxen teilten sich einen **Aktenkeller**. Akten von Patienten, deren Behandlung abgeschlossen war, wurden in diesem Aktenkeller aufbewahrt. Da der Keller aus allen Nähten zu platzen drohte, wurde der Sohn des Hausmeisters gebeten aufzuräumen. Dieser machte sich die Arbeit leicht und stellte kurzerhand die nicht mehr benötigten Patientenakten zu den Mülltonnen, damit die städtische Müllabfuhr den Rest erledigte. Doch die Mitarbeiter der Müllabfuhr zeigten mehr Sensibilität als die Ärzte und meldeten den Fund der Polizei. Gleich in drei Punkten wurde hier die ärztliche Schweigepflicht verletzt.

Das Patientengeheimnis ist auch zwischen den Arztpraxen zu beachten. Durch die **gemeinsame Nutzung eines Aktenkellers** war nicht auszuschließen, dass Mitarbeiter der einen Praxis unbefugt auf Patientenakten der anderen Praxis zugreifen konnten. Aufgrund unserer Ermittlungen wurden die Aktenkeller getrennt.

Will man einen Dritten, wie den Sohn des Hausmeisters, damit **beauftragen**, Patientenakten zu vernichten, so ist auszuschließen, dass dieser unbefugt Kenntnis vom Akteninhalt nehmen kann. Kaum ein Patient dürfte damit einverstanden sein, dass der Sohn des Hausmeisters in Patientenakten schmökern kann. Der verantwortliche Arzt sagte uns zu, dass der Sohn des Hausmeisters zukünftig nicht mehr beauftragt wird.

Mehr zur Patientendatenverarbeitung im Auftrag unter


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

Die **Entsorgung** von Patientenakten im allgemeinen Müll ist ebenfalls nicht datenschutzgerecht. Zu groß ist die Gefahr, dass die Patientenakten in falsche Hände – nicht nur die der Mitarbeiter der Müllabfuhr – gelangen. Aktenvernichtung ist einfach und sicher möglich, wie die Gütesiegel bestätigen, die das ULD an zwei Aktenvernichtungsunternehmen in Schleswig-Holstein vergeben hat.


www.datenschutzzentrum.de/guetesiegel/index.htm

Was ist zu tun?
Das Patientengeheimnis endet nicht mit dem Abschluss einer Behandlung. Bei Archivierung und Vernichtung muss der verantwortliche Arzt ausschließen, dass Unbefugte von Patientendaten Kenntnis nehmen können.

4.7.7 Anwaltsauftrag der Privatärztlichen Verrechnungsstelle zur dritten Mahnung

Darf die Privatärztliche Verrechnungsstelle (PVS) ein selbstständiges Anwaltsbüro damit beauftragen, die dritte Mahnung von säumigen Patientinnen und Patienten vorzunehmen, ohne dass eine direkte Beauftragung durch die Ärzte erfolgt?

Begibt sich ein Privatpatient in ärztliche Behandlung und will der Arzt nicht persönlich die Abrechnung vornehmen, so schaltet dieser oft die PVS ein. Erforderlich ist hierfür das **schriftliche Einverständnis des Patienten**, da mit der Abwicklung der Abrechnung die Offenbarung von Patientengeheimnissen verbunden ist. Die PVS erstellt anhand dieser Daten Rechnungen und fordert die Patienten zur Zahlung auf.


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

Ein Arzt unterrichtete das ULD darüber, dass die PVS ein **Anwaltsbüro** mit der dritten Mahnung **beauftragt**, wenn Patienten auf die Zahlungsaufforderung und vorangegangene Mahnungen nicht reagieren. Eine ausdrückliche Beauftragung durch den jeweiligen Arzt erfolgte nicht, ja dieser wusste überhaupt nicht, welchen Anwalt er angeblich beauftragt hatte. Diese Praxis entsprach nicht den Anforderungen an eine rechtmäßige Offenbarung von Patientendaten von der PVS an den Anwalt.

Die Einschaltung eines Anwaltsbüros bedingt eine Offenbarung von personenbezogenen Daten, die der ärztlichen Schweigepflicht unterliegen. Der Arzt ist zwar berechtigt, Patientendaten zum Zwecke der Geltendmachung von Forderungen einem Anwalt zu offenbaren, und darf sich bei der Beauftragung auch eines Bevollmächtigten, hier der PVS, bedienen. Dabei muss allerdings gewährleistet sein, dass der **Arzt „Herr des Geschehens“** bleibt, d. h., dass er zu jeder Zeit weiß, wer über welche Daten verfügt bzw. an wen welche Daten übermittelt werden. Es wäre ein Widerspruch, wenn bei der Entbindung von der Schweigepflicht die genaue Benennung des Datenempfängers gefordert würde, bei einer Anwaltsbeauftragung dagegen nicht.

Aus diesem Grunde benötigt die PVS für die Übermittlung von Patientendaten an einen Anwalt eine **ausdrückliche schriftliche Vollmacht** des jeweiligen Arztes. Dabei ist das Anwaltsbüro, das beauftragt werden soll, ausdrücklich zu benennen. Nur so werden die hohen Anforderungen an die medizinische Vertraulichkeit bei der Einschaltung eines Anwaltsbüros eingehalten. Die von der PVS genutzten Vordrucke einer „Honoraranweisung“ genügten diesen Anforderungen zunächst nicht. Die von der PVS eingeschaltete Kanzlei war nicht ausdrücklich genannt.

Nach eingehender Erörterung wurde mit der PVS mittlerweile eine akzeptable Einigung erzielt. In den Vordrucken wird nun gemäß unseren Vorgaben die Kanzlei ausdrücklich benannt. Im Falle eines Anwaltwechsels steht den Ärzten ein jederzeitiges Widerspruchsrecht zu.

4.8 Wissenschaft und Bildung

4.8.1 Fachhochschulen – Prüfungen im Doppelpack

Zwei Institutionen mit identischer Aufgabenstellung, nahezu gleiche Sicherheitsprobleme bei der personenbezogenen Datenverarbeitung, völlig unterschiedliche Abarbeitung der Prüfungsergebnisse – auch auf diese Weise zeigt sich die Datenschutzrealität.

Wenn Institutionen gleiche Aufgabenstellungen haben, müsste auch die Ausgestaltung der Datenverarbeitungsprozesse in etwa gleich sein. Die technischen und organisatorischen Maßnahmen zur Datensicherheit müssten ein einheitliches Niveau aufweisen. Bei zwei zeitgleich durchgeführten Prüfungen in den Fachhochschulen Lübeck und Flensburg haben wir im abgelaufenen Berichtszeitraum die **Probe aufs Exempel** gemacht.

Zunächst waren wir überrascht über die durchaus unterschiedlichen technischen und organisatorischen Lösungen im Bereich der Verarbeitung der personenbezogenen Studenten- und Mitarbeiterdaten. Die **sicherheitstechnischen Schwachstellen** waren dagegen nahezu identisch und hielten sich zudem in dem Rahmen, den wir bei vielen Landes- und Kommunalbehörden zu kritisieren haben:

- Die Dokumentationen und Dienstanweisungen waren unvollständig,
- es fehlten Sicherheitskonzepte und Risikoanalysen,
- die Passwortgestaltung war nicht ausreichend,
- die Löschungsregelungen waren unzureichend,
- nicht alle Datenbestände waren den jeweils Verantwortlichen zugänglich und
- Personalunterlagen wurden teilweise nicht verschlossen verwahrt.

Große Unterschiede zwischen den beiden Fachhochschulen ergaben sich jedoch zu unserer Überraschung bei der **Abarbeitung der jeweiligen Prüfungsberichte** und der Umsetzung unserer Verbesserungsvorschläge. Während die Fachhochschule Flensburg uns zeitnah eine Stellungnahme übersandte und darin die Abstellung der Mängel meldete bzw. entsprechende Maßnahmen ankündigte, reagierte die Fachhochschule Lübeck völlig anders. In ihrer Stellungnahme wurde sowohl die korrekte Darstellung der Verfahrensweisen bestritten als auch den sicherheitstechnischen Bewertungen widersprochen. Doch waren die schriftlichen Ausführungen in sich voller Widersprüche. Diese aufzuklären ist uns trotz einiger Mühen bislang nicht gelungen. Den vorläufigen „Höhepunkt“ eines sehr zähen Schriftwechsels bildet die Aussage, bestimmte Unterlagen unterlägen dem Datenschutz und könnten uns daher nicht vorgelegt werden.

Wir haben die Erörterungen an dieser Stelle zunächst abgebrochen und der Fachhochschule mitgeteilt, dass unter solchen Umständen mit einem Konsens nicht zu rechnen sein dürfte. Es liegt an der Fachhochschule, die **offenen Fragen** umfassend zu beantworten und ihrerseits konstruktiv zur Aufklärung der Sachverhalte beizutragen.

Was ist zu tun?
Die Fachhochschule Flensburg sollte den eingeschlagenen Weg zur Optimierung der sicherheitstechnischen Maßnahmen konsequent fortsetzen und den dann erreichten Standard halten. Die Fachhochschule Lübeck muss ihre Datenschutzpraxis ändern.

4.8.2 CAU startet Datenschutzmanagement

Ausgelöst durch frühere Missstände beim Datenschutz hat das Rektorat der Christian-Albrechts-Universität zu Kiel eine Arbeitsgruppe „Datenschutz" gegründet, deren Ziel es ist, den Datenschutz innerhalb der Organisationsstrukturen zu verbessern.

Aufgrund der komplizierten Strukturen einer Hochschule mit Instituten, Fakultäten und einer traditionellen Selbstständigkeit der einzelnen Einrichtungen und der Freiheit von Forschung und Lehre ist dieses Unterfangen nicht einfach; die Universität wird hierbei vom ULD tatkräftig unterstützt. Erste Maßnahme war die Herausgabe von **Hinweisen zur Gewährleistung des Datenschutzes** für alle Bereiche der Universität. Darin wird erstmals verbindlich und nachvollziehbar festgelegt, wer für die Datenverarbeitung innerhalb der Hochschule verantwortlich ist. Weiterhin werden besondere Verhaltensregeln im Umgang mit personenbezogenen Daten aufgestellt.

Das ULD begrüßt diese Initiative ausdrücklich, die – sofern sie konsequent weiterverfolgt wird – in ein echtes Datenschutzmanagement münden kann und damit die personenbezogene Datenverarbeitung innerhalb der Hochschule deutlich verbessert.

Was ist zu tun?
Die Arbeit der Arbeitsgruppe „Datenschutz" sollte kontinuierlich fortgeführt werden und in ein langfristiges Datenschutzmanagement einmünden.

4.8.3 Laufabzeichen im Sportunterricht? Eine noch bessere Sache mit Datenschutz!

Jährlich findet an schleswig-holsteinischen Schulen ein so genannter Lauftag statt. Hauptsponsor dieses sportlichen Ereignisses mit mehr als 85.000 Teilnehmerinnen und Teilnehmern ist die AOK Schleswig-Holstein. Als „Gegenleistung" für ihr finanzielles und personelles Engagement will diese die Daten von Schülern mit Billigung des Bildungsministeriums auch für Werbezwecke nutzen.

Die AOK des Landes wurde in der Vergangenheit hinsichtlich ihrer Datenerhebungspraxis bei Schülerinnen und Schülern für Werbezwecke von uns kritisiert. Dies mag der Grund dafür gewesen sein, dass sie dieses Mal den Dialog mit dem ULD vor Beginn ihrer Aktion suchte. Gemeinsam fanden wir eine Lösung, die **für alle Beteiligten** (Schule, Lehrer, Eltern und Schüler) eine größere **Transparenz** beim Umgang mit den für den Lauftag genutzten Daten brachte. Die Schülerinnen und Schüler werden auf den Teilnahmebögen explizit um ihre Einwilligung in die Datennutzung für Werbezwecke gebeten. Die Schulen wurden aufgefordert dafür Sorge zu tragen, dass den Schülern dieses Vorgehen in verständlicher Weise vermittelt wird. Darüber hinaus sollte sichergestellt werden, dass die Eltern zeitnah informiert werden, um ihnen die Möglichkeit zu geben, die Entscheidung ihrer Kinder zu beeinflussen oder gar zu revidieren.

Die AOK nimmt in ihre Datenbank für Werbezwecke nur Schülerinnen und Schüler auf, die bereits 15 Jahre alt sind und der Speicherung zugestimmt haben. Ab diesem Alter kann davon ausgegangen werden, dass die Betroffenen hinsichtlich der Bedeutung und der Folgen der Einverständniserklärung genügend **einsichtsfähig** sind. Die Daten aller anderen Veranstaltungsteilnehmer werden nur zur Abwicklung der Verteilung der von der AOK ausgelobten Preise verwendet. Die AOK stellt darüber hinaus sicher, dass die Daten von Betroffenen sofort gelöscht werden, wenn von Eltern oder Schülerinnen und Schülern nachträglich Einwände gegen die Datenverarbeitung für Werbezwecke erfolgen. Rückfragen besorgter Eltern und kritische Anmerkungen von Schulleitern zeigten uns trotz des datenschutzfreundlichen Grundkonzeptes, dass noch ein weiterer Verbesserungsbedarf besteht. Die AOK zeigte sich aufgeschlossen.

Was ist zu tun?
Bei einer künftigen Organisation des Lauftages sollten weitere datenschutzrechtliche Verbesserungen angestrebt werden.

4.8.4 Schulverwaltungsrechner gehen online

Nach längerem Stillstand treibt das Bildungsministerium die Anbindung der Schulverwaltungsrechner an das Landesnetz voran, sodass hierüber auch eine sichere Internetkommunikation möglich wird.

Um den Schulen untereinander und mit den Schulaufsichtsbehörden und dem Bildungsministerium eine sichere Kommunikation sowie einen geschützten Zugang zum Internet zu ermöglichen, unterbreiteten wir im Jahre 2001 Vorschläge zur sicheren Anbindung der Schulverwaltungsrechner an das **Datennetz des Landes**. Lange hat sich nichts getan (26. TB, Tz. 4.8.1). Nun wird damit begonnen, unseren Vorschlag umzusetzen. In Kooperation mit den Schulträgern macht sich das Land daran, den Schulverwaltungen den Weg zur elektronischen Kommunikation zu ebnen. Wir beteiligen uns in Form von Beratung und durch Unterstützung beim Erstellen der technischen Konzepte sowie bei der organisatorischen Umsetzung innerhalb der Schulen.

4.9 Steuerverwaltung

Niemand zahlt gerne Steuern, und alle wollen Steuergerechtigkeit. Es ist aber zweifelhaft, ob die Steuermoral durch steuerliche Personenkennzeichen, heimliche Kontenabfragen und Verpflichtungen zur Internetnutzung gehoben wird.

Bereits im letzten Tätigkeitsbericht hatten wir die Frage gestellt, ob die **wuchernde Steuergesetzgebung** nicht den Blick für die Verhältnismäßigkeit der immer neuen Eingriffe in die informationellen Selbstbestimmungsrechte der Bürger verstellt (26. TB, Tz. 4.9.1). Die Proteste gegen die einzelnen Rechtsvorschriften hielten sich vor einem Jahr noch in Grenzen, wohl weil man deren Tragweite noch nicht voll erkannt hatte. Es war nur eine Frage der Zeit, bis die Betroffenen kritische Fragen nach dem Nutzen und den Risiken stellen würden. Zwischenzeitlich regt sich in der Öffentlichkeit tatsächlich ein umso stärkerer Widerstand, je klarer das Ausmaß der geplanten Datenbestände und ihrer Nutzung wird.

- **Identifikationsnummer**

> ***Im Wortlaut: § 139a Abs. 1 AO***
>
> *Das Bundesamt für Finanzen teilt jedem Steuerpflichtigen zum Zwecke der eindeutigen Identifizierung im Besteuerungsverfahren ein einheitliches und dauerhaftes Merkmal (Identifikationsmerkmal) zu.*

In immer mehr Publikationen werden Vergleiche zwischen der steuerlichen Identifikationsnummer mit dem bereits vor Jahren als verfassungswidrig verworfenen **Personenkennzeichen** angestellt. Schon hinsichtlich des persönlichen Anwendungsbereichs ist fraglich, ob das Gebot der Verhältnismäßigkeit beachtet wird: Die Nummern werden nicht nur den tatsächlich Steuerpflichtigen, sondern bereits allen Neugeborenen zugeteilt und zentral gespeichert. Zudem sieht das Gesetz keine hinreichend klare Zweckbindung bei der Nutzung des Kennzeichens vor. Mit der umfassenden

Nutzungserlaubnis „zum Zwecke der eindeutigen Identifizierung in Besteuerungsverfahren“ wird eine übergreifende Ermächtigung erteilt. Eine Nutzung der Identifikationsnummer für beliebige Zwecke durch private Stellen, die die Nummer zwangsläufig ständig in der täglichen Wirtschafts- und Finanzkommunikation angeben müssen, ist nicht wirksam zu verhindern. Damit kann sie sich zu einem Baustein für einen Überwachungsapparat im gesamten Bereich der wirtschaftlichen Betätigung entwickeln.

- **Kontenanfrage**

Sind die kritischen Stimmen zur Identifikationsnummer zurzeit erst vereinzelt zu hören, nimmt der Protest gegen die so genannte Kontenabfrage sehr konkrete Formen an. Wissenschaftliche Gutachten konstatieren „den typischen Fall der verfassungswidrigen Datenerhebung für unbestimmte und auch nicht bestimmbare Zwecke auf Vorrat“ (Tz. 2.2). So weit mochte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder noch nicht gehen. Aber auch sie fordert in einer Entschließung, dass die staatliche Kontenkontrolle auf den Prüfstand muss. Die Neuregelung erlaubt nämlich einen **Online-Zugriff auf Bankdaten**, die von den Kreditinstituten bereits seit April 2003 zur Aufdeckung illegaler Finanztransaktionen und vor allem zur Terrorismusbekämpfung nach dem Kreditwesengesetz vorgehalten werden müssen. Dabei handelt es sich um Kontenstammdaten der Bankkunden und sonstigen Verfügungsberechtigten (Name, Geburtsdatum, Kontonummern).

Im Wortlaut:
§ 24c Abs. 1 Kreditwesengesetz

Ein Kreditinstitut hat eine Datei zu führen, in der unverzüglich folgende Daten zu speichern sind:

1. *die Nummer eines Kontos ...*
2. *der Name sowie bei natürlichen Personen der Tag der Geburt des Inhabers ...*

...
Das Kreditinstitut hat zu gewährleisten, dass die Bundesanstalt jederzeit Daten aus der Datei ... in einem von ihr bestimmten Verfahren automatisiert abrufen kann. Es hat durch technische und organisatorische Maßnahmen sicherzustellen, dass ihm Abrufe nicht zur Kenntnis gelangen.
...

Nunmehr sollen neben den Finanzbehörden auch andere Behörden, z. B. die zahlreichen **Sozialleistungsträger**, Auskunft erhalten, wenn die anfragende Behörde ein Gesetz anwendet, das „an Begriffe des Einkommenssteuergesetzes“ anknüpft und eigene Ermittlungen dieser Behörde ihrer Versicherung nach nicht zum Ziel geführt haben oder keinen Erfolg versprechen. Welche Behörden dies sein sollen, geht aus dem Gesetz nicht eindeutig hervor. Da das Einkommenssteuerrecht eine Vielzahl von Begriffen verwendet (neben

Im Wortlaut: § 93 Abs. 8 AO

Knüpft ein anderes Gesetz an Begriffe des Einkommenssteuergesetzes an, soll die Finanzbehörde auf Ersuchen der für die Anwendung des anderen Gesetzes zuständigen Behörde oder eines Gerichtes über das Bundesamt für Finanzen bei den Kreditinstituten einzelne Daten ... abrufen und der ersuchenden Behörde oder dem ersuchenden Gericht mitteilen ...

„Einkommen“ und „Einkünfte“ auch „Wohnung“, „Kindergeld“, „Arbeitnehmer“), ist nicht klar, welche Behörden letztendlich Auskunftsersuchen stellen dürfen. Dies ist jedoch nach dem verfassungsrechtlichen Bestimmtheitsgebot unverzichtbar. Zudem wird nicht deutlich, welche Zwecke Auskunftsersuchen rechtfertigen und nach welchen Regeln sie erfolgen sollen.

Von der Tatsache des Datenabrufs erfahren die Kreditinstitute und Betroffenen zunächst nichts. Die Betroffenen erhalten nach dem Gesetz hiervon allenfalls bei einer Diskrepanz zwischen ihren Angaben und den Ergebnissen der Kontenabfragen Kenntnis, nicht jedoch bei einer Bestätigung ihrer Angaben durch die Kontenabfragen. Die Auskunft erstreckt sich zwar nicht auf die Kontostände, aufgrund der durch den Abruf erlangten Erkenntnisse können jedoch in einem zweiten Schritt weitere Überprüfungen auch im Hinblick auf die Guthaben direkt beim Kreditinstitut erfolgen. Dass Betroffene von Abfragen, die zu keiner weiteren Überprüfung führen, nichts erfahren, widerspricht dem **verfassungsrechtlichen Transparenzgebot**. Danach sind sie von der Speicherung und über die Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Geschieht dies nicht, hat das zur Konsequenz, dass die Rechtsschutzgarantie des Artikel 19 Abs. 4 Grundgesetz verletzt wird. Die öffentliche Empörung über das geplante Verfahren verursachte inzwischen zumindest aufseiten des Bundestages verstärkte Sensibilität. So wird darüber diskutiert, per Verwaltungsregelung die Betroffenen über einen Abruf nachträglich zu informieren.

Das Bundesfinanzministerium hat im November 2004 die „Verbesserungen der Ermittlungsmöglichkeiten für Finanzbehörden und andere Behörden und Gerichte ab 01.04.2005“ wortreich mit dem „Grundrecht auf Besteuerungsgleichheit“ verteidigt, ohne aber vertieft auf die zu beachtende Verhältnismäßigkeit einzugehen. Letztendlich wird das **Bundesverfassungsgericht** über die Rechtmäßigkeit der Verfahrensweise entscheiden.

- **Zwang zur Internetnutzung**

Der dritte strittige Komplex betrifft die Verpflichtung aller Unternehmer und Arbeitgeber, ab dem 1. Januar 2005 die Umsatzsteuervoranmeldungen und die Lohnsteueranmeldungen auf elektronischem Wege an die Finanzämter zu übermitteln. Die notwendigen technischen Voraussetzungen hierfür sind ein Internetzugang und eine für die Datenübermittlung geeignete Software. Lapidar stellt das Bundesfinanzministerium zu seinem „**ELSTER-Verfahren**“ (**elektronische Steuererklärung**) in einem Merkblatt fest: „Die Funktion der korrekten elektronischen Datenübermittlung ist bereits in vielen gängigen Steuersoftwareprodukten integriert.“

Ein Steuerpflichtiger fragte uns: „Inwieweit ist es verfassungsrechtlich abgesichert, bei der Erfüllung einer Forderung nur einen einzigen, an erhebliche und teure Voraussetzungen gebundenen Verfahrensweg einhalten zu müssen, damit die Forderungsstelle daraus kostengünstigere Vorteile erzielen kann?“ Andere Steuerpflichtige wiesen darauf hin, dass der Staat sie zwinge, ihr IT-System mit einem **Netzwerk** zu verknüpfen, das per Definition **unsicher** sei und bei dem sie

mangels eines haftbaren Netzbetreibers keine Gewährleistungsansprüche hätten. Außerdem sei das Risiko, dass wegen der fehlenden Authentisierung Hacker oder Spaßvögel gefälschte Anmeldungen abgeben könnten, noch nicht ausreichend untersucht worden. Die Möglichkeit, dass das Finanzamt „zur Vermeidung von unbilligen Härten“ auf eine elektronische Übermittlung verzichten kann, hielten sie für ein „Feigenblatt“. Was sei denn eine unbillige Härte?

Dies dürfte in der Tat der entscheidende Punkt sein. Nur wenn die Finanzämter bezüglich der **Ausnahmegenehmigungen** großzügig verfahren, wird man einen Proteststurm der Klein- und Kleinstunternehmen und -arbeitgeber abwenden können. Eine staatlicherseits rigide durchgesetzte Pflicht zur Internetkommunikation ist auch unter Sicherheitsgesichtspunkten nicht zu vertreten. Das Hauptproblem liegt nicht nur in der Absicherung gegen Netzangriffe durch eine Transportverschlüsselung, sondern insbesondere in der Abwehr von Attacken gegen die an das Netz angeschlossenen Rechnersysteme. Unter Umständen ergibt sich hieraus bald eine staatlich verordnete Firewall-Pflicht.

Im Wortlaut: § 18 Abs. 1 Satz 1 Umsatzsteuergesetz

Der Unternehmer hat bis zum 10. Tag nach Ablauf jedes Voranmeldungszeitraums eine Voranmeldung nach amtlich vorgeschriebenem Vordruck auf elektronischem Weg nach Maßgabe der Steuerdatenübermittlungsverordnung zu übermitteln.
...

Im Wortlaut: § 41a Abs. 1 Einkommenssteuergesetz

...

Die Lohnsteueranmeldung ist nach amtlich vorgeschriebenem Vordruck auf elektronischem Weg nach Maßgabe der Steuerdatenübermittlungsverordnung zu übermitteln.
...

Was ist zu tun?
Auf die Identifikationsnummer sollte verzichtet, die Kontenabfrage sollte transparenter und differenzierter gestaltet und ein Zwangsinternetanschluss ausschließlich für steuerliche Zwecke vermieden werden.

4.9.1 Stand der Gesetzgebung zum Datenschutz im Steuerbereich

Viele Bestimmungen der Abgabenordnung tragen noch die Handschrift des Obrigkeitsstaates, zu dessen Zeit sie entstanden sind. Die Anpassung an das moderne europäische Datenschutzniveau fällt dem Bundesgesetzgeber schwer.

Während die Änderungen der Gesetze zum Zweck einer vollständigen Erfassung und Abwicklung steuerpflichtiger Vorgänge und Sachverhalte einander in einem rasanten Tempo folgen (Tz. 4.9), tut sich der Bundesgesetzgeber nach wie vor schwer, das steuerliche Verfahrensrecht in der Abgabenordnung an das Niveau der EU-Datenschutzrichtlinie anzupassen (25. TB, Tz. 4.6). Dabei stehen seit Jahren eine ganze Reihe von **Themen auf der Tagesordnung**, die dringend einer datenschutzrechtlichen Klärung bedürfen. Als die wichtigsten sind zu nennen:

- **Akteneinsichts- und Auskunftsrecht**

Gegen diese in praktisch allen anderen Verwaltungsbereichen bestehende gesetzliche Regelung sperrt man sich nach wie vor mit dem Hinweis auf Missbrauchsmöglichkeiten. Dass es hiergegen wirksame Ausnahmebestimmungen geben kann, will man nicht wahrhaben.

- **Befugnisse zur Auftragsdatenverarbeitung**

Die Wirkung des Steuergeheimnisses bei der Einschaltung externer Dienstleister bleibt weiterhin ungeklärt. Gleichzeitig werden mehr und mehr Verarbeitungsprozesse in Bereiche verlagert, für die das Steuergeheimnis nicht gilt.

- **Datentransfer zwischen den einzelnen Besteuerungsverfahren**

Die Steuerverwaltung betrachtet sich als eine informationstechnische Einheit. Daten, die für ein Besteuerungsverfahren erhoben worden sind, sollen auch für alle anderen Verfahren verfügbar sein. Dies steht im Widerspruch zum datenschutzrechtlichen Zweckbindungsgrundsatz.

- **Kontrollmitteilungen**

Da es sich hierbei um die klassische Form der Datenspeicherung auf Vorrat handelt, bedarf es einer verfassungskonformen Regelung, die dem Grundsatz der Verhältnismäßigkeit Rechnung trägt.

- **Löschung von Daten, Aufbewahrungsfristen**

Im Hinblick auf die Sensibilität der bei der Besteuerung anfallenden Daten kommt ihrer zeitgerechten Löschung eine besondere Bedeutung zu. Darüber, wie lange diese Daten „steuerlich relevant“ sein können, lässt sich trefflich streiten. Eine gesetzliche Klarstellung ist geboten.

Daneben bestehen weitere Möglichkeiten, die Abgabenordnung so zu gestalten, dass die Steuerpflichtigen stärker als bisher den Eindruck gewinnen können, dass die **Gebote der Fairness und der Transparenz** auch im Besteuerungsverfahren gelten. Hierüber wird derzeit in einer so genannten Koordinierungsrunde zwischen den Datenschutzbeauftragten des Bundes und der Länder und dem Bundesfinanzministerium verhandelt.

Was ist zu tun?
Der Bundesgesetzgeber sollte sich einer raschen Anpassung der Abgabenordnung an das Niveau der EU-Datenschutzrichtlinie nicht länger widersetzen.

4.9.2 Steuergeheimnis und Privatinsolvenzen II

Wenn jemand einen Brief bekommt, bei dem das Anschriftenfeld einen Hinweis auf ein bestehendes Insolvenzverfahren enthält, geht er von einer Verletzung des Steuergeheimnisses aus. Das muss nicht zwingend so sein, auch wenn die Adressierung zweifelsfrei fehlerhaft ist.

Wer so sehr in finanzielle Schwierigkeiten gerät, dass er eine Privatinsolvenz beantragen und sich unter die Kuratel eines Insolvenzverwalters begeben muss, befindet sich verständlicherweise in einer Stresssituation. Wenn dann auch noch das Finanzamt sich nicht so verhält, wie man es erwartet, ist dies besonders schmerzlich. So war es für die Ehefrau eines unter Insolvenz stehenden Steuerpflichtigen überraschend, dass ihr Einkommenssteuerbescheid dem Insolvenzverwalter bekannt gegeben werden durfte (26. TB, Tz. 4.9.2). In diesem Berichtszeitraum beschwerten sich mehrere Steuerpflichtige darüber, dass in dem **Anschriftenfeld von Fensterbriefumschlägen** der Post, die sie von den jeweiligen Finanzämtern erhalten hatten, erkennbar war, dass sie insolvent waren (vgl. Tz. 4.1.4). Sie sahen hierin einen Bruch des Steuergeheimnisses.

Unsere Nachprüfungen ergaben, dass es sich um Eingabefehler bei der Erfassung der so genannten Stammdaten gehandelt hatte. Diese wurden unverzüglich bereinigt. Einen Bruch des Steuergeheimnisses wollten die Finanzämter in den Fehlern nicht sehen. Dass z. B. ein Briefträger nicht erkennen sollte, dass der Empfänger eines Schreibens sich in Insolvenz befindet, wurde nicht bestritten. Aufgrund der Tatsache, dass dieser Umstand im **jedermann zugänglichen Insolvenzregister** veröffentlicht werde, handele es sich aber nicht mehr um ein steuerliches „Verhältnis“, das durch das Steuergeheimnis geschützt sei. Das habe die Rechtsprechung so bestätigt. Dieser Standpunkt ist formal zwar richtig, wird die Steuerpflichtigen jedoch nicht überzeugt haben. Für sie haben die Fehler der Finanzämter zu nachweisbaren „Beschwernissen“ geführt.

Was ist zu tun?
Bei der Behandlung von rechtlich und persönlich problematischen Steuerfällen sollten die Finanzämter eine besondere Sorgfalt walten lassen. Hierauf haben die betreffenden Steuerpflichtigen einen Anspruch.

4.9.3 Eine Lohnsteuerkarte zu viel

Lohnsteuerkarten, auch soweit sie noch nicht mit Eintragungen des Arbeitgebers versehen sind, enthalten Daten, die dem Steuergeheimnis unterliegen. Bekommt ein Arbeitnehmer nicht nur seine, sondern auch die seines Nachbarn zugesandt, hat die zuständige Meldebehörde ein Problem.

Die Kommunen sind in ihrer Eigenschaft als **Meldebehörden** Teil der Steuerverwaltung. Die Daten der Melderegister unterliegen damit zumindest zum Teil dem Steuergeheimnis. Dieser Umstand spielt in der täglichen Praxis eines Meldeamtes eine untergeordnete Rolle. Wenn aber z. B. bei der Versendung der Lohnsteuer-

karten neben der eigenen auch die Karte des Nachbarn im Briefumschlag steckt, wird das Steuergeheimnis virulent.

So geschehen im November 2004: Eines Morgens hatten unsere Mitarbeiter alle Hände voll zu tun, um die telefonischen Proteste gegen die **fehlerhafte Kuvertierung** entgegenzunehmen und die Frage zu beantworten, was denn mit der anderen Lohnsteuerkarte zu tun sei. Andere Arbeitnehmer, die bis dahin noch keine Steuerkarte im Briefkasten gefunden hatten, fragten an, ob ihr Exemplar möglicherweise in falsche Hände gelangt wäre.

Bei der von vielen Kommunen beim Rechenzentrum von dataport in Auftrag gegebenen Versendeaktion war ein **technischer Fehler** aufgetreten: Just das Modul, das Fehlkuvertierungen verhindern sollte, arbeitete nicht einwandfrei. So kam es zu dem zunächst unbemerkten Effekt, dass oft zwei Steuerkarten in einem Umschlag steckten. Die Aktion wurde gestoppt und das Gerät erst nach einer Reparatur wieder eingesetzt. Aus Sicht des Rechenzentrums handelte es sich um das technische Restrisiko, das aufgrund der Fehlererkenntnisse im Rahmen einer Neukonzeption weiter reduziert werden soll.

Alle betroffenen Meldebehörden wurden über diesen Vorfall informiert. Leider reagierten diese nicht mit der gleichen Konsequenz. Erst spät und teilweise erst nach unserer Intervention erläuterten sie den Lohnsteuerkartenempfängern durch **Presseveröffentlichungen**, was vorgefallen war, und gaben Hinweise, was mit den „zusätzlichen“ Steuerkarten geschehen sollte. Ihre Verantwortung für das Steuergeheimnis war den meisten Behörden gar nicht bewusst. Es mag kein strafrechtlich relevantes Verhalten vorgelegen haben. Doch zeigte es sich, dass sie die nach wie vor bei ihnen liegende Verantwortung für die routinemäßige alljährliche Versendungsaktion aus dem Auge verloren hatten. Das ist ein problematischer Nebeneffekt des Outsourcing (Tz. 6.1).

Was ist zu tun?
Technische Fehler beim Auftragnehmer sind nicht gänzlich zu verhindern. Wenn aber einmal etwas passiert, ist es Aufgabe des verantwortlichen Auftraggebers, unverzüglich für Schadensbegrenzung zu sorgen.

5 Datenschutz in der Wirtschaft

5.1 Querschnittsprüfungen in der Kreditwirtschaft – erste Ergebnisse

Die Zahl der Beschwerden über Kreditinstitute ist in den letzten Jahren spürbar gestiegen. Daher haben wir hier im Berichtszeitraum mit Querschnittsprüfungen begonnen.

Die Ergebnisse einer Sparkassenprüfung dürften exemplarisch sein: Wir mussten die Bestellung und Tätigkeit des **betrieblichen Datenschutzbeauftragten** beanstanden: Unvereinbarkeit mit der gleichzeitigen Funktion als Geldwäschebeauftragter, mangelhafte Schulung neuer Mitarbeiter, fehlende Überprüfung der Filialen, keine periodischen Tätigkeitsberichte, zu geringer Arbeitszeitanteil für die Funktion als Datenschutzbeauftragter. Das Bundesdatenschutzgesetz verlangt vom Unternehmen, personenbezogene EDV-Verfahren in einem Register zu dokumentieren. Dieses **Verfahrensregister** war unvollständig z. B. bezüglich konkreter Anwendungen oder der Benennung von Löschfristen. Bei einem Verfahren zur Auswertung von Kundendaten erfolgte keine **Protokollierung** der Änderungszugriffe. Bei einem Verfahren „Finanzdienstleistungsfiliale“ konnten Kundendaten aus unterschiedlichen Vertragsverhältnissen zusammengeführt und ausgewertet werden; es bestand zudem die Gefahr des Missbrauchs von Freitextfeldern.

Zur Einschätzung des Kreditrisikos wurden bei einem so genannten automatisierten **Scoring** Angaben zum Familienstand der Kunden ausgewertet. Für uns war der Bezug der Angaben „verheiratet“, „verwitwet“, „ledig“, „geschieden“, „getrennt lebend“ oder „eheähnliche Lebensgemeinschaft“ zur Vertragserfüllung nicht ersichtlich, weshalb wir eine Beanstandung aussprachen. Die fehlende Unterrichtung der Kunden über die Zweckbestimmung der Datenerhebung beim Scoring war ein weiterer Kritikpunkt. Da die Verfahren beim Scoring einrichtungsübergreifend festgelegt werden, löste unsere Prüfung eine grundsätzliche Diskussion aus, bei der zwischen uns und den Vertretern der Kreditinstitute noch viele Fragen strittig sind.

So genannte Löschlisten, mit denen die Löschung von Daten aus dem **Schuldnerverzeichnis** der Amtsgerichte mitgeteilt werden, müssten nach ihrer Auswertung unverzüglich vernichtet werden. Die bisherige Praxis der langfristigen Aufbewahrung der Löschlisten wurde auf unseren Hinweis hin sofort eingestellt. Auch die bisherige Praxis der Einholung von **SCHUFA-Abfragen**, selbst bei reinen Guthabenkonten, wurde nach unserer Kritik aufgegeben.

Teilweise trafen wir auch **vorbildliche Praktiken** an: Eine Analyse zur Kundenzufriedenheit mithilfe eines im Schalterraum aufgestellten Monitors wurde völlig anonym durchgeführt. Werbeschreiben an Kunden wurden nur versandt, wenn deren Einwilligung vorlag. Bezüglich der technisch-organisatorischen Datensicherheitsmaßnahmen, der Personalaktenführung und der eingesetzten Videoüberwachung hatten wir keinen Anlass zur Beanstandung.

Was ist zu tun?
Die Prüfungserfahrungen des ULD werden über Gespräche mit übergeordneten Einrichtungen auch auf andere Kreditinstitute übertragen. Weitere Kreditinstitute werden zu überprüfen sein.

5.2 Kommt der gläserne Mieter?

Mieterwarndateien spielen auf dem Wohnungsmarkt eine immer größere Rolle. Damit wird die Gefahr begründet, dass offene Zahlungsforderungen aus völlig anderen Lebensbereichen dazu führen, dass Menschen nicht mehr oder nur noch schwer einen Mietvertrag bekommen.

Wir kritisierten schon die Geschäftsfelderweiterung der SCHUFA auf den Bereich der Wohnungswirtschaft, die es Vermietern ermöglicht, durch SCHUFA-Anfragen die allgemeine Kreditwürdigkeit potenzieller Mieterinnen und Mieter zu durchleuchten (26. TB, Tz. 5.7). Mit Blick auf die existenzielle Bedeutung von Wohnraum für alle Menschen ist es nicht hinnehmbar, wenn die Weitergabe von Informationen, z. B. über eine nicht gezahlte Handyrechnung, am Ende den **Erhalt angemessenen Wohnraums** behindert oder gar ausschließt. Leider hat sich die Position der Betroffenen zwischenzeitlich weiter verschlechtert: Neue Anbieter von Mieterwarndateien drängen auf den Markt. Zudem beschaffen sich Vermieter zunehmend Informationen allgemeiner Auskunfteien, z. B. von Creditreform oder Infoscore. Mittlerweile liegen uns viele Einzelfallbeispiele vor. So wurde einer allein erziehenden Mutter in Neumüster unter Verweis auf ihre allgemein schlechte wirtschaftliche Lage der Abschluss eines Mietvertrages verweigert. Da die Anfragen bei Auskunfteien oft von größeren Wohnungsgesellschaften mit einem dichten Bestand von Wohnungen in ganzen Stadtteilen vorgenommen werden, kann es für die Betroffenen schwierig werden, dort überhaupt noch Fuß zu fassen.

Im Berichtszeitraum erreichten uns zwei Anfragen zur Errichtung von speziell für Vermieterinteressen geplante **meldepflichtige Warndateien**. Die vorgestellten Geschäftsmodelle stießen bei uns auf erhebliche datenschutzrechtliche Bedenken. Vermieteranfragen bei der Warndatei sollten durch die Einwilligung der Betroffenen legitimiert werden. Angesichts der oft bei der Wohnungssuche bestehenden Zwangslage dürfte regelmäßig die für die Einwilligung erforderliche Freiwilligkeit fehlen. Pläne der Betreiber, sehr weit gehende und oft ungesicherte Informationen über Mieterinnen und Mieter aus ganz unterschiedlichen Lebensbereichen vorzuhalten, können von uns nicht akzeptiert werden. Allenfalls die im Rahmen von Gerichtsverfahren gesicherten Informationen, z. B. Titel aus Räumungsklagen, mit einem Bezug auf das konkrete Verhalten von Betroffenen im Mieterverhältnis können die Speicherung zum Zweck der Weitergabe an andere Vermieter rechtfertigen. Ob die geplanten Datenbanken tatsächlich in Betrieb gehen werden, war zum Zeitpunkt der Berichterstellung noch offen.

Was ist zu tun?
Wohnungswirtschaft und Auskunfteien müssen damit rechnen, zukünftig verschärft auf die Einhaltung der genannten gesetzlichen Vorgaben geprüft zu werden. Das berechtigte Interesse von Vermietern an Kreditwürdigkeitsabfragen über potenzielle Mieter begegnet erheblichen rechtlichen Bedenken.

5.3 Bonitätsabfrage bei kostenlosen Testangeboten

Die Neugierde von Unternehmen über mögliche Kunden treibt manche hässliche Blüten. Wenn keine vertraglichen Bindungen eingegangen werden und kein kreditorisches Risiko besteht, darf sich ein Unternehmen bei einer Auskunftei auch keine Daten beschaffen.

Der Anbieter eines Informationsangebotes für Webseiten musste seine **Praxis der Vertragsanbahnung** korrigieren. Er warb mit einem für drei Monate kostenfreien Testangebot mit speziell dafür geschaffenen Internetseiten für das jeweilige Gewerbe. Ein Freiberufler meldete sich auf das verlockende Angebot und ließ sich für einen Platz im Internetangebot des Unternehmens registrieren. Er staunte nicht schlecht, als er kurze Zeit später eine unbegründete Absage erhielt. Noch überraschter war er über die Auskunft erst auf seine Nachfrage hin, eine Bonitätsabfrage bei einer bundesweit aktiven Auskunftei habe ergeben, dass ihm die notwendige Kreditwürdigkeit fehle.

Eine Bonitätsauskunft wegen der Reservierung für ein zunächst kostenfrei bleibendes Angebot ist unzulässig. Voraussetzung für die Einholung von solchen Auskünften ist ein „berechtigtes Interesse“. Hieran fehlt es, wenn dem anfragenden Unternehmen zunächst in keiner Weise ein **kreditorisches Risiko** entsteht. Das Unternehmen hat zwischenzeitlich seine Anfragepraxis den gesetzlichen Bestimmungen angepasst.

Was ist zu tun?
Durch ein effektives Datenschutzmanagement haben die Auskunfteien sowie die anfragenden Unternehmen sicherzustellen, dass Anfragen ohne berechtigtes Interesse nicht gestellt bzw. nicht beantwortet werden. Liegen über entsprechende Schutzvorkehrungen keine ausreichenden Nachweise vor, so können aufsichtsbehördliche Maßnahmen nötig werden.

5.4 Die äußerst fremdnützige Bonitätsabfrage

Eine steigende Anzahl von Privatunternehmen spezialisiert sich auf das scheinbar lukrative Geschäft des Handels mit Informationen über ihre Mitbürger. Viele private Unternehmen führen wegen ihres kreditorischen Risikos routinemäßig bei der Vertragsanbahnung Abfragen bei Auskunfteien durch. Da passiert es auch schon einmal, dass einzelne Mitarbeiter die eröffneten Abfragemöglichkeiten für ganz private Zwecke missbrauchen.

Als im Verlauf eines Rechtsstreits von der Gegenseite plötzlich eine Auskunft der Firma Bürgel vor Gericht präsentiert wurde, wandte sich ein Bürger Hilfe suchend an uns. Die Anfrage zu den Vermögensverhältnissen des Betroffenen war durch ein Unternehmen erfolgt, zu welchem zu keinem Zeitpunkt geschäftliche Beziehungen bestanden. Die **Buchhalterin des Unternehmens** hatte die Abfrage eigenmächtig durchgeführt, um ihre Cousine mit negativen Informationen für einen Prozess gegen den Betroffenen zu „munitionieren".

Die Abfrage der Kreditwürdigkeit des Betroffenen als auch die unbefugte Weitergabe für das anhängige Gerichtsverfahren waren erhebliche Verstöße gegen den Datenschutz. Wir mussten gegen die Verantwortliche ein der Schwere des Eingriffs angemessenes **Bußgeld** verhängen.

Was ist zu tun?
Verantwortliche Stellen, bei denen regelmäßig Auskunfteiabfragen durchgeführt werden, müssen ihre Mitarbeiter auf die Folgen unberechtigter Auskunfteiabfragen zu privaten Zwecken hinweisen. Missetäter haben mit empfindlichen Geldbußen zu rechnen.

5.5 Erhebung von Ausweisdaten bei der EC-Kartenzahlung

Viele Geschäfte und Kaufhäuser bieten die EC-Kartenzahlung als Zahlungsmöglichkeit an. Dabei müssen die Kundinnen und Kunden aufpassen, dass sie die Nutzung der kundenfreundlichen Zahlungsmöglichkeit nicht mit der Offenlegung ihrer Privatsphäre bezahlen.

Einzelhandelsunternehmen verlangen nicht selten die Vorlage eines Personalausweises oder Reisepasses, wenn Bürger Produkte unter Einsatz einer EC-Karte bezahlen wollen. Teilweise werden die personenbezogenen Daten des Kunden notiert, eine **Kopie des Ausweises** angefertigt und dem EC-Zahlungsbeleg für die Bank beigefügt. Mit diesem Verfahren wollen sich die Unternehmen gegen Betrug schützen und die Durchsetzung ihrer Forderung verbessern.

Stichprobenkontrollen der Ausweise sind problemlos möglich. Hierbei wird ausschließlich die Namensgleichheit des Bezahlenden mit dem Karteninhaber festgestellt. Die Speicherung personenbezogener Daten kommt jedoch nur bei einer **EC-Kartenzahlung mit Unterschrift** in Betracht. Bei Nutzung des PIN-Verfahrens wird die Freigabe des konkreten Zahlungsbetrages online bei dem kartenausgebenden Kreditinstitut eingeholt. Die Deckung des Betrages wird in Echtzeit bestätigt. Eine Identifizierung zur Forderungsrealisierung ist hier daher nicht erforderlich.

Bei der EC-Kartenzahlung mit Unterschrift kann eine kurzzeitige Speicherung von Name und Anschrift erfolgen, wenn durch **gut erkennbare Hinweisschilder** an der Kasse auf den Zweck der Erhebung hingewiesen wird. Wegen der besonderen Umstände – dem Zeitdruck an der Kasse – kann auf die Schriftlichkeit der Einwilligung verzichtet werden. Eine über die Erfassung von Name und Anschrift hinausgehende Anfertigung einer Ausweiskopie ist als eine nicht erforderliche Datenerhebung in der Regel unzulässig.

Die Freiwilligkeit der Einwilligung setzt voraus, dass an den Kassen zusätzlich eine **andere angemessene Zahlungsmöglichkeit** eingeräumt wird. Beim Verkauf vorwiegend hochpreisiger Waren sollte außer der Barzahlung noch eine weitere Zahlungsmöglichkeit bestehen. Kunden ist es kaum zuzumuten, große Barbeträge mit sich zu führen, um die eigenen personenbezogenen Daten nicht preisgeben zu müssen.

Den Namen und die Anschrift des Kunden darf das Unternehmen nur bis zum **Zeitpunkt der Zahlung** durch das Kreditinstitut vorhalten. Daher sollten Unternehmen aus praktischen Gründen davon Abstand nehmen, Name und Anschrift auf den EC-Kartenbelegen zu notieren. Soweit sie längerfristigen Aufbewahrungsfristen – z. B. den handels- und steuerrechtlichen Aufbewahrungsfristen von sechs oder sogar zehn Jahren – unterliegen, wäre eine aufwändige Schwärzung von Name und Anschrift nach Abwicklung der Zahlung durchzuführen. Die Adressdaten dürfen von den Kreditinstituten während der Speicherdauer ausschließlich dazu verwendet werden, im **Falle einer Nichtzahlung** ihren jeweiligen Zahlungsanspruch durchzusetzen. Insbesondere eine Zusammenführung und Auswertung zu anderen Zwecken, z. B. Marktforschung oder Werbung, ist unzulässig.

Was ist zu tun?
Kunden sollten vor einer EC-Kartenzahlung mit Unterschrift prüfen, ob ihr Name und ihre Anschrift aufgenommen werden, und sich unter Umständen für eine datensparsamere Zahlungsart entscheiden. Kunden, die ihre personenbezogenen Daten bereits angegeben haben, können sich nach Abbuchung der EC-Zahlung von ihrem Konto bei dem Unternehmen die Löschung ihrer Daten bestätigen lassen.

5.6 Personalausweis als Zwangspfand in der Disko

Im Berichtszeitraum häuften sich Beschwerden über die Eingangskontrolle von Diskotheken.

Eine Diskothek verlangte von ihren minderjährigen Besuchern die Hinterlegung des Personalausweises an der Eingangstür als Pfand. Der Ausweis wurde erst wieder herausgegeben, wenn die Jugendlichen die Diskothek verließen. Auf ihre Nachfrage, was dies soll, erhielt eine Besucherin zur Antwort: „Hier machen wir die Gesetze!“ Uns teilte die Diskothek mit, die Ausweiskontrollen dienten der Altersfeststellung der Diskothekenbesucher nach dem **Jugendschutzgesetz**. Die Minderjährigen hätten grundsätzlich mehrere Möglichkeiten der Pfandhinterlegung. Allerdings fehlte es an einem deutlichen Hinweis auf die Alternativen.

Das Personalausweisgesetz erlaubt die Verwendung des Personalausweises im Bereich der Privatwirtschaft als Ausweis- und Legitimationspapier sowie zur Altersfeststellung für Zwecke des Jugendschutzes. Da der Personalausweis im Besitz des Betroffenen steht, ist er grundsätzlich auch als Pfand geeignet. Die Hinterlegung des Ausweises muss aber freiwillig sein und darf den Jugendlichen nicht aufgezwungen werden. Pfandalternativen sind Handy, Schlüsselbund, Uhr oder Ähnliches. Wir haben der Diskothek im Interesse verbesserter Transparenz vorgeschlagen, an geeigneter Stelle im Eingangsbereich auf die Tatsache der Ausweiskontrolle und Notwendigkeit der **Pfandhinterlegung** mit einem Schild hinzuweisen, und gleich einen Formulierungsvorschlag mitgeliefert. Die Diskothek setzte unseren Vorschlag umgehend um.

Was ist zu tun?
Gastronomiebetriebe sollten den Personalausweis nicht als Zwangspfand benutzen. Die Besucher müssen die Möglichkeit zur Wahl zwischen mehreren Pfandgegenständen haben. Auf die Alternativen sind sie hinzuweisen.

5.7 Von wem kommt die Werbung denn nun?

Unternehmen müssen die Betroffenen bei der Ansprache zu Werbezwecken über die Identität der verantwortlichen Stelle – also des Absenders der Werbepost – unterrichten. Doch oftmals trügt der Schein.

Ein Bürger glaubte unaufgefordert eine Werbesendung eines **staatlichen Lotterieeinnehmers** erhalten zu haben. Jedenfalls ließen sowohl die äußere Aufmachung als auch der Inhalt der Sendung – Gewinnzertifikate und Lose einer Klassenlotterie – darauf schließen. Da sich in der Werbesendung aber auch Hinweise auf ein **Telekommunikationsunternehmen** befanden, bei dem der Bürger einen Handyvertrag hatte, vermutete er eine Weitergabe seiner Adresse durch den Telekommunikationsanbieter an den Lotterieeinnehmer. Tatsächlich hatte aber der Telekommunikationsanbieter die Werbeschreiben für die Klassenlotterie in deren Auftrag unter Verwendung seiner eigenen Kundendaten im eigenen Hause versandt. Eine Übermittlung von Adressdaten an Dritte hatte also

gar nicht stattgefunden. Wir haben den Telekommunikationsanbieter aufgefordert, künftig seine Identität als Versender bei Werbeaktionen deutlich zum Ausdruck zu bringen. Das Unternehmen hat dies zugesagt.

Was ist zu tun?
Alle Versender von Werbepost sind verpflichtet, ihre Identität gegenüber dem Empfänger offen zu legen.

5.8 Das staatliche Liegenschaftskataster ist kein Pool für Werbezwecke

Staatliche Liegenschaftskataster dienen vorrangig öffentlichen Zwecken. Die Nutzung der Daten durch private Energieversorgungsunternehmen ist eng begrenzt, für Werbezwecke ist sie unzulässig.

Mehrere Grundstückseigentümer wunderten sich über Werbepost eines **schleswig-holsteinischen Energieversorgers**, obwohl sie keine Kunden dieses Unternehmens waren. Sie wollten wissen, wer die Quelle ihrer Daten war. Das Energieversorgungsunternehmen, kürzlich durch Fusion eines hamburgischen mit einem schleswig-holsteinischen Unternehmen entstanden, hatte auf der Grundlage eines älteren Vertrages Daten von Grundstückseigentümern aus dem automatisierten Liegenschaftskataster der Stadt Hamburg erhalten. Nach der Fusion nutzte das Unternehmen die Adressdaten, um Neukunden zu gewinnen, was viele Betroffene verwunderte und ärgerte.

Der Umstand, dass die Adressen aufgrund eines Vertrages bei einer hamburgischen Behörde beschafft worden sind, ändert nichts daran, dass die Werbenutzung unzulässig war. Die entsprechende Verordnung der Hansestadt erlaubt die Datenweitergabe an Energieversorger nur zur Wahrnehmung ihrer Versorgungsaufgaben, z. B. zur Kontaktaufnahme mit Grundstückseigentümern zwecks Verlegung von Leitungen. Auch das schleswig-holsteinische Vermessungs- und Katastergesetz erlaubt die Weitergabe von Personendaten an Ver- und Entsorgungsunternehmen nur **zur rechtmäßigen Aufgabenerfüllung**.

Das Unternehmen zeigte sich zunächst nur bereit, die Daten der einzelnen Beschwerdeführer zu löschen. Unserer Forderung nach Sperrung sämtlicher bereits vorhandener Datensätze aus dem Liegenschaftskataster, soweit die Angeschriebenen inzwischen nicht zu Kunden geworden sind, wollte es nicht nachkommen. Dies sei aus übergeordneten Gründen gerechtfertigt: betriebswirtschaftliche Überlegungen, die Verdichtung des Kundennetzes, Verpflichtungen nach dem Energiewirtschaftsgesetz, die höhere Umweltverträglichkeit von Gas gegenüber Öl und schließlich die hohe Erfolgsquote der bisherigen Marketingaktionen. Es war für uns nicht einfach, das Unternehmen davon zu überzeugen, dass erfolgreiches Marketing nicht zwangsläufig auch zulässig ist. Schließlich versah das Unternehmen aber die Adressen aus dem Liegenschaftskataster mit einer **Werbesperre**.

Was ist zu tun?
Energieversorgungsunternehmen dürfen Adressen aus staatlichen Liegenschaftskatastern nur für ihre eigentlichen Versorgungsaufgaben nutzen, aber nicht für Werbezwecke.

5.9 Flugdatenaffäre – Hoffnungen liegen nun beim EuGH

Das Jahr 2004 brachte im Streit um die Übermittlung von Fluggastdaten an die USA zwar eine Rechtsgrundlage in Form eines internationalen Abkommens, die endgültige Klärung über die Rechtmäßigkeit der Datenübermittlung auf der Grundlage dieses Abkommens ist nunmehr jedoch Sache des Europäischen Gerichtshofs.

Nach langwierigen und zähen Verhandlungen zwischen der EU-Kommission und dem US-Heimatschutzministerium kam 2003 (26. TB, Tz. 11.1) ein Abkommen über die Weitergabe der Passagierflugdaten zustande. Das zwischen den Mitgliedstaaten der Europäischen Union und den Vereinigten Staaten beschlossene Abkommen nimmt für sich in Anspruch, bei der Regelung der **Übermittlung der so genannten PNR-Daten** (Passenger Name Record) die in der Öffentlichkeit vehement eingeforderten Datenschutzmaßnahmen zu berücksichtigen (zur Liste der geforderten Datenschutzvorkehrungen siehe 26. TB, Tz. 11.1).

Die EU-Datenschutzkonformität dieses Abkommens wurde bereits vor der Unterzeichnung massiv angezweifelt. Das Europäische Parlament hatte die ungenügende Beteiligung und den fehlenden Einfluss auf die Verhandlungen mit den USA gerügt. Nach dem Abschluss des Abkommens sahen sich die Parlamentarier veranlasst, im April 2004 mehrheitlich die **Anrufung des Europäischen Gerichtshofs (EuGH)** zu beschließen. Die Kritik des Europäischen Parlaments beeindruckte die EU-Kommission sowie die EU-Außenminister offensichtlich nicht, sodass das Abkommen Ende Mai 2004 in Kraft trat. Die Außenminister schlossen sich der Ansicht der EU-Kommission an, die Angemessenheit des ausgehandelten Datenschutzniveaus sei gegeben.

Diese so genannte Angemessenheitsentscheidung der Kommission war Anlass für eine Stellungnahme der **Artikel-29-Datenschutzgruppe** der EU, in der zu Recht festgestellt wird, dass die zwingend geforderten Datenschutzmaßnahmen im Abkommen nur teilweise realisiert worden sind. Die Gruppe veröffentlichte **Informationstexte**, in welchen die Fluggäste über die Auswirkungen des Abkommens sowie ihre Rechte als Betroffene unterrichtet werden. Den Flugpassagieren soll bereits bei der Buchung ihres Flugtickets eine meinungsfördernde Kurzversion zur Verfügung stehen. Detaillierte Informationen sollten über die Internetpräsenz der Fluggesellschaft nachlesbar sein.

Im August 2004 sprach sich das Europäische Parlament abermals gegen die praktizierte Flugdatenweitergabe aus und forderte die Annullierung des bestehenden Abkommens über ein **Schnellverfahren vor dem EuGH**. Angegriffen wurde die Entscheidung des Rates zum Abschluss des Abkommens sowie die Entscheidung der Kommission zur Angemessenheit des verabredeten Datenschutzniveaus auf US-amerikanischer Seite. Der EuGH verweigerte jedoch eine Entscheidung im Schnellverfahren im September 2004. Nun ist mit einer Entscheidung im Hauptverfahren frühestens im Jahr 2005 zu rechnen. Weitere Informationen zur Flugdatenaffäre finden Sie im entsprechenden Dossier des Virtuellen Datenschutzbüros unter

www.datenschutz.de/feature/flugdaten/

Was ist zu tun?
Aufgrund einer von Parlamentariern und Datenschützern heftig kritisierten internationalen Regelung werden Passagierdaten zur Terrorismusbekämpfung in die USA weitergegeben. Dem können sich die Betroffenen nur durch Verzicht von Reisen in die USA entziehen. Es ist zu hoffen, dass es bei Prüfung dieses Abkommens nicht zu einem Absenken des europäischen Datenschutzniveaus kommt.

5.10 Videoüberwachung – quo vadis?

Videoüberwachung durch Private greift im täglichen Leben immer mehr um sich. Der Preisverfall bei der Videotechnik treibt gefährliche, manchmal auch kuriose Blüten: Fast jeder kann es sich finanziell leisten, doch darf jeder nicht alles.

- **Videoüberwachung in Umkleidekabinen**

Ein **Freibad** wollte die Schränke in den **Umkleidekabinen** per Video überwachen. Anlass waren diverse Diebstähle. Nun ist es nicht ausgeschlossen, dass Badegäste unbekleidet an ihren Spind treten und dass sie dann Videoaufnahmen als einen massiven Eingriff in ihre Intimsphäre empfinden. Wir haben den Betreiber aufgefordert, die Beobachtung auf den Außenbereich zu beschränken. Diebstahlschutz lässt sich auch ohne Videoüberwachung realisieren. Die Eingriffe in die Intimsphäre werden dadurch nicht geringer, dass mit Schildern auf die Videoüberwachung hingewiesen wird.

- **Videoüberwachung von öffentlichen Straßen und Gehwegen**

Ein Bürger beschränkte das Blickfeld seiner Kameras nicht auf sein Grundstück, sondern erfasste auch **Straße und Gehweg**. Damit wollte er unzulässig Parkende sowie Menschen, die Abfälle auf sein Grundstück werfen, überführen: „Die Polizei tut ja nichts, also muss ich selbst etwas machen." Der Bürger war erst nach eindringlicher rechtlicher Aufklärung zähneknirschend bereit, den Erfassungsbereich der Kameras auf sein Grundstück zu beschränken. Auch eine Dienstaufsichtsbeschwerde und eine Eingabe beim Petitionsausschuss des Schleswig-

Holsteinischen Landtages waren nicht geeignet, an der eindeutigen Rechtslage etwas zu ändern.

- **Videoüberwachung von Hauseingängen**

Eine Wohnungsbaugesellschaft wollte ihren Mietern einen besonderen Service anbieten: Sie installierte an der Haupteingangstür eine Videokamera, deren Bilder per Kabel an die **Fernseher aller Mieter** übertragen wurden. Wer wollte, konnte über einen bestimmten Kanal mit seinem Fernsehgerät beobachten, wer wann das Haus betritt oder verlässt. Erst nach einem Ortstermin war die Wohnungsbaugesellschaft bereit, die Technik so zu verändern, dass nur noch derjenige Mieter, bei dem geklingelt wird, das Bild vom Hauseingang beobachten kann.

Diese Beispiele sind nur die Spitze eines immer größer werdenden Eisberges. Patentlösungen haben auch wir nicht. Offensichtlich ist das erst im Jahr 2001 erlassene **Gesetz zur Videoüberwachung** nicht in der Lage, dieses Problem wirksam einzugrenzen. Per Kamera überwacht zu werden ist den Menschen alles andere als egal. Dies konnten wir anlässlich einer von uns durchgeführten Meinungsumfrage feststellen.


www.datenschutzzentrum.de/material/themen/video/umfrage_2004.htm

Was ist zu tun?
Die ausufernde Videoüberwachung im Privatbereich kann wohl nur durch strengere gesetzliche Anforderungen, z. B. die Einführung einer Meldepflicht bei öffentlicher Videoüberwachung, eingedämmt werden.

5.11 Datenschutz bei Steuerberatern, Rechtsanwälten und anderen freien Berufen

Steuerberater, Wirtschaftsprüfer und Rechtsanwälte unterliegen eigenen berufsrechtlichen Regelungen, die auch den Schutz personenbezogener Daten bewirken. Daneben findet das Bundesdatenschutzgesetz Anwendung.

Im Jahr 2004 liefen **Umsetzungsfristen** des im Jahr 2001 novellierten Bundesdatenschutzgesetzes aus. Dies nahmen Schulungsanbieter und Datenschutzdienstleister zum Anlass, bei Steuerberatern und Rechtsanwälten mit Hinweisen auf drohende Bußgelder bei Nichtumsetzung der datenschutzrechtlichen Vorgaben für ihre Dienste zu werben. Um der Verunsicherung vieler Freiberufler entgegenzuwirken, haben wir die betroffenen Berufsgruppen über die materiellen Vorgaben des Datenschutzrechts informiert und in Einzelfragen beraten.

Berufliche Geheimhaltungspflichten stellen eine spezielle, **zusätzliche Ebene des Schutzes** personenbezogener Daten dar. Das Bundesdatenschutzgesetz (BDSG) räumt solchen Vorschriften entweder Vorrang oder gleichrangige Geltung ein. Bestehen für bestimmte Bereiche keine berufsrechtlichen Vorgaben, so gelten die allgemeinen Regelungen des BDSG und gegebenenfalls des bereichsspezifischen Datenschutzrechts.

Da berufsrechtliche Regelungen der genannten Berufsgruppen keine internen Kontrollinstanzen für den Datenschutz vorsehen, sind insbesondere auch die Vorschriften über die Einführung eines **betrieblichen Datenschutzmanagements** auf die Steuerberater und Wirtschaftsprüfer anwendbar, soweit mehr als vier Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Um einen kostengünstigen, unbürokratischen Umgang mit den gesetzlichen Anforderungen zu ermöglichen, hat das ULD Informationen zur Umsetzung der rechtlichen Vorgaben bereitgestellt, die auf seiner Website und in den Kammernachrichten der schleswig-holsteinischen Steuerberaterkammer veröffentlicht sind.


www.datenschutzzentrum.de/wirtschaft/dsm_steuerberater.htm

Der **Datenschutzausschuss der Bundesrechtsanwaltskammer** ist der Ansicht, für die Verarbeitung von Mandantendaten durch Rechtsanwälte finde das BDSG keine Anwendung. Diese Ansicht trifft nicht zu, wie auch der Arbeitskreis Informationstechnologie des Deutschen Anwaltsvereins festgestellt hat. Soweit nicht die konkrete Prozesstätigkeit betroffen ist, sind die Aufsichtsbehörden nach dem BDSG für die Datenschutzkontrolle zuständig (26. TB, Tz. 5.9). Dass datenschutzrechtliche Kontrollen notwendig sind, zeigen die Fälle der letzten Jahre (24. TB, Tz. 6.4.4; 26. TB, Tz. 5.9).


www.datenschutzzentrum.de/wirtschaft/stellungnahme_brak.htm

Was ist zu tun?
Steuerberater, Wirtschaftsprüfer und Rechtsanwälte sollten bedenken, dass die Vertrauensbeziehung zu ihren Mandanten von besonderer Bedeutung für ihren Geschäftserfolg sein kann und die Beachtung des informationellen Selbstbestimmungsrechts daher in ihrem eigenen Interesse liegt. Das Datenschutzrecht gibt Hilfestellung für einen systematischen Schutz personenbezogener Daten. Sie sollten sich daher mit den gesetzlichen Vorgaben vertraut machen und diese für sich umsetzen.

5.12 Ohne Unabhängigkeit keine Selbstkontrolle

Moderner Datenschutz beruht in starkem Maße auf eigenverantwortlicher Kontrolle durch betriebliche Datenschutzbeauftragte. Diese Kontrolle kann nur gelingen, wenn die dazu bestellten Personen ihre Aufgabe – wie vom Gesetz gefordert – unabhängig erfüllen können.

Der Betriebsrat eines mittelgroßen Unternehmens informierte uns über den Leiter der EDV-Abteilung, der zugleich die Funktion des **betrieblichen Datenschutzbeauftragten** wahrgenommen hatte. In Abstimmung mit der Firmenleitung machte dieser sich für die Einführung einer Fernwartungssoftware stark. Der Betriebsrat wehrte sich hiergegen, weil die Software eine Überwachung der Beschäftigten ermöglichte. Zudem wurde dem EDV-Leiter vorgeworfen, am Betriebsrat vorbei die überwachungsgeneigte Software auf einer Reihe von Rechnern installiert und angewendet zu haben.

Ein Leiter einer EDV-Abteilung darf grundsätzlich nicht zugleich die Aufgabe des betrieblichen Datenschutzbeauftragten übernehmen. Da können die vorhandenen Spezialkenntnisse für die Bewältigung dieser Aufgabe noch so gut sein. Grund ist die **Interessenkollision**, die fast zwangsläufig entsteht, wenn eine Person zwei sich widersprechende Funktionen ausüben muss. Die EDV-Leitung vollzieht zumeist die unter Produktivitätsgesichtspunkten getroffenen Entscheidungen der Geschäftsleitung und hat vorrangig das Funktionieren der automatisierten Datenverarbeitung im Blick. Der betriebliche Datenschutzbeauftragte nimmt demgegenüber eine unabhängige Kontrollfunktion innerhalb des Unternehmens wahr und ist der Wahrung der Persönlichkeitsrechte der Mitarbeiter und Kunden verpflichtet. Wie der konkrete Fall zeigt, können beide Aufgaben nicht wirksam von einer Person wahrgenommen werden. Unsere Intervention führte zur Abberufung des EDV-Leiters als Datenschutzbeauftragter und zur Bestellung eines anderen Mitarbeiters.

Was ist zu tun?
Die Verquickung unterschiedlicher Interessen in der Person des Datenschutzbeauftragten fördert den Unfrieden und gefährdet den Datenschutz im Unternehmen. Die Aufsichtsbehörde kann die Abberufung von nicht hinreichend unabhängigen Datenschutzbeauftragten anordnen. Unternehmen sollten es erst gar nicht so weit kommen lassen.

5.13 Wer sich verweigert, der muss büßen

Datenverarbeiter müssen der Datenschutzaufsichtsbehörde auf Verlangen unverzüglich die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte erteilen. Spammer tun sich mit dieser gesetzlichen Verpflichtung schwer.

Die Versendung unerwünschter E-Mail-Werbung (Spamming) greift immer weiter um sich. Nicht nur Beschwerden von Betroffenen zeigen, wie lästig diese Art von Werbung ist. Auch das ULD wird wie jede andere öffentliche oder private Stelle damit zugeschüttet. Die Versender dieser Massen-E-Mails sind oft **Einmannfirmen**, deren datenschutzrechtliches Grundwissen und Bewusstsein gegen null tendiert. Sie sehen keine Veranlassung, auf Auskunftsanforderungen der Aufsichtsbehörde zu reagieren. Widersprüche der Betroffenen gegen die Datennutzung werden ignoriert, Nutzer werden weiterhin mit Werbemails bombardiert.

Ein Spamversender aus Schleswig-Holstein ignorierte mehrfach den Widerspruch eines Betroffenen. Unsere Auskunftsersuchen als Aufsichtsbehörde blieben unbeantwortet, Werbemails wurden weiter verschickt. Daher sahen wir uns gezwungen, ein **Bußgeld** in Höhe von 1000 Euro zu verhängen. Die prompte Reaktion des Spammers: Er sei Spätaussiedler, psychisch krank, lebe von der Sozialhilfe und stehe unter Betreuung. Seine finanzielle Situation erlaube ihm eine Bezahlung des Bußgeldes nicht. Der Betreuer, Mitarbeiter einer anerkannten, landesweit tätigen Wohlfahrtsorganisation, bestätigte die Angaben glaubhaft. Wir mussten die

Vollstreckung der Bußgeldforderung aussetzen. Dies ist aber kein Freibrief für diesen Spamversender. Im Wiederholungsfall können weitergehende Maßnahmen nötig werden.

Was ist zu tun?
Die gesetzlichen Möglichkeiten zur Verhinderung des Spamming sind nicht befriedigend. In Extremfällen müsste es möglich sein, das eingesetzte Gerät einzuziehen.

6 Systemdatenschutz

6.1 Pflichten des Auftraggebers beim Outsourcing

Werden personenbezogene Daten nicht von der verantwortlichen Behörde selbst verarbeitet, sondern externe Dienstleister beauftragt, obliegt dem Auftraggeber eine Kontrollpflicht. Viele Behörden werden dieser Verantwortung nicht gerecht, weil sie bezüglich der Sicherheit ihrer Daten nach der Devise handeln: „Aus dem Auge, aus dem Sinn."

Die Bürgerinnen und Bürger haben einen Anspruch darauf, dass Daten, die eine Behörde über sie erhebt, grundsätzlich nur von ihr verarbeitet werden. Abweichungen von dem Grundsatz bedürfen einer Legitimation durch Zweckänderungs- und Übermittlungsvorschriften oder durch eine vertragliche Vereinbarung. Als eine weitere Ausnahme sind die datenschutzrechtlichen Regelungen über die **Auftragsdatenverarbeitung** (im Wirtschaftsleben wird alternativ oft der Begriff „Outsourcing" gebraucht) anzusehen. Sie gestatten es, unter bestimmten Voraussetzungen andere öffentliche oder private Stellen mit der Durchführung der Datenverarbeitung zu betrauen.

Dies ist als ein Privileg anzusehen. Bei Schaffung der Regelungen standen nicht die Interessen der Betroffenen im Vordergrund, sondern die der Daten verarbeitenden Stellen. Wie dominant der ökonomische Aspekt heute ist, zeigt eine aktuelle Studie, in der als **Gründe für ein Outsourcing** die folgende Rangfolge ermittelt wurde:

- Reduzierung der Kosten,
- Konzentration auf das Kerngeschäft,
- Ergänzung fehlender interner Ressourcen,
- Profitieren vom Prozess-Know-how des Dienstleisters,
- Aufrechterhaltung der Servicequalität,
- fehlendes internes Know-how,
- Steigerung der Anwenderzufriedenheit und
- Freiräume schaffen für Innovationen.

Von einem **Mehrwert für die Kunden** bzw. die Bürger ist in diesem Zusammenhang nicht die Rede.

In der Verwaltungspraxis begegnen uns neben den klassischen Rechenzentrumsaktivitäten die Auftragsdatenverarbeitungsverhältnisse in sehr unterschiedlichen Erscheinungsformen. Externe Dienstleister bieten sich an als:

- Internetprovider,
- Betreiber von Verzeichnisdiensten,
- Zertifizierungsinstanzen,
- Application-Service-Provider,
- Fernwartungseinrichtungen,
- Telekommunikationsdienstleister,
- Hard- und Software-Supporter,
- Trainings- und Coachingdienstleister,
- BackUp-Einrichtungen,
- Langzeitarchive,
- Kuriertransportdienste,
- Ermittlungs- und Inkassodienste usw.

Im Wortlaut: § 17 LDSG

Verarbeitung personenbezogener Daten im Auftrag, Wartung

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

Die datenschutzrechtliche Zulässigkeit derartiger Formen der Auftragsdatenverarbeitung ist an konkrete Bedingungen geknüpft. Diese differieren leicht in den Datenschutzgesetzen des Bundes und der Länder bzw. in den bereichsspezifischen Gesetzen. Als gemeinsame Basis sind allerdings die folgenden Kriterien anzusehen:

- **Gewährleistung der Verantwortlichkeit des Auftraggebers**

In der Fachliteratur ist häufig zu lesen, dass Unternehmen ihre gesamte Informationstechnologie outsourcen. Bei genauerer Analyse stellt man allerdings fest, dass dies nicht für die **unternehmenskritischen Verarbeitungsprozesse** gilt. Diese geben Unternehmen grundsätzlich nicht in fremde Hände. Bei der personenbezogenen Verarbeitung von Verwaltungsdaten käme eine Verantwortungsverlagerung einer Aufgabenübertragung gleich. Dies ist jedoch grundsätzlich nur durch ein Gesetz oder aufgrund eines Gesetzes möglich. Bei der Einschaltung externer Dienstleister muss also die auftraggebende Behörde stets **Herr des Verfahrens** bleiben. Das hat auch verwaltungsverfahrensrechtliche Gründe, z. B. im Hinblick auf die Zurechenbarkeit von Verwaltungsakten.

- **Erfüllung der Ansprüche der Betroffenen**

Durch ein Outsourcing dürfen außerdem die Rechte der Betroffenen, z. B. auf **Sperrung, Berichtigung, Löschung und Beauskunftung** von Daten, nicht beeinträchtigt werden. Kann ein externer Dienstleister derartige Funktionen nicht bereitstellen, scheidet er aus dem Kreis der Bewerber um einen Auftrag aus. Auch einige der marktführenden Standardsoftwareprodukte, die vorzugsweise von externen Dienstleistern eingesetzt werden, sind bei weitem nicht so datenschutz-

konform, wie ihre Verkäufer es uns glauben machen wollen. Wer z. B. Daten nicht wirklich löscht, sondern sie nur langzeitarchiviert, bereitet damit einer Stelle, die Daten aus Rechtsgründen löschen muss (gesetzliche Bestimmungen, Gerichtsurteile), unlösbare Probleme. Eine Stelle, die das Angebot eines externen Dienstleisters nicht vorher genau bezüglich dieser Funktionalitäten prüft, kann später in erhebliche rechtliche Probleme geraten.

- **Sorgfältige Auswahl des externen Dienstleisters**

Externe Dienstleister wollen Gewinne machen, um Reinvestitionen tätigen bzw. den Kapitalgebern Dividenden ausschütten zu können. Da Sicherheit nicht zum Nulltarif erreicht werden kann, versucht man, auch auf diesem Gebiet nicht mehr Aufwand zu treiben, als die Kunden verlangen. Erfahrungsgemäß verlassen sich diese wiederum nur allzu gern auf Versprechungen. Deshalb ist es in der Praxis eher eine Ausnahme, dass externe Dienstleister ihre Sicherheitsmaßnahmen freiwillig offen legen. Welcher Provider beschreibt z. B. die Filtermechanismen seiner Firewall für den Kunden verständlich und verrät, was passiert, wenn ein Angriff (möglicherweise) doch erfolgreich war. Da „security by obscurity“ kein tragbares Fundament für eine Auftragsdatenverarbeitung sein kann, darf es nicht zu einem Vertragsabschluss kommen, bevor der Dienstleister seinen Kunden nicht sein **Sicherheitskonzept erläutert** hat.

- **Schriftform der Aufträge**

Für Dienstverträge, die eine personenbezogene Datenverarbeitung zur Grundlage haben, wird gesetzlich die Schriftform gefordert, weil es in diesem Bereich eines **Höchstmaßes an Transparenz** bedarf. Dieses Ziel wird faktisch von nahezu allen externen Dienstleistern konterkariert. Formal wird die Schriftform zwar eingehalten, der Inhalt der Verträge und der häufig diversen Anlagen (Leistungsbeschreibungen) sagt jedoch in der Regel wenig darüber aus, zu welchen Leistungen sich der Auftragnehmer tatsächlich im Einzelnen verpflichtet. Kaum eine datenschutzrechtliche Prüfung durch uns bleibt in diesem Bereich ohne Beanstandung. Würden die rechtlichen Anforderungen hart umgesetzt, dann dürften viele Auftragsverhältnisse nur sehr eingeschränkt fortgesetzt werden. Besonders bedenklich ist, dass der Trend in die falsche Richtung geht. In den vergangenen Jahren wurden vertragliche Vereinbarungen in der Regel detaillierter und aussagekräftiger formuliert als heute. Das gilt besonders im Bereich des E-Government und betrifft nicht nur die privaten, sondern auch die in öffentlich-rechtlicher Trägerschaft stehenden Provider.

- **Ergänzende Weisungen zur Datensicherheit**

Ein Auftraggeber darf seine Datenbestände einem externen Dienstleister nur zur Verfügung stellen, nachdem er sich vergewissert hat, dass das dortige Sicherheitsniveau mindestens ebenso hoch ist wie das im eigenen Haus. Wer ein preiswertes Standardangebot in Anspruch nehmen will, muss sich fragen, ob seine speziellen rechtlichen Rahmenbedingungen nicht eigentlich ein **höheres als das angebotene Sicherheitsniveau** erfordern. Hier herrscht in der Praxis eine ebenso große Nachlässigkeit wie bei der gesamten Vertragsgestaltung. Welcher Amtsarzt hat sich z. B. Gedanken darüber gemacht, dass eine an ihn gerichtete E-Mail beim Provi-

der nicht dem Schutz des Patientengeheimnisses unterliegt und dass er deshalb extrem kurze Löschungsfristen vereinbaren müsste? Welcher Personalchef, Steuer- oder Sozialamtsleiter weiß wirklich, wie mit dem Papierschrott in einem Druckzentrum umgegangen wird? Wer weiß, ob durch den Druck auf die Löschtaste des Telefons eine Voice-Mail tatsächlich physisch oder nicht nur logisch und damit rekonstruierbar gelöscht wird?

- **Genehmigung von Unterauftragsverhältnissen**

Externe Dienstleister lassen sich oft Unterauftragsverhältnisse genehmigen. Mit wem sie diese einzugehen gedenken und welche Verarbeitungsprozesse weiterdelegiert werden, wird von ihnen jedoch nicht offen gelegt. In der Regel bleibt den Auftraggebern also verborgen, welche **weiteren Unternehmen** Kenntnis von den im Auftrag verarbeiteten Daten erhalten bzw. die Verfügungsgewalt über die Datenbestände erlangen. Es wird seitens der externen Dienstleister unterstellt, dass die Auftraggeber ihr stillschweigendes Einverständnis gegeben haben, um den Erfolg der Outsourcingmaßnahmen nicht zu gefährden (z. B. zur Einschaltung von Spezialisten bei technischen Problemen; ein klassischer Fall ist auch die Rekonstruktion von inkonsistenten Datenbanken im Hause des Softwarelieferanten). Jeder Auftraggeber sollte darauf achten, dass Unterauftragsverhältnisse zunächst einmal ausgeschlossen sind und Ausnahmen von seiner ausdrücklichen schriftlichen Genehmigung abhängen.

- **Kontrollen durch den Auftraggeber**

Zunehmend werden nicht nur einzelne Verarbeitungsschritte, sondern die gesamte Informationsverarbeitung auf externe Dienstleister verlagert. Dazu gehört auch das „Hosting“ der Rechnersysteme und deren Administration. Im Hause des Auftraggebers verbleibt oft nur die Bedienung der Arbeitsplatzrechner. Auf eigenes **IT-Know-how** wird aus Kostengründen bewusst verzichtet. Diese Verfahrensweise wird als **Application-Service-Providing** bezeichnet und ist im Bereich der Webpräsentation und in anderen rechtlich nicht besonders reglementierten Bereichen auch problemlos.

Bei der personenbezogenen Datenverarbeitung tun sich jedoch erhebliche Probleme auf. Wenn beim Auftraggeber nicht das erforderliche Wissen verfügbar ist, um die Arbeit des Auftragnehmers zu überprüfen, entsteht dort ein kontrollfreier Raum, den man im eigenen Hause nie und nimmer dulden würde und der folgender Grundregel widerspricht: „Die Daten verarbeitende Stelle hat sicherzustellen, dass die Verarbeitungsprozesse rechtskonform ablaufen.“ In einem gewissen Umfang ist es zwar immer möglich, die fachliche Korrektheit der Verarbeitungsergebnisse zu überprüfen (Inaugenscheinnahme der gespeicherten Daten und der ausgedruckten Verwaltungsakte). Ob aber z. B. die Zugriffsrechte der Benutzer und die Kommunikationsströme bei Netzverknüpfungen richtig konfiguriert sind, ist an den Arbeitsplätzen faktisch nicht prüfbar. Man kann zwar feststellen, dass zu wenige Rechte, nicht aber, ob zu viele Rechte erteilt worden sind.

Besonders bedenklich ist, dass in diesen Fällen eine Spirale in Gang gesetzt wird. Je weniger der Auftraggeber selbst in der Lage ist, IT-Konzepte zu entwickeln und umzusetzen, desto weniger kann er die Qualität der vom externen Dienstleister

vorgeschlagenen Konzepte beurteilen. Er ist ihm bereits nach kurzer Zeit faktisch ausgeliefert. Es bleibt im Grunde nur noch, einen vertrauenswürdigen Dritten als Revisor einzuschalten. Es ist zu befürchten, dass sich dieser Trend gerade in den kleinen und mittelgroßen Organisationseinheiten der Verwaltung verstärken und zu einem zentralen Problem entwickeln wird. Das als Allheilmittel propagierte E-Government führt zu einer immer stärkeren Vernetzung lokaler Rechnersysteme und damit zu höheren Anforderungen an die Systemadministration. Diese wiederum führen zu einem verstärkten Outsourcing und damit zu einer Bevormundung der eigentlich Verantwortlichen. Datenschutzrechtlich und sicherheitstechnisch kann dies nicht akzeptiert werden.

- **Kontrollen durch Datenschutzinstitutionen**

In den Diskussionen wird die Ideallösung oft darin gesehen, dass man unsere Kontrollkompetenzen in Anspruch nimmt. Dabei handelt es sich aber keineswegs um eine generelle Problembereinigung. Weder sind wir in der Lage, alle Outsourcingfälle im Auge zu behalten, noch können wir die Kontrollen stets zu dem Zeitpunkt durchführen, an dem eine Modifikation der Verfahrensweise noch möglich ist. Letztlich wären derartige Aktivitäten durch das ULD auch nur dann sinnvoll, wenn wir **Fehlentwicklungen unterbinden** und Nachlässigkeiten bei den externen Dienstleistern sanktionieren könnten.

Was ist zu tun?
Die derzeitige praktische Ausgestaltung des Outsourcing in der öffentlichen Verwaltung im Lande gibt aus datenschutzrechtlicher und sicherheitstechnischer Sicht Anlass zur Sorge. Es ist höchste Zeit, dass das Management der Verwaltung und die Dienstleister sich auf rechtlich tragfähige und zukunftsfähige Grundkonzepte besinnen. Die Aufgabe des ULD kann neben der Intensivierung seiner Kontrollen (und Beanstandungen) in diesem Bereich nur darin bestehen, dass es ausreichende Kapazitäten für die Zertifizierung von Produkten und Dienstleistungen (Datenschutz-Gütesiegel) und die Auditierung von Verarbeitungsprozessen (Behördenaudit) bereithält. Das ist geschehen.

6.2 Hat dataport eine Sonderstellung?

Dadurch, dass die Länder Hamburg und Schleswig-Holstein als Träger von dataport deren Geschäftspolitik beeinflussen können, erlangt diese Anstalt keinen datenschutzrechtlichen Sonderstatus gegenüber anderen IT-Dienstleistern. Wer ihr Aufträge erteilt, muss prüfen, ob sie korrekt ausgeführt worden sind. Das liegt auch im Interesse von dataport.

Als vor über 30 Jahren die **Datenzentrale** durch die Landesregierung gegründet wurde, definierte man deren Aufgaben wie folgt: „Die Datenzentrale soll die Erledigung von Aufgaben der öffentlichen Verwaltung im Lande Schleswig-Holstein durch elektronische Datenverarbeitung ermöglichen. Die Geschäfte sind ... nach kaufmännischen Gesichtspunkten zu führen.“ In gemeinsamen Geschäftsanweisungen wurde festgelegt, dass die Kapazität der Datenzentrale möglichst wirtschaftlich eingesetzt und ausgenutzt werden sollte. Die Kontrollpflichten wurden

den Fachverwaltungen und dem Organisationsreferat des Innenministeriums auferlegt.

Bei der Verabschiedung des ersten Datenschutzgesetzes im Land (LDSG) gab es keine Diskussionen darüber, dass die Aktivitäten der Datenzentrale in datenschutzrechtlichem Sinne als „normale“ Auftragsdatenverarbeitung zu betrachten waren. Es wurde nur Wert darauf gelegt, dass sie aufgrund ihrer Rechtsform als Anstalt öffentlichen Rechts und ihrer Reputation grundsätzlich als „**sorgfältig ausgewählt**“ galt. Diesen Status teilte sie sich mit einer Anzahl anderer öffentlicher Rechenzentren (von Stadtwerken, Sparkassen, Verkehrsbetrieben usw.), die (auch) für andere Behörden tätig waren.

Die Klassifikation von dataport als „externer Dienstleister“ war bis zum September 2004 gemeinsame Auffassung aller Beteiligten. In seiner Stellungnahme zu unserem 26. TB (Umdruck 15/4945) stellte jedoch der Innenminister im Einvernehmen mit dem Finanzminister überraschenderweise fest, dass eine entsprechende Formulierung unter Tz. 6.5 „nicht zutreffend“ sei. Der Gesetzgeber habe entschieden, die IT-Unterstützung der Landesverwaltung, insbesondere wegen der hoheitlichen Aufgaben, öffentlich-rechtlich zu organisieren, sie aus wirtschaftlichen Gründen an einer Stelle zu konzentrieren und einer uneinheitlichen IT-Infrastruktur entgegenzuwirken. Daher sei dataport eine **„interne“ IT-Dienstleisterin** des Landes Schleswig-Holstein.

Ungeachtet der Tatsache, dass die Aussage nicht uneingeschränkt zutrifft – vgl. z. B. die Inanspruchnahme der Firma Telekom für die Administration der Telekommunikationsrechner, die Beauftragung des Freistaates Bayern mit der Verarbeitung der InVeKos-Daten und den Aufbau der Clearingstellen in Bayern und Nordrhein-Westfalen für die Verarbeitung von Elster-Daten –, könnte man diesen Unterschied als semantische Petitesse abtun, wenn damit nicht Konsequenzen verbunden wären. In einer Innen- und Rechtsausschusssitzung im September 2004 wurde vom Innenministerium des Landes zugestanden, dass auf die Dienstleistungen von dataport die datenschutzrechtlichen Vorschriften der Auftragsdatenverarbeitung anzuwenden sind. Eine Veranlassung, dataport **besonders zu kontrollieren**, sehe das Innenministerium jedoch nicht. Insgesamt dürfe man die Verantwortung der Verwaltung nicht überziehen. Es sei nicht sinnvoll, die ganze Kraft auf eine Innenkontrolle zu legen. Man könne dataport nicht mit einer normalen Firma wie z. B. IBM gleichsetzen, denn dataport sei eine Anstalt öffentlichen Rechts. Folgt man dieser Argumentation, stellt sich die Frage, in welchem Maße die Kontrollintensität bei einer Beauftragung von dataport im Vergleich zu einem entsprechenden Auftragsverhältnis mit der Firma IBM reduziert werden könnte. Für beide Fälle gilt jedoch die nebenstehende gesetzliche Regelung.

Im Wortlaut: § 17 Abs. 2 LDSG

Die Daten verarbeitende Stelle hat dafür Sorge zu tragen, dass personenbezogene Daten nur im Rahmen ihrer Weisungen verarbeitet werden. Sie hat die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um dies sicherzustellen. ...

Dataport selbst beansprucht für sich **keine Sonderstellung**, wie sich aus einer jüngst neu aufgelegten Kundeninformation ergibt. Dort wird ausdrücklich hervorgehoben, dass jeder Auftraggeber das Recht habe, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen durch dataport im erforderlichen Umfang zu kontrollieren. Dataport erteile dem Kunden jederzeit Auskünfte zu seinen den Vertrag betreffenden Fragen und gewähre auf Anforderung Einblick in die während der Verarbeitung erzeugten Unterlagen sowie in die Dokumentation der Verfahren und Systeme.

Diese (selbstverständliche) Offenheit lässt die Diskussion mit der Landesregierung obsolet erscheinen, wäre da nicht die Erfahrung aus anderen Verwaltungsbereichen, dass sich Auftraggeber nur zu leicht und zu gern ihrer **Kontrollpflichten entziehen** (Tz. 6.1). Aus dem Umstand, dass dataport vergaberechtlich als integraler Bestandteil der Landesverwaltung angesehen wird (mit der Folge, dass eine Beauftragung ohne Ausschreibung zulässig ist), kann nicht geschlossen werden, dass auftraggebende Behörden sich nicht von der Einhaltung vereinbarter Sicherheitsstandards überzeugen müssen. Ein solches Verständnis von „interner Dienstleistung“ wäre unzulässig. Alle Landes- und Kommunalbehörden haben in Abhängigkeit davon, wie sicherheitskritisch die Verarbeitungsprozesse sind, die „erforderlichen und angemessenen“ Maßnahmen zu ergreifen, um insbesondere die Vertraulichkeit und Integrität der personenbezogenen Daten zu gewährleisten. Dies hat auch bei dataport im Wege der Prävention (Vereinbarung von Sicherheitskonzepten) und der Revision (Kontrollen) zu geschehen, unabhängig von den sonstigen Einflussmöglichkeiten auf die Art der Durchführung der Dienstleistungen durch die Träger und Organe der Anstalt.

Was ist zu tun?
Die öffentlichen Auftraggeber von dataport sollten ihre rechtliche Bewertung und ihre Praxis bei der Kontrolle des Auftragnehmers überdenken. Dataport sollte im eigenen Interesse dafür sorgen, dass den Kunden ihre Kontrollobliegenheiten so weit wie möglich erleichtert werden. Dies würde sicher von allen als vertrauensbildende Maßnahme begrüßt.

6.3 Die neuen IT-Richtlinien des Landes

Das Land tut sich schwer, die neuen Zuständigkeitsregelungen für die IT-Basisinfrastruktur in die Praxis umzusetzen. Wegen fehlender Schnittstellendefinitionen besteht in Teilbereichen nach wie vor eine unklare Sicherheitslage.

Nachdem im Jahr 2003 der grundlegende Umbau der IT-Organisation des Landes durch die Zuständigkeitskonzentration beim Finanzminister in Gang gesetzt worden ist (26. TB, Tz. 6.5), bestand im vergangenen Jahr der dringende Bedarf, die **neuen Schnittstellen** zwischen den IT-Aufgaben der einzelnen Ministerien und den ressortübergreifenden Aufgaben des Finanzministeriums neu zu **definieren**. Wie schwierig dieser Prozess ist, zeigen folgende Merkmale:

- Es brauchte ca. 18 Monate, um einen Text zu formulieren, der nur knapp vier Seiten umfasst.
- Der Finanzminister betitelt das Papier nicht wie in vergleichbaren Fällen üblich als „Erlass“, sondern nur als „Richtlinie“.
- Nicht alle Regelungen sind abschließend, einige bedürfen der Ergänzung durch so genannte „IT-Ausführungsbestimmungen“.
- Für das Justizministerium gilt eine Sonderregelung.

Das Ganze ist vor dem Hintergrund zu sehen, dass einerseits sehr wichtige **Grundsatzfragen der künftigen IT-Konzeption** des Landes der Entscheidung harren (E-Government innerhalb der Landesverwaltung, Einbindung der Kommunen in die IT-Infrastruktur des Landes, Kooperation mit anderen Bundesländern, Aufbau bundesweiter Netzwerke, Outsourcing von IT-Verarbeitungsprozessen), andererseits bezüglich der konkreten Verantwortlichkeiten nach wie vor ein Regelungsvakuum besteht.

Die Tragweite der **Sonderregelung für die Justiz** ist nicht zu unterschätzen. Der zugrunde liegende Organisationserlass der Landesregierung legt das ressortübergreifende strategische und operative IT-Management sowie die Zuständigkeit für die zentralen Komponenten und Services der IT-Infrastruktur der Landesverwaltung ohne Einschränkungen in die Verantwortung des Finanzministeriums. Trotzdem finden die IT-Richtlinien in der Justizverwaltung keine Anwendung, „soweit durch sie die richterliche Unabhängigkeit beeinträchtigt wird“. Außerdem hat das Justizministerium als einziges Ressort das Recht, über „Ausnahmen im Bereich der Gerichte und Staatsanwaltschaften“ eigenständig zu entscheiden. Über die infrage kommenden bzw. betroffenen Sachverhalte schweigen sich die offiziellen Erläuterungen des Finanzministeriums zu den Richtlinien aus.

Betrachtet man die Richtlinien genauer, fallen folgende **Eckpunkte für das zentrale IT-Management** mit Datenschutzrelevanz ins Auge, von denen es keine Ausnahmen für einzelne Ressorts geben darf, soll nicht das Gesamtkonzept ins Wanken geraten:

- Das beim Finanzministerium angesiedelte zentrale IT-Management definiert die IT-Basisinfrastruktur und schreibt sie fort.
- Es beauftragt Dienstleister mit dem Betrieb dieser Infrastruktur.
- Es regelt dessen Nutzung und überwacht den ordnungsgemäßen Betrieb.
- Die Entwicklung und Umsetzung der jeweiligen IT-Ressortstrategie erfolgen unter Berücksichtigung der IT-Gesamtstrategie.
- Die IT-Kommission beschließt (nur noch) in Form von Empfehlungen.

Eine derartige (noch zu konkretisierende) **Verantwortungsabgrenzung** zwischen den Ressorts, der IT-Kommission und den externen Dienstleistern wurde von uns seit Jahren gefordert (vgl. erstmalig die Kritik am CAMPUS-Netz im Jahr 1997, 20. TB, Tz. 6.7.6). Sie ist der Schlüssel für das lange überfällige grundlegende

Sicherheitskonzept des Landes. Wenn nicht einmal die IT-Basisinfrastruktur auf ein solides und einheitliches Sicherheitsfundament gestellt wird, können die darauf aufbauenden ressortspezifischen Anwendungen kaum ein adäquates Sicherheitsniveau erreichen. Deshalb sollte eine der ersten Ausführungsbestimmungen das Sicherheitskonzept des zentralen IT-Managements zum Gegenstand haben. „Öffnungsklauseln“ in Sachen Sicherheit für einzelne Ressorts verbieten sich von selbst bzw. sind als Ultima Ratio zu behandeln.

Was ist zu tun?
Der Finanzminister sollte kurzfristig ein umfassendes Sicherheitskonzept für sämtliche Komponenten der IT-Basisinfrastruktur erarbeiten und die Beachtung durch alle Daten verarbeitenden Stellen des Landes durchsetzen. Eine Auditierung durch das ULD kann dazu beitragen, Gründe für „Sonderwege“ einzelner Ressorts weitestgehend auszuschließen.

6.4 Auswirkungen der E-Government-Vereinbarung auf die Kommunen

Vorübergehend hatte es den Anschein, das Land wolle die Kreise verpflichten, über Kreisnetze bestimmte Dienstleistungen für die kreisangehörigen Kommunen zu erbringen. Fehlinterpretationen der E-Government-Vereinbarung und Kommunikationsprobleme zwischen dem Land und den Kommunen waren die Ursache. Inzwischen ist unstrittig, dass die Vereinbarung keine Kommune zu etwas zwingt, was sie meint nicht verantworten zu können.

Manchmal ist es sogar im Zusammenhang mit Fragen der IT-Infrastruktur und der Verantwortlichkeit für IT-Sicherheit erforderlich, sich auf die verfassungsrechtlichen Grundzüge des Aufbaus unseres Landes zu besinnen. Was zunächst etwas weit hergeholt erscheint, war im vergangenen Jahr ein wesentlicher Aspekt bei der Diskussion über die E-Government-Vereinbarung, die das Land, vertreten durch den Finanzminister, im Jahr 2003 mit den kommunalen Landesverbänden geschlossen hat (26. TB, Tz. 6.6). In dieser Vereinbarung bekundet das Land seine Absicht, im Einzelnen bezeichnete IT-Maßnahmen der „kommunalen Familie“ zu fördern, sofern diese mit den **Standardisierungsbemühungen** und den E-Government-Zielen des Landes konform gehen.

Derartige Konzepte sind unter Datenschutz- und Sicherheitsaspekten grundsätzlich zu begrüßen, weil sich aufgrund der einheitlicheren Strukturen in der Regel Lösungen mit **weniger Schnittstellenproblemen** ergeben. Allerdings findet der Nutzen der Vereinheitlichung dort seine Grenzen, wo über die Köpfe der Verantwortlichen hinweg entschieden wird. Diese Gefahr hat für einige Teilbereiche der E-Government-Vereinbarung durchaus bestanden, konnte aber zwischenzeitlich – nicht zuletzt durch unsere Intervention und Beratung – behoben werden.

Die Landesregierung und die kommunalen Landesverbände sehen in der Vereinbarung nämlich u. a. folgende Infrastrukturmaßnahmen als dringlich an und wollen die dazu erforderliche Basisinfrastruktur gemeinsam aufbauen:

- landesweit standardisierte Kreisnetze als integraler Bestandteil des landesweiten Datennetzes,
- ein landesweit wirksamer Verzeichnisdienst,
- eine landesweit einheitliche PKI mit digitaler Signatur und Ver- und Entschlüsselungsfunktionen und
- eine zentrale Datendrehscheibe für die Steuerung der Datenströme.

Hierzu wurde eine Lenkungsgruppe, eine Geschäftsstelle und eine Projektorganisation eingerichtet. Zudem erhalten die Kreise in ihrer Eigenschaft **als untere Landesbehörden** „zwangsweise" einen Anschluss an das Landesnetz. Zunächst bestand für sie aber noch kein Zwang, ihn zu nutzen bzw. auf ihren IT-Systemen Applikationen des Landes zu installieren und zum Ablauf zu bringen.

Zu Verwirrungen führten dann jedoch die Konsequenzen aus den Regelungen im Landesmeldegesetz und der **Landesmeldeverordnung**, nach denen der Datenaustausch zwischen Meldebehörden spätestens ab 2007 über „geschlossene Kommunikationsnetze" zu erfolgen hat.

Im Wortlaut: § 6 Abs. 1 Landesmeldeverordnung (LMV)

Die Datenübermittlungen zwischen Meldebehörden erfolgen durch Datenübertragung über geschlossene Kommunikationsnetze. ...

Hieraus schloss man, es dürfe nur das Landesnetz genutzt werden; um dies den ca. 220 Meldebehörden zu ermöglichen, bedürfte es eines Anschlusses entsprechend der E-Government-Vereinbarung in allen Kreisen und Kreisnetzen. Die Kreise seien mithin zur Erbringung dieser Dienstleistung gegenüber den ihnen angehörenden Gemeinden, Ämtern und Städten verpflichtet. Es schwirrten schon Begriffe wie **„virtuelle" und „dedizierte" Kreisnetze** im Raum. Wir wurden mit Fragen besorgter Systemadministratoren überhäuft, worin denn der Unterschied bestehe und nach welchen Sicherheitskonzepten der Anschluss der lokalen Netzwerke zu erfolgen habe. Offensichtlich wegen einer nicht sehr glücklichen Aufklärungsarbeit der beteiligten Stellen (Innenministerium, Finanzministerium, dataport und kommunale Landesverbände) sind zwei unterschiedliche Sachverhalte miteinander vermischt worden:

Richtig ist, dass die Meldebehörden gemäß der Meldeverordnung der Landesregierung über eine **technische Verknüpfungsstelle** zu kommunizieren haben. Zu diesem Zweck müssen alle Meldebehörden dataport mit dem Transport ihrer Meldedaten beauftragen. Es handelt sich also um den seltenen Fall, dass dem Bürgermeister die Installation und der Betrieb bestimmter IT-Komponenten und die Inanspruchnahme eines bestimmten externen Dienstleisters vorgeschrieben wird (Tz. 6.2). Mit der Frage, ob dies auf dem Verordnungswege möglich ist,

mögen sich Kommunalverfassungsrechtler befassen; sicherheitstechnisch bedarf es jedenfalls eines transparenten Sicherheitskonzeptes für die Verknüpfungsstelle (Tz. 6.3).

Unrichtig ist dagegen, dass die E-Government-Vereinbarung die Kreise verpflichtet, **Kreisnetze aufzubauen**, zu dem Zweck, die Meldedaten zu „kanalisieren", an die Verknüpfungsstelle weiterzuleiten und in umgekehrter Richtung als Verteiler zu agieren. Sie sind eben keine Meldebehörden und bezüglich ihres Serviceangebotes gegenüber ihren kreisangehörigen Kommunen entscheidungsfrei. Daran ändert auch die Tatsache nichts, dass der Landkreistag der Vereinbarung zugestimmt hat.

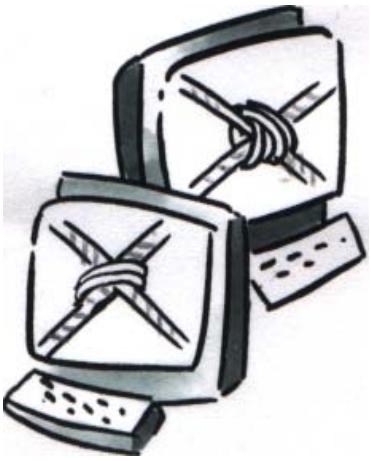
Dies ist nunmehr durch eine De-facto-Änderung der E-Government-Vereinbarung klargestellt worden. Der Finanzminister als Betreiber des Landesnetzes bietet nur noch „**kommunale Landesnetzanschlüsse**" an. Das gilt für jede einzelne Kommune, gleich welchen kommunalverfassungsrechtlichen Status sie hat und wie groß ihre Verwaltung ist. Hierüber schließt er mit ihr einen Vertrag. Kreisnetze werden aus der Sicht des Landesnetzes wie lokale Netzwerke des betreffenden Kreises behandelt. Die Beziehungen zwischen Kreis und Kommune basieren auf gesonderten (individuellen) Vereinbarungen; das Land ist daran nicht beteiligt. Für die Freischaltung der Kommunikationsbeziehungen in den Routern und deren sonstige Administration sind von den direkt angeschlossenen Kommunen bzw. den Kreisen spezielle Verträge mit dataport zu schließen, da der Finanzminister ihr durch einen Betreibervertrag die alleinige Administrationsbefugnis übertragen hat.

Diese intensiv ausdiskutierte **Lösung** zeichnet sich dadurch aus, dass die kommunalen Entscheidungsspielräume nur insoweit eingeschränkt werden, wie das Melderecht es vorsieht. Außerdem ergibt sich eine aus sicherheitstechnischen Gründen unabdingbare Möglichkeit der klaren Trennung der Verantwortungsbereiche der einzelnen Daten verarbeitenden Stellen. Die E-Government-Vereinbarung behält ihren ursprünglichen Status: Sie ist eine wichtige Absichtserklärung des Landes für die Zusammenarbeit mit den Kommunen auf dem Gebiet der Informationstechnik, sie hat aber für die einzelne Kommune keine verpflichtende Wirkung.

Was ist zu tun?
Bei der weiteren Projektplanung zur IT-Synchronisation zwischen dem Land und der „kommunalen Familie" sollten durch mehr Transparenz und frühzeitigere Beteiligung der letztendlich verantwortlichen Stellen Fehlinterpretationen vermieden werden. Die aktuellen Projekte „Verknüpfungsstelle", „PKI" und „Verzeichnisdienste" bieten hierzu gute Gelegenheiten.

6.5 PKI, virtuelle Poststellen, Clearingstellen und sonstige Geheimnisse

„E-Government“ verliert zunehmend die Aura des Besonderen. In den Vordergrund treten konkrete Fragestellungen zu den einzelnen Projekten. Diese befriedigend zu beantworten ist die Aufgabe der für den Echtbetrieb des E-Government Verantwortlichen. Geheimnisse darf es auf diesem Gebiet bald nicht mehr geben.



Die Anzahl und die Ausführlichkeit der Abhandlungen über die Segnungen des E-Government, die in den letzten fünf bis sechs Jahren verfasst worden sind, lassen viele andere Themen aus dem Bereich der Informationstechnik nebensächlich erscheinen. Trotzdem geht es im Augenblick mit der Sache nach **anfänglicher Euphorie** nicht so recht voran. Zitat eines Teilnehmers an einer der vielen E-Government-Kick-off-Veranstaltungen (an den Referenten gerichtet): „Ich danke Ihnen für die erneute anschauliche Darstellung von Zielvorstellungen, über die wir uns bereits vor einem Jahr unterhalten haben.“

Die Ursache für die zurückgehende Dynamik ist darin zu sehen, dass die **Visionen von den Realitäten eingeholt** werden. Sehr plastisch wird dies, wenn man sich die neueren Publikationen der Landesregierung zu dem Thema E-Government anschaut. Nach wie vor findet man die abstrakte Darstellung der „E-Government-Plattform“ als Wolke oder umfassendes Oval. Sie ist aber nur noch die gemeinsame Überschrift über die immer größer werdende Zahl der realen Applikationen, Dienstleistungen, Standards, Basisinfrastrukturen usw., die die bisher weitgehend leere Hülle ausfüllen.

Im Augenblick stehen folgende Begriffe im Raum:

- Landesnetz
- IKOTECH III / KITS
- PKI-SH
- elektronische Signatur
- CA TESTA
- Verzeichnisdienste
- Verwaltungsportal
- Verwaltungsdienstverzeichnis
- virtuelle Poststelle
- Workflow-System
- Formularserver
- Content-Management
- Dokumentenmanagement
- digitaler Atlas
- Mailverbund
- Internetgateway
- zentrales Virenmanagement
- zentrales Firewalling
- Clearingstelle
- kommunale Landesnetzanschlüsse

- Dienstleistungswegweiser
- Zahlungsplattform
- Geodatenkopfstellen
- Verlagerung von Front-Office-Prozessen
- Verlagerung von Back-Office-Prozessen
- Bündelung von regionalen Back-Office-Prozessen
- Lebenslagenkonzept
- Metropolregionkonzept
- private-public-partnership

Die Aufzählung ist sicher nicht vollständig. Es dürfte nur wenige IT-Spezialisten und noch weniger Verwaltungsfachleute im Lande geben, die alle Bezeichnungen richtig interpretieren und die praktischen Auswirkungen beurteilen können. Für viele sind die meisten Begriffe noch geheimnisvoll. Auch uns fällt der **Überblick zunehmend schwerer**. Dieser ist jedoch unabdingbar, denn hinter jedem Begriff verbirgt sich ein konkretes automatisiertes Verfahren, das unter Berücksichtigung der datenschutzrechtlichen und sicherheitstechnischen Rahmenbedingungen zu gestalten ist. Da es auf diesem Gebiet bisher nur vereinzelt verbindliche Verfahrensbeschreibungen und Sicherheitskonzepte gibt, sind wir auf „Dinge vom Hörensagen“ und auf die Interpretation von Ideenskizzen angewiesen. Dabei tun sich weit mehr Fragen auf, als wir Antworten finden.

Das beginnt z. B. mit der Festlegung, welche der vorgenannten Komplexe als Bestandteile der **IT-Basisinfrastruktur** anzusehen sind und damit der Verantwortung des zentralen IT-Management beim Finanzminister unterliegen. Einige Teile werden sicher als **Produkt bzw. Dienstleistung durch dataport** vermarktet werden. Beim Internetgateway ist das bereits heute der Fall mit der Folge, dass jeder Nutzer hierüber vertragliche Vereinbarungen direkt mit dataport zu schließen hat. Wer die virtuelle Poststelle repräsentiert und wann und durch welchen technischen Vorgang in dieser Stelle der rechtliche Übergang, also die Datenübermittlung vom Absender an den Empfänger erfolgt, ist offensichtlich noch nicht geklärt. Das Gleiche gilt für die Clearingstelle (Datendrehscheibe). Seitens des Melderechts gibt es zwar einige Vorgaben, über die Art ihrer Umsetzung und die Handhabung anderer Datenströme liegen jedoch noch keine Aussagen vor.

Von großer rechtlicher und sicherheitstechnischer Tragweite ist auch die Ausgestaltung der PKI (**private key infrastructure**). Im Teilbereich Verschlüsselung muss gewährleistet werden, dass keine Datenbestände entstehen, die die verantwortliche Behörde nicht selbst entschlüsseln kann. Bei der elektronischen Unterschrift lautet dagegen die Gretchenfrage: „Liegt der private Schlüssel unauslesbar in der Chipkarte des Benutzers oder als Datei im System desjenigen, dem gegenüber er rechtsverbindlich wirksam werden soll?“

In allen Fällen, in denen die örtlichen oder fachlichen Zuständigkeiten von Behörden durch (noch so sinnvolle) Integrationsmaßnahmen geändert werden sollen, bedarf es rechtlich einwandfreier **Rahmenbedingungen** (Auftragsdatenverarbeitungen, Aufgabenübertragungen, gesetzliche Experimentierklauseln u. Ä.), da andernfalls „verantwortungsfreie“ Räume entstehen könnten. Das gilt insbeson-

dere für das Management zentralisierter Datenbestände in Verzeichnisdiensten, Zahlungsplattformen, Zertifizierungsinstanzen, Workflow-Systemen usw. Dabei sollte ein besonderes sicherheitstechnisches Augenmerk auf diejenigen E-Government-Prozesse gerichtet werden, in die die Bürger eingebunden sind (Mailverkehr, Verwaltungsportal, Formularserver, Zahlungsplattform, Online-Fachanwendungen wie z. B. die Online-Melderegister und -Handelsregister sowie die Sachstandsauskünfte). In diesen Fällen tragen die Behörden, ähnlich wie die Geldinstitute beim Online-Banking, eine Mitverantwortung dafür, dass auch durch eine (etwas) fehlerhafte Nutzung der Dienste keine wesentlichen Risiken für die IT-Systeme der Nutzer entstehen.

Alles in allem dürfte es dringend an der Zeit sein, eine Prioritätenliste für die Verfahren zu erstellen und entsprechend dieser **Reihenfolge „belastbare" IT-Konzepte und Sicherheitsvorgaben** zu erarbeiten. Fatal wäre es, wenn durch Koordinationsdefizite an einer Stelle technische Fakten geschaffen würden, die an anderer Stelle zu schwer handhabbaren Sicherheitsproblemen führen. Insoweit besteht insbesondere im Bereich der Verzeichnisdienste und der Administration von Schnittstellenkomponenten Anlass zur Sorge.

Was ist zu tun?
Die Vielzahl der Absichtserklärungen und Planungen unter dem gemeinsamen Signum „E-Government" sollten kurzfristig priorisiert und auf die Ebene konkreter IT-Projekte gehoben werden. Die offenen Fragen zur Rechtmäßigkeit, zu Zuständigkeiten und zur Sicherheit sind umso besser zu lösen, je frühzeitiger sie formuliert und diskutiert werden.

6.6 Kontrollen vor Ort – ausgewählte Ergebnisse

6.6.1 Krankenhausinformationssystem Itzehoe

Obwohl die Sicherheitsdefizite im Krankenhaus Itzehoe von uns öffentlich kritisiert worden sind, konnten wir bislang keine entscheidenden Verbesserungen feststellen. Erst hat das Krankenhaus gegen die Veröffentlichung protestiert, jetzt schweigt es.

Bei der Vorstellung unseres Tätigkeitsberichtes für das Jahr 2003 (26. TB, Tz. 6.7.1) hatten wir das Zweckverbandskrankenhaus Itzehoe in Bezug auf dessen Patientendatenverarbeitung im Krankenhausinformationssystem als ein besonders problematisches Beispiel für die **schleppende Behebung von sicherheitstechnischen Mängeln** bezeichnet. Dies führte dort zu einer gehörigen Entrüstung und zu Widersprüchen in der örtlichen Presse.

Anfang 2004, also zwei Jahre nach Feststellung der Mängel, wurde noch nicht über deren tatsächliche Behebung, sondern nur über die Absicht, dies zu tun, gesprochen. Man habe jemanden beauftragt, einen Plan zu entwickeln. Es mag sein, dass dies in der Vergangenheit geschehen ist. Vielleicht sind auch einzelne Maßnahmen ergriffen worden. Uns ist darüber jedoch bis zum Redaktionsschluss dieses Berichtes nichts bekannt geworden. Da offensichtlich auch der Appell an

die Repräsentanten des Zweckverbandes als dem Träger des Krankenhauses nichts Entscheidendes bewirkt hat, haben wir uns entschieden, das Krankenhaus in die Liste derjenigen Stellen aufzunehmen, bei denen eine **Nachprüfung** unumgänglich ist. Dies wird geschehen, sobald hierfür die personellen Kapazitäten zur Verfügung stehen.

Was ist zu tun?
Falls das Krankenhaus zwischenzeitlich konkrete Verbesserungen in Bezug auf die Sicherheit der Patientendatenverarbeitung vorgenommen hat, sollten uns diese zum Zweck der Begutachtung bekannt gegeben werden.

6.6.2 Klein, aber oho!

Es kommt nicht auf die Größe einer Verwaltung an, wenn es um die Realisierung guter Sicherheitskonzepte geht. Eine kleine Amtsverwaltung wurde „Testsieger“ mit der Note „sehr gut“.

In den vergangenen Jahren gab es immer wieder Prüfungen, bei denen wir keinen Grund zu Beanstandungen gefunden haben bzw. bei denen die vorgefundenen Mängel von so geringer Bedeutung waren, dass uns das Wort „Beanstandung“ überzogen erschien. Aber auch in diesen Fällen haben wir einen Katalog von **Vorschlägen zur Verbesserung** der Datensicherheit hinterlassen und im Einzelnen mit der Behördenleitung und den Systemadministratoren erörtert.

Im abgelaufenen Berichtszeitraum haben wir erstmalig den Fall gehabt, dass uns keine schriftlich zu formulierenden Verbesserungsvorschläge eingefallen sind. Beim Amt Hanerau-Hademarschen handelt es sich um eine **kleine Amtsverwaltung** mit weniger als 20 IT-Arbeitsplätzen. Im Gegensatz zu der langläufigen Meinung, dass derartige Organisationseinheiten ihre IT-Systeme nicht effektiv und sicher managen könnten, fanden wir hier ein Konzept vor, das den Vergleich mit vielen großen Netzwerken standhält.

Worin liegt das Geheimnis der Lösung? Man hat nur solche Dinge in die Praxis umgesetzt, die **tatsächlich erforderlich** und **durch die Mitarbeiter beherrschbar** sind. Wenn also z. B. die Nutzung des Internets mit erheblichen Sicherheitsrisiken verbunden ist, warum muss man dann eine Verknüpfung mit dem gesamten lokalen Netz vornehmen? Ein Einzelplatzrechner als Internetstation reicht aus. Eingehende E-Mails werden ausgedruckt, mit einem Eingangsstempel versehen und wie ein normaler Posteingang behandelt. Von ausgehenden E-Mails braucht man ohnehin eine Kopie in den Akten. Wenn man sich beim Surfen oder beim Mailen trotz aller Vorsicht einen Virus oder ein anderes bösartiges Programm einfängt, wird der Internetrechner neu aufgesetzt, fertig! Die Fernwartung wird selbstverständlich nur im Bedarfsfall freigeschaltet; die Arbeiten des externen

Dienstleisters werden überwacht. Der leitende Verwaltungsbeamte hat zu Kontrollzwecken Zugriffsrechte auf alle Verzeichnisse. Der Systemadministrator und sein Vertreter haben getrennte Benutzerkennungen für ihre Aktivitäten als Administratoren und als normale Sachbearbeiter. Die Passwortregelungen sind plausibel, und das Gesamtsystem ist so dokumentiert, dass man sich auch darin zurechtfindet, wenn die Administratoren einmal nicht zur Verfügung stehen sollten. Kennzeichnend für die Einstellung der betreffenden Verwaltung war die Aussage: „Mehr brauchen wir nicht, warum sollen wir mehr machen?“

Was ist zu tun?
Die Amtsverwaltung Hanerau-Hademarschen sollte ihr gutes Konzept weiterverfolgen. Es ist zu hoffen, dass sie nicht durch Einflüsse von außen (z. B. Online-Kommunikationspflichten) zu Lösungen gezwungen wird, die das erreichte Sicherheitsniveau absenken.

6.6.3 Kreisnetz – klare Verhältnisse zwischen Kreis und Amtsverwaltung

Kein Kreis ist gezwungen, den ihm angeschlossenen Kommunen Netzdienstleistungen anzubieten. Tut er dies gleichwohl, müssen die Regelungen zur Auftragsdatenverarbeitung und zur Datensicherheit beachtet werden. Dies ist im Kreis Plön geschehen.

Parallel zu den vielfältigen Erörterungen über die Ausgestaltung von Kreisnetzen und der interkommunalen Zusammenarbeit auf der Basis von IT-Netzwerken (Tzn. 6.1 und 6.4) haben einige Kreise und Gemeinden bereits Fakten geschaffen. Sie haben Vereinbarungen über Kreisnetze getroffen und befinden sich im **Produktionsbetrieb**.

Auf einen solchen Kreisnetzanschluss sind wir bei einer sehr kleinen Amtsverwaltung gestoßen und deshalb insbesondere den Fragen nachgegangen: Bleibt das Amt noch **Herr des Geschehens**, oder ist es dem Kreis „ausgeliefert“? Lässt sich aus der Perspektive des Amtes nachvollziehen, was der Kreis tut, oder ist das Kreisnetz eine „Blackbox“?

Im Hinblick auf die Klarheit der Ausgestaltung des Auftragsverhältnisses und das erreichte Sicherheitsniveau aufseiten des Amtes und des Kreises Plön waren wir angenehm überrascht, dies umso mehr, als in dem netzunabhängigen Teil der IT-gestützten Datenverarbeitung des Amtes die üblichen Schwachstellen zu verzeichnen waren. Als **positive Eckpunkte des Kreisnetzanschlusses** sind hervorzuheben:

- In dem auf einem schriftlichen Betreibervertrag basierenden Sicherheits- und Betreiberkonzept ist festgelegt, dass der Datentransport über sternförmige dedizierte Kommunikationsleitungen (DSL-Leitungen) erfolgt. Die Daten werden auf dem Transportweg verschlüsselt.

- Die Fachanwendungen werden auf der Basis eines Terminalserversystems betrieben. Sie werden aufgrund spezifischer Nutzungsvereinbarungen beim Kreis „gehostet“.
- Die Kommunikation erfolgt stets über eine Service-Area beim Kreis. Direkte Verbindungen zwischen den Teilnehmern am Kreisnetz bestehen nicht.
- Es sind mehrere logische Netze definiert, die jeweils in eigenen Sicherheitsbereichen (DMZ) betrieben werden (z. B. Extranet-KoKoNet, Extranet-Landesnetz, Internet-Area).
- Die einzelnen Kommunen werden in einem Active Directory als Organisationseinheiten (OE) abgebildet. Der Administrator der jeweiligen Kommune behält die Befugnis, die Benutzerkonten der Mitarbeiter zu verwalten.
- Der Internetserver für E-Mail und WWW wird von der Kreisverwaltung betrieben. Die E-Mail- und WWW-Nutzung darf nur zu dienstlichen Zwecken erfolgen. Jeder Benutzer erhält eine Kreisnetz-E-Mail-Adresse. Darüber hinaus erhält jede Kommune eine „funktionale“, nicht personenbezogene E-Mail-Adresse.
- Zwischen der Kommune und der Service-Area des Kreises werden eine Firewall und ein Virenscanner eingesetzt. Der ein- und ausgehende E-Mail-Verkehr sowie der Aufruf von Webseiten wird für Kontrollzwecke protokolliert. Die Protokolle werden auf Anfrage der Kommunen den Verantwortlichen zur Verfügung gestellt. Die Löschung erfolgt nach sechs Monaten.
- Es erfolgt eine Content-Filterung der E-Mail-Dateianhänge. Anhänge mit bestimmten Dateiendungen werden geblockt.
- Downloads werden auf dem Internet-Proxy-Server in der Service-Area abgelegt. Auf lokalen Rechnern der Kommunen können keine Downloads abgelegt werden. Der Zugriff auf die Webseiten wird gefiltert. ActiveX-Controls, Java und Flash sind deaktiviert.

Das Konzept des Kreisnetzes stellt sich für die Kommune als **zweckmäßig und überschaubar** dar. Die organisatorischen Regelungen sind systematisch gegliedert und geben ihr einen ausreichenden Überblick über den Aufbau des Kreisnetzes und die darüber zur Verfügung gestellten Services. Die Zuständigkeiten der Kreisverwaltung und die der Kommune sind klar abgegrenzt. Für die Nutzung der Fachverfahren und der Internetdienste hat die Kreisverwaltung für die Kommunen einheitliche Regeln hoher Sicherheit festgelegt, die hinreichend durch Firewall-Systeme und Sicherheitssoftware umgesetzt wurden. Durch den Einsatz der Terminalservertechnologie in Verbindung mit einer Spezialsoftware lassen sich die Zugriffsbefugnisse der Kommunen auf die Services zentral administrieren.

Was ist zu tun?
Es ist an der Zeit, dass die Kreise, die ihren Kommunen Kreisnetzdienstleistungen anbieten, das jeweils erreichte Sicherheitsniveau und die Vertragsgestaltung untereinander abgleichen und soweit erforderlich optimieren.

6.7 Datenschutzmanagement erfolgreich automatisieren

Unternehmen und Behörden verlagern immer mehr Informationen in interne Netze. Dabei entstehen umfangreiche, unterschiedlich strukturierte Datenbestände mit einer Fülle von Zugriffsberechtigungen für Mitarbeiter, aber auch Externe. Solche Netze sind bisher für Unternehmen, Behörden und deren Datenschutzbeauftragte nur mit beträchtlichem personellen Einsatz und hohem technischen Fachwissen datenschutzrechtlich unter Kontrolle zu halten.

Eine effektive Lösung für die Einhaltung des Datenschutzes in solchen Umgebungen zu akzeptablen Kosten soll ein automatisiertes Datenschutzmanagement auf Netzebene bieten. Zu diesem Zweck werden vom World Wide Web Consortium (W3C), großen Softwareunternehmen und Forschungseinrichtungen technische Plattformen entwickelt, mit deren Hilfe notwendige Kontextinformationen zu personenbezogenen Daten so im Netz verfügbar gemacht werden, dass vor datenschutzrechtlich relevanten Vorgängen **eine automatisierte Prüfung der Zulässigkeit** des Vorgangs stattfinden kann.

So kann ein Autohändler gemäß einer unternehmensweiten Datenschutzpolicy freigeben, dass Werkstattmitarbeiter zur Beschaffung von Ersatzteilen die zu Servicezwecken gespeicherte Fahrgestellnummer seiner Kunden nutzt, dass die Auswertung derselben Daten durch die Marketingabteilung mit anschließender Werbeaktion aber vom System unterbunden wird. Die Umsetzung der Policy erfolgt auf technischem Wege durch die datenschutzgerechte **Zuweisung von Zugriffsrechten** für den Abrufenden.

Um international entwickelte technische Plattformen für ein automatisiertes Datenschutzmanagement auch für das deutsche Datenschutzrecht und damit **für Unternehmen und Behörden in Schleswig-Holstein nutzbar** zu machen, begleiten wir die Entwicklung der Systeme und bringen unser rechtliches Know-how zum deutschen Datenschutzrecht und die technischen Erfahrungen aus dem schon abgeschlossenen Projekt „Datenschutz im Internet mit Platform for Privacy Preferences (P3P)“ ein. Zu diesem Zweck veranstalteten wir zusammen mit der International School for New Media (isnm) und IBM in Lübeck einen mehrtägigen Workshop zur Umsetzung deutscher Rechtsnormen in Policies für ein automatisiertes Datenschutzmanagement.

www.datenschutzzentrum.de/adam/

Was ist zu tun?
Behörden und Unternehmen können ihre Organisation durch ein automatisiertes Datenschutzmanagement optimieren.

7 Neue Medien

7.1 Dienstvereinbarung Internet und E-Mail

Zwischen dem Finanzministerium des Landes einerseits und dem Deutschen Gewerkschaftsbund und dem Beamtenbund andererseits ist eine so genannte 59er-Vereinbarung über die Nutzung von Internet und E-Mail abgeschlossen worden. Wir haben an dieser Vereinbarung beratend mitgewirkt.

Die Richtlinie (Amtsblatt Schl.-H. 2005, S. 27) regelt die Grundsätze der dienstlichen und privaten Nutzung der Dienste Internet und E-Mail durch Landesbedienstete. Sie hat den Charakter eines **Kompromisses**, auch unter Gesichtspunkten des Datenschutzes. Unter den gegebenen Bedingungen bietet sie aber eine tragfähige Grundlage für die private Nutzung des dienstlichen Internetanschlusses. Nach Ablauf von zwei Jahren soll sie unter unserer Beteiligung auf „ihre Wirksamkeit und Zweckmäßigkeit einschließlich ihrer Auswirkungen auf die Datensicherheit“ überprüft werden.

Uns war wichtig, dass der als Arbeitsmittel bereitgestellte **E-Mail-Account** nicht für private Zwecke geöffnet wird. Eine solche Zulassung hätte nämlich zur Folge, dass eine aus Sicherheitsgründen nicht akzeptable Trennung zwischen privater und dienstlicher Kommunikation bei einem Account hätte stattfinden müssen. Um die Nutzung privater E-Mail über die dienstliche Anbindung nicht gänzlich auszuschließen, ist die Nutzung eines privaten E-Mail-Postfaches bei einem externen Diensteanbieter über **Webmail** zugelassen worden. Das Einschleppen schadhafter Anhänge soll dadurch vermieden werden, dass die Nutzung auf einen lesenden und schreibenden Zugriff beschränkt wird. Wie tragfähig diese Lösung ist, wird die spätere Evaluierung zeigen. Allen E-Mail-Nutzern sollte schon jetzt bewusst sein: Ein dienstlicher E-Mail-Account wie z. B. name@landsh.de ist keine private Adresse.

Die Richtlinie lässt eine private Nutzung des dienstlichen Internetzuganges mit zwei wichtigen **Einschränkungen** zu. Es dürfen erstens keine dienstlichen Interessen entgegenstehen. Zweitens ist nur die Nutzung von Webdiensten, aber z. B. nicht der Download von Dateien zu privaten Zwecken zulässig.

Von besonderer Bedeutung sind die Grundsätze über die Protokollierung und ihre Kontrolle. Die Richtlinie schließt eine individuelle Verhaltens- und Leistungskontrolle durch Auswertung von Protokolldaten grundsätzlich aus. Zum Zweck der Missbrauchskontrolle sieht die Richtlinie ein aus unserer Sicht vorbildliches gestuftes, am Grundsatz der Verhältnismäßigkeit orientiertes Kontrollverfahren vor. **Protokolldaten** werden zunächst nur anonymisiert ausgewertet. Erst wenn diese Auswertung Hinweise auf eine unzulässige Nutzung z. B. von inkriminierten Webseiten ergibt, ist der betroffene Kreis der infrage kommenden Nutzer auf die Unzulässigkeit dieses Verhaltens und die ab jetzt möglichen gezielten Kontrollen hinzuweisen. Werden weiterhin Verstöße festgestellt, lässt die Richtlinie eine gezielte Kontrolle nach einem gesondert festzusetzenden Verfahren zu. Die Richt-

linie implementiert auf diese Weise ein datensparsames und für die Nutzer transparentes Verfahren. Sie geht grundsätzlich von einem verantwortungsvollen Umgang mit dem Medium aus. Leider war es nicht möglich, das Kontrollverfahren bereits in der Richtlinie festzulegen.

Von praktischer Bedeutung sind die in der Anlage 1 getroffenen Regelungen über die Behandlung von **E-Mails mit einem Gefährdungs- und Belästigungspotenzial**. Um den strafrechtlichen Tatbestand der Nachrichtenunterdrückung zu vermeiden, werden solche E-Mails entweder mit einem Warnhinweis an den Empfänger übermittelt oder aber an der Firewall für die Dauer von 10 Tagen für den Empfänger zurückgehalten. Dieser wird darüber informiert, dass er die E-Mail zur Übermittlung anfordern kann.

Im Rahmen der Evaluierung wird zu bewerten sein, ob die **Speicherdauer** für die E-Mail-Protokolldaten sowie die Internetnutzungsdaten von 10 Tagen tatsächlich erforderlich ist. Nach unseren Erfahrungen werden Protokolldaten bereits aus Kapazitätsgründen selbst bei kritischen Vorfällen nicht länger als 48 Stunden gezielt zurückverfolgt.

Für die betriebliche Praxis ist von Bedeutung, dass die Kommunikation mit der **Personalvertretung** sowie mit besonderen Beauftragten wie dem behördlichen Datenschutzbeauftragten grundsätzlich nicht überwacht werden darf.

Nicht glücklich sind wir, dass die Richtlinie eine dienstliche Nutzung von **Anonymisierungsdiensten** ausdrücklich verbietet. Unseres Erachtens haben die Parteien dieser Vereinbarung verkannt, dass es aus Sicherheitsgründen auch ein erhebliches Interesse an einer unbeobachteten dienstlichen Nutzung von Internetdiensten geben kann.

Was ist zu tun?
Das Verfahren der Kontrolle von Protokolldaten ist von den Daten verarbeitenden Stellen jetzt zügig festzulegen, um für den Bedarfsfall keine Rechtsunsicherheiten aufkommen zu lassen. Die vorgesehene Evaluierung ist rechtzeitig vorzubereiten, damit die zur Bewertung erforderlichen Informationen nach Ablauf von zwei Jahren zur Verfügung stehen.

7.2 Digitales Kopieren

Wer digitale Kopiergeräte beschafft oder nutzt, sollte wissen, dass jedes kopierte Dokument mit den darin enthaltenen personenbezogenen Daten in dem Gerät elektronisch gespeichert wird. Aus diesem Grund haben wir erste Gestaltungsanforderungen aus Datenschutzsicht formuliert.

Beim digitalen Kopieren muss verhindert werden, dass Unbefugte von den auf der Festplatte gespeicherten Daten Kenntnis nehmen können. Da aus praktischen Gründen oft nicht festgelegt werden kann, wer im Einzelfall ein Dokument kopieren darf, muss die **Standardeinstellung** gewährleisten, dass der Kopiervorgang **keine Spuren** hinterlässt.

Die Speicherung eines Dokumentes darf nur über eine gesonderte Funktion des Nutzers ausgelöst werden. In diesen Fällen ist die Dokumentenspeicherung mit einem **exklusiven Lese- und Löschungsrecht** zu versehen, das von dem berechtigten Nutzer bzw. von der für die Verarbeitung verantwortlichen Stelle ausgeübt wird. Diese Anforderung wird umgesetzt, indem jedem Dokument eine Quellenkennung zugeordnet wird. Dem Systembetreiber muss es möglich sein, jederzeit alle gespeicherten Dokumente zu löschen – unabhängig von der Quelle, aus der die Daten stammen. So wird eine risikofreie Wartung oder Entsorgung des Gerätes ermöglicht.

Was ist zu tun?
Beim Einsatz digitaler Kopierer sind besondere Gestaltungsanforderungen zu beachten, um Datenschutzrisiken zu minimieren. Hersteller sollten sich für ihre Produkte um ein Datenschutz-Gütesiegel bemühen.

7.3 Eintrag im Telefonbuch: Widerspruch tut Not!

Wer vermeiden will, dass Dritte seine Rufnummer oder Anschrift über das gedruckte oder elektronische Telefonbuch erfahren, sollte hiergegen bei seinem Netzbetreiber Widerspruch einlegen. Dieses Recht kann jederzeit mit Wirkung für die Zukunft wahrgenommen werden.

Telefonbücher können praktisch sein: Wer die Rufnummer einer Person sucht, schaut häufig im gedruckten oder elektronischen **Telefonbuch** nach oder ruft die Auskunft an. Vielleicht findet man auf diesem Weg sogar die Adresse der gesuchten Person. Im Telefonbuch zu stehen kann aber auch lästig sein: Jeder kann einen anrufen oder aus dem Verzeichnis die Anschrift erfahren. Wer dies nicht will, sollte drei Dinge beachten:

- Im Telefonbuch steht man freiwillig. Der Teilnehmer bestimmt durch seinen **Antrag** beim Netzbetreiber, ob und mit welchen Angaben er im Telefonbuch steht.
- Eine Auskunft über seine Rufnummer kann der Teilnehmer unterbinden, indem er bei seinem Netzbetreiber gegen diese Praxis **Widerspruch** einlegt. Ohne ausdrückliche Einwilligung des Teilnehmers darf keine Auskunft über seine im Telefonbuch veröffentlichte Adresse erteilt werden.
- Seit Ende Juni 2004 darf die Auskunft bei Nennung einer Rufnummer den Namen und die Anschrift des gesuchten Anschlussinhabers nennen (so genannte **Inverssuche**). Voraussetzung ist, dass sich der Teilnehmer mit diesen Angaben in das Telefonbuch hat eintragen lassen. Dieser Inverssuche kann man ebenfalls bei seinem Netzbetreiber **widersprechen**.

Für die Datenschutzkontrolle der Netzbetreiber ist der Bundesbeauftragte für den Datenschutz zuständig. Die Aufsicht über die Netzbetreiber liegt bei der Regulierungsbehörde für Telekommunikation und Post.

Was ist zu tun?
Wer seine Privatsphäre schützen und selbst bestimmen will, welche Person seine Rufnummer bzw. Anschrift kennt, sollte entweder auf einen Eintrag in das Telefonbuch verzichten oder bei seinem Netzbetreiber gegen eine Auskunft über seine Daten widersprechen.

7.4 Safer Surfen ohne Verkehrsdatenspeicherung

Unsere Überprüfung der schleswig-holsteinischen Internetzugangsanbieter für Privat- und Einzelkunden brachte ein positives Ergebnis: Letztlich konnte bei allen überprüften Zugangsanbietern ein datenschutzkonformer Umgang mit den Daten der Internetnutzer festgestellt oder nach einem Dialog erreicht werden.

Schwerpunkt unserer Überprüfung war die Frage der **Speicherung und Nutzung der IP-Adresse** der Internetsurfer. Diese Adresse des Nutzerrechners ermöglicht beim Surfen im Internet die Übermittlung der aufgerufenen Webseiten. Sie wird von den Zugangsanbietern zumeist bei der Einwahl in das Internet für den Zeitraum dieser Nutzung vergeben (dynamische IP-Adresse). Mithilfe der IP-Adresse ist die Identifizierung des einzelnen Nutzers und das Ausforschen von dessen Surfgewohnheiten möglich.

Unseriöse Inhaltsanbieter im Internet speichern die IP-Adresse der Nutzer sowie die von ihnen besuchten Webseiten, um entgegen der geltenden Rechtslage **personenbezogene Verhaltensprofile** über die Internetnutzung zu bilden. Der Datenschutz im Internet steht und fällt mit der Frage, wie die mit der Speicherung der IP-Adresse verbundenen Datenschutzrisiken vermieden werden können. IP-Adressen dürfen entweder keinen Personenbezug aufweisen oder sind unmittelbar nach der Beendigung der Nutzung zu löschen bzw. zu sperren. Ausnahmen sind im Rahmen der Erforderlichkeit nur zur Abrechnung der Nutzung einzelner Webangebote zulässig. Diese Erforderlichkeit besteht in der Praxis bei Zugangs- und Inhaltsanbietern nur selten.

Unsere Prüfung galt der Frage, ob die **Internetprovider in Schleswig-Holstein** mit dem von ihnen gewählten Verfahren diese gesetzlichen Bestimmungen beachten. Das Ergebnis: Alle geprüften Internetzugangsanbieter verzichten auf eine längerfristige Speicherung dynamischer IP-Adressen in ungekürzter Form. In einigen Fällen lagen jedoch atypische Konstellationen vor, z. B. bei der Verwendung fester IP-Adressen oder bei so genannten virtuellen Providern, die nur die technischen Leistungen Dritter verkaufen. Diese Konstellationen wurden von unserer Standardprüfung ausgeklammert.

Unsere Recherche betraf sämtliche personenbezogenen Bestands- und Nutzungsdaten: Wie lange werden diese gespeichert? Werden sie für andere als die Erhebungszwecke genutzt? Gegenstand unserer Kontrolle war außerdem die Durchführung von Bonitätsprüfungen bei Vertragsabschluss und die Datenschutzkonformität der allgemeinen Vertragsbedingungen. Auch insofern konnten wir den Provi-

dern, teilweise nach Änderungen der Allgemeinen Geschäftsbedingungen, gute Noten ausstellen. Das Prüfungsergebnis bestätigt die gute Wettbewerbsposition Schleswig-Holsteins in Sachen Datenschutz. **Vom überzeugenden Datenschutzniveau der schleswig-holsteinischen Zugangsanbieter** zum Internet profitieren die Unternehmer wie die Nutzer. Datenschutz ist für Schleswig-Holsteins Internetprovider ein Standortvorteil, der über das Land hinausreicht.

Was ist zu tun?
Die Bürger sollten im Interesse ihrer Privatsphäre ihren Internetzugangsprovider sorgfältig auswählen und sich dabei bewusst für datenschutzkonform arbeitende Internetzugangsprovider entscheiden.

7.5 Sensitive Internetberatung

Im Internet werden teilweise kostenfreie Beratungsdienstleistungen angeboten, bei denen die Nutzer den Beratern sensitive personenbezogene Daten offenbaren. Die Anbieter müssen dabei Maßnahmen zum Schutz der Privatsphäre ihrer Nutzer ergreifen.

Die Beratung Suchtkranker und ihrer Angehörigen, die Telefonseelsorge oder die Opferberatung sind nur einige Beispiele für Dienstleistungen, die auch im Internet Zuspruch finden. Eine niedrige Hemmschwelle bei ihrer Nutzung im heimischen Umfeld und die weltweite Verfügbarkeit machen das **Internet als Übertragungsmedium** hier attraktiv.

Mit seiner Beratungsanfrage übermittelt der Nutzer in der Regel **hochpersönliche Daten**. Eine unverschlüsselte E-Mail ist hierfür kein geeignetes Mittel. Es sollten technische Lösungen gewählt werden, bei denen die komplette Beratungskommunikation auf dem Server des Beraters verwahrt und nach den gesetzlichen Vorgaben geschützt und gelöscht wird. Das Einstellen von Fragen und der Abruf von Antworten können z. B. über beinahe jedem Nutzer zugängliche **SSL-verschlüsselte Verbindungen** stattfinden.

Auch bei anderen Formen der Kommunikation, etwa in Chaträumen mit sensiblen Themen, sind verschlüsselte Datenverbindungen anzubieten. Erfolgt die Kommunikation nicht in Echtzeit, hat der Anbieter sicherzustellen, dass die **Rückantwort** tatsächlich den Fragesteller erreicht. Die Beratung eines missbrauchten Mädchens, das eine gemeinsame E-Mail-Adresse wie ihr Vater – in diesem Fall dem Täter – verwendet, würde dazu führen, dass die Beratungsantwort dem Peiniger zur Verfügung steht.

Der Internetberater muss dafür sorgen, dass auch **externe Dienstleister**, z. B. Hosting-Provider, auf sensitive Nutzerinformationen keinen Zugriff erhalten. Eine verschlüsselte Speicherung der Nutzerdaten auf den Servern stellt eine mögliche Lösung für diese Anforderung dar. Außerdem ist darauf zu achten, dass personenbezogene Daten, wie z. B. die IP-Adresse der Besucher der Website, nicht gespeichert werden. Eine Anleitung des Nutzers zur Verwendung eigener Anonymitätstools, wie z. B. des JAP, sind darüber hinaus sehr sinnvoll (Tz. 8.3).

Transparenz für den Nutzer in allen Datenschutzfragen sollte im Rahmen des Vertrauensverhältnisses zwischen Berater und Nutzer selbstverständlich sein. Eine **Datenschutzerklärung** möglichst im P3P-Format und ein besonderer Ansprechpartner für Datenschutzfragen sollten daher zur Grundausstattung jedes seriösen Internetberaters gehören.

 www.datenschutzzentrum.de/p3p/

Was ist zu tun?
Bürger, die Beratungsdienstleistungen über das Internet nachfragen, sollten die Seriosität und Vertrauenswürdigkeit des Anbieters auf die genannten Kriterien hin überprüfen.

7.6 GEZ kauft Daten beim Adresshandel ein

Wer ein Rundfunk- oder Fernsehgerät zum Empfang bereithält, muss Rundfunkgebühren bezahlen. Zwecks Feststellung der Gebührenpflicht erwirbt die Gebühreneinzugszentrale Adressdaten auf dem gewerblichen Markt. Gegen die Legalisierung dieser bisher unzulässigen Praxis haben wir Einspruch erhoben.

Der Einzug der Rundfunkgebühren ist eine hoheitliche Angelegenheit, die von der **Gebühreneinzugszentrale** (GEZ) im Auftrag der Rundfunkanstalten durchgeführt wird. Wer in welcher Wohnung wohnt und damit gebührenpflichtig sein könnte, darf die GEZ über das Melderegister ermitteln. Man sollte meinen, dass diese integre Quelle genügt, um Zu- und Wegzüge nachvollziehen zu können. Den öffentlichen Rundfunkanstalten reichte dies aber nicht aus. Durch eine Änderung des Staatsvertrages über die Rundfunkgebühren wurde der GEZ das Recht eingeräumt, sich zur Feststellung von Rundfunkteilnehmerverhältnissen Adressen auch bei privaten **Adresshändlern** zu kaufen – natürlich gebührenfinanziert.

Die neue Regelung ist das krasse Gegenteil einer bereichsspezifischen Erhebungsnorm. Sie begrenzt die Erhebung nicht, sondern verweist pauschal auf die **für die Privatwirtschaft einschlägigen Verarbeitungsregeln**. Damit hat der Landesgesetzgeber, der diesen Staatsvertrag ratifizieren musste, der GEZ viele Scheunentore zusätzlicher Erhebungs- und Verwendungsmöglichkeiten eröffnet, die es nun mühsam wieder zu schließen gilt. Nach dem Buchstaben des Gesetzes darf die GEZ nun – um nur zwei Beispiele zu nennen – personenbezogene Daten für Zwecke der Werbung an Dritte übermitteln. Sie dürfte sogar besondere Datenarten – hierzu zählen Informationen über den Gesundheitszustand, die Religion oder Rasse einer Person – erheben, verarbeiten oder nutzen. Dass eine solche Regelung der verfassungsrechtlichen Mindestanforderung nicht genügt, liegt auf der Hand.

Die neue Regelung eröffnet der GEZ zudem die Möglichkeit, zwischen hoheitlichen und privatrechtlichen Befugnissen zu „pendeln“ und sich je nach Wunsch und Bedarf den gebotenen öffentlich-rechtlichen Gesetzesbindungen zu entziehen.

Auch dies ist verfassungsrechtlich unzulässig. Juristen nennen dies einen **Formenmissbrauch**.

Nach Landesdatenschutzrecht müssen die Daten grundsätzlich offen bei den Betroffenen erhoben werden – die neue Erhebungsermächtigung aber ist geschaffen worden, um eine **heimliche Datenbeschaffung** an den Betroffenen vorbei zu ermöglichen.

Datenschutzbeauftragte aus Bund und Ländern haben diese Regelung kritisiert. Dennoch wurde der Staatsvertrag von den Landesparlamenten ratifiziert, auch vom **Landtag Schleswig-Holstein**. Immerhin hat dieser auf unsere Intervention hin die Landesregierung aufgefordert, unsere Bedenken kritisch zu würdigen und rechtzeitig vor der nächsten Änderung des Rundfunkgebührenstaatsvertrages über die Ergebnisse zu berichten.

Was ist zu tun?
Die Landesregierung sollte sich dafür einsetzen, dass die neue Regelung so bald wie möglich wieder außer Kraft gesetzt wird. Die Finanzierung des öffentlich-rechtlichen Rundfunks ist auf ein datensparsames Verfahren umzustellen.

8 Modellprojekte zum Datenschutz

Projekte zur datenschutzkonformen Technikgestaltung sind ein fester Bestandteil unserer Arbeit. Ihr Grundmotiv ist die Erkenntnis, dass das Anliegen des Datenschutzes, nämlich die Selbstbestimmung und Handlungsfähigkeit der Bürgerinnen und Bürger in einer zivilen Informationsgesellschaft zu gewährleisten, nicht ohne eine proaktive Gestaltung der Technik und ihrer organisatorischen und rechtlichen Rahmenbedingungen verwirklicht werden kann. „**Je früher desto besser – Datenschutz durch Technik**“ lautet unser Motto.

Die Vielzahl der Projekte bringt uns mit zahlreichen interessanten Partnern aus **Wirtschaft und Wissenschaft im In- und Ausland** in Verbindung, die unseren Sachverstand im Datenschutz suchen, um gemeinsam Ideen und innovative Konzepte und Produkte zu entwickeln. In diesem **Netzwerk** hat der Datenschutz als Gestaltungskomponente und als Akzeptanzfaktor ein großes Gewicht. Wir bringen unsere Datenschutzkompetenz ein, aber wir lernen dadurch auch eine Menge über die technische Entwicklung, über neue Anwendungen und erfolgreiche oder gescheiterte Geschäftsmodelle und ihre Hintergründe. Weil Kommunikation und Beratung für uns zentrale Merkmale unserer „Dienstleistung Datenschutz“ sind, ist das ULD über die Grenzen Schleswig-Holsteins hinaus mittlerweile ein gefragter Partner und begründet auf diese Weise zumindest einen weichen Standortfaktor für dieses Land.

8.1 Wettbewerbsvorteile mit dem ULD-i

Ziel des im Juni 2004 gegründeten Innovationszentrums Datenschutz & Datensicherheit (ULD-i) ist es, innovative Ideen rund um den Datenschutz und die Datensicherheit zu bündeln, um so neue und Erfolg versprechende Projekte zu initiieren.

Über die Projekte sollen **datenschutzkonforme Produkte** entwickelt werden, die neue Märkte für die Wirtschaft erschließen. Diese Integration von Datenschutz und Datensicherheit in die Produkte von morgen kann für Unternehmen einen wesentlichen Wettbewerbsvorteil bedeuten. Das ULD-i ist neben dem Datenschutz-Gütesiegel ein weiteres Hilfsmittel für die Wirtschaft, um sich von den Mitbewerbern abzuheben (26. TB, Tz. 1.1).

ULD-i
Datenschutz innovativ

Das ULD-i wirkt als **Innovations- und Servicezentrum** für Datenschutz und Datensicherheit. Es berät seine Partner über attraktive Fördermöglichkeiten, unterstützt die Antragstellung bei potenziellen Förderern, knüpft Kontakte zwischen Wirtschaft, Wissenschaft und weiteren Ideenträgern und vermittelt bei entsprechendem Bedarf kompetente Projektpart-

ner. Das ULD-i steht auch für die Durchführung und die Begleitung von Datenschutz- und Datensicherheitsprojekten zur Verfügung. Im Interesse der Entwicklung von datenschutzgerechten Produkten und entsprechenden Geschäftsmodellen und mit dem Ziel des Wissenstransfers und der konstruktiven Diskussion haben die Mitarbeiterinnen und Mitarbeiter des ULD-i im Berichtsjahr an vielen Veranstaltungen, insbesondere in Schleswig-Holstein, teilgenommen. Auf der CeBIT 2005 hat sich das ULD-i unter dem Motto „Ihr Wettbewerbsvorteil: Datenschutz durch Technik“ präsentiert.

Das ULD-i sieht sich nicht als Konkurrenz zu bestehenden Innovationszentren oder -stiftungen in Schleswig-Holstein, sondern als sinnvolle Ergänzung mit **Spezialisierung auf die Fragen von Datenschutz und Datensicherheit**: Die beteiligten Projektpartner sollen das Alleinstellungsmerkmal „Datenschutzkonformität“ zu ihrem Wettbewerbsvorteil nutzen und zugleich den Wirtschaftsstandort Schleswig-Holstein stärken. Unter

www.uld-i.de

präsentiert sich das Innovationszentrum auch online mit aktuellen Projekten, Gutachten und Informationen über neue Datenschutztechnologien. Der Servicebereich wird ständig weiter ausgebaut. In Kürze wird eine **Internetinnovationsbörse** zur Kontaktaufnahme zwischen verschiedenen Partnern mit Ideen rund um Datenschutz und Datensicherheit allgemein verfügbar sein.

Der Service des Innovationszentrums ist für alle Interessierte kostenlos. Ermöglicht wird das ULD-i durch eine bis Ende 2006 laufende **Kofinanzierung der Europäischen Union und des ULD**. Die Koordination erfolgte durch das Wirtschaftsministerium des Landes über das Regionalprogramm 2000 im Rahmen der Förderung der Technologieregion K.E.R.N.

Was kann das ULD-i für Sie tun?
Nehmen Sie Kontakt mit uns auf:

ULD-i
Holstenstr. 98, 24103 Kiel
Tel.: 0431/988-1399
kontakt@uld-i.de
http://www.uld-i.de

8.2 Identitätsmanagement

Identitätsmanagement ist für uns ein Schlüsselthema der Informationsgesellschaft. Es geht um die anspruchsvolle Aufgabe, welche Mechanismen und Werkzeuge wir den Nutzern in der elektronischen Welt anbieten sollen und müssen, damit sie wie im realen Leben auch in unterschiedlichen Rollen kommunikations- und handlungsfähig bleiben können.

Im Rahmen einer für die Firma T-Systems erstellten Studie in Kooperation mit der TU Dresden haben wir die rechtlichen Implikationen von Identitäts- und Rollenmanagement näher untersucht:

Bei Verwendung der Begriffe „Identitätsmanagement“ bzw. „Identitätsmanagementsystem“ gibt es grundsätzlich **drei verschiedene Verständnisarten**. Zum einen wird hierunter das Profiling verstanden, bei dem Organisationen bzw. Firmen Daten über ihre Interessenten und Kunden sammeln und verwalten. Diese Begriffe werden außerdem im Sinne eines Accountmanagement benutzt; dabei geht es um die Verwaltung der (Zugriffs-) Rechte der Mitarbeiterinnen und Mitarbeiter. Identitätsmanagement aus Datenschutzsicht hat den Nutzer als handelnde Person im Blick. Dieser soll in die Lage versetzt werden, über „Teilidentitäten“ Zugangsdaten, Konten oder Profile selbst zu verwalten und unter seiner Kontrolle zu halten.

Beim Einsatz von Identitätsmanagementsystemen müssen die **Grundsätze des Datenschutzes** beachtet werden. Nur die Daten dürfen verarbeitet werden, die für den entsprechenden Zweck erforderlich sind. Über den ursprünglich bei der Datenerfassung festgesetzten Zweck darf die Datenverarbeitung nicht hinausgehen. Grundsätzlich bedarf es hierfür der Einwilligung des Betroffenen. Schließlich ist der Betroffene über die näheren Umstände der Datenverarbeitung wie auch über seine Rechte umfassend aufzuklären. Zu diesen Grundsätzen gibt es teilweise Verschärfungen – etwa bei besonders sensiblen Daten wie Religionszugehörigkeit und dem Sexualleben – als auch Erleichterungen – etwa im Rahmen der Pflege von Kundenbeziehungen. Für alle Fälle gelten die Grundsätze der Datenvermeidung und Datensparsamkeit. Verfahren sind so zu gestalten, dass möglichst wenig personenbezogene Datenverarbeitung notwendig ist. Hieraus ergeben sich interessante Konstellationen im Rahmen der verschiedenen Arten von Identitätsmanagement.

- **Profiling**

Die vom Grundgesetz garantierte allgemeine Handlungsfreiheit begründet das Recht, als Betroffener bei der Angabe personenbezogener Daten unter Umständen die Unwahrheit zu sagen. Dies gilt nur dann nicht, wenn die Rechte Dritter und die allgemeinen Gesetze verletzt würden. In ein sehr wissbegieriges Formular für ein ausdrücklich kostenloses Chatsystem oder einen Newsletter darf derjenige, der sich anmelden will, z. B. falsche Angaben bei den Adressdaten eingeben. Etwas anderes gilt allerdings, wenn dies ausdrücklich oder konkludent vertraglich vereinbart wurde. Selbst bei Rechtsgeschäften kann beim „Handeln unter frem-

dem Namen“ eine **falsche Identität** angegeben werden, wenn hierdurch dem Geschäftspartner keine Nachteile entstehen, etwa weil die bestellte Ware sofort bezahlt wird, und kein sonstiges schützenswertes Interesse an der wahren Identität besteht. Das Interesse an Kundendaten zu Marketingzwecken fällt in der Regel nicht hierunter, sofern es nicht ausdrücklich Inhalt einer Vereinbarung war. Erfolgt eine bewusste Vorspiegelung einer anderen Identität, so sind die allgemeinen Vertretungsregeln anwendbar; der Täuschende haftet wie ein Vertreter ohne Vertretungsmacht.

Die Daten verarbeitende Stelle ist verpflichtet, nur so viele Daten zu verarbeiten, wie sie unbedingt zur Zweckerfüllung benötigt. Daher ist es dem Nutzer nicht zu verübeln, wenn er **falsche Daten** an den Stellen angibt, die unnötig sind. Dies ist weder rechtlich angreifbar noch moralisch verwerflich. Verwerflich ist eher, mehr Daten als nötig einzufordern. Im Rahmen der Verhältnismäßigkeit besteht für ein Unternehmen sogar die Verpflichtung, dem Betroffenen die Möglichkeit der **pseudonymen bzw. anonymen Nutzung** eines Dienstes einzuräumen. Dies ist bei der Gestaltung der Systeme von Anfang an zu berücksichtigen. Pseudonymisierungstechniken, sogar pseudonyme elektronische Signaturen sind vorhanden; in der Regel dürfte der Aufwand in Bezug auf die damit eröffneten Möglichkeiten verhältnismäßig sein. Die Bereitstellung von Identitätsmanagementkomponenten darf nicht als Option, sie muss oft als eine Verpflichtung angesehen werden. Gerichtsurteile hierzu gibt es zwar noch nicht, doch wurde z. B. Microsoft von der Artikel-29-Gruppe der Europäischen Union aufgefordert, sein Produkt .NET Passport auch für eine pseudonyme Nutzung ohne gültige E-Mail-Adresse anzubieten. Microsoft hatte zugesagt, diese Anforderung zu erfüllen.

- **Accountverwaltung / Personaldatenverwaltung**

Werden in Unternehmen die Accounts der einzelnen Mitarbeiter mit den jeweiligen Rechten verwaltet, so hat der **Arbeitnehmerdatenschutz** eine zentrale Bedeutung. Arbeitsverträge und Betriebsvereinbarungen sind dabei von Relevanz. Ist z. B. die private Internet- bzw. E-Mail-Nutzung erlaubt, hat der Arbeitgeber insofern nur beschränkte Überwachungsrechte. Ihm kann auferlegt sein, Sicherheits- und Datenschutzvorkehrungen wie ein normaler Internetprovider zu treffen. Dies betrifft auch eingehende E-Mails, was selbst das Überprüfen auf Spam zum rechtlichen Problem werden lässt. Es empfiehlt sich, in diesem Kontext den Mitarbeitern zwei unterschiedliche Accounts einzurichten, einen dienstlichen und einen privaten, für die dann auch unterschiedliche Regelungen gelten.

- **Identitätsmanagement durch die Mitarbeiter selbst**

Selbst innerhalb einer Organisation kann es notwendig sein, den Mitarbeitern die Wahl zwischen **verschiedenen Rollen** einzuräumen. Dies betrifft nicht nur das Handeln als Privatperson und Betriebsangehöriger. So haben z. B. Datenschutzbeauftragte wie auch Betriebsratsmitglieder besondere Rechte und Pflichten, die sie berechtigen, gegenüber der Organisationsleitung und selbst dem Administrator bei der Internetnutzung unbeobachtet zu bleiben. Mit Identitätsmanagementsystemen können derartige Rollen klar definiert und abgegrenzt werden. Für diese besonderen Rollen könnten z. B. Anonymisierungstools zugelassen werden.

Weitere Informationen zum Bereich Identitätsmanagement finden sich im Internet unter


www.datenschutzzentrum.de/idmanage/

8.2.1 Mit PRIME zu einem datenschutzkonformen Identitätsmanagement

Datenschutzgerechtes Identitätsmanagement in der Praxis ist der Fokus des EU-Projektes PRIME (Privacy and Identity Management for Europe). In dem Vierjahresprojekt entwickeln die 20 Partner Anwendungsszenarien und Prototypen, mit denen Nutzer mithilfe von selbstbestimmtem Identitätsmanagement ihre Datenschutzrechte leichter und effektiver wahrnehmen können.

PRIME ist im März 2004 gestartet. Gefördert wird es im Rahmen des 6. Europäischen Forschungsprogramms „Technologien für die Informationsgesellschaft“ (26. TB, Tz. 8.5). **Partner** sind Industrieunternehmen und Forschungseinrichtungen aus dem In- und Ausland: IBM France als Projektkoordinator, IBM Research, Zürich Research Lab (Schweiz), Technische Universität Dresden (Deutschland), Katholieke Universiteit Leuven (Belgien), Universiteit van Tilburg (Niederlande), Hewlett-Packard (England), Karlstads Universitet (Schweden), Università di Milano (Italien), Joint Research Centre Ispra (Italien), Centre National de la Recherche Scientifique – LAAS (Frankreich), Johann Wolfgang Goethe-Universität Frankfurt a. M. (Deutschland), Chaum LLC (USA), RWTH Aachen (Deutschland), Institut EURECOM (Frankreich), Erasmus University Rotterdam (Niederlande), Fondazione Centro San Raffaele del Monte Tabor (Italien), Deutsche Lufthansa (Deutschland), Swisscom (Schweiz) und T-Mobile (Deutschland).

PRIME entwickelt einen **Prototyp eines Identitätsmanagementsystems**, der als Open-Source-Software von jedermann eingesetzt und weiterentwickelt werden kann. Angestrebt werden Lösungen, die die Menschen unterstützen, die Kontrolle über ihre Privatsphäre zu behalten und sich in den diversen Rollen des privaten und geschäftlichen Lebens zu managen. Angeregt werden soll der nachhaltige Einsatz von datenschutzfördernden Identitätsmanagementlösungen.

Die Projektarbeit wird begleitet von Experten aus den Bereichen **Recht, Sozialökonomie und Benutzungsfreundlichkeit**. Die Rahmenbedingungen und Spezifikationen für Lösungen eines Identitätsmanagements werden in PRIME untersucht und vorangetrieben. Auch die Standardisierung liegt im Blickpunkt von PRIME. Das WWW-Konsortium (W3C) arbeitet als Unterauftragnehmer mit.

Unsere Aufgaben bestehen in der rechtlichen, insbesondere datenschutzrechtlichen Begleitung, der Erarbeitung von speziellen Kriterien für datenschutzfreundliche Lösungen, die Gestaltung von Nutzungsoberflächen sowie die Vermittlung des Gesamtprojektes in der Öffentlichkeit. Weitere Informationen zum Projekt befinden sich im Internet unter


www.prime-project.eu.org
www.datenschutzzentrum.de/idmanage/

Was ist zu tun?
Wir werden maßgeblichen Einfluss auf die datenschutzgerechte Gestaltung von Identitätsmanagementsystemen nehmen und stehen Ihnen als Ansprechpartner zur Verfügung.

8.2.2 FIDIS – Projekt zur Zukunft der Identität in der Informationsgesellschaft

Wie sieht die Identität der Zukunft aus? Das ist auch aus Datenschutzsicht eine spannende Frage. Wir bringen unser Know-how in das EU-Projekt FIDIS (Future of Identity in the Information Society) ein, das im Rahmen des 6. Europäischen Forschungsprogramms „Technologien für die Informationsgesellschaft" gefördert wird.

Im Vordergrund steht bei FIDIS der Aufbau eines interdisziplinären „**Network of Excellence**" (26. TB, Tz. 8.5). Insgesamt 24 europäische Institutionen diskutieren seit April 2004 unter der Geschäftsführung von Prof. Dr. Rannenberg, Universität Frankfurt, über Fragen rund um Identität und Identitätsmanagementsysteme. Ziel des Projekts mit einer Laufzeit von fünf Jahren ist die Gestaltung der Zukunft im Sinne einer gerechten Informationsgesellschaft. 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.

Wir vertreten die Aspekte Datenschutz- und Datensicherheitssicht in vielen der FIDIS-Aktivitäten, z. B. wenn es um „Identity Theft" (Identitätsdiebstahl) oder „Profiling" geht. Eine leitende Funktion haben wir im **Workpackage** zu „High-tech IDs", das sich mit den Themen Identitätsmanagement, digitale Signaturen und PKI, ubiquitäres Computing (Tz. 8.6), mobile Identitäten und Biometrie auseinander setzt. Unsere Beiträge stellen die Datenschutzsicht zu neuen Technologien zur Diskussion, um im Netzwerk Lösungen für rechtliche und technische Probleme erarbeiten zu können. Die Ergebnisse der Arbeit sollen in die **internationale Standardisierung** einfließen.


www.fidis.net
www.datenschutzzentrum.de/idmanage/

Was ist zu tun?
Das datenschutzkonforme Identitätsmanagement der Zukunft bedarf der Einbindung in Anwendungen. Hierzu ist die Beteiligung an der technischen Standardisierung notwendig.

8.2.3 Aufbau einer Datenbank zu Identitätsmanagementsystemen

Im Rahmen des Projekts FIDIS ist das ULD damit betraut, eine Datenbank zu Identitätsmanagementsystemen zu entwickeln und aufzubauen. Es geht um eine bisher einzigartige Aufbereitung der Marktlage bei „Identitätsmanagern".

Gemeinsam mit dem Institut für Technologische Zukunftsforschung (IPTS) der Generaldirektion Gemeinsame Forschungsstelle in Sevilla (Spanien) haben wir die Struktur für eine Datenbank erarbeitet, die seit Anfang 2005 zunächst von den übrigen FIDIS-Partnern mit Informationen über Identitätsmanagementsysteme gefüllt wird. Dafür wurden vom ULD Richtlinien erarbeitet. Die Struktur der Datenbank soll Details über einzelne Produkte vermitteln und einen schnellen **Überblick über den Markt und die Entwicklung** in diesem Bereich verschaffen. Die Ergebnisse unserer IMS-Studie vom vergangenen Jahr (26. TB, Tz. 8.5), in der unter anderem die Systeme Microsoft .NET Passport, Liberty Alliance, Yodlee, CookieCooker, Mozilla, Outlook Express und Novel DigitalMe besprochen wurden, dienten als Vorlage für die Datenbank. Wir haben außerdem eine Liste mit über hundert Einzelanwendungen und Techniken zusammengestellt und in die Datenbank eingepflegt. Die Übersicht soll sowohl wissenschaftlichen Ansprüchen genügen als auch die Basis für fundierte Endanwenderinformationen bilden.

Die rasante Entwicklung auf diesem Markt führte zur Einstellung einzelner Produkte, z. B. DigitalMe; vor allem sind aber zahlreiche Neuentwicklungen hinzugekommen. In einem nächsten Arbeitsschritt werden wir einige dieser **Neuentwicklungen** in unserem IT-Labor genauer untersuchen und testen.

Was ist zu tun?
Neuerscheinungen auf dem Gebiet der Identitätsmanager sind gründlich zu untersuchen und zu testen. Der Markt ist ständig im Blick zu behalten, um neue Trends berücksichtigen zu können.

8.3 AN.ON

Die Förderung des Anonymisierungsdienstes AN.ON konnte bis März 2006 verlängert werden. Zahlreiche Medienberichte trugen zur Steigerung der Nutzerzahlen bei. Das Projekt findet auch verstärkt Zuspruch; weitere Institutionen beteiligen sich mit so genannten Mixservern.

Das seit Anfang 2001 bei uns in Kooperation mit der Technischen Universität (TU) Dresden, der Freien Universität Berlin, der Humboldt-Universität Berlin und der Universität Regensburg durchgeführte und vom **Bundesministerium für Wirtschaft und Arbeit** geförderte Projekt „AN.ON – Anonymität online" (26. TB, Tz. 8.3) wird bis März 2006 weiter gefördert. Mittlerweile konnte die technische Basis durch weitere Mixbetreiber erweitert werden. Seit Ende 2004 betreibt der Chaos Computer Club (CCC) einen eigenen Mixserver.

Die Software JAP kann von jedermann kostenlos aus dem Internet heruntergeladen werden. Mithilfe dieses Tools wird die anonyme Nutzung von Diensten im World Wide Web ermöglicht. Bei Verwendung von JAP erfolgt der Kontakt zu den Webservern nicht – wie sonst üblich – unmittelbar, sondern für den Nutzer unsichtbar über eine **Kette von Verschlüsselungsservern** (so genannte Mixserver). Diese sorgen dafür, dass niemand Kenntnis von der IP-Adresse des Nutzers erlangen kann. Hierin besteht die Besonderheit von AN.ON gegenüber anderen Anonymisierungsdiensten. AN.ON garantiert Anonymität und Unbeobachtbarkeit nicht nur gegenüber dem Anbieter der angesurften Webseiten sowie dem eigenen Serviceprovider, sondern auch gegenüber den Betreibern des Anonymisierungsdienstes selbst.

Auch 2004 lag eine unserer Aufgaben im Rahmen des AN.ON-Projektes darin, **Anfragen von Strafverfolgungsbehörden und Privatleuten** nach Informationen über Nutzer des AN.ON-Dienstes zu beantworten. Wir geben stets die Auskunft, dass AN.ON-Nutzerdaten im Einklang mit den gesetzlichen Regelungen nicht vorliegen und daher auch nicht herausgegeben werden können. Dem deutlichen Anwachsen der Zahl von gleichzeitigen Nutzern des Dienstes steht nur eine geringe Zunahme der Anfragen wegen Missbrauchs gegenüber, sodass wir davon ausgehen, dass der Missbrauch des Dienstes gering ist.

Im Mai 2004 organisierten wir gemeinsam mit dem Innenministerium des Landes in Kiel einen **Workshop** zu Fragen von **Strafverfolgung und Datenschutz** im Internet. Auslöser hierfür waren die Gerichtsbeschlüsse des vergangenen Jahres in Sachen BKA gegen AN.ON Behandelt wurden von den Vertretern der Polizei, der Justiz, von Datenschutzinstitutionen, der Wissenschaft, von Internetprovidern und AN.ON grundsätzliche Fragen der Strafverfolgung im Internet. Die Strafverfolger berichteten aus verschiedenen Ermittlungsverfahren, u. a. im Bereich der Kinderpornografie, von Problemen bei der Rückverfolgung von IP-Adressen. Die Provider wiesen auf die abnehmende Bedeutung der IP-Adresse hin und zeigten dennoch Wege für Strafermittlungen. Die Vertreter von AN.ON stellten aktuelle und zukünftige Entwicklungen im Bereich Anonymität und Identitätsmanagement vor. In der Diskussion wurde herausgearbeitet, unter welchen Bedingungen eine Funktion zur Mitprotokollierung von Zugriffen auf bestimmte Seiten aktiviert werden darf und zur Identifizierung der IP-Adresse bzw. deren Nutzer rechtlich möglich sein kann.

Der „**BKA-Fall**“ beschäftigte uns im Berichtsjahr weiter (26. TB, Tz. 8.3). Der Hessische Datenschutzbeauftragte teilte uns Anfang 2004 mit, die Staatsanwaltschaft Frankfurt a. M. habe nach eigenen Aussagen in der Ermittlungsakte die unzulässig beschlagnahmte IP-Adresse durch Schwärzung der letzten sieben Stellen anonymisiert. Das Bundeskriminalamt (BKA) sei aufgefordert worden, in seinen Unterlagen entsprechend zu verfahren, geschwärzt wurden dann aber nur die letzten fünf Stellen. Speicherungen in Amtszentral- oder Verbunddateien des BKA seien nicht erfolgt. Das BKA hatte zunächst erklärt, der beschlagnahmte Datensatz mit der mitgeloggten IP-Adresse sei an das Landeskriminalamt (LKA) Sachsen übermittelt worden. Dieses erklärte uns hingegen, den Protokolldatensatz nicht erhalten zu haben. Das LKA habe zwar bei der Durchsuchung dem BKA Amtshilfe geleistet, aber keine Daten zu keinem Zeitpunkt gespeichert. Offen-

sichtlich wurde im LKA in Dresden die Datei auf einem BKA-Laptop über einen Internetzugang des LKA Sachsen heruntergeladen. Kopien wurden nach polizeilichen Angaben nicht erstellt. Damit ist unsere Suche nach dem beschlagnahmten Datensatz zunächst abgeschlossen. Der Fall zeigte uns exemplarisch, wie schwierig es ist, den Verlauf einmal von Sicherheitsbehörden erfasster Daten nachzuvollziehen und Löschungsrechte durchzusetzen. Sicherheit über die restlose Löschung von Daten ist kaum zu erlangen. Der beste Datenschutz ist, die betreffenden Daten erst gar nicht zu erheben.

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

Was ist zu tun?
Internetnutzern steht zum Schutz ihrer eigenen Kommunikation der Anonymisierungsdienst AN.ON zur Verfügung. Jeder kann sich als Mixbetreiber an dem Projekt beteiligen. Gemeinsam mit Strafverfolgungsbehörden sind Lösungen zur Bekämpfung von Internetkriminalität zu finden.

8.4 Das Virtuelle Datenschutzbüro gedeiht

Das Virtuelle Datenschutzbüro erfreut sich weiterhin eines wachsenden öffentlichen Interesses. Inhaltliche Weiterentwicklungen sowie eine gesteigerte Beteiligung vieler Projektpartner machen das Datenschutzportal zu einer zentralen Informationsquelle.

Das Virtuelle Datenschutzbüro konnte seine Stellung als **erste Anlaufstelle zu Fragen des Datenschutzes** im deutschsprachigen Raum im Berichtszeitraum behaupten. So ist www.datenschutz.de weiterhin unangefochten die Nummer eins in der Suchmaschine Google, wenn man den Begriff „Datenschutz“ eingibt.

Das Virtuelle Datenschutzbüro wurde im Zuge der bestehenden Projektpartnerschaft des Norddeutschen Rundfunks (NDR) in den **Videotext**-Content mit einer eigenen Serviceseite aufgenommen und ist damit auch in diesem viel genutzten Medium präsent. Es wird eine stets erreichbare Multipage (Videotextseite 662) seitens des NDR bereitgestellt, welche Basisinformationen zum Datenschutzportal enthält. Zudem besteht für das Virtuelle Datenschutzbüro die Möglichkeit, nach Absprache mit der Redaktion des NDR aktuelle Datenschutznachrichten auch in diesem Medium bereitzustellen.

Im letzten Jahr wartete das Virtuelle Datenschutzbüro (zuletzt 26. TB, Tz. 8.2) mit einer optisch aufgefrischten Startseite und weiteren **Neuerungen** auf. Das Zusammenstellen und Aktualisieren von Feature-Seiten zu bestimmten Schwerpunktthemen erweist sich als wichtiger Service, wie gezielte Anfragen oder Linkverweise anderer Webseiten belegen. Das Hinzufügen weiterer, sich aus der aktuellen Datenschutzdiskussion anbietender Schwerpunktthemen hängt von den Ressourcen und der Mitwirkung einzelner Projektpartner ab.

Die 2003 implementierte chronologische **Veranstaltungsübersicht** einzelner Fortbildungskurse hat sich bewährt. Veranstaltungsanbieter, die zumeist zugleich Kooperationspartner des Virtuellen Datenschutzbüros sind, nutzen diese Veranstaltungsdatenbank für eigene Kurshinweise. Damit wird Interessenten die Möglichkeit des direkten Vergleichs von infrage kommenden Angeboten gegeben.

In der Realisierung zeitintensiv war die Fertigstellung und Implementierung einer **Datenbank zu Literatur und Gerichtsentscheidungen** als neuem Service des Virtuellen Datenschutzbüros. Diese datenschutzspezifische Literaturdatenbank erweitert das bereits bestehende Angebot um den Nachweis von Offline-Beiträgen. Dokumentiert werden hauptsächlich Beiträge aus klassischen Datenschutzzeitschriften (Datenschutz und Datensicherheit – DuD, Computer und Recht – CR, Recht der Datenverarbeitung – RDV). Mittlerweile weist die Literaturdatenbank über 600 Einträge auf. Wie bei den Meldungen von News, Artikeln und Veranstaltungen lebt auch dieses Angebot von der aktiven Mitgestaltung der Projekt- und Kooperationspartner.

Einen Mehrwert bietet die Literaturdatenbank durch ihre Verzahnung mit dem bereits bestehenden Schlagwortsystem. Der Nutzer erreicht die Literatureinträge über den **Schnellverweis** (Quicklink) „Literatur“ des jeweiligen Schlagwortes. Dieses System ist den Nutzern bereits von den Schnellverweisen „Presse“, „Glossar“, „Tätigkeitsbericht“ und „Gesetze“ her bekannt. Zusätzlich steht dem neuen Angebot eine **eigenständige Suchfunktion** zur Verfügung, in der explizit nach Autor, Stichwort und Publikationsart innerhalb der Literaturdatenbank recherchiert werden kann. Unterstützte Publikationsarten sind Bücher, Buchbeiträge, Zeitschriftenbeiträge und Gerichtsentscheidungen. Leider ist die Nutzung und insbesondere die weitere Ergänzung von datenschutzspezifischen Literaturhinweisen bislang hinter den Erwartungen und Möglichkeiten zurückgeblieben. Dem soll durch verstärkte Information bei Projekt- und Kooperationspartnern sowie in der Öffentlichkeit im kommenden Jahr entgegengewirkt werden.

Der Erfolg und Fortbetrieb des Projekts ist auch von den **finanziellen und inhaltlichen Beiträgen** der Projektpartner abhängig. Es ist erfreulich, dass sich mehrere Projektpartner verstärkt beteiligen. Die Attraktivität des Internetportals für den Nutzer wird mit jeder einzelnen Artikel-, News-, Veranstaltungs- oder Publikationsmeldung gesteigert. Der die Meldung verfassende Partner kann durch seinen Beitrag den Bekanntheitsgrad des Virtuellen Datenschutzbüros erhöhen und zugleich die eigenen Informationen einer breiteren Öffentlichkeit zugänglich machen.

www.datenschutz.de

Was ist zu tun?
Das Virtuelle Datenschutzbüro ist die Plattform des deutschsprachigen Datenschutzes. Seinen Aufschwung gilt es zu sichern und zu verstärken. Die ständig wachsende Informationsfülle macht die aktive Mitwirkung vieler Projektpartner unerlässlich.

8.5 RISER – Datenschutzgestaltung einer europäischen Melderegisterauskunft

Die europäische Melderegisterauskunft RISER ist ein E-Government-Dienst, mit dem grenzüberschreitend in Europa Auskünfte aus den in den Ländern bestehenden Melderegistern eingeholt werden können. Unsere Aufgabe ist die datenschutzkonforme Gestaltung dieses Dienstes.

Der Service RISER (Registry Information Service on European Residents) richtet sich an Unternehmen und Bürger und bietet einen einheitlichen Zugang zu den unterschiedlichen Melderegistern in Europa, soweit nach Art und Umfang eine „Jedermann"-Auskunft zulässig ist. Über das Portal www.riser.eu.com werden die **Meldeanfragen** als Datei- oder Einzelanfrage an die zuständige Meldebehörde weitergeleitet und von dort beantwortet. RISER übernimmt lediglich die Funktion eines Zustellers. Seit September 2004 können Melderegisterauskünfte in Deutschland und seit Dezember 2004 auch in Österreich in Auftrag gegeben werden. Ein Service zur Adressverifizierung für Irland ist in Vorbereitung. In den kommenden Monaten werden weitere Mitgliedstaaten der Europäischen Union folgen.

Wir begleiten die Gestaltung von RISER, um eine datenschutzkonforme Gestaltung dieses Dienstes zu gewährleisten. Sicherzustellen ist insbesondere, dass die Adressdaten aus den Anfragen nicht zentral gespeichert und verarbeitet werden und **kein europäisches Melderegister** aufgebaut wird. In einem Datenschutzreport werden die unterschiedlichen nationalen Anforderungen des Datenschutzes auf den verschiedenen rechtlichen Ebenen des Melderechts und der elektronischen Kommunikation formuliert und dargestellt. In Richtlinien zur Datensicherheit und zum Datenschutz sind diese Anforderungen konkretisiert.

Bei der technischen Umsetzung des Dienstes kann RISER in Deutschland mit **XMeld** auf ein getestetes und bei den Meldebehörden im Einsatz befindliches Datenformat zurückgreifen. Der Einsatz des offenen Standards **OSCI-Transport** zur sicheren Datenübermittlung gestaltet sich zurzeit noch schwierig, da dieser Standard bei den Meldebehörden noch nicht weit verbreitet ist; er ist aber vorgesehen.

Das Projekt wird seit März 2004 bis August 2005 von der Europäischen Kommission aus dem Programm eTen gefördert. Durchgeführt wird es von einem internationalen Konsortium unter der Führung eines Berliner Softwarehauses, der PSI AG, mit weiteren **Partnern** aus Deutschland, Österreich, Irland und Polen. Aus Deutschland sind neben uns und der PSI AG das Fraunhofer-Institut Fokus und das Landeseinwohneramt Berlin beteiligt, aus Österreich das Zentrum für Verwaltungsforschung (KDZ), aus Irland das Waterford Institute of Technology (WIT) sowie aus Polen die Einrichtung ARAM.

www.datenschutzzentrum.de/riser/index.htm
www.riser.eu.com/

Was ist zu tun?
Damit RISER für einen grenzüberschreitenden E-Government-Dienst in Europa eine Vorbildfunktion bekommt, müssen die europäischen Datenschutzstandards implementiert werden.

8.6 TAUCIS: Ubiquitäres Computing datenschutzkonform gestaltet

RFID ist nur der Vorbote einer nicht allzu fernen Zukunft, in der die an Gegenständen des täglichen Lebens angebrachten Prozessoren untereinander über ihre Inhaber zu sprechen beginnen. Wir untersuchen die Folgen des „ubiquitären Computing" und die datenschutzkonformen Gestaltungsmöglichkeiten dieser neuen Technologie.

TAUCIS steht für „Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung". Ubiquitäres Computing bedeutet **allgegenwärtige Datenverarbeitung**. Diese neue Generation der Datenverarbeitung stellt den Datenschutz vor neue Herausforderungen. Alltagsgegenstände sollen künftig mit zusätzlichen Funktionen ausgestattet werden, die durch sehr kleine Prozessoren, Speicher, Sensoren und Kommunikationsschnittstellen Daten über ihre Umgebung erfassen, speichern, auswerten und übermitteln. Auf diese Weise soll sich z. B. die Alltagsumgebung auf die Vorlieben und Gewohnheiten der Menschen, die sie nutzen, optimal einstellen können.

Ein erster Schritt auf dem Weg in diese schöne neue Welt ist die Ausstattung von Waren mit kleinen Transpondern, so genannten RFID-Tags. Mit **Radio Frequency Identification** erfolgt eine individuelle Identifizierung von Waren oder sonstigen Objekten. Ob auf dem Speichermedium oder in den mächtigen Hintergrundsystemen mit Lesegeräten – ubiquitäres Computing eröffnet heute noch kaum vorstellbare Möglichkeiten, das Verhalten von Menschen über die Objekte, die sie mit sich tragen oder nutzen, zu erfassen und zu verarbeiten.

> **?** ***RFID***
>
> *Radio Frequency Identification – auf Deutsch: Identifikation per Funk – dient dem kontaktlosen Auslesen und Einspeichern von Daten. Die Daten werden auf so genannten RFID-Tags gespeichert, die keine eigene Energieversorgung benötigen. Die Tags können wegen ihrer geringen Größe als Etiketten nahezu überall angebracht werden. Mit ihnen kann eine eindeutige Identifikation von Produkten und, wenn diese von Personen mitgeführt werden, auch von Menschen erfolgen. Wegen der kontaktfreien Datenübertragung können sie vom Träger unbemerkt ausgelesen werden.*

Diese Technik bietet unbestreitbare wirtschaftliche Vorteile, z. B. in der Warenlogistik. Umso wichtiger ist ihre datenschutzkonforme Gestaltung, wenn die Daten der Bürgerinnen und Bürger erfasst werden. Denkbar ist die Technik zur **elektronischen Überwachung** von großen Menschenmassen. Dies wird im Großversuch anlässlich der Fußballweltmeisterschaft 2006 erprobt werden.

www.datenschutzzentrum.de/allgemein/wmticket/
www.datenschutzzentrum.de/material/themen/presse/20050311-dsbk-wm.htm

Unser **Partner** bei dem bis März 2006 terminierten Projekt ist das Institut für Wirtschaftsinformatik an der Humboldt-Universität Berlin, das bereits seit längerem über ubiquitäres Computing und Privacy-Aspekte forscht. Zur Förderung ausgewählt wurde das Projekt im Rahmen des Wettbewerbes „Innovationspotenziale der Informations- und Kommunikationstechnologie“ des Bundesministeriums für Bildung und Forschung. Informationen zum Projekt gibt es unter

www.datenschutzzentrum.de/taucis/

Was ist zu tun?
Die allgegenwärtige und mobile Datenkommunikation ist eine neue Herausforderung für den Datenschutz. Es gilt ihre wirtschaftlichen Vorteile zu ermöglichen, aber die Risiken für den Datenschutz der Bürgerinnen und Bürger durch Technikgestaltung auszuschließen.

8.7 Privacy4DRM

Die Inhaber der Rechte an elektronischen Musikstücken und Filmen versuchen eine unbefugte Verbreitung und Nutzung ohne jede Bezahlung durch besondere technische Schutzsysteme zu verhindern. Wir analysieren die Konsequenzen für den Datenschutz und erstellen einen Anforderungskatalog für die datenschutzkonforme Gestaltung solcher Systeme.

Die Schutzsysteme digitaler Rechte werden als Digital-Rights-Management-Systeme (DRM-Systeme) bezeichnet. Ihre unterschiedlichen Funktionsmechanismen sind sehr komplex. In der Regel versuchen sie, über gesonderte Mechanismen die Datenspur des jeweiligen Nutzers zu verfolgen, und werfen damit Datenschutzprobleme auf. Unsere Forderung ist ein **DRM mit Datenschutz**; aus diesem Grund heißt unser Projekt „Privacy4DRM“ (*4: four* – steht für *for*). Ziel des nur auf wenige Monate begrenzten Projektes ist die Analyse von DRM-Systemen, um Material für einen Anforderungskatalog datenschutzkonformer DRM-Systeme zu gewinnen. Unser Partner bei diesem seit Oktober 2004 bis Mai 2005 laufenden Kurzprojekt ist das Fraunhofer-Institut für Digitale Medientechnologie (IDMT) in Ilmenau sowie die Technische Universität Ilmenau. Zur Förderung ausgewählt wurde das Projekt im Rahmen des Wettbewerbes „Innovationspotenziale der Informations- und Kommunikationstechnologie“ des Bundesministeriums für Bildung und Forschung.

www.datenschutzzentrum.de/privacy4drm/

Was ist zu tun?
Die Sicherheit für die Verwertung von Rechten an digitalen Werken darf die informationelle Selbstbestimmung der Nutzenden nicht ignorieren. Nur datenschutzkonforme Systeme dürfen zum Einsatz kommen.

9 Gütesiegel und Audit

9.1 Datenschutz-Gütesiegel

9.1.1 Projektabschluss „e-Region“: Innovationspreis für Schleswig-Holstein

Das Projekt „IT-Gütesiegel“, das von uns in den Jahren 2002 und 2003 im Rahmen eines von der EU und vom Wirtschaftsministerium Schleswig-Holstein geförderten Programms durchgeführt wurde, ist in einem Wettbewerb von der Europäischen Kommission mit einem Innovationspreis ausgezeichnet worden.

Nach Abschluss des EU-geförderten Projekts „e-Region Schleswig-Holstein“ (26. TB, Tz. 8.1) hat das Wirtschaftsministerium des Landes das ULD-Projekt „IT-Gütesiegel“ zum **EU-Wettbewerb „Regionale Innovation in Europa“** gemeldet, an dem sich insgesamt 126 europäische Regionen um eine Auszeichnung in den drei Bereichen „wissensbasierte Wirtschaft“, „Informationsgesellschaft“ und „nachhaltige Entwicklung“ beteiligt hatten. Ziel dieses Wettbewerbs, der von der Europäischen Kommission – Generaldirektion Regionalpolitik – initiiert wurde, war es, innovative Praktiken ausfindig zu machen und weiterzuverbreiten.

Die Jury hat das schleswig-holsteinische Projekt „IT-Gütesiegel“ auf den dritten Platz in der **Kategorie „Informationsgesellschaft“** gewählt. Die Preisverleihung fand im Europäischen Parlament in Brüssel im Rahmen der Sitzung des Ausschusses der Regionen statt. Verbunden mit der Preisverleihung war eine zweitägige Ausstellung der Preisträger im Gebäude des Europäischen Parlaments, bei der wir Gelegenheit hatten, unser Projekt zu präsentieren.

Was ist zu tun?
Die Auszeichnung mit einem europäischen Innovationspreis belegt, dass ein moderner Datenschutz zum Standortvorteil für eine ganze Region werden kann. Auch der Bund sollte über eine Modernisierung des Datenschutzes nachdenken, um sich einen vorderen Platz in der Informationsgesellschaft zu sichern.

9.1.2 Abgeschlossene Gütesiegelverfahren

Neben den aus dem Projekt „e-Region Schleswig-Holstein“ verbliebenen Verfahren haben wir im Berichtszeitraum eine Reihe weiterer Zertifizierungsverfahren durchgeführt.

Auch in diesem Jahr konnten wir weitere Gütesiegelverfahren erfolgreich abschließen. Insgesamt haben wir **sieben weitere Produkte** mit einem Gütesiegel ausgezeichnet. Drei dieser Verfahren waren Teil des Projekts „e-Region Schleswig-Holstein“, in dem wir unsere Leistungen gebührenfrei erbrachten und die Begutachtungskosten aus dem Förderprogramm bezuschusst wurden.

Im Rahmen des geförderten Verfahrens wurden folgende Produkte zertifiziert:

- active-city, Version 2.3, ein modulares Online-Redaktionssystem für Kommunal- und Kreisverwaltungen zum Einsatz einzelner Informationsbereiche bis zum dynamischen Aufbau und zur Verwaltung vollständiger Portale mit E-Government-Funktionen,
- ALLRIS, Version 3.7, ein Ratsinformationssystem für den kommunalen Sitzungsdienst, mit dem Sitzungen vor- und nachbereitet sowie Informationen abgestuft Amtsangehörigen, Ratsangehörigen und Bürgern zugänglich gemacht werden können,
- TIGRIS, Version TIGRIS 2003 Release SP4, eine Software zur Unterstützung der Aufgabenerfüllung von Gewerbeämtern, insbesondere zur Unterstützung bei der Abwicklung von An-, Um- und Abmeldungen.

Über das Ende des EU-geförderten Projekts hinaus verzeichnen wir eine konstant hohe Nachfrage nach dem Gütesiegel. Im vergangenen Jahr haben wir laufend weitere Anträge erhalten und bereits vier Produkte ausgezeichnet. Dies sind:

- PROSOZ/S für Windows, Version 7.1 inklusive Update, ein Dialogverfahren zur Erfassung von Sozialhilfedaten, Berechnung rechtlicher Ansprüche und Ausgabe entsprechender Bescheide direkt am Arbeitsplatz,
- Verfahren der Firma Reisswolf, Stand Mai 2004, zur Vernichtung von Akten, elektronischen und optischen Datenträgern zur Löschung von personenbezogenen Daten im Auftrag für Auftraggeber aus dem öffentlichen und nichtöffentlichen Bereich,
- LN-Card, Stand 5.10.2004, eine Bonuskarte für Abonnenten der *Lübecker Nachrichten*,
- VISOR, Version 2.0, Software zur Online-Prüfung von PCs im Hinblick auf Sicherheitslücken.

Einen Gesamtüberblick über die zertifizierten Produkte enthält das Register auf unserer Homepage unter

www.datenschutzzentrum.de/guetesiegel/

Im Wortlaut: § 1 Abs. 2 DSAVO

IT-Produkte im Sinne dieser Verordnung sind Hardware, Software und automatisierte Verfahren, die zur Nutzung durch öffentliche Stellen geeignet sind.

Einige Anfragen von Herstellern mussten wir leider zurückweisen, da die rechtlichen Voraussetzungen für eine Zertifizierung nicht vorlagen. Die Datenschutzauditverordnung eröffnet das Zertifizierungsverfahren nur für Produkte, die zur **Nutzung durch öffentliche Stellen** geeignet sind. Ein tatsächlicher Einsatz des Produkts in einer schleswig-holsteinischen Behörde muss nicht unmittelbar beabsichtigt sein, aber das Produkt muss für einen solchen Einsatz geeignet sein. Bei den meisten der uns erreichenden Anfragen ist das Produkt für

öffentliche Stellen zur Nutzung geeignet. In seltenen Fällen ist ein Einsatz des Produkts in Behörden nicht denkbar.

Zu den nicht zertifizierten Produkten gehören in der Regel **Bonuskarten**, die Unternehmen für treue Kunden ausgeben. Betreiber solcher Systeme haben im vergangenen Jahr ein deutliches Interesse an der Zertifizierung ihrer Bonussysteme durch uns gezeigt. In der Regel fehlt es in diesen Fällen jedoch an einer Einsatzmöglichkeit für öffentliche Stellen, die an solchen Systemen allenfalls als Endkunden teilnehmen. Anders war die Lage bei der LN-Card der *Lübecker Nachrichten*. An diesem System können sich regionale Partnerunternehmen beteiligen, zu denen auch öffentliche Stellen, etwa Schwimmbäder oder Museen, gehören können.

Eine Anfrage eines Anbieters eines **Anonymisierungsdienstes im Internet**, der ein Gütesiegel für das Angebot eines anonymen Zugriffs auf Online-Tauschbörsen anstrebte, mussten wir ablehnen, weil das Verfahren für öffentliche Stellen nicht geeignet war.

9.1.3 Anerkennung von Sachverständigen

Für die Begutachtung der Produkte im Zertifizierungsverfahren sind Sachverständige nötig, die wir auf Antrag akkreditieren. Die Zahl der bei uns eingehenden Anträge belegt das fortwährende Interesse an der Gutachtertätigkeit.

Im Berichtszeitraum haben wir **neun Sachverständige** anerkannt. Neun Anträge auf Anerkennung wurden im Berichtszeitraum gestellt, fünf weitere Verfahren wurden aus dem Vorjahr übernommen. Zwei der insgesamt vierzehn im Berichtszeitraum bearbeiteten Anträge wurden nach Beratung zurückgenommen, drei Verfahren sind noch nicht beendet.

Sachverständige können für die Bereiche **Recht und/oder Technik** anerkannt werden. Von den im Berichtszeitraum ausgesprochenen Anerkennungen ist eine Anerkennung für beide Bereiche erfolgt, vier Sachverständige wurden ausschließlich für den Bereich Technik und weitere vier ausschließlich für den Bereich Recht anerkannt.

Die Anerkennung ist nicht nur für Einzelpersonen möglich, sondern auch für Organisationen oder organisatorische Einheiten innerhalb einer Organisation. Unter den neun im Berichtszeitraum anerkannten Gutachtern befinden sich zwei **sachverständige Prüfstellen**.

Eine **Übersicht** über die anerkannten Sachverständigen und sachverständigen Prüfstellen ist abrufbar unter

www.datenschutzzentrum.de/guetesiegel/

9.1.4 Rezertifizierung und Gebühren

Gütesiegel werden für die Dauer von zwei Jahren für die vorgelegte Produktversion verliehen. Möchte der Hersteller danach das Gütesiegel weiterverwenden oder ändert sich das zertifizierte Produkt innerhalb der Gültigkeitsdauer erheblich, so ist eine Rezertifizierung erforderlich.

Den Ablauf des Rezertifizierungsverfahrens und die Fallgruppen, die eine Rezertifizierung nötig werden lassen, haben wir bereits im letzten Tätigkeitsbericht erläutert (26. TB, Tz. 9.1.4). Eine Rezertifizierung ist erforderlich, wenn das Produkt **erhebliche Änderungen** erfährt oder sich die rechtlichen bzw. technischen Rahmenbedingungen wesentlich ändern. Nach Ablauf der zweijährigen Gültigkeitsdauer ist in jedem Fall eine Rezertifizierung erforderlich.

Die ULD-Benutzungs- und Entgeltsatzung, die Gebühren für die Zertifizierung festlegt, wurde zum 1. Dezember 2004 um eine Gebührenregelung für das Rezertifizierungsverfahren ergänzt. Diese Regelung sieht eine **Grundgebühr** für das Rezertifizierungsverfahren in Höhe von 280 Euro vor. Diese relativ geringe Grundgebühr fällt an, wenn ein Produkt in bestimmten Teilen geändert wurde, sodass das Gutachten aus dem vorigen Zertifizierungsverfahren in den nicht geänderten Teilen weiterhin gültig bleibt. Voraussetzung für die Anwendung dieses Gebührenbausteins ist, dass der Hersteller eine Aufstellung über die vorgenommenen Änderungen vorlegt. Diese wird dem Gutachter zur Verfügung gestellt, sodass sich die erforderliche Neubegutachtung auf die geänderten Teile sowie gegebenenfalls auf die geänderten technischen oder rechtlichen Rahmenbedingungen beschränken kann.

Für Produkte, die nicht oder nur unwesentlich geändert wurden und ebenfalls keinen oder nur geringen Änderungen der Rahmenbedingungen unterliegen, enthält die Gebührenregelung einen **Ermäßigungstatbestand**. Danach kann die Gebühr bis auf 70 Euro reduziert werden. Auf der anderen Seite sieht die Gebührenregelung eine **Erhöhung** auf bis zu 1120 Euro für besondere Fälle vor. Die Erhöhung kann etwa bei umfangreichen Änderungen des Produkts oder der Rahmenbedingungen zur Anwendung kommen. Möglich ist eine Erhöhung auch, wenn der Hersteller keine Aufstellung über die vorgenommenen Änderungen zur Verfügung stellt, sodass die Begutachtung im Rezertifizierungsverfahren für das gesamte Produkt wiederholt werden muss.

9.1.5 PETTEP – Privacy Enhancing Technologies Testing and Evaluation Project

Fortschritte bei der Marktdurchdringung datenschutzfreundlicher Technik sind erkennbar. Verstärkt weisen Hersteller auf solche Produktmerkmale in der Werbung hin oder fragen beim ULD nach dem Datenschutz-Gütesiegel, um ihre Produkteigenschaften nach außen transparent machen zu können. Doch was sind die Kriterien für eine datenschutzfreundliche Technik? Und sind diese Kriterien international vergleichbar?

Hinter dem Namen PETTEP – Privacy Enhancing Technologies Testing and Evaluation Project – verbirgt sich eine **internationale Initiative**, die die Entwicklung von Kriterien für datenschutzfördernde Technik (Privacy Enhancing Technologies) und für den Test von Produkten voranbringen will. Schon im 26. TB (Tz. 9.1.6) war über dieses Team, das auf eine Initiative der Datenschutzdienststelle in Ontario, Kanada, zurückgeht, berichtet worden. Mitglieder sind Experten aus Datenschutzbehörden (u. a. Ontario, Kroatien, Brandenburg, Schleswig-Holstein), Wissenschaft und Wirtschaft. Nach 2001 und 2003 fand auch 2004 anlässlich der Sommerakademie erneut ein PETTEP-Workshop in Kiel statt, bei dem das künftige Vorgehen abgestimmt wurde. Derzeit arbeitet PETTEP an einem Zugang zur weltweiten **ISO-Normung**. Unterstützt wird es dabei durch einen Beschluss der 26. Internationalen Konferenz der Datenschutzbeauftragten in Wroclaw vom September 2004, in dem die ISO (International Organization for Standardization) zur Einbindung der PETTEP-Arbeiten aufgefordert wird.

Ausgangspunkt der **PETTEP-Kriterien** sind die „Fair Information Practices“, die als Eckpunkte für den Datenschutz international anerkannt sind. Sie werden um weitere wichtige Prinzipien, etwa Datensparsamkeit und Datenvermeidung, erweitert und müssen in die Sprache technischer Normen „übersetzt“ werden.

Zwischen den Zielen des Datenschutz-Gütesiegels und denen von PETTEP gibt es viele Überschneidungen. Leider ist die **Entwicklung von Standards** wegen der vielen beteiligten Partner und Abstimmungen sehr zeitaufwändig und dauert mitunter Jahre. Daher erwies sich unsere Entscheidung, das Datenschutz-Gütesiegel voranzubringen und zeitgleich bei PETTEP mitzuwirken, als richtig: Die Erfahrungen des ULD aus dem Gütesiegelbereich sind wertvoll für PETTEP. Umgekehrt können Erkenntnisse aus der technischen Normung für das Gütesiegelverfahren genutzt werden; dies erlaubt eine Verzahnung des Gütesiegels mit international anerkannten Kriterien und verbreitet so seine Wirkung. Zwar können rein technische Kriterien eine datenschutzrechtliche Prüfung nicht vollständig abbilden, doch sind sie ein wichtiger **Bestandteil**.

Was ist zu tun?
Die PETTEP-Datenschutzkriterien müssen weiterentwickelt und in den global geltenden ISO-Normungsprozess integriert werden. Damit lässt sich die Idee einer datenschutzfördernden Technik weiterverbreiten.

9.1.6 Bundesdatenschutzauditgesetz

In Sachen Bundesdatenschutzaudit herrschte lange Zeit Stillstand. Nun scheint neue Bewegung in die Gesetzgebung zu kommen.

Das Thema Datenschutz-Audit ist eines der wichtigen datenschutzrechtlichen Themen im **Koalitionsvertrag** der Regierungsparteien auf Bundesebene. Nachdem von den Koalitionsfraktionen der Entwurf eines Informationsfreiheitsgesetzes in das parlamentarische Verfahren eingebracht worden ist (Tz. 11.2), verständigten sich diese, als Nächstes ein Bundesdatenschutzauditgesetz in Angriff zu nehmen. Die Erfahrungen aus Schleswig-Holstein mit dem Datenschutz-Gütesiegel und Behördenaudit werden hierbei eine wichtige Rolle spielen.

Zur **Vorbereitung des Bundesdatenschutzauditgesetzes** hat der Deutsche Akkreditierungsrat, Sektorkomitee Security, im Jahr 2003 eine Projektgruppe „Datenschutzaudit“ gegründet, an der wir beteiligt waren (26. TB, Tz. 9.1.3). Aufgabe der Projektgruppe war die Entwicklung von Kriterien für die Gutachteranerkennung und für die Produktprüfung. Verschiedene Modelle wurden dafür gegenübergestellt und diskutiert. Wir haben für die Arbeitsgruppe auf der Grundlage des ULD-Informations- und Pflichtenkataloges für Sachverständige einen Regelungsvorschlag für die Sachverständigenanerkennung erarbeitet, der dem Akkreditierungsrat als Arbeitsergebnis vorgelegt wird.

9.2 Datenschutz-Audit

9.2.1 ostseecard*

Die ostseecard* wird seit Mai 2004 zur Zahlung der Tourismusabgabe an 18 Kurorten der schleswig-holsteinischen Ostseeküste eingesetzt. Die mehrjährige Beratung mündete im November 2004 ein in der Verleihung eines Datenschutz-Audits.

Die Ausgabe der ostseecard* und die Verwaltung des zugrunde liegenden **Chipkartensystems** wird federführend für die beteiligten Gemeinden von dem Ostsee-Holstein-Tourismus e.V. koordiniert. Die Besonderheit des Verfahrens liegt in der Verbindung hoheitlicher Aufgaben der Gemeinde, die Erhebung der Kurabgabe, mit wirtschaftlichem Handeln privater Anbieter, die kostenpflichtige Leistungspakete und Rabatte zur Verfügung stellen.

Die Besucherinnen und Besucher erhalten eine Chipkarte, mit der sie während der Dauer ihres Urlaubs die touristischen Angebote in allen teilnehmenden Gemeinden nutzen können. Die Ausgabe der Chipkarte ist mit dem Ausfüllen des Meldescheins bei der Ankunft im Urlaubsquartier verknüpft. Auf Wunsch kann der Übernachtungsgast der Speicherung seiner Adressdaten zustimmen, um mit Informationsmaterial über die Ostsee beworben zu werden. Zusätzlich kann er weitere

Leistungen wie Pauschaltickets erwerben und auf seine Karte buchen lassen. Jede Nutzung der Karte wird elektronisch erfasst. Dies gilt für kontrollierende (z. B. die Zugangskontrolle zum Strand) wie auch verbrauchende Nutzungen (dem Abreißen einer Eintrittskarte vergleichbar). Technisch wäre es so möglich, ein **engmaschiges Datenprofil** der einzelnen Urlauber zu erstellen.

Ergebnis der datenschutzrechtlichen Beratung des Ostsee-Holstein-Tourismus e.V. und seiner technischen Partner war eine **datenschutzfreundliche Lösung**, mit der das Entstehen eines solchen Profils verhindert wird. Auf der Karte werden keine personenbezogenen Daten der Urlauber, sondern lediglich eine Kartennummer als Pseudonym gespeichert. Nur anhand dieser Nummer können die Kartennutzungen, die in einer Datenbank ohne Zugriffsmöglichkeit für die einzelnen Anbieter gespeichert werden, zugeordnet werden. Eine Verknüpfung mit den Adressdaten erfolgt im Rahmen der täglichen Nutzung nicht. Die Datenspeicherung auf den Karten ist so organisiert, dass jede beteiligte Stelle Leistungen auf der Karte abbuchen kann, ohne Zugriff auf die Leistungsdaten anderer Anbieter nehmen zu können. Eine Stelle kann also nicht erkennen, welche Leistungen der Urlauber bei der Konkurrenz erworben und eventuell in Anspruch genommen hat. Damit die Urlauber kontrollieren können, welche Leistungen auf ihren Karten aufgebucht wurden, wurde eine Auskunftsfunktion mithilfe von Selbstbedienungsterminals geschaffen. Eine Mustersatzung für die beteiligten Gemeinden, ein solides technisches Konzept und eine klare vertragliche Regelung zwischen den Gemeinden, dem Ostsee-Holstein-Tourismus e.V. und den beteiligten Firmen schaffen für alle Beteiligten rechtliche Klarheit und definieren präzise Rechte und Pflichten der Partner.

Der Diskussionsprozess war nicht immer einfach. Die zum Teil **gegensätzlichen Interessen** der Gemeinden, des Ostseemarketings, der privaten Leistungsanbieter, der Daten verarbeitenden Firmen und nicht zuletzt des Datenschutzes und des Melderechtes mussten mit den technischen Möglichkeiten **in Einklang** gebracht werden. Es war daher nur konsequent, das erfolgreiche Ergebnis der langjährigen Beratung in ein Datenschutz-Audit münden zu lassen. So wird auch für die Urlaubsgäste sichtbar, dass sie datenschutzrechtlich gut an der Ostsee aufgehoben sind. Erweiterungen und Änderungen des Verfahrens ostseecard* sind schon für die kommende Saison in Planung. Wesentliche Änderungen des Verfahrens haben zur Folge, dass das Datenschutzauditzeichen keine weitere Gültigkeit haben kann. Bei der Umsetzung von wesentlichen Änderungen des Verfahrens ist daher eine Reauditierung erforderlich.

Was ist zu tun?
Der Ostsee-Holstein-Tourismus e.V. sollte auch weiterhin bei der Erweiterung und Ausgestaltung des Verfahrens die konstruktive Zusammenarbeit mit dem ULD fortsetzen.

9.2.2 Stadt Neumünster

Mängelrügen einer Datensicherheitskontrolle sollen positive Wirkungen entfalten. Sie können zu einer grundlegenden Neugestaltung der „Security Policy", ja sogar bis zur Verleihung des Auditzeichens für einen wichtigen Teilbereich führen.

So geschehen bei der Stadtverwaltung Neumünster: Als wir im Jahr 2001 eine Überprüfung der technischen und organisatorischen Sicherheitsmaßnahmen vorgenommen hatten, war die Liste der vorgefundenen Mängel erschreckend lang (24. TB, Tz. 7.5.1). Deren zügige Abarbeitung wurde zugesagt. In regelmäßigen Abständen wurden wir über die Zwischenergebnisse unterrichtet. So waren wir nicht überrascht, dass die Stadt Ende 2003 an uns herantrat, um ihr Projekt „Anschluss des internen Netzes der **Stadtverwaltung Neumünster an das Internet**" auditieren zu lassen. Man legte dabei Wert darauf, sich einem internen und externen Penetrationstest zu unterziehen. Die Details dieser neu geschaffenen Möglichkeit sind unter Tz. 10.1 dargestellt.

Das Audit konnte zügig und erfolgreich abgewickelt werden. Die zuständige Abteilung, der „Fachdienst EDV-Dienste", hatte den Internetanschluss auf einem technisch **hohen Niveau** realisiert und für sachverständige Dritte gut nachvollziehbar dokumentiert. Grundlagen für die Realisierung des Anschlusses waren ein Sicherheits- und ein Realisierungskonzept mit folgenden signifikanten Festlegungen:

- Zum Schutz vor Übergriffen aus dem Internet werden mehrere Firewall-Systeme eingesetzt. Sie verfügen über „demilitarisierte Zonen" (DMZ), die in vordefinierte Sicherheitsebenen (Security Level) unterteilt sind.
- Pakete von einer Stelle mit einem geringeren Security Level werden nur an eine DMZ mit höherem Security Level weitergeleitet, wenn dafür eine explizite Firewall-Regel eingetragen ist. Alle anderen Pakete werden ausgefiltert.
- Es werden keine Datenpakete, die als Anfragen aus dem Internet kommen, in das Verwaltungsnetz direkt durchgeleitet.
- Die Überwachung und Administration der eingesetzten Firewall-Komponenten erfolgen ausschließlich durch den Fachdienst. Eine Fernadministration der Firewall-Komponenten ist nicht gestattet.
- Unerlaubte Zugriffe werden auf der physikalischen Ebene protokolliert und abgewehrt. Ereignisse von sicherheitsrelevanter Bedeutung führen zu gesonderten Warnmeldungen.
- Es werden nur die E-Mails an den Arbeitsplatz geleitet, die virenüberprüft sind und zugelassene Attachments (z. B. TXT, RTF) enthalten.
- Der Zugriff auf die Webseiten wird in Bezug auf die sicherheitskritischen Komponenten ActiveX, Java und VBScript gefiltert.
- Webseiten werden anhand von Textzensurskripten geprüft und gegebenenfalls für den Aufruf nicht zugelassen.

- Das Herunterladen ausführbarer Programme und Dateien auf die Arbeitsplatzrechner ist nicht zugelassen.
- Über ein Intrusion Detection System (IDS) werden bei Angriffen auf die Firewall Protokolleinträge generiert, die in regelmäßigen Abständen vom Fachdienst ausgewertet werden. Bei Verdacht eines „Einbruches“ wird das Netz durch die Deaktivierung des entsprechenden Netzwerkinterfaces sofort vom Internet getrennt.

Der **Penetrationstest** des Internetanschlusses der Stadtverwaltung wurde in Zusammenarbeit mit einem von uns beauftragten externen Spezialisten durchgeführt. Dieser versuchte als „Hacker“ das Netz zu kompromittieren und Sicherheitsdefizite aufzudecken. Der Test beinhaltete umfangreiche Systemanalyseverfahren sowie den Einsatz zahlreicher „Hackertools“. Im Ergebnis zeigte sich, dass die Angriffe auf das Verwaltungsnetz von innen und von außen nicht erfolgreich waren – ein Erfolg des Sicherheitssystems! Die guten Erfahrungen mit dem Audit ermutigten nun die Stadt, auch den Teilbereich „Interne Datenverarbeitung“ auditieren zu lassen.

Was ist zu tun?
Datenverarbeitungsprozesse einer Verwaltung müssen nicht sofort in ihrer Gesamtheit auditiert werden. Sicherheitstechnisch und rechtlich auditiert werden können auch abtrennbare Module.

9.2.3 Stadt Bad Schwartau

Datenschutz-Audits erleichtern die Arbeit des behördlichen Datenschutzbeauftragten. Auf dieser soliden Grundlage kann er durch Soll-Ist-Vergleiche auf ein etwaiges Absinken des Datenschutz- und Sicherheitsniveaus reagieren.

Das Audit bei der Stadt Bad Schwartau wurde bezeichnenderweise von den Systemadministratoren initiiert. Sie wollten auf diese Weise bestätigt bekommen, dass sie mit einem modernen, aber in der Verwaltung noch nicht weit verbreiteten **Betriebssystem** ein hinreichendes Sicherheitsniveau erreicht haben.

Die automatisierte Datenverarbeitung dieser Stadtverwaltung wird auf der Basis eines **Terminal-Server-Konzeptes** abgewickelt. Es beruht darauf, dass Softwareanwendungen sowie die mit ihnen verarbeiteten Daten zentral auf einem Rechner abgelegt werden. Die Arbeitsplatz-PCs der Benutzer dienen nur noch als Verbindungssysteme für Ein- und Ausgabevorgänge. Zu diesem Zweck benötigen die Clients selbst keine leistungsstarke Hardware. Bei ihnen kann es sich um einen normalen PC mit spezieller Client-Software (Terminalserver-Client) oder um ein dediziertes Windows-Terminal (Thin Client) handeln. Derzeit werden bei der Stadtverwaltung sowohl abgerüstete PCs als auch Thin Clients eingesetzt.

Sicherheitstechnisch hat das Konzept den Vorteil, dass der Benutzer nur diejenigen Ressourcen auf seinem **Arbeitsplatz-PC** nutzen kann, die ihm explizit zur

Verfügung gestellt werden. Die Nutzung und das Installieren von nicht erwünschten Anwendungen sowie das lokale Abspeichern von Daten werden ausgeschlossen, indem derartige Zugriffe nicht unterstützt werden.

Die Fachanwendungen befinden sich auf mehreren Terminal-Servern (Serverfarm), um eine Lastverteilung zu gewährleisten. Für eine **sichere und ordnungsgemäße Datenverarbeitung** sind folgende Anforderungen an das Sicherheitsniveau erfüllt worden:

- Gewährleistung der Datenabschottung durch eine nachvollziehbare Benutzer- und Rechteverwaltung,
- Bereitstellung der Fachanwendungen auf den Arbeitsplatz-PCs nur im erforderlichen Umfang,
- strukturierte zentrale Datenverwaltung,
- Dokumentation aller Einstellungen an Hard- und Software,
- Aufbau einer qualifizierten IT-Koordination,
- Kontrolle und Überwachung durch den behördlichen Datenschutzbeauftragten.

Hieraus wurden die folgenden konkreten Sicherheitsmaßnahmen abgeleitet:

- Die Verfügungsgewalt (Überwachung und Administration) über die eingesetzten Firewall-Komponenten liegt bei der Stadtverwaltung selbst. Es erfolgt keine Fernadministration der Firewall.
- Es wird sichergestellt, dass Angriffe auf der physikalischen Ebene erkannt und abgewehrt werden. Die Firewall protokolliert alle nicht erlaubten Aktivitäten. Das Protokoll wird täglich von den Administratoren ausgewertet.
- Ausgehende E-Mails dürfen keine personenbezogenen Daten enthalten.
- Kopien der ein- und ausgehenden E-Mails werden für Kontrollzwecke in einem gesonderten Archiv gespeichert.
- Es werden nur virenüberprüfte E-Mails an den Arbeitsplatz geleitet.
- E-Mails mit Anhängen werden in einem nur für den Administrator zugänglichen Fach gespeichert, während eine Kopie der E-Mail ohne Anhang an den Empfänger geleitet wird. Der Empfänger erhält einen Hinweis, dass der Anhang vom Administrator nach vorheriger Überprüfung zugestellt werden kann.
- WWW-Seiten ohne dienstlichen Bezug sind deaktiviert. Es sind nur Webseiten vertrauenswürdiger Stellen freigeschaltet.
- Das Herunterladen ausführbarer Programme und Dateien durch „normale“ Benutzer wird nicht zugelassen.
- Die ordnungsgemäße Nutzung der Internetdienste wird regelmäßig vom behördlichen Datenschutzbeauftragten überwacht.

Sicherheitstechnisch waren keine Schwachstellen erkennbar, die die Rechte der betroffenen Bürger und der Mitarbeiter der Stadtverwaltung beeinträchtigen könnten. Die modular aufgebauten Sicherheitskonzepte bilden die Grundlage für ein wirksames **Datenschutzmanagement** im laufenden Betrieb der automatisierten Verfahren. Der mit dieser Aufgabe betraute behördliche Datenschutzbeauftragte wird in die Lage versetzt, durch einen effektiven Soll-Ist-Vergleich auf Veränderungen in den tatsächlichen Abläufen zu reagieren und Fehlentwicklungen offen zu legen. Diese Rahmenbedingungen sind die Grundlage für eine Steigerung der Effizienz und der Sicherheit der automatisierten Prozesse.

Was ist zu tun?
Dem sicherheitstechnischen Audit könnten vorrangig rechtliche Audits zu den fachlichen Anwendungen folgen.

9.2.4 Gemeinde Timmendorfer Strand

Auch kleine Kommunen sind in der Lage, ihre IT-Systeme so zu gestalten, dass sie erfolgreich zertifiziert werden können. Die technischen Voraussetzungen hierfür sind mit unterschiedlichen Betriebssystemen zu realisieren. Entscheidend ist die Qualität der IT- und Sicherheitskonzepte.

Mit der zunehmenden Zahl von Audits im kommunalen Bereich zeigt sich immer deutlicher, dass es in der Praxis eine Art Königsweg gibt, um die Sicherheit der lokalen Netzwerke und den Anschluss an das Internet zu gewährleisten. Das eingesetzte Betriebssystem und die Behördengröße sind wichtige Parameter, aber nicht entscheidend. Letztendlich kommt es auf die Qualität der IT- und **Sicherheitskonzepte** an. Nachfolgend werden die wesentlichen Merkmale der von der Gemeinde Timmendorfer Strand realisierten Konzeption dargestellt, die sich in einigen, aber nicht in allen Punkten mit denen der anderen auditierten Verwaltungen (Tzn. 9.2.2 und 9.2.3) deckt. Das Sicherheitsniveau der IT-Systeme ist wie folgt zu kennzeichnen:

- Gewährleistung einer Datenabschottung durch eine nachvollziehbare Benutzer- und Rechteverwaltung,
- Reduzierung der Funktionalitäten der Arbeitsplatz-PCs auf das erforderliche Maß,
- strukturierte zentrale Datenverwaltung,
- Dokumentation aller Einstellungen an Hard- und Software,
- Aufbau einer qualifizierten IT-Koordination,
- Kontrolle und Überwachung durch den Leiter des Hauptamtes.

Für die **Arbeitsplatzrechner** und die **Server** sowie für die **Schnittstellen** zum Internet ergeben sich hieraus folgende sicherheitstechnische Maßnahmen und Einstellungen:

- Eine Fernwartung durch externe Dienstleister wird nur auf Veranlassung der IT-Koordinatoren durchgeführt. Für die Firewall-Komponenten ist eine Fernwartung nicht zugelassen.
- Die Disketten- und CD-ROM-Laufwerke sowie die USB-Ports sind mit einer speziellen Sicherheitssoftware deaktiviert.
- Die auf den Arbeitsplatz-PCs verfügbaren Systemfunktionen sind durch Gruppenrichtlinien festgelegt.
- Die Einrichtung und Abschottung von Word- und Exceldateien erfolgt nach einem an den Geschäftsverteilungsplan angelehnten Datenablagekonzept.
- Es besteht ein nach Ämtern strukturiertes Active Directory für die Benutzer- und Gruppenverwaltung.
- Alle Fachanwendungen und die mit ihnen verarbeiteten Daten werden auf den Servern zentral verwaltet.
- Ausgehende E-Mails dürfen keine personenbezogenen Daten enthalten.
- Kopien der ein- und ausgehenden E-Mails werden für Kontrollzwecke in einem gesonderten Archiv gespeichert.
- Es werden nur die E-Mails an den Arbeitsplatz geleitet, die virenüberprüft sind und zugelassene Attachments (z. B. TXT, RTF) enthalten.
- Der Zugriff auf die Webseiten wird in Bezug auf die sicherheitskritischen Komponenten ActiveX, Java und VBScript gefiltert.
- Webseiten werden durch Textzensurskripte geprüft und gegebenenfalls für den Aufruf nicht zugelassen.
- Das Herunterladen ausführbarer Programme und Dateien auf die Arbeitsplatzrechner ist nicht zugelassen.
- Alle Einstellungen an den Internetkomponenten werden nachvollziehbar dokumentiert.
- Das Systemprotokoll der Firewall erfasst alle nicht erlaubten Aktivitäten. Es wird täglich von der IT-Koordination ausgewertet.
- Die ordnungsgemäße Nutzung der Internetdienste wird in regelmäßigen Abständen von der IT-Koordination und dem Hauptamtsleiter überwacht.
- Wegen der zurzeit noch nicht hinreichend transparenten Funktionalität des Übergaberouters ist der bestehende Landesnetzanschluss durch eine zusätzliche, von der Gemeinde administrierte Firewall gesichert.

Die IT-Koordination verfügt über eine **Testumgebung** (Server und Clients), in der die umzusetzenden sicherheitstechnischen Maßnahmen zunächst getestet werden können. Sie nutzt die Testumgebung außerdem für die Vertiefung ihres sicherheitstechnischen Know-hows. Derartige vorbildliche Systeme sind in Kommunen dieser Größenordnung leider nur selten anzutreffen.

Was ist zu tun?
Die derzeit noch bestehenden Defizite in den vertraglichen Beziehungen zur Nutzung des Landesnetzanschlusses sollten so bald wie möglich behoben werden. Über die Funktionalität des Übergaberouters muss sich die Gemeinde kurzfristig Klarheit verschaffen.

9.3 Gütesiegel, Audit und PRIME

Der Zusammenhang zwischen Gütesiegel, Audit und dem Projekt PRIME, das sich mit der datenschutzfreundlichen Gestaltung von Identitätsmanagementsystemen beschäftigt, liegt nicht unmittelbar auf der Hand. Doch gibt es gemeinsame interessante Ansatzpunkte.

Das Projekt PRIME (Tz. 8.2.1) beschäftigt sich nicht nur theoretisch mit **datenschutzfreundlichen Identitätsmanagementsystemen**, sondern auch mit der praktischen Umsetzung in Form von Software. Eines der Projektziele ist es, ein nachgewiesen datenschutzkonformes Softwarepaket bereitzustellen. Ein solcher Nachweis kann mithilfe von Zertifikaten geführt werden, die nach einer positiven Evaluation durch unabhängige Dritte verliehen werden. Doch welche förmlichen Verfahren überprüfen die datenschutzgerechte Gestaltung, und welche Kriterien werden dabei zugrunde gelegt? Dieses herauszufinden ist eine der Aufgaben des Projektes. Dafür sind Informationen über die verschiedenen nationalen und internationalen IT-Sicherheits- und Datenschutzzertifizierungen zusammenzutragen und vergleichend zu bewerten.

Diese Aufgabe wird gemeinsam von der Johann Wolfgang Goethe-Universität Frankfurt und uns bearbeitet. Im Rahmen der Entwicklung des Gütesiegels haben wir bereits Vorarbeiten erledigt, auf die nun zurückgegriffen werden kann. Da aber die Entwicklung von Zertifizierungen und auch der zugrunde liegenden Kriterien recht dynamisch verläuft, müssen die Ergebnisse fortlaufend aktualisiert und fortgeschrieben sowie neue Verfahren integriert werden. Ziel der Arbeiten ist es, aus den **Evaluationskriterien** solche **für das Softwaredesign** zu gewinnen, über die Datenschutzbelange schon während der Entwicklung berücksichtigt werden.

Technische Zertifizierungsverfahren betrachten in der Regel ausschließlich die IT-Sicherheit, ohne spezifisch auf den Datenschutz, z. B. die Datensparsamkeit, einzugehen. Das Datenschutz-Gütesiegel umfasst neben technischen auch **rechtliche Fragestellungen** und stellt somit die notwendige Kombination aus Recht und Technik dar, ist aber dem deutschen Datenschutzrecht verhaftet. Für eine Anwendung in PRIME müssen die rechtlichen Fragestellungen nach internationalen Maßstäben integriert werden.

Was ist zu tun?
Durch die Mitarbeit in PRIME ergibt sich die Gelegenheit, die internationalen Erkenntnisse zu Zertifizierungsverfahren aufzuarbeiten und so für die Arbeiten am Datenschutz-Gütesiegel nutzbar zu machen. Diese Ergebnisse können wiederum in die Arbeit beim Projekt PETTEP (Tz. 9.1.5) einfließen.

10 Aus dem IT-Labor

10.1 Neue Methode: Penetrationstests

Wie sicher IT-Systeme gegenüber Angreifern abgeschottet sind, zeigt sich, wenn sie Hackerangriffen ausgesetzt werden. Dies geht nicht unter Laborbedingungen. Realitätsnahe Tests dürfen die Systeme aber auch nicht zerstören. Ein neues SUSA-Angebot bietet eine sichere Alternative.

Die meisten Daten verarbeitenden Stellen sind sich der Tatsache bewusst, dass sie sich mit der Vernetzung ihrer IT-Systeme Angriffen auf die Datensicherheit aussetzen. Dies führt zu Sicherheitsmaßnahmen, die nicht erlaubte Aktivitäten unterbinden bzw. sensible Daten vor unberechtigten Zugriffen schützen sollen. Welche **Qualität ihre Sicherheitspolicy** allerdings tatsächlich erreicht, kann von ihnen in der Regel nur schwer erkannt werden. Es steht oft die Frage im Raum: „Könnte vielleicht nicht doch ein Angreifer an den Sicherheitsbarrieren vorbei auf vertrauliche Daten zugreifen?“ Um dies zuverlässig beantworten zu können, ist eine professionelle Analyse der Sicherheitspolicy erforderlich.

An dieser Stelle setzt unser neues Angebot im Rahmen des Projektes „**Systemdatenschutz – ULD-Support für Administratoren** (SUSA)“ an. Dabei werden die getroffenen Sicherheitsmaßnahmen in einem „aggressiven“, gleichwohl kontrollierten Verfahren unter Produktionsbedingungen auf ihre Wirksamkeit hin untersucht. Die Daten verarbeitenden Stellen können also ihre IT-Sicherheit durch gezielte Testangriffe überprüfen lassen.

Dazu bilden unsere Mitarbeiter und von uns beauftragte externe Dienstleister mit Spezial-Know-how ein „**Security-Analyseteam**“, das mit Methoden arbeitet, die bei internen oder externen Hackern bekannt sind.

- Die Konfiguration der IT-Systeme wird systematisch nach Schwachstellen durchsucht. Die Mitarbeiter-PCs werden bezüglich ihres Funktionsumfanges, der den Benutzern zugewiesenen Befugnisse sowie der Datenverwaltung analysiert, Defizite aufgedeckt und zu Demonstrationszwecken ausgenutzt.
- Bei der Überprüfung der Firewall-Systeme werden „klassische“ Penetrationstests durchgeführt. Unter Einsatz gängiger Hackertools wird von außen ein unberechtigter Zugriff auf die IT-Systeme und auf die Daten versucht.
- Die IT-Systeme der Daten verarbeitenden Stellen sind in der Regel alle miteinander vernetzt. Darüber hinaus gibt es häufig Schnittstellen zu anderen Netzen bzw. Außenstellen, Einwahl- bzw. Fernwartungszugängen oder gar die Integration von Funknetzen (Wireless LAN). Ziel spezieller Penetrationstests ist es, sich von innen oder von außen unerkannt in das Netzwerk einzuschleusen, um z. B. die auf den Leitungen transportierten Informationen abzugreifen. Auch in diesem Bereich erfolgt die Aufdeckung von Sicherheitslücken lediglich zu Demonstrationszwecken.

Derartige Sicherheitsüberprüfungen laufen in **vier Phasen** ab.

- Die erste Phase umfasst im Wesentlichen die Durchführung der Penetrationstests. Der Daten verarbeitenden Stelle werden in einem Bericht der Überprüfungsgegenstand, die eingesetzten Angriffsmethoden sowie die Ergebnisse erläutert.
- Die zweite Phase befasst sich mit der Beseitigung der technischen Mängel. Die erarbeiteten Lösungsansätze werden in einem Konzept beschrieben. Es macht die einzelnen Schritte der Mängelbeseitigung transparent. Die IT-Systeme werden anschließend einem erneuten Penetrationstest ausgesetzt, um sicherzugehen, dass alle Defizite beseitigt wurden.
- In der dritten Phase erfolgt die Beseitigung der organisatorischen Mängel. Darunter fallen insbesondere die Erstellung von korrekten Dokumentationsunterlagen sowie die Anpassung der aufbau- und ablauforganisatorischen Regelungen.
- Sofern die Daten verarbeitende Stelle vom ULD ein Zertifikat wünscht, das den ordnungsgemäßen Einsatz der überprüften IT-Systeme bescheinigt, schließt sich in einer vierten Phase ein **Auditverfahren** an (Tz. 9.2). Dies setzt den Aufbau eines Datenschutzmanagementsystems voraus, das die dauerhafte Aufrechterhaltung und Kontrolle des erreichten Sicherheitsniveaus zum Ziel hat.

Die durchzuführenden Arbeiten, die handelnden Personen, der Zeitaufwand und die Kosten werden zwischen der Daten verarbeitenden Stelle und dem ULD **vertraglich festgelegt**. Die Überprüfung wird grundsätzlich unter Beteiligung der IT-Verantwortlichen der Daten verarbeitenden Stelle transparent durchgeführt. Das gilt insbesondere auch für die Aktivitäten der externen Spezialisten.

Was ist zu tun?
Verwaltungen mit großen IT-Netzwerken und/oder mit Übergängen in das Internet bzw. andere externe Netzwerke sollten den Aufwand für Penetrationstests abschätzen lassen. Es zeigt sich, dass er geringer wiegt als das latente Risiko von Lücken in der IT-Sicherheit.

10.2 Wenn der Postmann dauernd klingelt – neue Ansätze an der Spamfront

Eine wahre Flut an Viren und unerwünschter Werbung ergießt sich Tag für Tag in die E-Mail-Postfächer von Firmen, Behörden und Privatpersonen und richtet mitunter immensen Schaden an. Ein international standardisiertes Verfahren, das diese Flut eindämmen sollte, scheiterte letztlich an Softwarepatenten.

Inzwischen ist geklärt, dass zwischen der Verbreitung von **Viren und Spam** – unerwünschte Werbung – per E-Mail ein Zusammenhang besteht: Moderne Viren verbreiten sich nicht nur selbst weiter, sie nutzen die infizierten Systeme auch, um über diese Spam-E-Mails – in der Regel unter falschem Absender – zu verbreiten. Dazu wird den Verbreitern der Viren eine Hintertür geöffnet, durch die der befallene Rechner kontrolliert und ausspioniert werden kann.

Mehrere Gruppen der Open-Source-Bewegung sowie kommerzielle Unternehmen arbeiten seit einiger Zeit an Verfahren, die das Versenden von E-Mails unter **falschem Absender** deutlich erschweren bzw. zumindest erkennbar machen sollen. Die meisten dieser Verfahren beruhen darauf, dass im Domain Name Service (DNS) ein zusätzlicher Eintrag vorgenommen wird, der angibt, über welche Server E-Mails einer bestimmten Absende-Domain verschickt werden dürfen. Empfangende E-Mail-Server können dann prüfen, ob eine E-Mail über einen autorisierten Server verschickt wurde oder aus einer nicht autorisierten Quelle, z. B. von einem infizierten PC, stammt.

> **? *DNS***
>
> *Domain Name Service – Internetdienst, der zu einem Domain-Namen u. a. die zugehörige IP-Adresse liefert.*

Trotz unterschiedlicher Ansätze schien es, dass unter der Bezeichnung „SenderID“ ein konsensfähiger Vorschlag für einen IETF-Standard geschaffen würde. In quasi letzter Minute jedoch löste sich die zuständige Arbeitsgruppe der IETF selbst auf, nachdem festgestellt wurde, dass Microsoft auf Teile dieses softwarebasierten Verfahrens **Patentansprüche** geltend machte. Damit ist ein allgemein akzeptierter Standard in weite Ferne gerückt, sodass Anwenderinnen und Anwendern auch weiterhin nur geraten werden kann, den eigenen Rechner selbst zu schützen. Das ULD liefert Hinweise und Anleitungen dazu auf seinen Webseiten.

> **? *IETF***
>
> *Internet Engineering Task Force – offene, internationale Vereinigung zur technischen Standardisierung des Internets.*

www.datenschutzzentrum.de/selbstdatenschutz/internet/

10.3 Jagd nach PINs und TANs per Phishing

Unter Phishing-Mails versteht man elektronische Nachrichten, die eine seriöse Herkunft vortäuschen und den Nutzer auf gefälschte Webseiten locken. In der Mail wird versucht, den Nutzer zur Angabe von sensiblen Daten auf dieser gefälschten Seite zu bewegen. Solche Versuche gab es bereits früher, oft unter Vorspiegelung einer Systemadministrator-Mail. Seit Anfang 2004 geistern zunehmend geschicktere „Bauernfänger“ durchs Netz.

Unter Ausnutzung diverser Sicherheitslücken und Eigenarten von Mailprogrammen und Browsern entwickelten sich die so genannten Phishing-Mails zu einem Phänomen, dem viele Nutzer hilflos gegenüberstanden. Anfangs waren es nur kaschierte Links in der betreffenden E-Mail. So stand unter einer hochoffiziell wirkenden Mail, die auf den ersten Blick von der Postbank stammte, ein Link auf „http://postbank.info“. Die Mail forderte den Nutzer auf, sich auf der Seite anzumelden, um Benutzerdaten zu aktualisieren. Auf der verlinkten Seite wartete ein **originalgetreuer Nachbau** von postbank.de.

Später tauchten Phishing-Mails auf, die bei einem Klick auf einen ganz anderen als den angezeigten Link verwiesen. Mittels eines HTML-Formularfeldes wurde im Mailprogramm zwar die korrekte Adresse einer Bank angezeigt, der Klick führte jedoch auf eine **Fälschung**. Skeptische Nutzer konnten spätestens hier stutzig werden, denn der Browser zeigte die falsche Adresse durchaus an. Aber auch hierfür fanden Gauner eine Lösung: Mithilfe von JavaScript, Flash oder XUL-Dateien lassen sich in nahezu allen aktuellen Browsern einzelne Elemente der Benutzeroberfläche manipulieren. Das führt dazu, dass in der Adressleiste des Browsers eine andere URL angezeigt wird oder sogar ein kleines Schloss – Symbol für eine sichere SSL-Verbindung.

Die Faustregel, wichtige Adressen wie die seiner Bank stets manuell einzugeben, erschien zuerst logisch. Nur durch den Klick auf einen Link in einer E-Mail gelang es den Betrügern bislang, den Browser auf gefälschte Seiten zu lotsen. Wer hingegen ein Lesezeichen im Browser eingerichtet hatte oder die Adresse stets manuell eintrug, war sprichwörtlich „auf der sicheren Seite“. Doch auch diese Strategie wurde bald unterwandert. Es gelang den „Phishern“ durch einen in die Mails eingebetteten Code, **manipulierte Host-Dateien** auf den Rechnern ahnungsloser Nutzer zu installieren. In dieser Host-Datei sind statische Zuordnungen von Domain-Namen zu IP-Adressen gespeichert. Unter normalen Umständen enthält diese Datei keinerlei Einträge, die Auflösung eines Domain-Namens zur entsprechenden IP-Adresse wird online durch den DNS-Server des Providers vorgenommen. Wird in die Host-Datei jedoch beispielsweise die Zeile „213.178.69.184 postbank.de“ eingetragen, so würde der Rechner die Seite des ULD ansteuern, wenn „postbank.de“ aufgerufen wird. Das Perfide an dieser Variante ist, dass es für den Nutzer unter Umständen vollständig unsichtbar ist, dass er sich auf einer falschen Seite befindet, wenn diese das Original entsprechend gut imitiert.

Den Urhebern all dieser Fälschungen geht es stets um eines: Benutzerdaten und -kennungen für diverse Online-Dienste, meist von Banken, zu erschleichen. Insbesondere das **PIN/TAN-Verfahren** ist für dieses Vorgehen anfällig: Kann ein Nutzer dazu gebracht werden, auf einer gefälschten Seite seine PIN und eine gültige TAN einzugeben, gelangt der „Phisher“ in den Besitz einer gültigen PIN/TAN-Kombination und könnte umgehend selbst eine Buchung

? PIN/TAN

Hinter den Kürzeln PIN und TAN verbergen sich die Begriffe „Persönliche Identifikationsnummer“ und „Transaktionsnummer“.

Bei der PIN handelt es sich um eine Geheimnummer, die einem bestimmten Nutzer einmalig zugewiesen wird. So authentifiziert sich z. B. der Nutzer einer EC-Karte mit der dazugehörigen PIN gegenüber dem Geldautomaten.

Die TAN hingegen ist nur für eine einzige Transaktion gültig. Online-Banking-Kunden erhalten eine Reihe von TANs, den so genannten TAN-Block. Soll beispielsweise eine Überweisung im Internet getätigt werden, meldet sich der Kunde mit seiner PIN bei seiner Bank an und bestätigt die Überweisung mit einer TAN. Diese Nummer wird danach aus der Liste gestrichen, sie ist fortan ungültig. Für die nächste Transaktion ist wieder die PIN des Kunden und eine andere TAN nötig.

tätigen. Allerdings wäre dieses Vorgehen auffällig. Im schlimmsten Fall leitet daher die gefälschte Webseite den Nutzer einfach mit einer kurzen Fehlermeldung und dem Hinweis, die TAN sei ungültig, auf die korrekte Seite um. Hier gibt der Nutzer nun eine andere TAN ein, erledigt seine Transaktion und vergisst die Fehlermeldung. In Wahrheit ist der Betrüger im Besitz einer gültigen, d. h. unbenutzten PIN/TAN-Kombination.

Alternativ zu PIN und TAN bieten viele Banken das **HBCI-Verfahren** an, bei dem sich der Nutzer über eine Chipkarte gegenüber der Webseite authentifiziert. Dazu muss am PC ein spezielles Lesegerät installiert werden, das im Regelfall ein eigenes Tastenfeld besitzt. Auf diesem Tastenfeld gibt der Nutzer eine PIN ein und startet so den Authentifizierungsvorgang. Dritte haben keine Möglichkeit, diesen Vorgang zu beeinflussen oder abzuhören, da er ausschließlich im Chipkartenleser stattfindet. Eventuell auf dem Rechner eingeschleuste Überwachungsprogramme für die Tastatur (so genannte Keylogger) bleiben wirkungslos, weil die PIN-Eingabe ausschließlich auf dem Lesegerät vorgenommen wird.

Die Manipulation des Betriebssystems ist nur durch Ausnutzung von **Schwachstellen in Webapplikationen** möglich. Auch deshalb sollten Nutzer die Verwendung alternativer Mailprogramme und vor allem Browser in Betracht ziehen. E-Mail-Programme, die keinerlei aktiven Code ausführen können, bieten deutlich mehr Sicherheit. Kommt ein solches Programm nicht infrage, sollte die Ausführung von aktivem Code unbedingt abgeschaltet werden. Aufseiten des Webbrowsers ist der Internet Explorer nicht zu Unrecht in Verruf geraten – kein anderer Webbrowser hat mehr Schwachstellen. Durch seine große Verbreitung ist er zudem erstes Angriffsziel. Alternativen wie Firefox, Mozilla und Opera bieten hier deutlich mehr Sicherheit.

PIN und TAN bieten zwar große **Flexibilität** und Unabhängigkeit von einem speziellen PC. Gerade diese Mobilität birgt jedoch das Risiko des Missbrauchs durch Dritte. HBCI ist aufwändiger und weniger flexibel, jedoch gegen bisher bekannte Missbrauchsversuche resistent.

Was ist zu tun?
Nutzer sollten alle Links, die in E-Mails stehen, mit größter Skepsis betrachten. Im Zweifelsfall ist die Adresse manuell in den Browser einzugeben. Die Verwendung von alternativen Browsern und Mailprogrammen ist ratsam. Bietet die Hausbank HBCI an, ist dies unter Sicherheitsaspekten gegenüber PIN/TAN die bessere Wahl.

10.4 Internettelefonie – VoIP

Voice-over-IP ermöglicht Telefonieren über eine Internetanbindung oder in einem lokalen Computernetz. Da Telefonie und Datenkommunikation sich dabei die gleichen Leitungen teilen, erübrigt sich eine eigene Telefoninfrastruktur. Die neue Technik bringt nicht nur Kostenvorteile mit sich, sondern wirft auch Fragen des Datenschutzes auf.

Mit Voice-over-IP **(VoIP)** kann prinzipiell jeder, der über das technische Know-how und ein wenig Kapital verfügt, zum **Anbieter von Sprachdiensten** werden, ohne erst kilometerlange Kabel in der Republik verlegen zu müssen. Einige Internetprovider bieten ihren Kunden inzwischen VoIP als Zusatzdienst an. Netzinterne Gespräche sind dabei in der Regel kostenlos.

Wirtschaftliche Hürde ist in der Regel eher der **Zusammenschluss mit dem herkömmlichen Telefonnetz**, denn dann werden Gebühren an die Telefongesellschaften fällig. Sollen die VoIP-Kunden per Rufnummer aus dem Festnetz erreichbar sein, muss zudem ein entsprechender Rufnummernblock von der Regulierungsbehörde für Telekommunikation und Post (RegTP) erstanden werden. Über die Frage, wer unter welchen Bedingungen welche Nummernblöcke bekommen darf, wird noch gestritten.

Angesichts der Diskussion über Geld und Technik gerät die Frage nach Datenschutz und Datensicherheit leider in den Hintergrund. Die Technik bietet einerseits die Möglichkeit, **vertrauliche Kommunikation** abhörsicher zu gestalten. Doch ignorieren einige Anbieter andererseits bei dem Wirbel um technische Funktionalität, Verbindungsgebühren und Rufnummernvergabe schon mal datenschutzrechtliche Vorschriften, wie sie z. B. bei der Erfassung und Abrechnung von Gesprächsverbindungen gelten.

> **? *RTP***
>
> *Real-Time Transfer Protocol – Protokoll zur Datenübertragung in Echtzeit*

Die Frage der Abhörsicherheit ist bei VoIP noch relevanter als bei herkömmlicher Telefonie: Auf ihrem Weg durchs Internet können die zur Übertragung verwendeten Datenpakete auf jeder Station unbemerkt gelesen werden. Insbesondere für Unternehmen, die ihre Mitarbeiter ins Ausland senden, ist VoIP eine günstige Methode, die Kommunikation mit dem Team daheim zu gewährleisten. Durch konsequenten Einsatz von **Verschlüsselung** können sie sich vor Wirtschaftsspionage wirksam schützen.

> **? *SIP***
>
> *Session Initiation Protocol – Protokoll zum Aufbau einer Verbindung*

Gängige Protokolle für VoIP wie SIP und RTP sind auch in verschlüsselnden Varianten definiert. Doch gibt es bisher nahezu keine endkundentauglichen Geräte, die Verschlüsselung unterstützen. Hier liegt zweifelsohne ein großer Markt

brach. Im Rahmen unseres Innovationszentrums ULD-i versuchen wir, Partner aus Wirtschaft und Wissenschaft zu finden, damit Bürgerinnen und Bürgern ebenso wie Unternehmen in diesem Marktsegment datenschutzfördernde Techniklösungen angeboten werden können.

Was ist zu tun?
Anbieter von VoIP-Produkten müssen Lösungen mit sicherer Ende-zu-Ende-Verschlüsselung auf den Markt bringen. Provider für VoIP-Verbindungen müssen die Einhaltung datenschutzrechtlicher Vorgaben sicherstellen.

10.5 WPA – neuer Anlauf bei der WLAN-Verschlüsselung

Funknetzwerke sind beliebt und begehrt. Vom Heimanwender, der im Garten via Notebook surfen möchte, über Krankenhäuser mit mobiler Datenerfassung bis hin zur Anwaltskanzlei, die ihre Räumlichkeiten flexibel und ohne lästige Kabel vernetzen möchte, reicht die Bandbreite. Inzwischen spricht sich herum, dass Funknetzwerke in Sachen Sicherheit – vorsichtig ausgedrückt – problematisch sind.

Die Hardware der ersten Generation von Funknetzen – auch WLAN (Wireless Local Area Networks) genannt – verfügt über eine als WEP bezeichnete **Verschlüsselung**, die sicherheitstechnisch als gleichwertig zu drahtgebundenen Lösungen konzipiert war. Diese Verschlüsselung wurde jedoch umgehend **gebrochen**, und Programme, die ein solches „Aufbrechen" von verschlüsselten Funknetzwerken ermöglichen, sind frei verfügbar. Da man kein Kryptoexperte sein muss, um solche Tools zu nutzen, ist jeder interessierte Nutzer technisch in der Lage, in WEP-geschützte Netze einzubrechen.

Schlimmer als diese offenkundige Schwäche der WEP-Verschlüsselung wiegt der Umstand, dass viele WLAN-Geräte standardmäßig mit einer komplett **deaktivierten Verschlüsselung** ausgeliefert werden, sodass sie für eine Nutzung durch Dritte weitgehend offen sind. Dieser Umstand ändert sich nur allmählich.

Im Jahre 2000 wurde mit der Entwicklung eines Nachfolgers von WEP begonnen. Um die Zwischenzeit bis zu seiner Fertigstellung zu überbrücken, entschloss sich das Institute of Electrical and Electronic Engineers (IEEE), das die Entwicklung und Standardisierung für Funknetzwerke vorantreibt, zu einem **Zwischenschritt**. Mit WPA wurde im Jahr 2003 ein Teilstandard veröffentlicht, der dem dringenden Bedarf nach einer einheitlichen und brauchbaren Lösung Rechnung tragen soll. WPA ist der bisherigen WEP-Verschlüsselung in mehreren Punkten überlegen: Die Achillesferse von WEP war der Initialisierungsvektor. Mit seinen 24 Bit ermöglichte er eine sehr begrenzte Anzahl solcher Vektoren. WPA stellt für den Initialisierungsvektor nun statt 24 eine Länge von 48 Bit zur Verfügung. Die Integritätsprüfung wurde deutlich verbessert und verhindert nun, dass Datenpakete aufgefangen, verändert und dann weitergesendet werden können. Des Weiteren wurde der bei WEP konstante Schlüssel über ein Temporal Key Integrity Protocol (TKIP) durch dynamische Schlüssel ersetzt, die pro Benutzer und Datenpaket erzeugt werden.

WPA setzt als Zwischenlösung nicht alle von der IEEE geplanten Verbesserungen um, insbesondere im Hinblick auf das **verwendete Verschlüsselungsverfahren**. Das liegt vor allem an der angestrebten Hardwarekompatibilität: WPA soll weitgehend auf bisheriger WLAN-Hardware laufen und dort durch ein Softwareupdate realisierbar sein. Ende 2004 wurde schließlich WPA2 unter dem offiziellen Namen „**802.11i**“ als Standard veröffentlicht. Zur Verschlüsselung kommt ein grundlegend anderer Algorithmus zum Einsatz, der „Advanced Encryption Standard“ (AES). Dieser ist weithin erprobt und gilt als praktisch sicher. Allerdings benötigt AES zur Ver- und Entschlüsselung deutlich mehr Rechenleistung, weshalb WPA2 auf bisheriger Hardware nicht lauffähig ist.

Erste berichtete Schwächen von **WPA2** beziehen sich lediglich auf die für den Verschlüsselungsaufbau notwendigen Passwörter. Diese können einfach durchprobiert werden. Ist das Passwort schwach, ist auch die damit gesicherte Verschlüsselung leicht zu brechen. Schlechte Passwörter sind jedoch keine Schwäche des Verschlüsselungsalgorithmus. Ein weiteres Problem liegt in den höheren Hardwareanforderungen des 802.11i-Standards, die neue Hardware nötig machen. Bestehende Geräte lassen sich allenfalls auf die Zwischenlösung WPA umrüsten. Ein Mischbetrieb aus WPA und WPA2 ist nicht möglich bzw. führt dazu, dass alle Geräte mit WPA arbeiten. Nach wie vor sind Virtuelle Private Netzwerke (VPNs) eine Alternative, in denen verschlüsselte Verbindungen zwischen den Rechnern Ende-zu-Ende aufgebaut werden. Diese sind von dem dazwischen liegenden Netz und dessen Technik und Sicherheit unabhängig.

Was ist zu tun?
Bestehende mit WEP betriebene WLAN-Hardware sollte umgehend auf WPA-Tauglichkeit überprüft und möglichst umgerüstet werden. Zur Initialisierung nötige Passwörter sollten auf keinen Fall normalsprachlicher Natur sein, sondern Sonderzeichen und Zahlen enthalten und ausreichend lang sein. Sollen über ein Funknetzwerk sensible Daten übertragen werden, ist zusätzlich ein Virtual Private Network notwendig, um von möglichen Schwächen der WLAN-Verschlüsselung unabhängig zu sein.

10.6 Viel Wirbel um GMail

Mit GMail bietet Suchmaschinenprimus Google einen E-Mail-Service an. Dieser ist kostenlos und bietet neben 1 Gigabyte Speicherplatz und Tools zur Mailverwaltung auch reichlich Zündstoff für Datenschutzdiskussionen.

Die Kernkompetenz von Google liegt im Suchen und Finden von Daten. GMail unterscheidet sich von anderen Webmailanbietern darin, dass die E-Mails nicht strukturiert in Ordnern und Unterordnern gespeichert, sondern über eine Suchfunktion erschlossen werden. Finanzieren soll sich der Dienst über eingeblendete Werbung. Die Aufmerksamkeit der Datenschützer zog GMail auf sich, da zum **Einblenden der Anzeigen** die Inhalte der E-Mails ausgewertet werden. Die Werbung soll so im Kontext der jeweils aufgerufenen E-Mail angezeigt werden.

Während man beim Empfänger, d. h. dem GMail-Nutzer, vielleicht noch von einer Einwilligung zum „Lesen der eigenen Post“ ausgehen kann, ist dies beim Absender in der Regel nicht gegeben.

Neben diesem offensichtlichen Eingriff in die Vertraulichkeit der persönlichen Kommunikation finden sich in der **Datenschutzerklärung** (Privacy Policy) des Dienstes weitere Haken. So behält sich Google vor, auch nach Auflösung des Accounts die E-Mails weiter zu speichern. Zudem will Google das Verhalten der Nutzer auswerten, z. B. auf welche Werbung mit einem Klick reagiert wurde. Google sichert dabei auf sehr eigentümliche Art Vertraulichkeit zu: „We do not disclose your personally identifying information to third parties unless we believe we are required to do so.“ Einzige Voraussetzung für die Datenweitergabe ist es also für Google zu glauben, diese sei erforderlich.

Während die automatische Auswertung von E-Mails zu Werbezwecken ein besonders negatives Licht auf Google wirft, ist die Firma mit ihrer Datenschutzerklärung zu GMail kein vereinzeltes schwarzes Schaf. In den Bedingungen und **Erklärungen anderer Dienste** findet man meist ähnlich gruselige Bedingungen.

Was ist zu tun?
Jeder sollte sich vor der Nutzung von Diensten die Datenschutzerklärungen genau durchlesen und gegebenenfalls überlegen, ob er tatsächlich bereit ist, einen „kostenlosen“ Dienst mit seiner Privatsphäre zu bezahlen.

10.7 Windows XP ServicePack 2: Paradigmenwechsel bei Microsoft?

Viel war spekuliert worden im Vorfeld des zweiten ServicePacks für Windows XP. Von einer neuen Windows-Version namens „Reloaded“ war die Rede, es sollte keine Updates für illegale Windows-Versionen geben, und Tauschbörsen sollten unter Windows XP nicht mehr funktionieren. Service-Pack 2 kam – und damit vieles anders, als viele erwartet hatten.

Mit dem ServicePack 2 – kurz: SP2 – schlägt Microsoft eine grundlegend neue Marschrichtung ein. Galt bislang die Prämisse, alles müsse so einfach wie möglich funktionieren, führt Microsoft mit SP2 plötzlich **Sicherheitsmechanismen** ein, die einige Funktionalitäten beeinträchtigen. Auf Betriebssystemebene wird beispielsweise mit der NX-Funktion für 64-Bit-Prozessoren und deren Softwarenachbildung für andere CPUs das Auftreten von Buffer-Overflows deutlich erschwert. In der Folge funktionierten etliche Programme mit dem neuen Service-Pack nicht oder nur eingeschränkt: Unsauber programmierte Software, die bislang vom System toleriert wurde, kollidierte mit den schärferen Ausführungsbestimmungen. Auch der Internet Explorer zeigt eine Abkehr von der bisherigen Strategie. Was sich mit der P3P-basierten Cookie-Behandlung angekündigt hatte, wird

jetzt mit standardmäßig aktiviertem Pop-Up-Blocker und eingeschränkten ActiveX-Funktionalitäten fortgeführt. Auch hier funktionierten einige Webseiten nicht ordnungsgemäß, die beispielsweise wichtige Informationen in Pop-Up-Fenstern anzeigen oder Plug-Ins automatisch installieren wollten. Die Einführung eines neuen Systemdienstes namens „Sicherheitscenter“ erinnert den Nutzer sehr eindringlich (man möchte sagen: penetrant) an die Installation von Antivirensoftware, einer PC-Firewall und aktuellen Sicherheitsupdates.

Bei vielen Anwendern führten die angekündigten Veränderungen durch das ServicePack 2 zu Verunsicherungen, wie Anfragen bei uns belegen. Dabei können die Sicherheitsfunktionen des SP2 nur auf den ersten Blick überzeugen. So lässt sich das Sicherheitscenter leicht, vor allem auch scriptgesteuert abschalten, ohne dass der Nutzer davon etwas merkt. Die integrierte Firewall macht bei der Übernahme der Regeln der Vorversion mitunter **grobe Fehler** und gibt Drucker und Verzeichnisse nicht nur im lokalen Netz, sondern im gesamten Internet frei.

Ein Hauptproblem beim Einsatz von Windows bleiben die **Benutzerrechte**. Die meisten Anwender melden sich als Administrator am System an und ermöglichen auf diese Weise auf dem PC befindlichen schädlichen Programmen die Übernahme des Rechners. Die Warnungen des Sicherheitscenters beispielsweise lassen sich über einen Registry-Schlüssel deaktivieren. Ein Wurm, innerhalb eines Administratorkontos ausgeführt, kann diesen Eintrag in der Registry ändern, was ohne Administratorrechte nicht möglich ist. So lindert das ServicePack 2 sicherlich einige **Symptome**, die **Ursachen** massiv unsicherer Windows-Systeme vor allem im Heimbereich werden jedoch nicht beseitigt. Hinzu kommen Ungereimtheiten in den Sicherheitsfunktionen des SP2. So meldet das Sicherheitscenter nicht unbedingt, wenn der Virenscanner nicht läuft, sondern leuchtet dem Nutzer mit einem grünen „Aktiv“-Hinweis entgegen. Auch der Schutz vor Buffer-Overflows ist löchrig und lässt sich mit etwas Aufwand aushebeln.

ServicePack 2 für Windows XP ist ein Schritt in die richtige Richtung. In der Standardkonfiguration wird ein XP-System deutlich sicherer. Überflüssige Funktionen wie der Nachrichtendienst oder die ActiveX-Installation sind automatisch deaktiviert, Sicherheitsfunktionen wie der Download-Schutz für den Internet Explorer oder die rudimentäre Firewall sind bereits ohne Zutun des Nutzers aktiv. Trotzdem verteidigt Microsoft erfolgreich seinen Ruf, **unausgereifte Software** zu veröffentlichen. Etliche der Sicherheitsfunktionen besitzen Schwachstellen, die in absehbarer Zeit ausgenutzt werden dürften. Anwender können sich also auch mit dem ServicePack 2 noch nicht entspannt zurücklehnen.

10.8 Trusted Computing

Unter dem Begriff „Trusted Computing“ wird ein Mehr an Sicherheit versprochen. Nach wie vor ist nicht eindeutig erkennbar, wer damit vor wem geschützt werden soll.

Im letzten Tätigkeitsbericht (26. TB, Tz. 11.2) hatten wir die Grundzüge von Trusted Computing beschrieben. Trotz der Kritik der Datenschützer, der sich

namhafte Interessenvertreter anderer Bereiche anschlossen, hat sich seitdem im Bereich der Hardwarespezifikation nicht viel getan. Der Gesamtverband der deutschen **Versicherungswirtschaft** äußerte sich zum Thema „Risiko Trusted Computing“ und kommt zu ähnlichen Schlüssen wie wir:

„Die sich hier abzeichnenden Risiken sind für die Versicherungswirtschaft inakzeptabel, da sie nicht zuletzt infolge gesetzlicher Vorschriften als verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes die vollständige Kontrolle über ihre Daten, Inhalte und Geräte behalten muss.“

„Die vorgeschlagenen Techniken des Trusted Computing basieren auf Vertrauen gegenüber den bereitstellenden Firmen, ohne dass in irgendeiner Form entsprechende gesetzliche Kontrollen und Möglichkeiten der Anwender zur Durchsetzung ihrer Schutzinteressen existieren.“

Im Bereich von **Trustworthy Computing**, so die Microsoft-Bezeichnung für deren Softwareerweiterungen auf Betriebssystemebene, wurde von Microsoft das Projekt NGSCB (Next Generation Secure Computing Base) vorerst auf Eis gelegt. Stattdessen scheint sich Microsoft auf die NX (No eXecution)-Prozessortechnologie zu konzentrieren, die Speicherüberläufe reduzieren soll, welche die üblichen Angriffspunkte für bösartigen Programmcode darstellen, und Entwicklern erlaubt, Speicherseiten als nichtausführbar zu markieren. Neuere Vorschauversionen von Microsofts nächster Version von MS Windows (Longhorn), enthalten kein NGSCB mehr. Bevor man hier die Datenschutzimplikationen betrachtet, muss man auf Microsofts neue Konzepte warten.

Was ist zu tun?
Daten verarbeitende Stellen müssen vom Einsatz von Trusted Computing absehen, solange nicht die vollständige Kontrolle durch die Anwender über Daten, Schlüssel, Inhalte und Geräte gegeben ist.

10.9 Anonymes Logging – eine Problemanalyse

Jeder Betreiber einer Homepage möchte wissen, wie sich die Besucher seiner Seite verhalten. Das Mitloggen der IP-Adressen der Besucher führt regelmäßig zu Konflikten mit dem Datenschutz. Abhilfe könnte hier eine Anonymisierung der Daten schaffen. Dies erweist sich jedoch schwieriger, als es auf den ersten Blick scheint.

Wie viele Nutzer besuchen täglich meine Homepage? Wie lange verweilen sie? Über welche Links auf fremden Webangeboten gelangt der Nutzer zu meinem Angebot? Welche Bereiche meiner Homepage sind besonders attraktiv, und welche finden kein Interesse? Auf welchen Pfaden bewegt sich ein Nutzer durch mein Webangebot? Das sind die wohl meistgestellten **Fragen von Homepage-Betreibern**. Um Antworten zu erhalten, wird der eingesetzte Webserver so konfiguriert, dass die vom Rechner des Nutzers übermittelten Daten in ein Logfile geschrieben werden. **Auswertungstools** analysieren diese Logfiles und bereiten

die Ergebnisse grafisch auf. Je nach Speicherdauer der Logfiles erhält der Betreiber so die Möglichkeit, einen Überblick über das Verhalten seiner Besucher über einen bestimmten Zeitraum zu bekommen.

Aber zur aussagekräftigen Beantwortung der Fragen nach Besucherzahl und deren Bewegungen auf der Seite verlangen die Auswertungstools eindeutige Identifikatoren, um einzelne Seitenaufrufe korrekt Besuchern zuordnen zu können. Nichts liegt also näher, als die IP-Adressen der Besucher mitzuloggen, die diese eindeutigen Zuordnungen ermöglichen. Diese von fast allen Homepage-Betreibern ausgeübte Praxis wird von uns kritisiert: Die als **personenbezogen** einzustufenden **IP-Adressen** werden mitunter über sehr lange Zeiträume gespeichert, z. B. für Jahresauswertungen zur Erkennung von saisonalen Unterschieden. Letztendlich lassen sich aus der Menge der mitgeloggten Daten auch aussagekräftige Profile der einzelnen Besucher herstellen.

Ein gängiger Lösungsversuch ist die Pseudonymisierung der IP-Adressen durch **Abtrennen der ersten beiden Ziffernblöcke**. Falls ein Serviceanbieter mit weltweitem Kundenstamm keine weiteren Merkmale der Nutzer auswertet, z. B. die Sprachauswahl oder die Browserkennung, erfüllt diese Praxis zumindest den Sinn der Pseudonymisierung. Immerhin ca. 65.000 IP-Adressen nutzen jeweils dieselben letzten beiden Ziffernblöcke. Die Auswertung des Nutzerverhaltens verliert so aber an Aussagekraft. Beschränkt sich das Serviceangebot nur auf bestimmte Regionen, nimmt auch der Grad der Pseudonymisierung stark ab, da ganze IP-Adressräume als mögliche IP-Adresse der Nutzer nicht mehr infrage kommen. Zusammenfassend: Beim Abschneiden von Ziffernblöcken von IP-Adressen ohne Erfassung weiterer Merkmale verhält sich der Grad der Pseudonymisierung umgekehrt proportional zur Aussagekraft der Logfile-Auswertung.

Als einfacher Ausweg aus der Misere erscheint die Substitution der IP-Adresse durch einen beliebigen Platzhalter. Um allerdings korrektes Besucherverhalten reproduzieren zu können, muss einer IP-Adresse immer wieder derselbe Platzhalter zugeordnet werden. Dies ließe sich natürlich durch eine **Zuordnungstabelle** bewerkstelligen. Wird diese genauso lange gespeichert wie die Logfiles, ist keine Besserung des Problems aufgetreten. Im Falle einer regelmäßigen und kurzzeitigen Löschung dieser Tabelle entstehen Verfälschungen in den Auswertungen der Besucherströme. Denn ein Besucher kurz vor der Löschung der Zuordnungstabelle wird nach der Löschung als ein neuer Besucher identifiziert werden, sodass die Besucheranzahl fälschlicherweise steigt und die Besucherpfade um den Löschpunkt herum keine Aussagekraft mehr besitzen. Setzt der Anbieter die Löschung der Zuordnungstabelle auf den Tageszeitpunkt, an dem seine Seite am wenigsten besucht wird, hält sich die Artefaktbildung in der Auswertung in Grenzen.

Der nächste logische Schritt ist das Ersetzen der IP-Adresse ohne Speicherung der Zuordnung von IP-Adresse und Pseudonym. Hier drängt sich der Einsatz einer **Einweg-Hash-Funktion** (Secure Hash) förmlich auf. Diese Funktion bietet die Möglichkeit, sozusagen on-the-fly eine IP-Adresse in eine verschlüsselte Nachricht umzuwandeln. Ein großer Vorteil dieser Funktion ist die Unumkehrbarkeit, was bedeutet, dass sich aus einer verschlüsselten Nachricht nicht der Originaltext (hier wäre es die IP-Adresse) erzeugen ließe. Einen zweiten Vorteil stellt die

Eindeutigkeit dar, die besagt, dass aus einer Originalnachricht immer der gleiche verschlüsselte Text errechnet wird. Für unseren Fall, der Anonymisierung von IP-Adressen mit Erhaltung der Auswertbarkeit, scheinen die genannten Vorteile unschlagbar zu sein. Leider versteckt sich innerhalb des zweiten Vorteils ein K.-o.-Kriterium für die verfolgte Zielsetzung: Die Anzahl der Originalnachrichten ist beschränkt und ihr Aussehen bekannt.

Jeder Computerbesitzer ist in der Lage, von allen existierenden IP-Adressen den zugehörigen Hash-Wert zu erzeugen. Wahrscheinlich ist so eine Liste sogar im Internet zu finden. Ob nun wirklich von allen 4,2 Milliarden IP-Adressen der Hash-Wert zu errechnen ist, um ein pseudonymisiertes Logfile zu repersonalisieren, hängt wiederum vom Webangebot ab. Ein regionaler mitteleuropäischer Serviceanbieter wird sich sicherlich nicht für die einzelnen IP-Adressen aus Asien in seinem Logfile interessieren, welche mit großer Wahrscheinlichkeit von dort stationierten Suchmaschinen stammen. Nach Streichung von nicht relevanten und verbotenen IP-Adressen verbleiben maximal zehn Prozent aller IP-Adressen, die für diesen Anbieter als potenzielle Kunden-IP-Adressen in Betracht kommen. Eine **Zuordnungstabelle** von IP-Adressen **zu** ihren **Hash-Werten** in dieser Größe zu erzeugen ist für aktuelle Heimcomputer keine schwierige Aufgabe. Leider entwickelt die Secure-Hash-Funktion ihre größte Stärke genau dann, wenn ihre Ausgangsmenge nicht beschränkt ist, sodass sie für die Anonymisierung von Logfiles nicht infrage kommt.

Der **Bedarf** an intelligenten Lösungen ist vorhanden. Viele Anbieter haben uns gegenüber schon ein großes Interesse an der Möglichkeit des anonymen Loggings gezeigt. Es verwundert, dass noch keine zufrieden stellende Lösung existiert. Dies mag ein Indiz für den Schwierigkeitsgrad der Lösung sein.

Was ist zu tun?
Für die datenschutzgerechte Auswertung von Internetnutzungsverhalten wäre eine Anwendung die ideale Lösung, die Logdaten anonymisiert, bevor sie ins Logfile geschrieben werden, und dabei die Logauswertung so gering wie möglich verändert. Eine solche Lösung sollte nicht nur auf das Weblogging beschränkt sein, sondern sollte sich auch auf andere Logprozesse (z. B. auf einem Mailserver oder einer Firewall) anwenden lassen.

11 Informationsfreiheit

Auch nach fünf Jahren Informationsfreiheitsgesetz Schleswig-Holstein (IFG-SH) besteht hierzu großer **Beratungsbedarf** bei den Behörden und Bürgern. Durch unsere Vermittlung bei Beschwerden und Anfragen ist es zumeist möglich, Konflikte zur Zufriedenheit der Behörden wie der Petenten zu lösen.

Vermittlungsversuche sind dann erfolglos, wenn beide Seiten voneinander abweichende klare rechtliche Standpunkte vertreten. In diesen Fällen ist oft ein **gerichtliches Verfahren** nicht zu vermeiden. Dies muss nicht nur negativ gesehen werden, eignen sich doch solche Musterverfahren zur rechtlichen Klärung streitiger Fragen. Ein Streitpunkt betraf die Frage, ob das IFG-SH auf fiskalisches Handeln einer Behörde anwendbar ist. Davon sind wir seit Jahren überzeugt (24. TB, Tz. 13.1; 25. TB, Tz. 13.2; 26. TB, Tz. 12.2). Unsere Auffassung wurde durch ein nunmehr rechtskräftiges Urteil bestätigt (Tz. 11.1).

11.1 Interessante Einzelfälle

- **Beanstandung wegen Untätigkeit**

Ein Petent wollte in Erfahrung bringen, wann ein städtisches Heizkraftwerk veräußert worden und in welcher Form die Stadt weiterhin an dem Kraftwerk beteiligt ist. Ihn interessierte insbesondere, in welcher Weise die Stadt Wahlstedt Einfluss auf die Betriebsführung des Kraftwerkes nehmen kann und welche vertraglichen Vereinbarungen über die Versorgung des Stadtgebietes getroffen worden sind. Der Petent erhielt auf seine Anfragen nie eine Antwort. Auch unsere mehrfachen Aufforderungen zur Stellungnahme blieben schlichtweg ohne Antwort. Dies zwang uns zu einer **förmlichen Beanstandung**, verbunden mit der Erwartung, dass die Kommunalaufsicht diese Rechtsverweigerung beendet. Unabhängig davon prüfen der Petent und seine Rechtsanwälte ein gerichtliches Vorgehen gegen die Stadt.

- **Anwendbarkeit des IFG im Zwangsgeldverfahren?**

Gerichte, Strafverfolgungs- und Strafvollstreckungsbehörden sowie Disziplinarbehörden sind, soweit sie als Organe der Rechtspflege oder aufgrund besonderer Rechtsvorschriften in richterlicher Unabhängigkeit tätig werden, vom Anwendungsbereich des IFG-SH ausgenommen. **Zwangsgeldverfahren**, die der Vollstreckung hoheitlicher Anordnungen dienen, unterliegen den Vorschriften des **Landesverwaltungsgesetzes**. Bei diesen öffentlichen Verwaltungstätigkeiten findet das IFG-SH ohne Einschränkung Anwendung. Bürger haben also grundsätzlich Anspruch auf Einsicht in eine Androhung oder die Festsetzung eines Zwangsgeldes. Berechtigten Interessen – der Behörde oder Dritter, deren Betriebsgeheimnisse bzw. personenbezogenen Daten betroffen sein könnten – kann ausreichend durch die Ausnahmetatbestände und Ausschlussgründe, die das IFG-SH vorsieht, Rechnung getragen werden.

- **Aufsicht über die Bauaufsicht**

Kann ein Mieter in die bauaufsichtsrechtlichen Akten seines Vermieters Einsicht nehmen? Mit dieser Frage wandte sich eine Behörde an uns. Der Mieter hatte den Verdacht, dass seine Kellerwohnung nach den baurechtlichen Vorschriften gar nicht als Wohnraum hätte vermietet werden dürfen. Bei den Bauaufsichtsunterlagen handelt es sich um personenbezogene Daten, weshalb eine Offenbarung nur in Betracht kommt, wenn der Antragsteller bei der Behörde glaubhaft machen kann, dass er ein **rechtliches Interesse** an der Offenbarung der Information hat und überwiegende schutzwürdige Belange des Betroffenen nicht entgegenstehen.

Hier bestand ein berechtigtes Interesse des Petenten in einem möglichen **zivilrechtlichen Anspruch** gegen seinen Vermieter. Sollte sich herausstellen, dass keine Genehmigung zur Vermietung des Kellergeschosses vorlag, so könnte sich hieraus eine Schadensersatzpflicht ergeben. Schutzwürdige Belange des Vermieters lagen demgegenüber nicht vor.

- **Einsicht in Unterlagen über die Erhebung von Ausbaubeiträgen**

Nach Ausbau mehrerer Straßen im Rahmen eines gemeindlichen Bauprojektes wurden die Eigentümer der Anliegergrundstücke zu Straßenausbaubeiträgen herangezogen. Einer der betroffenen Grundstückseigentümer begehrte Einsicht in die maßgeblichen Kalkulationen der Ausbaubeiträge. Dabei wollte er nicht nur eine allgemeine Kostenzusammenstellung, sondern auch die Bescheide der anderen Grundstückseigentümer einsehen. Die Behörde hatte berechtigte Bedenken gegen die Offenbarung der Beitragsbescheide. Der Informationsanspruch des Grundstückseigentümers war zu beschränken. Eine Offenbarung der Daten der anderen Eigentümer ist nur ausnahmsweise zulässig, soweit ein rechtliches Interesse an der Offenbarung dieser Daten besteht. Dieses Interesse ist durch **schlüssige Tatsachen glaubhaft** zu machen. Ist eine personenbezogene Offenbarung nicht möglich, kann eine Einsichtnahme dennoch nach erfolgter Anonymisierung erfolgen. Wegen des kleinen betroffenen Personenkreises war dies jedoch hier nicht möglich. Möglich bleibt die **Einholung der Einwilligung** der anderen Grundstückseigentümer. Der Antragsteller ist hierauf und auf die Notwendigkeit eines entsprechenden Antrags hinzuweisen.

- **Transparenz bei Gebühren für die Abwasserbeseitigung**

Ein Bürger einer Gemeinde interessierte sich für die Gebührenberechnungsunterlagen der Abwasserbeseitigung. Die Gemeinde war bereit, ihm Einsicht zu gewähren. Kopien der Berechnungen wollte sie jedoch trotz Bitte des Petenten nicht zulassen. Wir wiesen die Gemeinde darauf hin, dass nach dem IFG-SH auch ein Anspruch auf Erstellung und gegebenenfalls auf **Versendung von Kopien** besteht. Doch auch dies befriedigte den Petenten noch nicht. Er beantragte nunmehr Einsicht in die Unterlagen, die Grundlage für die gemeindliche Berechnung der Flächen waren. Hierdurch wären personenbezogene Daten von Grundstückseigentümern offen gelegt worden. Es wurde daher eine **Anonymisierung** der Flächenermittlung vereinbart. Nach mehrfacher Überprüfung der Daten wurde von

der Gemeinde eine Aggregation der Daten erstellt, bei denen ein Bezug zu den einzelnen Grundstückseigentümern ausgeschlossen werden konnte. Später wurde deutlich, dass es dem Petenten insbesondere um die Flächenberechnungen bei den gemeindeeigenen Grundstücken ging. Gegen eine Offenbarung dieser Daten bestanden keine Bedenken, da keine **privaten Grundstückseigentümer** betroffen sind.

- **Auskunft an einen Stadtvertreter**

Ausschusssitzungen der Städte bzw. Gemeinden finden zum Teil unter Ausschluss der Öffentlichkeit statt. Hinsichtlich des nichtöffentlichen Teils der Sitzungen sind die Stadtvertreter verpflichtet, die erhaltenen Informationen nicht weiterzugeben. Nun wandte sich ein **Stadtvertreter als Privatperson** an seine Stadt und bat dort um Informationen. Er wollte Auskunft über die Anzahl der Wohneinheiten, der Stellplätze und der genauen Lokalität bei einem bestimmten Objekt erhalten. Die gewünschten Informationen sind dem Petenten dann aus dem Protokoll des nichtöffentlichen Teils einer Ausschusssitzung, an der er als Stadtvertreter teilgenommen hat, verlesen worden. Diese Vorgehensweise der Stadt führte dazu, dass sich der Petent wegen seiner Verschwiegenheitsverpflichtung als Stadtvertreter an einer Weitergabe der Informationen gehindert sah. Wir machten die Stadt darauf aufmerksam, dass der Petent Auskunft als Privatperson und nicht in seiner Funktion als Stadtvertreter ersucht hat. Die Behörde teilte daraufhin die Informationen ohne jede Einschränkungen erneut mit.

- **Anwendbarkeit des IFG auf private Unternehmen**

Anfragen betreffen immer wieder den Anwendungsbereich des IFG-SH. Das Gesetz ist auf juristische **Personen des Privatrechts** anwendbar, wenn eine Behörde sich dieser Person zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben bedient oder dieser Person die Erfüllung solcher Aufgaben übertragen wird. Erfasst werden außerdem juristische Personen des Privatrechts, denen öffentlich-rechtliche Aufgaben komplett und auf Dauer zur Erfüllung im eigenen Namen übertragen wurden. Es kommt also nicht allein auf die Trägerschaft der öffentlichen Hand an, diese hat nur eine Indizwirkung.

In einem Fall begehrte ein Petent bei einer Telekommunikationsgesellschaft Auskunft über Zuwendungen von einer Stadt, die Alleingesellschafterin dieser GmbH war. Aufgabe der Telekommunikationsgesellschaft war der Aufbau eines eigenen Telefonnetzes und die Erbringung von Telekommunikationsdienstleistungen. Waren dieser GmbH **öffentlich-rechtliche Aufgaben** komplett und auf Dauer zur Erfüllung im eigenen Namen übertragen worden? Seit der **Liberalisierung** des **Telekommunikationsmarktes** gehört die Erbringung von Telekommunikationsdienstleistungen nicht mehr zum Bereich der Daseinsvorsorge. Es ging nicht um die Erfüllung einer öffentlich-rechtlichen Aufgabe, weshalb das IFG-SH auf die Telekommunikationsgesellschaft nicht anwendbar war.

Nicht beantwortet ist damit die Frage, ob ein Anspruch auf Zugang zu den Informationen besteht, die der **Bürgermeister** in seiner Funktion als **Aufsichtsratsvorsitzender** bei der juristischen Person des Privatrechts besitzt. Der Bürgermeister der Stadt war – durch Gesellschaftsvertrag bestimmt – Aufsichtsratsvorsitzender der Gesellschaft. Ein Bürgermeister ist nach dem Gesetz eine Behörde. Für den Behördenbegriff ist entscheidend, dass es sich im organisatorischen Sinne um eine Stelle handelt, die Verwaltungsaufgaben wahrnimmt. Ist dies der Fall, ist der Anwendungsbereich des IFG-SH eröffnet, selbst wenn die Behörde nicht verwaltend tätig wird. Dies gilt auch, wenn der Bürgermeister die Unterlagen nicht in seiner Funktion als Bürgermeister, sondern in seiner Funktion als Aufsichtsratsvorsitzender besitzt. Eine andere Sicht widerspräche der gesetzgeberischen Intention einer **größtmöglichen Transparenz** bei Behördenentscheidungen. Der Bürgermeister als Aufsichtsratsvorsitzender wird nicht als Privatperson tätig. Seine Tätigkeit ist – entsprechend dem Gesellschaftsvertrag – an seine Funktion als Bürgermeister geknüpft. Aufgrund dieser Sachnähe zur Funktion als Bürgermeister unterfiel der Sachverhalt dem Anwendungsbereich des IFG.

- **Anwendbarkeit des IFG-SH auf Unterlagen über fiskalisches Handeln**

Im Jahr 2003 berichteten wir über einen Antrag auf Einsicht in Wärmelieferungsverträge, die ein schleswig-holsteinischer Kreis zur Versorgung seiner eigenen Gebäude mit zwei großen Energieversorgern geschlossen hat (25. TB, Tz. 13.2). Der Kreis hatte die Einsicht unter Hinweis auf die Nichtanwendbarkeit des IFG-SH bei **behördlichem fiskalischen Handeln** verweigert. Das Schleswig-Holsteinische Verwaltungsgericht hat den Fall inzwischen entschieden und die vom Innenministerium vertretene Position zurückgewiesen, wonach das IFG-SH ausschließlich auf öffentlich-rechtliches Verwaltungshandeln anwendbar sei. Das IFG-SH ergibt nach seinem Wortlaut, seiner Entstehungsgeschichte sowie seinem Sinn und Zweck keinen Anlass für eine derartige Beschränkung.

Nach dem organisationsrechtlichen Behördenbegriff, von dem das Landesverwaltungsgesetz ausgeht, ist die Behördeneigenschaft unabhängig von der öffentlich- oder privatrechtlichen Handlungsform. Da das IFG-SH auf die Definition des Landesverwaltungsgesetzes verweist, ist nach Ansicht des Gerichts nach dem **Gesetzeswortlaut** die Anwendung gerade nicht auf die Ausübung öffentlich-rechtlicher Tätigkeiten beschränkt. Auch **Sinn und Zweck** des Gesetzes, nämlich eine Erhöhung der Transparenz, der Nachvollziehbarkeit und der Akzeptanz von Verwaltungsentscheidungen, ließen eine solche Beschränkung nicht zu.

Mit dieser Auffassung bestätigte das Verwaltungsgericht die von uns vertretene Linie. Das ULD hat die Ablehnung von Informationsersuchen, die sich auf privatrechtliche Geschäftstätigkeit von Behörden bezogen, mehrfach beanstandet (24. TB, Tz. 13.1; 25. TB, Tz. 13.2; 26. TB, Tz. 12.2). Gerade privatrechtliche Geschäfte der Verwaltung sind für die Allgemeinheit von großem Interesse und Bedeutung, z. B. bei dem **Verdacht von Vetternwirtschaft und Korruption** oder im Hinblick auf die Sparsamkeit und Wirtschaftlichkeit der Haushaltsführung.

11.2 Bundesinformationsfreiheitsgesetz

Nach langer Zeit der Stagnation kam in die Verhandlungen für ein Informationsfreiheitsgesetz auf Bundesebene während des Berichtszeitraumes frischer Wind.

Im April 2004 legten Bürgerrechts- und Journalistenverbände den Entwurf eines Bundesinformationsfreiheitsgesetzes vor. Wir unterstützten den Vorschlag der fünf Organisationen (DJV, netzwerk recherche, ver.di, HU, Transparency International), der sich inhaltlich am IFG unseres Landes orientierte. Die Dringlichkeit von **mehr Transparenz in der Bundesverwaltung** zeigte sich an aktuellen Beispielen, etwa Vorgängen um die Bundesagentur für Arbeit oder den Vertrag zur Lkw-Maut.

Ein von den Bundestagsfraktionen SPD und BÜNDNIS 90/DIE GRÜNEN im Juli 2004 vorgelegter Entwurf stieß wegen seiner vielen **Ausnahmetatbestände** auf starke öffentliche Kritik. Nachdem es offensichtlich nicht möglich war, einen vollständig zwischen den Fraktionen und dem federführenden Bundesinnenministerium abgestimmten Vorschlag ins Gesetzgebungsverfahren einzubringen, hat die Regierungskoalition die Initiative ergriffen und im November 2004 einen Gesetzesvorschlag förmlich in den Bundestag eingebracht. In die Gesetzesberatungen haben wir unsere insgesamt positiven Erfahrungen aus Schleswig-Holstein einfließen lassen können. Die durch zahlreiche Ausnahmeregelungen gekennzeichnete Zurückhaltung des Bundesgesetzgebers ist nicht gerechtfertigt und droht das wichtige Anliegen einer transparenten und bürgernahen Verwaltung zu konterkarieren.


www.datenschutzzentrum.de/informationsfreiheit/stellungnahme-050304.htm

Was ist zu tun?
Das Informationsfreiheitsgesetz des Bundes sollte so gestaltet werden, dass eine weitestgehende Transparenz der Verwaltung erreicht und damit auch präventiv der Korruption entgegengewirkt wird. Auf generalklauselartige Verweigerungsgründe sollte verzichtet werden.

11.3 Novellierung des Informationsfreiheitsgesetzes in Schleswig-Holstein

Im September 2004 legte die SSW-Landtagsgruppe einen Entwurf zur Novellierung des IFG-SH vor, um Unklarheiten aus der Gesetzesanwendung zu beheben und den Anwendungsbereich des Gesetzes auszuweiten. Zugleich sollte die Europäische Umweltinformationsrichtlinie auf Landesebene umgesetzt werden.

Der vom SSW vorgelegte Entwurf integrierte die Umsetzung der Europäischen Umweltinformationsrichtlinie in das bestehende IFG-SH. Diese **Integration** wird von uns begrüßt, weil auf diese Weise ein bürokratisches Nebeneinander von

allgemeinen Informationsansprüchen und solchen aus dem Umweltrecht und damit verbundene Abgrenzungsschwierigkeiten vermieden werden können.

Der Entwurf stellte klar, dass privatrechtliches Handeln von Behörden unter den Anwendungsbereich des IFG-SH fällt (Tz. 11.1). Er bleibt aber nicht hierbei stehen: Vielmehr sollte der Anwendungsbereich des Gesetzes auf natürliche oder juristische Personen des privaten Rechts ausgedehnt werden, die öffentliche Aufgaben wahrnehmen oder öffentliche Dienstleistungen erbringen. Diese **Ausdehnung des Anwendungsbereichs** wurde von uns angesichts der zunehmenden Verlagerung von öffentlichen Aufgaben in den privaten Bereich unterstützt.

Nach dem Entwurf sollte die **Einsichtnahme** in Unterlagen vor Ort **kostenfrei** sein. Dies ist im Lande schon weit verbreitete Praxis. Dennoch gibt es immer wieder Beispiele, bei denen mit einer Kostenforderung offensichtlich der Zweck verfolgt wird, die Bürgerinnen und Bürger von einer Inanspruchnahme des IFG abzuhalten. Im Sinne einer Vereinheitlichung und der Schaffung einer für den Bürger verlässlichen Regelung ist eine solche Vorgabe durch den Gesetzgeber sinnvoll. Sie gewährleistet einen einfachen und unbürokratischen Zugang zu Informationen.

In den **Beratungen des Entwurfes** signalisierten alle Seiten eine weitgehende Zustimmung zu dem Vorschlag, aber auch Diskussionsbedarf im Detail. Das Ende der Legislaturperiode im Februar 2005 stand letztlich einer Einigung über konkrete Formulierungen entgegen. So ist es zu erklären, dass die SPD-Fraktion zwar einen dem SSW-Vorschlag weitgehend entsprechenden Änderungsantrag stellte, die SSW-Landtagsgruppe aber ihren ursprünglichen Entwurf zurückzog, sodass es zu keinem Gesetzesbeschluss mehr kam. Es bleibt abzuwarten, ob **nach der Landtagswahl** ein erneuter Anlauf unternommen wird.

Was ist zu tun?
Das geplante Umweltinformationsgesetz für Schleswig-Holstein sollte in das bestehende IFG-SH integriert werden.

12 Was es sonst noch zu berichten gibt

12.1 Stadtinspektoranwärterinnen und -anwärter hospitieren beim ULD

Eine Idee wurde zu einer festen Institution. Seit 2003 absolvieren einige Stadtinspektoranwärterinnen und -anwärter der Landeshauptstadt Kiel einen Teil ihrer Ausbildung beim ULD. In dem drei bis vier Monate dauernden Praxisblock werden die **Grundlagen des Datenschutzrechtes in der kommunalen Verwaltung** vermittelt. Die Anwärter können eigenständig datenschutzrechtliche Fragestellungen klären und für die Verwaltung Lösungsansätze erarbeiten. Die Begeisterung der Anwärter ist für uns eine Bestätigung. Es kommt wohl nicht von ungefähr, dass bislang alle Anwärter und Anwärterinnen, die beim ULD hospitierten, anschließend ein datenschutzrechtliches Thema für ihre Diplomarbeit auswählten. Natürlich steht auch anderen Verwaltungen in Schleswig-Holstein diese Möglichkeit offen.

12.2 ULD bildet aus: erster Datenschutzazubi in Schleswig-Holstein

Schon lange bildet das ULD Praktikanten und Referendare aus, betreut Diplom- und sonstige Abschlussarbeiten. Nun haben wir mit der Lehrausbildung zum Fachinformatiker Systemintegration begonnen. Diese erfolgt im Rahmen einer Umschulung und dauert zwei Jahre.

Im Berichtsjahr wurden wieder viele Rechtsreferendare und **Praktikanten aus Verwaltung und Wirtschaft** vom ULD betreut. Hiervon profitieren nicht nur die Auszubildenden, sondern auch die Dienststelle, zumal diejenigen, die sich für eine praktische Zeit im ULD bewerben, in Sachen Datenschutz hoch motiviert sind. Außerdem werden vom ULD verschiedene **Hochschulabschlussarbeiten** betreut, traditionelle Diplom- und Magisterarbeiten sowie Arbeiten für die neuen internationalen Abschlüsse Bachelor und Master. Die Themen der unterstützten Arbeiten waren in diesem Jahr z. B. Trusted Computing, datenschutzfreundliche E-Mail-Systeme, Radio Frequency Identification (RFID) und datenschutzgerechtes Logging.

Angeregt durch die Ausbildungsinitiative des Landes Schleswig-Holstein wollten wir einen datenschutzbezogenen Ausbildungsplatz im eigenen Hause realisieren. Dank Unterstützung der Industrie- und Handelskammer bei der Klärung der Ausbildungseignung von Betrieb und Personal konnten wir im August 2004 mit einer Ausbildung zum **Fachinformatiker Systemintegration** beginnen.

Einen geeigneten Auszubildenden zu finden war kein Problem, da ehemalige Praktikanten des ULD bereits Interesse bekundet hatten. Die Wahl fiel auf einen Umschüler, der bereits im Praktikum durch fundiertes Wissen positiv in Erscheinung getreten war. Dank der Umschulung ist eine Ausbildungsverkürzung auf zwei Jahre möglich. Sollten sich die bisherigen positiven Erfahrungen verfestigen, werden wir das Lehrstellenangebot dauerhaft in den Betreuungskatalog des ULD aufnehmen.

13 Rückblick

13.1 „Flächendeckende“ Prüfungen bei den Kommunen

Das von uns verfolgte Ziel, in absehbarer Zeit eine Flächendeckung der Kontrollen im kommunalen Bereich zu erreichen (26. TB, Tz. 6.7), konnte im Jahr 2004 kontinuierlich, jedoch nicht in dem eigentlich wünschenswerten Umfang weiterverfolgt werden. Aktuelle **außerplanmäßige Anforderungen**, insbesondere in den Bereichen „E-Government“ und „Internetsicherheit“, ließen immer wieder personelle Engpässe entstehen, die zulasten des „Prüfungsgeschäftes“ gingen. Gleichwohl liegt die Flächendeckung derzeit bei ca. 60 %.

Auch einigen Bürgermeistern geht dies zu langsam, wie folgendes Beispiel zeigt. Anfang des Jahres wurden wir von einem Verwaltungschef gefragt: „Haben Sie etwas gegen uns? In mehreren Gemeinden rund um uns herum haben Sie bereits geprüft. Ich möchte für unser IT-System auch gerne einen **Datenschutzcheck** bekommen.“ Wir versprachen „bevorzugte“ Behandlung. Zwischenzeitlich ist auch diese Prüfung abgeschlossen.

13.2 MESTA

MESTA – das Automationsverfahren der Staatsanwaltschaft – ist ein langjähriges Problem. Unsere vor zwei Jahren formulierten Bedenken gegen die Errichtungsanordnung wurden bis heute nicht berücksichtigt.

Der Generalstaatsanwalt meinte damals, durch die Neuregelung der Vorschriften über staatsanwaltschaftliche Dateien in der Strafprozessordnung (StPO) würde abschließend die **Erforderlichkeit eines landesweiten Verfahrensregisters** „festgeschrieben“ (25. TB, Tz. 4.3.2). Unseres Erachtens traf und trifft dies weiterhin nicht zu. Die Einrichtung steht im Ermessen der Staatsanwaltschaft. Die Prüfung der Erforderlichkeit, die uns bis heute nicht dargelegt wurde, muss in einer Errichtungsanordnung zum Ausdruck kommen. Die landesweite Abrufbarkeit von Daten anderer Personen als des Beschuldigten ist nicht vereinbar mit dem – nach wie vor insoweit gültigen – Gesetz über die staatsanwaltschaftlichen Verfahrensregister (StARegG). Der erfasste Personenkreis ist nach wie vor zu groß. Im Fall einer Klage eines Betroffenen gegen die Speicherungspraxis in MESTA sehen wir ein hohes Prozessrisiko für das Land Schleswig-Holstein.

Was ist zu tun?
Die Errichtungsanordnung muss endlich mit dem StARegG in Einklang gebracht werden.

13.3 Schweigepflichtentbindungserklärung der privaten Krankenversicherung

Im 25. und 26. Tätigkeitsbericht (Tz. 4.8.3 und Tz. 4.7.8) hatten wir über die Problematik der von privaten Krankenversicherungen genutzten Schweigepflichtentbindungserklärungen berichtet. Der Versicherte willigt bei Vertragsabschluss einmalig pauschal darin ein, dass die Versicherung bei behandelnden Ärzten Patientendaten abfragt. Auch in diesem Jahr konnte keine Einigung zwischen der Versicherungswirtschaft und den obersten Aufsichtsbehörden erzielt werden. Die Versicherungswirtschaft hält weiterhin an der **datenschutzwidrigen** – ihrer Auffassung nach zulässigen – **Verfahrensweise** fest. Die Einholung von Schweigepflichtentbindungserklärungen im Einzelfall würde zu erheblichen Verzögerungen der Bearbeitung führen und beträchtliche Kosten verursachen. Es wurde lediglich die Bereitschaft erklärt, die Versicherungsnehmer regelmäßig an die bei Vertragsabschluss abgegebene Erklärung zu erinnern.

Vertreter der Versicherungswirtschaft stellten das „**Widerspruchsmodell**“ zur Diskussion. Danach würde der Versicherungsnehmer im Falle einer Anfrage beim Arzt zeitgleich hierüber informiert und hätte innerhalb einer gewissen Frist die Möglichkeit, Widerspruch einzulegen. Erst nach Fristablauf dürfe der Arzt Fragen beantworten, falls kein Widerspruch eingelegt wurde. Die Bundesärztekammer hatte dieses Verfahren bereits als „Konstruktion der Genehmigungsfiktion“ abgelehnt. Aufgrund der kontroversen Ansichten ist eine Einigung nicht absehbar. Die obersten Datenschutzaufsichtsbehörden werden beharrlich auf eine datenschutzkonforme Lösung drängen.

13.4 Das ULD in der Öffentlichkeit

Wer wie wir in Schleswig-Holstein für einen modernen Datenschutz eintritt, der mit den Elementen Beratung und Konzeptentwicklung, Technikgestaltung und Datenschutzmanagement sowie mit der Vergabe eines Datenschutz-Gütesiegels für eine positive Wettbewerbsorientierung steht, ist auch in der Öffentlichkeit gefordert. Höhepunkt des Datenschutzjahres war die **Sommerakademie** zum Thema Identitätsmanagement – zugleich der letzte Arbeitstag des ehemaligen Landesbeauftragten für den Datenschutz Dr. Helmut Bäumler. Die Sommerakademie 2005 wird der datenschutzkonformen Gestaltung des E-Government gewidmet sein.

Unsere Kompetenz ist bei **Anhörungen** im Bundestag und Landtagen gefragt. Zahlreiche Vortragseinladungen zu Themen des Datenschutzes ermöglichen unseren Mitarbeiterinnen und Mitarbeitern die Teilnahme auf internationalen und nationalen **Konferenzen** und tragen gleichzeitig zu unserer Fortbildung bei. Unsere Konzepte zum Datenschutz haben wir auf **Messen** wie der CeBIT 2004 in Hannover, aber vor allem auch auf zahlreichen regionalen Veranstaltungen wie den Flensburger Gesundheitstagen, der KielBit oder den Mediatagen Nord vertreten. Mit einem Ausstellungsstand haben wir uns an dem „Schleswig-Holstein-Tag“ in Flensburg sowie dem „Tag der offenen Tür“ des Landtags in Kiel präsentiert.

Die Verfügbarkeit für die **Medienöffentlichkeit** aus Presse, Funk und Fernsehen, insbesondere für Hintergrundinformationen, ist ein wichtiger Bestandteil unserer Arbeit. Zahlreiche **Schriften** und Handreichungen wie die „backUP-Magazine“ zum Systemdatenschutz, die Hinweise zum Landesmelderecht oder das Kooperationsprodukt mit der Verbraucherzentrale Bundesverband e.V. „99+1 Beispiele und viele Tipps zum Bundesdatenschutzgesetz“ sichern die Nachhaltigkeit unserer Arbeit. Mitarbeiterinnen und Mitarbeiter sind zudem als **Autoren und Herausgeber** von Fachpublikationen über ihre eigentliche Arbeit hinaus im Thema Datenschutz engagiert.

Qualität in der Breite bemühen wir uns durch ein **Schulungskonzept** zum Datenschutz zu erreichen. Tragende Säule sind die Kurse zur Fort- und Weiterbildung der **DATENSCHUTZAKADEMIE Schleswig-Holstein** (Tz. 14). Mit der Fortbildung von Systemadministratoren im Lande machen wir gute Erfahrungen. Im Rahmen unserer Ressourcen bemühen wir uns um Kooperationspartner wie die Fachhochschule Kiel oder den MediaCampus, um den Datenschutz mit seiner Gestaltungskomponente in die **technischen Studiengänge** zu integrieren.

Was ist zu tun?
Mit einem gezielten, aber auch vielfältigen Angebot bemühen wir uns, die für den System- und Selbstdatenschutz erforderlichen Informationen zu vermitteln.

13.5 Knoppix-CD mit installiertem JAP

Auf Initiative und in Zusammenarbeit mit der EDV-Abteilung des Landtages wurde eine Linux-CD zusammengestellt, die u. a. während des „Tages der offenen Tür“ des Schleswig-Holsteinischen Landtages kostenlos verteilt wurde. Die CD enthält ein lauffähiges Linux-Betriebssystem und ist gleichzeitig mit dem **Anonymisierungstool JAP** ausgestattet. Beim Start des Rechners muss sie nur in das CD-Laufwerk eingelegt werden und startet von dort automatisch. Der Anwender kann dann im Internet surfen, ohne dass sein PC angreifbar wäre. Durch die Verwendung von JAP bewegt sich der Internetserver zudem auch völlig anonym im Internet. Darüber hinaus enthält die CD eine Fülle von Informationen über die Arbeit des Landtages und des ULD. Sie kann weiterhin beim ULD kostenfrei angefordert werden.

14 DATENSCHUTZAKADEMIE Schleswig-Holstein

- **Konsolidierung und Kontinuität – Schwerpunkte der Akademiearbeit**

Nach einem personellen **Wechsel in der Geschäftsführung** wird die inhaltliche Arbeit der DATENSCHUTZAKADEMIE Schleswig-Holstein in bewährter Weise fortgeführt als Kooperationsprojekt des ULD mit der Nordsee Akademie Leck sowie der Verwaltungsakademie Bordesholm. Die enge Zusammenarbeit mit dem Institut für Qualitätssicherung an Schulen Schleswig-Holsteins (IQSH) sichert die Verbreitung datenschutzrelevanter Inhalte an unseren Schulen.

Zur Stärkung der Außenpräsentation schloss sich die DSA dem „**Kieler Forum Weiterbildung**“ an, einem Verbund verschiedener Bildungsträger in der Region Kiel. Gemeinsam mit 35 Partnern nutzt die DATENSCHUTZAKADEMIE Schleswig-Holstein das Forum, um ihr Kurs- und Seminarangebot den Bürgerinnen und Bürgern nahe zu bringen. Die DATENSCHUTZAKADEMIE Schleswig-Holstein vermittelt auch im 11. Jahr ihres Bestehens mit ihrem preisgünstigen und qualitativ hochrangigen Fortbildungsprogramm Strategien eines erfolgreichen Datenschutzes für Bürgerinnen und Bürger, Verwaltung und Wirtschaft des Landes – und zunehmend auch anderer Bundesländer.

Fragen von Datenschutz und Datensicherheit rücken immer mehr von den Rändern ins Zentrum von behördlichen und betrieblichen Entscheidungsprozessen. Erfolgreiches betriebliches **Datenschutzmanagement** ist ein Wettbewerbsvorteil und notwendiger denn je. Die Erlangung und Vertiefung von Fachwissen bei den Datenschutzbeauftragten vor Ort ist vom Gesetzgeber vorgeschrieben. Angemessene Vermittlung von Medienkompetenz ist eine Grundvoraussetzung für selbstbestimmtes Handeln in der Informationsgesellschaft. Für besonders sensible Patienten- und Sozialdaten ist ein besonders qualifizierter Umgang vonnöten.

Die **Nutzung von Internet und Informationstechnik** wächst in allen gesellschaftlichen Bereichen. Die mit der Verarbeitung von Personendaten beschäftigten Menschen benötigen grundlegende Kenntnisse in den relevanten Technologien. Ein qualifizierter Systemadministrator zeichnet sich auch und vor allem durch seine Kompetenz im Bereich Datenschutz aus. Ein breites Spektrum dieser und weiterer Fragen wird in unseren Veranstaltungen behandelt. Dabei wird den Teilnehmerinnen und Teilnehmern ein geeignetes Instrumentarium zur Lösung von Praxisproblemen zur Verfügung gestellt.

- **Jahresprogramm 2005 der DATENSCHUTZAKADEMIE**

Veranstaltungsübersicht 2005 für die Kurse der DATENSCHUTZAKADEMIE Schleswig-Holstein			
März:	Windows 2003 Sicherheit I	WIN-I 9	01. - 04.03.2005
	Grundkurs Bundesdatenschutzgesetz	BDSG-I 6	07.03.2005
	Betriebliches Datenschutzmanagement nach dem BDSG	BDSG-II 5	08.03.2005
	Technischer Datenschutz/ Systemdatenschutz nach dem BDSG	SIB 8	09.03.2005
	IT-Revision	ITR 7	10.03.2005
	Safer Surfen im Internet	SURF 5	15.03.2005
	Workshop für betriebliche Datenschutzbeauftragte	DWBT 4	16.03.2005
April:	Datenschutzrecht für behördliche Datenschutzbeauftragte	DR 9	04. - 05.04.2005
	Datenschutz im Krankenhaus	DK 4	05.04.2005
	Datensicherheitsrecht, Prüfung und Bewertung von Sicherheitsmaßnahmen durch behördliche Datenschutzbeauftragte	DT 9	06. - 08.04.2005
Mai:	Einführung Datenschutz im Schulsekretariat	ES 17	09.05.2005
	Schutz von Personaldaten	P 13	18. –19.05.2005
	Datenschutz in der Schule	L 34	25.05.2005
Juni:	Einführung in datenschutzgerechtes Linux	LIN-I 2	07.06.2005
	Windows 2003 Sicherheit II	WIN-II 1	07. - 10.06.2005
	Informationsfreiheitsgesetz Schleswig-Holstein	IFG 11	14.06.2005
September:	Datenschutzgerechte Firewalls unter Linux	LIN-FW 2	06.09.2005
	Windows 2003 Sicherheit I	WIN-I 10	13. - 16.09.2005
	Datenschutzrecht für behördliche Datenschutzbeauftragte	DR 10	26. - 27.09.2005
	Datensicherheitsrecht, Prüfung und Bewertung von Sicherheitsmaßnahmen durch behördliche Datenschutzbeauftragte	DT 10	28. - 30.09.2005
Oktober:	Grundkurs Bundesdatenschutzgesetz	BDSG-I 7	17.10.2005
	Betriebliches Datenschutzmanagement nach dem BDSG	BDSG-II 6	18.10.2005
	Technischer Datenschutz/ Systemdatenschutz nach dem BDSG	SIB 9	19.10.2005
	Führung von Personalakten	PA 13	24. - 25.10.2005
	Sozialdatenschutzrecht	S 11	24. - 26.10.2005
	Datenschutz bei der Internetnutzung	NET 8	25. - 26.10.2005
	IT-Revision	ITR 8	26.10.2005
	Technik und Recht von Firewalls	FW 11	27.10.2005

November:	Windows 2003 Sicherheit II	WIN-II 2	15. - 18.11.2005
	Datenschutz bei der Internetnutzung durch Schulen	L-INT 2	23.11.2005
	Prüfung zum Systemadministrator mit Datenschutzzertifikat	SDZ 3	29.11.2005

Sommerakademie 2005 * Sommerakademie 2005 * Sommerakademie 2005

Dienst per Mausklick

Datenschutzgerechtes E-Government

„Electronic Government“ soll der Verwaltung das Verwalten leichter machen: Die Daten sollen laufen, nicht die Menschen in und außerhalb der Verwaltung – so die Metapher.

Wohin sollen die Daten in den modernen vernetzten Systemen laufen, in welchen Bahnen, zu welchen Anwendungszwecken? Mit welchen Sicherungen der Technik werden sie gegen fremde Zugriffe geschützt? Ist die Datensicherheit schon eine Herausforderung für die Verwaltung der Zukunft? Wie stellen wir den Datenschutz sicher, damit die Menschen ausreichendes Vertrauen in das Online-Angebot ihrer Verwaltung entwickeln können? Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) sucht mit Ihnen als Gesprächspartner auf der Sommerakademie nach praxisorientierten innovativen rechtlichen und technischen Antworten.

29. August 2005
Kieler Schloss

Weitere Informationen zur Sommerakademie werden veröffentlicht auf unserer Homepage unter

www.datenschutzzentrum.de

Die Teilnahme ist kostenfrei. Wenn Sie eine Einladung zu dieser Veranstaltung wünschen und noch nicht in unserem Versandverteiler geführt werden, lassen Sie sich gerne vormerken unter

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstraße 98, 24103 Kiel
Tel.: 0431/988-1200
Fax: 0431/988-1223
E-Mail: akademie@datenschutzzentrum.de

- **Schulungsbetrieb 2004**

Im Jahr 2004 fanden 32 **Kurse**, Seminare und Workshops statt, in denen 457 Personen Grundlagen- und Spezialwissen zu Datenschutzfragen erlangen konnten. In insgesamt 15 Sonderkursen vermittelten die ULD-Referentinnen und Referenten landesweit 305 Interessierten ihr Fachwissen zu Themen wie neues Melderecht, Schutz von Personaldaten, Datenschutz in Landes- und Justizverwaltung sowie Rechte und Pflichten der Personalvertretung.

Die **Kursunterlagen**, die in gebundener Form mit kompaktem, didaktisch aufbereitetem Wissen aufwarten, sind modular aufgebaut. Insgesamt können in der DATENSCHUTZAKADEMIE Schleswig-Holstein 205 Datenschutzthemen für die Anforderungen der verschiedenen Kurse zusammengestellt werden. Die Module werden unmittelbar vor den Kursen von den Referenten aktualisiert.

- **Haben Sie Interesse?**

Auf Wunsch werden spezielle Themenbereiche von der DATENSCHUTZAKADEMIE Schleswig-Holstein als Inhouse-Veranstaltungen in Ihrer Behörde oder Ihrem Betrieb durchgeführt. Organisatorische Abwicklung und inhaltliche Schwerpunkte können abgesprochen werden. Voraussetzung ist die Teilnahme von mindestens 15 Personen.

Nähere Informationen dazu unter

E-Mail: akademie@datenschutzzentrum.de
oder Tel.: 0431/988-1281

- **Datenschutzzertifikate für Systemadministratoren**

Unser schon seit langem verfolgtes Bestreben, im sicherheitstechnischen Bereich neben einer profunden Theorievermittlung zunehmend das Praxistraining zu fördern, zeigte auch in diesem Jahr erfreuliche Resultate. In der Nordsee Akademie Leck und in der ULD-Dienststelle in Kiel wurde für die technischen Kurse die unterschiedlich konfigurierte Ausstattung der jeweiligen IT-Labors eingesetzt. Der Überprüfung des erworbenen Fachwissens können sich die Absolventen durch die Prüfung zum **Systemadministrator mit Datenschutzzertifikat** unterziehen.

Die Erlangung des Zertifikats schließt Kenntnisse in folgenden Bereichen ein:

- 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, NFTS- 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 Internetdienste E-Mail und WWW, mögliche Sicherheitsmaßnahmen und Schwachstellen.

Das anspruchsvolle Niveau der eintägigen **theoretischen und praktischen Prüfung** garantiert den Behörden sorgfältig ausgebildete Mitarbeiter. Die Absolventen selbst erhöhen durch eine gefragte Zusatzqualifikation nicht unerheblich ihren Marktwert. Aufgrund der steigenden Nachfrage erwägt die DATENSCHUTZAKADEMIE Schleswig-Holstein, im kommenden Jahr zwei oder gar drei Prüfungstage anzubieten.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z