SCHLESWIG-HOLSTEINISCHER LANDTAG **Drucksache 16/550**
16. Wahlperiode 21.03.2006

Bericht

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

Tätigkeitsbericht 2006

Tätigkeitsbericht 2006

des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

Berichtszeitraum: 2005, Redaktionsschluss: 15.02.2006
Landtagsdrucksache 16/550

(28. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz)

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

Impressum

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Holstenstraße 98
24103 Kiel

Mail: mail@datenschutzzentrum.de
Web: www.datenschutzzentrum.de

Satz und Lektorat: Gunna Westphal, Kiel
Illustrationen: Reinhard Alff, Dortmund
Umschlaggestaltung: Martin Papp, Eyekey Design, Kiel
Druck: hansadruck, Kiel

Inhaltsverzeichnis

1 Datenschutz in Schleswig-Holstein

1.1 Welchen Datenschutz können wir uns noch leisten?

Diese Frage stellen sich viele Menschen in der heutigen Zeit, die geprägt ist von Haushaltsdefiziten, wirtschaftlicher Globalisierung, internationalen Terroranschlägen und einer atemberaubenden Technikentwicklung. Die Diskussion über Kosten und Nutzen des Datenschutzes findet auch in Schleswig-Holstein statt.

Die Arbeit des ULD wird in Schleswig-Holstein von vielen mit **Wohlwollen** verfolgt: Jeder hat eine Privatsphäre, die er geschützt wissen will. Zugleich ist aber die Vorstellung sehr weit verbreitet, eigentlich habe man auch nichts zu verbergen. Angesichts terroristischer Anschläge und spektakulärer Kriminalität, großkalibriger Steuerverkürzung und des Missbrauchs staatlicher Leistungen betrachten viele den Datenschutz eher als Luxus, den sie sich wegen knapper Ressourcen und wegen Wichtigerem nicht mehr wie bisher leisten können.

Diese **reservierte Haltung** gegenüber dem Datenschutz wird verstärkt durch die Kritik, die Datenschützer immer wieder üben müssen bei der Erneuerung der IT-Infrastruktur in der öffentlichen Verwaltung oder bei der Durchsetzung neuer Eingriffsbefugnisse für staatliche Einrichtungen – vom Sozialamt bis zur Polizei. Hinzu kommt die Erfahrung mit scheinbar übermäßigen bürokratischen Anforderungen: Pflichten zur Meldung von Verfahren, zur Vorabkontrolle, zur Dokumentation von Verarbeitungs- und Sicherheitskonzepten, zur Erprobung und Freigabe, zur Protokollierung von Prozessen und zur Protokollkontrolle – all dies versperrt bei vielen Betreibern, Anwendern und sonstigen Verantwortlichen leicht den Blick darauf, dass es beim Datenschutz vor allem um eines geht: um Grundrechtsschutz.

Die Frage nach Sinn und Unsinn bzw. Art und Umfang des Datenschutzes stellt sich heute zudem anders als noch ein Jahr zuvor: Sowohl in Schleswig-Holstein als auch auf Bundesebene wurde bisher mit knappen Regierungsmehrheiten regiert. Diese politisch unsichere Lage mag ein Grund gewesen sein, dem Datenschutz besonders aufgeschlossen gegenüberzutreten und Interesse daran zu zeigen, dass die unabhängigen Datenschutzkontrollinstanzen die Politik mit einer freundlichen Grundeinstellung begleiten. Nun regieren im Bund sowie in unserem Land große Koalitionen, die angesichts **satter Mehrheiten** zumindest rechnerisch keine Rücksichten mehr nehmen müssen auf solche speziellen gesellschaftlichen Anliegen.

Eigentlich ist die Frage, ob wir uns Datenschutz noch leisten können, mit einem Blick ins Grundgesetz einfach zu beantworten: Es stellt sich nicht die Frage, ob wir können – wir müssen. Mit erfrischender Klarheit machte gerade in jüngster Vergangenheit das Bundesverfassungsgericht immer wieder deutlich, dass alle scheinbaren faktischen Zwänge kein Anlass dafür sein dürfen, das Grundrecht auf informationelle Selbstbestimmung zu opfern. Als Maßstab für den Zustand einer Demokratie wird immer wieder – zu Recht – der Umgang einer Gesellschaft mit seinen Minderheiten herangezogen. Diese Messmethode lässt sich auf den Daten-

schutz übertragen: **Maßstab für die Freiheitlichkeit** unserer Informationsgesellschaft ist deren Umgang mit dem Datenschutz.

Beim Datenschutz – ebenso wie beim Minderheitenschutz – geht es nicht vorrangig um die Wahrung von Partikularinteressen. Es geht ums Gemeinwohl, d. h. auch um die **Interessen der Mehrheiten** und damit derer, die weitgehend ohne gefühlte persönlichkeitsrechtliche Konflikte mitten in unserer Gesellschaft stehen. Jeder Mensch schwebt in der Gefahr, aus der Mitte der Gesellschaft an den Rand gedrängt zu werden. Durch die tatsächlich erfolgende tausendfache Erfassung von allen Menschen besteht ein latentes weiter zunehmendes Risiko für alle Bürgerinnen und Bürger für deren Persönlichkeitsrechte, z. B. durch fehlerhafte oder zweckwidrige Verarbeitung ihrer Daten. Datenschutz ist nicht nur Bestandteil unserer Rechtsordnung, sondern auch unserer Kultur, die das Leben angenehm und lebenswert macht.

1.2 Die Gewinnrechnung des Datenschutzes

Das ULD baut nicht allein auf die verfassungsrechtliche Unersetzlichkeit des Datenschutzes. Unser Ziel ist es vielmehr darauf hinzuwirken, dass sich Datenschutz auch greifbar lohnt – als kultureller, wirtschaftlicher und finanzieller Gewinn.

Das Land Schleswig-Holstein soll von der Arbeit des ULD äußerlich sichtbar profitieren. Dies bedeutet für uns, dass wir uns nicht auf das einfache Kontrollieren beschränken, also auf das nachträgliche Überprüfen, ob von öffentlichen und privaten Stellen die Datenschutzvorschriften beachtet wurden. Wir verfolgen vielmehr zusätzlich einen **präventiven Ansatz**, der Aufsicht nicht als Konfrontation, sondern als eine kommunikative Aufgabe versteht, und der Anreize zur Befolgung der Regeln gibt. Die Beachtung des Datenschutzes soll – in vieler Hinsicht – sich lohnen und belohnt werden.

Dieser Ansatz ist beileibe nichts revolutionär Neues. Schon das erste Datenschutzgesetz des Landes aus dem Jahr 1978 erklärt die Beratung der Daten verarbeitenden Stellen zur Kernaufgabe. Dies ändert nichts daran, dass das ULD als Datenschutzaufsicht prüfen muss und dies auch tut. Dies gilt sowohl für die zeitnahe Bearbeitung von Hinweisen und Beschwerden als auch für Stichproben- und Querschnittsprüfungen. Selbst wenn in einem konkreten Zusammenhang eine **Beratung** erfolgt, kann auf **Prüfungen** nicht völlig verzichtet werden. Dennoch hält sich das ULD mit Prüfungen zurück, wenn Beratungskontakte bestehen. Hierdurch lassen sich Irritationen über die Rolle des ULD vermeiden. Kontrollen mit Mängelfeststellungen können wiederum der Beginn einer konstruktiven Beratung sein.

Neben dem klassischen Beratungsgeschäft hat das ULD seit dem Jahr 2000 auf gesetzlicher Basis sein **präventives Instrumentarium** ausgebaut. Hierbei handelt es sich nicht um teuren „Luxus“, sondern um den Versuch, das Grundanliegen des Schutzes informationeller Selbstbestimmung intelligent, d. h. umfassender, billiger und wirksamer zu verwirklichen als allein mit Kontrollen und Beratung.

Während Prüfungen und Beratungen vom ULD bisher weitgehend unentgeltlich erfolgen, werden für die **Auditierung** von Verfahren und die Verleihung von **Datenschutz-Gütesiegeln** für IT-Produkte Gebühren erhoben. Hierdurch wird nicht nur der Landeshaushalt entlastet, alle Beteiligten haben hiervon einen Nutzen: Die für die Verarbeitung Verantwortlichen können sich darauf verlassen, dass ihr Produkt oder ihr Verfahren geprüft und für gut befunden wurde. Dies erhöht die Rechtssicherheit. Zugleich ist dies ein wichtiges Argument im Wettbewerb, mit dem Vertrauen von Partnern sowie von Bürgerinnen und Bürgern gewonnen werden kann. Letztere gewinnen an informationeller Selbstbestimmung. Und selbst für die professionellen Datenschützer in Behörden und Betrieben wird das Geschäft erleichtert durch Standardisierung, qualifizierte Dokumentation und Einbeziehung fremden Sachverstands. Dass wir hier in Schleswig-Holstein als Pionier auf dem richtigen Weg sind, zeigt die nationale und internationale Resonanz: Die Datenschutzbeauftragten des Bundes und der Länder erwarten vom Bundesgesetzgeber endlich den Erlass des per Gesetz seit 2001 angekündigten Bundesdatenschutzauditgesetzes. Dieser Forderung schließen sich zunehmend Unternehmen, insbesondere aus der IT-Branche, an. Die französische Datenschutzaufsichtsbehörde zeigt sich interessiert, unsere Verfahren auf die dortige Situation zu übertragen (Tz. 9.2.6). Selbst Vertreter weltweit agierender IT-Konzerne kommen nach Kiel, um von unseren Auditerfahrungen zu profitieren.

Die DATENSCHUTZAKADEMIE Schleswig-Holstein ist eine – vom ULD gemeinsam mit dem Deutschen Grenzverein schon im zwölften Jahr erfolgreich tätige – sich finanziell weitgehend selbst tragende **Bildungseinrichtung** im Bereich Datenschutz. Zwischen Prüfung, Beratung und Schulung bestehen enge Wechselwirkungen: Bei Schulungsmaßnahmen kann anstelle einer Einzelberatung sofort eine Vielzahl von Personen erreicht werden. Es wird Verständnis für den Datenschutz vermittelt, was die Grundlage für die Beachtung rechtlicher Vorgaben ist. Zugleich wird durch den Gedanken- und Informationsaustausch bei den Schulungen bewirkt, dass die Kursteilnehmer sich gegenseitig motivieren und dass die Unterrichtenden Rückmeldungen aus der behördlichen oder betrieblichen Praxis erhalten. Beides ist von unschätzbarem Wert, sowohl für die Einzelberatung als auch für die Prüftätigkeit. Ein positiver Nebeneffekt der DATENSCHUTZAKADEMIE und der Kooperation mit dem Deutschen Grenzverein e.V. liegt darin, dass auch Menschen außerhalb Schleswig-Holsteins in unser schönes Land „gelockt“ werden, um sich weiterzubilden. Für den Standort Leck erfolgt derart – in zugegeben kleinem Umfang – eine regionale Wirtschaftsförderung (Tz. 13).

Eine völlig kostenneutrale Bildungsarbeit besteht in **Kooperationen** des ULD mit weiteren Bildungsträgern in Schleswig-Holstein, u. a. mit der Universität Kiel, dem dortigen Multimedia Campus oder der Fachhochschule Kiel. Die von Mitarbeitern des ULD angebotenen Lehrveranstaltungen werden freiwillig als Nebentätigkeit ausgeübt; hierin liegt eine Zusatzleistung der Mitarbeiter, von der die Bildungseinrichtungen sowie das ULD und nicht zuletzt die Studierenden profitieren.

Die **Öffentlichkeitsarbeit** hat für die Außenwirkung des ULD eine immense Bedeutung. Der personelle und finanzielle Aufwand hierfür ist dagegen eher gering. Im Ergebnis handelt es sich um nichts anderes als die mediale Aufbereitung ohnehin erarbeiteter Arbeitsergebnisse. Voraussetzung der Beachtung des Grundrechtes auf informationelle Selbstbestimmung ist, dass die Mitarbeiterinnen und Mitarbeiter der öffentlichen und der privaten Stellen die Datenschutzregelungen kennen und verstehen lernen, um diese in der betrieblichen bzw. behördlichen Praxis umsetzen zu können. Über die elektronischen und gedruckten Veröffentlichungen des ULD werden Sensibilität und Know-how für einen effektiven Grundrechtsschutz vermittelt. Durch Verweis hierauf kann der Beratungsaufwand reduziert und optimiert werden. Unser Informationsangebot findet großen Zuspruch und zeigt durchgängig positive Wirkungen – nicht nur, aber vor allem in Schleswig-Holstein.

Die Veröffentlichungen des ULD sollen auch die **Bürgerinnen und Bürger** ansprechen. Im Interesse eines effektiven Ressourceneinsatzes zur Wahrung der rechtlich geschützten Interessen der Betroffenen kann hierdurch für diese mehr Transparenz bei der Verarbeitung ihrer Daten geschaffen werden. Es werden Hilfen zur Selbsthilfe geboten. Überall dort, wo sich die Betroffenen selbst helfen können, ist nicht mehr die Unterstützung des Staates durch Beschwerdebearbeitung oder Beratung erforderlich. Das ULD versteht Öffentlichkeitsarbeit als Werbung für den Datenschutz und für das Land Schleswig-Holstein. Insbesondere der Webauftritt soll den Anspruch auf Transparenz einlösen, mit dem das ULD – nicht zuletzt auch als Informationsfreiheitsbehörde – konfrontiert ist.

Das ULD beteiligt sich an vielen **Forschungs- und Diskursprojekten** im Bereich Datenschutz und an der Entwicklung von Innovationen. Es erstellt im Auftrag von Ministerien wissenschaftliche Gutachten. Diese Projekte stellen für das Land keine finanzielle Belastung dar, weil sie weitgehend kostendeckend über Drittmittel finanziert werden. Durch Synergieeffekte besteht sogar die Möglichkeit der Nutzung der Projektressourcen für die Wahrnehmung der Kernaufgaben des ULD. Zugleich werden – leider immer nur befristet – hoch qualifizierte Arbeitsplätze geschaffen. Eine Zielsetzung der Projekte liegt in der Förderung moderner Technologien. Schleswig-Holstein macht in den Bereichen der Informations- und der Biotechnik große Anstrengungen, um angesichts des globalen Wettbewerbs auch in Zukunft wirtschaftlich erfolgreich zu sein. Gerade in diesen **Schlüsseltechnologien** ist die Implementierung von Datenschutz eine zentrale Rahmenbedingung auf dem Markt. In Marktsegmenten, bei denen es um die menschengerechte Einbettung von Hightech in eine größere gesellschaftliche Infrastruktur geht, hat Deutschland gegenüber vielen anderen Staaten einen Standortvorteil. Zu diesen Segmenten gehört der Datenschutz. Durch Private-Public-Partnerships – vorzugsweise mit Unternehmen des Landes – versucht das ULD, die eigene Kompetenz auch für die Wirtschaft des Landes nutzbar zu machen. Für den Wissenstransfer steht als besondere Abteilung des ULD dessen Innovationszentrum zur Verfügung (ULD-i).

Was ist zu tun?
Die Tätigkeit des ULD steht nicht nur auf einem datenschutzrechtlichen Prüfstand. Da das ULD öffentliche Mittel in Anspruch nimmt, gibt es auch Rechenschaft darüber ab, wie diese Mittel eingesetzt und welche Effekte hierdurch erreicht werden.

1.3 Die Gesetzgebung

Das Datenschutz- und Informationsfreiheitsrecht von Schleswig-Holstein ist durch Kürze, Klarheit und Grundrechtsfreundlichkeit geprägt. Dieser Weg sollte nicht verlassen werden.

Im Berichtszeitraum wurden von der Landesregierung **Gesetzesvorschläge** gemacht, mit denen das Polizeirecht und die Informationsfreiheit neu geregelt werden sollen. So unterschiedlich die Regelungsmaterien sind, so Besorgnis erregend sind einige Gemeinsamkeiten.

Bisher zeichnet sich das **Landesverwaltungsgesetz**, das die Rechte und Pflichten der Polizei des Landes regelt, dadurch aus, dass es in einer für Bürger wie Polizisten verständlichen Sprache klar definierte Eingriffsbefugnisse festlegt, die sich an der Aufgabe, Gefahren abzuwehren, orientieren. Damit soll jetzt Schluss sein: Ein von der Landesregierung vorgelegter Entwurf ist in vieler Hinsicht zu weitgehend. Er öffnet die Tür für Grundrechtseingriffe, die aus fachlicher Sicht nicht notwendig sind. Er überschreitet zudem sprachlich und systematisch bisherige Grenzen: Durch neue unbestimmte Rechtsbegriffe, wortreiche Umschreibungen und Verweisungen verliert der Gesetzestext an Praktikabilität. Damit ist niemandem gedient (Tz. 4.2.1).

Die gleiche Problematik eröffnet sich nun mit der Überarbeitung des **Informationsfreiheitsgesetzes** (IFG). Dieses hat sich in den sechs Jahren seiner Geltung bewährt. Nachdem nun die Notwendigkeit entstanden ist, auf Landesebene das Umweltinformationsrecht zu regeln, hätte es nahe gelegen, die positiven Erfahrungen mit dem IFG hierauf zu erweitern und ein einheitliches schlankes Gesetz zu schaffen. Das federführende Innenministerium will den umgekehrten Weg gehen: Zwar hat es den Einblick in Umweltinformationen und in allgemeine Verwaltungsinformationen in einen Gesetzentwurf mit einer Überschrift aufgenommen, doch nutzte es nicht die Chance, beide Regelungsbereiche inhaltlich zusammenzuführen. Nicht nur, dass dadurch zwei Gesetze einfach zusammengepackt und dadurch unübersichtlich werden – die Gelegenheit der Gesetzesnovellierung wurde genutzt, um die informationsfreundlichen Regelungen des allgemeinen IFG zurückzuschrauben und den Zugang zu Verwaltungsinformationen mit zusätzlichen bürokratischen Hürden zu versehen. Vorstellungen des Innenministeriums, die sich weder bei dem Erlass des ersten IFG noch über Gerichtsurteile verwirklichen ließen, sollen nun – sozusagen durch die Hintertür – verbindlich vorgegeben werden (Tz. 12.1).

Was ist zu tun?
Bei der Gesetzgebung im Bereich des Informationsrechtes sollten die schleswig-holsteinischen Tugenden nicht aufgegeben werden: Kürze, Klarheit und Grundrechtsfreundlichkeit.

2 Datenschutz in Deutschland

Im Jahr 2005 wechselte der **Vorsitz der Konferenz der Datenschutzbeauftragten** des Bundes und der Länder turnusgemäß vom Saarland nach Schleswig-Holstein. Es fanden zwei Konferenzen statt, am 10. und 11. März 2005 im Landtag in Kiel sowie am 27. und 28. Oktober 2005 im Hoghehus der Industrie- und Handelskammer zu Lübeck. Auf den Konferenzen wurde eine Vielzahl von Entschließungen getroffen, die im Internet dokumentiert sind unter

www.datenschutzzentrum.de/material/themen/presse/20050311-dsbk.htm
www.datenschutzzentrum.de/material/themen/presse/20051028-dsbk.htm

Im Berichtsjahr gab der Hamburgische Datenschutzbeauftragte seinen bisherigen **Vorsitz des Arbeitskreises Sicherheit** der Datenschutzkonferenz auf. Das ULD erklärte sich bereit, diesen zu übernehmen. Dem Arbeitskreis obliegt der bundesweite Erfahrungsaustausch zwischen den Datenschutzbeauftragten in Bezug auf den Datenschutz bei Polizei und Geheimdiensten, der Dialog mit den Behörden sowie die Erarbeitung gemeinsamer Positionen und Strategien. Die aktuelle Entwicklung im Polizeirecht, die bevorstehende Fußballweltmeisterschaft und die hierbei vorgesehenen informationellen Sicherheitsmaßnahmen unterstreichen die Notwendigkeit eines Austausches in diesem Bereich (Tz. 4.2.9).

2.1 Nichts geht mehr

Nicht nur in Schleswig-Holstein, auch auf Bundesebene wird der Regierungswechsel eine Veränderung der Datenschutzpolitik mit sich bringen. Die Art der Veränderung ist noch nicht absehbar.

Die vorgezogene Bundestagswahl hatte zur Folge, dass eine Vielzahl von informationsrechtlichen Projekten der rotgrünen Regierungskoalition nicht mehr umgesetzt werden konnte. Zwar wurde – sprichwörtlich in letzter Minute – das Informationsfreiheitsgesetz des Bundes unter Dach und Fach gebracht. Andere **Gesetzesprojekte** blieben aber auf der Strecke: Ein Genomanalysegesetz war schon weit gediehen. Dagegen hatten die Bundesregierung und auch die Regierungsfraktionen offensichtlich schon früher ihren Plan aufgegeben, nach der Novellierung des Bundesdatenschutzgesetzes im Jahr 2001 in einer zweiten Stufe eine umfassende Modernisierung des allgemeinen Datenschutzrechtes anzugehen. Selbst die Pläne für ein Bundesdatenschutzauditgesetz wurden vom federführenden Bundesinnenministerium nicht mehr ernsthaft verfolgt. Die seit über zehn Jahren mit teilweise größerem und dann wieder abnehmendem Engagement verfolgten Pläne der Erarbeitung eines Arbeitnehmerdatenschutzgesetzes waren schon länger ganz weit hinten in den Schubladen der zuständigen Ministerien verschwunden.

Um den im Bereich des Datenschutzes bestehenden **Reformstau abzubauen**, hat sich die Konferenz der Datenschutzbeauftragten auf Vorschlag des ULD auf eine Entschließung geeinigt, in der die Erwartungen für die neue Legislaturperiode dargestellt werden.

www.datenschutzzentrum.de/material/themen/presse/20051028-dsbk-informationsgesellschaft.htm

Leider greift die **Koalitionsvereinbarung** diese Vorschläge der Datenschutzbeauftragten nicht auf. Vielmehr fällt diese in überwunden gedachte Schwarz-Weiß-Muster zurück. Die Koalitionspartner wollen prüfen, „inwieweit rechtliche Regelungen etwa des Datenschutzes einer effektiven Bekämpfung des Terrorismus und der Kriminalität entgegenstehen". Bezüglich der Überarbeitung und Fortentwicklung des allgemeinen Datenschutzrechtes wird als Zielrichtung ausschließlich der „Abbau überflüssiger Bürokratie" thematisiert.

Was dabei als Bürokratieabbau verstanden wird, lässt sich aus einer ersten Initiative ableiten, deren Ziel es ist, die Zahl der Mitarbeitenden zu erhöhen, ab der ein **betrieblicher Datenschutzbeauftragter** bestellt werden muss. Dieser Gesetzesvorschlag führt nicht zum Bürokratieabbau. Ein solcher könnte vor allem dadurch realisiert werden, dass Datenschutzaufgaben eigenständig vom jeweiligen Unternehmen selbst ausgeübt werden. Aufgrund zwingender europarechtlicher Vorgaben zu Melde- und Registrierungspflichten hat der Vorschlag zur Entbindung kleiner Unternehmen von der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten aber den Effekt, dass die Melde- und Registrierungspflichten von den staatlichen Datenschutzaufsichtsbehörden wahrgenommen werden müssen.

In welche Richtung eine **Modernisierung des Datenschutzrechtes** gehen könnte, wird in einem Gutachten, das im Auftrag des Bundesinnenministeriums erarbeitet und im Jahr 2001 vorgelegt wurde, ausführlich erörtert. Es besteht die Gefahr, dass diese Vorschläge in Vergessenheit geraten. Sie zielen auf eine Vereinfachung und Bereinigung des inzwischen unleserlich gewordenen Bundesdatenschutzgesetzes hin, ohne jedoch das Datenschutzniveau zu senken. Es wird ein Instrumentenmix vorgeschlagen, bei dem Datenschutz durch Technik, Selbstregulierung der Wirtschaft, eine verstärkte Einbeziehung der Betroffenen, die Nutzung von Datenschutz-Audit und -Gütesiegel sowie eine Anpassung an die Gegebenheiten moderner Informationstechnik wichtige Bestandteile sind. Mit einem solchen modernen Datenschutzgesetz könnte Deutschland wieder seine Vorreiterrolle in der internationalen Datenschutzdiskussion erlangen und zum Wegbereiter einer freiheitlichen Informationsgesellschaft werden, in der Datenschutz nicht als Hindernis wahrgenommen wird, sondern als Grundbedingung für die Weiterentwicklung der Informationswirtschaft.

Was ist zu tun?
Die Bundesregierung wäre gut beraten, wenn sie zur Stärkung des Informationstechnikstandortes die Modernisierung des Datenschutzrechtes in Angriff nehmen würde.

2.2 Alles geht?

So zurückhaltend die neue Bundesregierung beim Datenschutz ist, so offensiv propagiert sie die Ausweitung von Überwachungsbefugnissen, insbesondere im Sicherheitsbereich.

Wir kennen es aus Schleswig-Holstein: Dort haben die Koalitionspartner **neue Eingriffsbefugnisse für die Polizei** vereinbart, deren Notwendigkeit selbst aus Polizeisicht infrage gestellt wird. Entsprechendes erfolgte kein halbes Jahr später in Berlin: Schnellstmöglich sollen eine „Antiterrordatei" geschaffen, der Datenaustausch zwischen Polizei und Nachrichtendiensten intensiviert, Präventivbefugnisse für das Bundeskriminalamt (BKA) eingeräumt, das Ausländerzentralregister ausgebaut, biometrische Verfahren verstärkt eingesetzt, das Visa- und das Schengener Informationssystem ausgebaut werden ...

Es ist unbestritten, dass **adäquate Maßnahmen** ergriffen werden müssen, um bestehenden Sicherheitsrisiken zu begegnen. Doch darf dies nicht überstürzt erfolgen. Bei aller nötigen Eile sind Bedacht und die Wahrung der rechtsstaatlichen Erfordernisse geboten. Gesetzgebungsaktionismus bringt ebenso wenig mehr Sicherheit wie das undifferenzierte Ansammeln und Abgleichen von personenbezogenen Daten. Gerade wird bundesweit angesichts des Großereignisses Fußballweltmeisterschaft 2006 ein Verfahren begonnen, bei dem unter Missachtung bestehender Datenschutzgrundsätze von Zuschauern und Berufshelfern jede Menge Daten gesammelt und mit Sicherheitsdateien abgeglichen werden (Tz. 4.2.9). Diejenigen, die dies kritisieren, sind keine vaterlandslosen Gesellen. Es mag sich dabei viel eher um Verfassungspatrioten handeln, die Grundrechtseingriffe nicht als Bagatelle abtun, für die es keiner konkreten Rechtfertigung bedarf.

Im Sicherheitsrecht bewirken Schnellschüsse und Allheilmittel oft genau das **Gegenteil dessen, was sie bewirken sollen**: Statt die Bevölkerung zu beruhigen, werden die Menschen unter Umständen beunruhigt. Statt effektiver Eingriffsmöglichkeit wird ein Kompetenzwirrwarr von Bund und Ländern und konkurrierenden Behörden geschaffen. Statt gezielt Gefahren aufzuspüren, droht eventuell durch den Datenwust der Verlust des Überblicks und des Blicks für das Wesentliche. Statt Ressourcen zu bündeln, werden möglicherweise personelle und sachliche Mittel in Aktionen verschwendet, die keinen positiven Sicherheitseffekt haben. Mit informationellen Eingriffen ist in sehr vielen Fällen die Einschränkung der Freiheits- und Datenschutzrechte von Unverdächtigen, Unbeteiligten und Ungefährlichen verbunden.

Flankierend – nicht alternativ zu hinreichend bestimmten, verhältnismäßigen Eingriffsbefugnissen – sind technische, organisatorische und verfahrensrechtliche Sicherungen von Verfassungs wegen geboten. Eine dieser Sicherungen besteht in einer effektiven Verarbeitungskontrolle durch unabhängige Datenschutzbeauftragte. Zur Verhinderung von Willkür und Eigenleben der Nachrichtendienste auf Bundesebene ist derzeit die Schaffung der Stelle eines **Geheimdienstbeauftragten** in der Diskussion. Eine solche Einrichtung kann einen wichtigen Beitrag dazu leisten, dass die zwangsläufig im Geheimen operierenden Dienste nicht der rechtsstaatlichen und demokratischen Kontrolle entgleiten. Da es Überschneidungen mit der Datenschutzkontrolle geben würde, sollte eine enge Zusammenarbeit zwischen beiden Bereichen institutionalisiert werden.

Ein weiteres wichtiges rechtsstaatliches Hilfsmittel zur Überprüfung von neuen Gesetzen ist die unabhängige **Evaluierung von Sicherheitsbefugnissen**. Erweist sich im Nachhinein, dass eine Befugnis zu übermäßigen Eingriffen – eventuell gegenüber Unbeteiligten – führt oder dass sie völlig unergiebig ist, so müssen hieraus sowohl praktische als auch gesetzgeberische Konsequenzen gezogen werden. Unlauter war insofern die bei der Rasterfahndung auf Bundes- wie auf Landesebene gewählte Argumentation der Innenverwaltungen, die als Beleg für die Wirksamkeit der Maßnahme deren Erfolglosigkeit heranzogen: Die Rasterfahndung habe ergeben, dass es in Deutschland keine weiteren Schläfer gebe; als Erfolg wurde sogar der Einschüchterungseffekt gewertet, der mit dieser Maßnahme einhergegangen sei und der potenzielle Terroristen vom bösen Tun abgehalten habe. Evaluation bedeutet, mit Fakten zu arbeiten, nicht mit Theorien und Spekulationen.

Was ist zu tun?
Das Land Schleswig-Holstein ist über den Bundesrat an der Bundesgesetzgebung beteiligt. Sicherheitsgesetze des Bundes müssen von Behörden des Landes umgesetzt werden. Dies ist Grund genug, bei der bundespolitischen Diskussion dafür einzutreten, dass ein Ausgleich zwischen Bürgerrechts- und Sicherheitsbelangen gesucht und gefunden wird.

3 Datenschutz im Landtag

Der Wechsel der Mehrheiten im Landtag hat nicht zu einem Wechsel der Datenschutzpolitik im „hohen Haus“ geführt. Das Datenschutzgremium kümmert sich engagiert um die Datenschutzbelange des Parlaments.

Zwar brachte die neue Legislaturperiode eine teilweise neue Besetzung des für die Datenschutzbelange des Parlaments zuständigen **Datenschutzgremiums** mit sich, doch hat sich am Engagement nichts geändert. Das Gremium musste sich mit einzelnen Eingaben beschäftigen. Auch seinen anlassunabhängigen Prüfauftrag nimmt das Gremium ernst. Im Vordergrund der Arbeit der Gremiums standen aber grundsätzliche Fragen, die mit dem IT-Einsatz im Landtag verbunden sind. Insbesondere die Anbindung des Landtags mit seinem Daten- bzw. Sprachnetz nach draußen stellt wegen der fortschreitenden technischen Entwicklung eine dauernde Herausforderung dar. So wird z. B. der Umstieg bei der Telefonanlage auf Internettechnologie im Landessprachnetz erwogen. Dabei geht es darum, dass die Vertraulichkeit der Kommunikation der Abgeordneten, aber auch der hier tätigen Journalisten, Bediensteten und der Bürgerinnen und Bürger gewährleistet bleibt. Wir beraten sowohl die Landtagsverwaltung als auch das Datenschutzgremium. Das Datenschutzgremium ist mit einem eigenen Informationsangebot im Internet präsent unter

www.sh-landtag.de/parlament/datenschutz/index.html

Im Rahmen der Beratung des Datenschutzgremiums stellte sich aufgrund von Petentenbeschwerden die Frage, inwieweit Betroffene gegenüber dem Landtag, namentlich dem Petitionsausschuss, Auskunfts- und **Akteneinsichtsansprüche** haben. Selbstverständlich gelten Grundrechte auch gegenüber dem Parlament, weshalb grundsätzlich ein Anspruch auf Akteneinsicht besteht. Die Datenschutzordnung des Landtages sieht ausdrücklich einen Auskunftsanspruch vor. Ein Grund zur Verweigerung der Kenntnisgabe gegenüber dem Betroffenen besteht aber, wenn die ordnungsgemäße Aufgabenerfüllung der parlamentarischen Aufgaben gefährdet würde. Schon die Beeinträchtigung des **Beratungsgeheimnisses** stellt eine derartige Gefährdung dar. Dies gilt insbesondere bei Petitionen; die Petentinnen und Petenten haben keinen Anspruch darauf, zu erfahren, wie der Landtag in seiner parlamentarischen Unabhängigkeit mit einer Eingabe verfahren ist. Grundsätzlich genügt die Information über den Ausgang des Verfahrens, bei dem nicht nur eine rechtliche Prüfung erfolgt, sondern auch politische Erwägungen eine Rolle spielen. Das Beratungsgeheimnis gilt auch bei sensiblen Betroffenendaten z. B. aus Personalakten oder aus ärztlichen Unterlagen.

Als Bestandteil des umfassenderen Sicherheitskonzeptes hat das ULD bisher die **Videoanlage des Landtages** noch nicht auditiert (27. TB, Tz. 3.1). Dabei treten zunächst die generellen Fragestellungen bei Videoüberwachung im öffentlichen Raum auf, die an einem Ort der demokratischen Begegnung, an dem zugleich auch ein hohes Sicherheitsrisiko besteht, mit hoher Sensibilität beantwortet werden müssen. Damit aber nicht genug: Die Videoüberwachung rund um den

Landtag lässt erkennen, wer hier mit wem unterwegs ist und wer sich mit wem trifft. Diese Informationen haben eine über den Persönlichkeitsschutz hinausgehende politische und grundrechtliche Brisanz. Daher begrüßen wir es, dass sich das Datenschutzgremium für die Auditierung des Videokonzeptes des Landtages ausgesprochen hat. Der Landtagspräsident hat sich diese Initiative zu Eigen gemacht und die für die Realisierung zuständige Gebäudemanagement Schleswig-Holstein (GMSH) gebeten, auch diesen Teil des Sicherheitskonzeptes auditieren zu lassen. Dieses Audit wird bundesweit das erste Verfahren in Sachen Videoüberwachung darstellen.

4 Datenschutz in der Verwaltung

4.1 Allgemeine Verwaltung

4.1.1 E-Government im Meldewesen

Die Übermittlung von Meldedaten durch automatisierte Abrufverfahren wurde von uns aus aktuellem Anlass geprüft. Mit Erschrecken mussten wir massive Rechtsverstöße feststellen. Die Beseitigung der Mängel muss vor der beabsichtigten Ausweitung der Abrufmöglichkeiten oberste Priorität haben.

Automatisierte Abrufverfahren werden demnächst die Verfügbarkeit von Meldedaten bei allen öffentlichen und privaten Stellen deutlich verbessern und zu erheblichen Rationalisierungseffekten sowohl bei den Meldebehörden als auch bei den empfangenden Stellen führen. Der Datenschutz darf dabei allerdings nicht auf der Strecke bleiben. Wir haben deshalb bereits bestehende Abrufverfahren bei einer Stadt geprüft und mussten erhebliche Mängel bei der Ausgestaltung der Verfahren feststellen.

- **Polizeiabrufverfahren**

Im Rahmen dieses Verfahrens haben Polizeidienststellen des Landes jederzeit die Möglichkeit, Meldedaten online bei dataport abzurufen. Dataport führt zu diesem Zweck im Auftrag der einzelnen Meldebehörden eine **nach einzelnen Kommunen gegliederte Spiegeldatei** der jeweiligen Originalmelderegister.

Folgende **Mängel** müssen abgestellt werden:

- Es waren keine ausreichenden schriftlichen Aufträge und ergänzenden Weisungen gegenüber dem Auftragnehmer zur Ausgestaltung des Abrufverfahrens vorhanden. Der geprüften Stadt war weder die Funktionsweise des Verfahrens bekannt, noch lagen schriftliche Unterlagen (z. B. ein Bedienerhandbuch) vor.
- Die Stadt selbst hatte keinen Zugriff auf ihre in der Spiegeldatei bei dataport gespeicherten Daten. Damit bestand keine Möglichkeit, die Richtigkeit gespeicherter Daten oder die Rechtmäßigkeit des Auskunftsverhaltens zu prüfen.
- Im Verfahren fand keine ausreichende Identitätsprüfung hinsichtlich der jeweils gesuchten Person statt, mit der Folge, dass auf eine konkrete Anfrage eine Vielzahl von Personendatensätzen übermittelt wurde, von denen naturgemäß nur einer zur rechtmäßigen Aufgabenerfüllung der Polizei erforderlich sein konnte.
- Im Falle einer Datenübermittlung wurden immer komplette Datensätze weitergegeben. So wurde z. B. im Fall einer Aufenthaltsermittlung bei einem Ordnungswidrigkeitenverfahren regelmäßig auch das Geburtsdatum, der Geburtsort, die Nationalität, eventuelle Nebenwohnungen und Übermittlungssperren weitergeleitet, obwohl diese Angaben für das polizeiliche Verfahren nicht benötigt wurden.

- Die vorgeschriebene Dokumentation der einzelnen Datenabrufe durch die Polizei war jedenfalls bei der Stadt nicht verfügbar. Insoweit fehlte auch die notwendige Grundlage für eine Revisionsmöglichkeit der Datenabrufe der Polizei.
- Wird das Melderegister nachträglich berichtigt, etwa weil sich ein Betroffener verspätet angemeldet hat, sind von der Meldebehörde die Stellen zu unterrichten, denen zuvor die unrichtigen Daten übermittelt worden sind. Diese Nachberichtspflicht wurde von der Stadt nicht beachtet, wohl auch, weil die dafür notwendige technische Unterstützung in Form einer automatischen Auswertung der Dokumentation nicht vorhanden war.
- Die für eine ordnungsgemäße automatisierte Datenverarbeitung vorgeschriebene Verfahrensdokumentation, Test und Freigabe konnten nicht nachgewiesen werden.

- **Behördeninternes Meldedatenabrufverfahren**

Das ebenfalls geprüfte behördeninterne Meldedatenabrufverfahren, bei dem **andere Fachämter** innerhalb des Rathauses online auf die Meldedaten zugreifen können, unterscheidet sich vom Polizeiabrufverfahren vor allem dadurch, dass der Zugriff unmittelbar auf den Originaldatenbestand erfolgt, das Verfahren selbst bei der Kommune verfügbar ist und eigenständig konfiguriert werden kann. Die festgestellten Mängel fielen daher eher in den unmittelbaren Verantwortungsbereich der Stadt:

- Es fehlte die vorgeschriebene schriftliche Dienstanweisung, in der die notwendigen Details zur Ausgestaltung des Abrufverfahrens fachbereichsübergreifend festgelegt werden müssen.
- Zugriffsrechteverwaltung und Suchfunktionen für das Verfahren wurden erst im Rahmen der Prüfungsankündigung an die Rechtslage angepasst. Folglich stand für die Vergangenheit keine ausreichende Protokollierung der Datenabrufe durch die Fachämter zur Verfügung.
- Die vorgeschriebene Revision der Datenabrufe hatte nicht stattgefunden.
- Die Nachberichtspflicht wurde wie im Polizeiauskunftsverfahren nicht erfüllt.
- Auch hier konnte keine ausreichende Verfahrensdokumentation, Test und Freigabe nachgewiesen werden.

Die festgestellten Mängel sind insbesondere im Polizeiabrufverfahren durchweg auch **auf andere Kommunen übertragbar**. Wir werden deshalb auch im laufenden Jahr unser besonderes Augenmerk auf diesen Bereich richten und die notwendigen datenschutzrechtlichen Verbesserungen in angemessener Form begleiten.

Was ist zu tun?
Die Meldebehörden sollten die Prüfungsergebnisse zum Anlass nehmen, um sich insbesondere ihrer Verantwortung als Auftraggeber bei der Auftragsdatenverarbeitung bewusst zu werden, und die notwendigen schriftlichen Weisungen und Kontrollen gegenüber dem Auftragnehmer unverzüglich in die Wege leiten.

4.1.2 Gibt es eine vorläufige Auskunftssperre im Melderegister?

Die Handhabung einer so genannten vorläufigen Auskunftssperre ist für die Dauer des Antragsverfahrens gesetzlich nicht geregelt. Die schutzwürdigen Interessen der Betroffenen sind hier besonders zu beachten.

Durch mehrere Anfragen wurden wir auf ein besonderes Problem bei der Eintragung von Auskunftssperren in das Melderegister aufmerksam. Mit Auskunftssperren soll vor allem verhindert werden, dass aus bestimmten Gründen die **Adresse von gefährdeten Personen** über eine Melderegisterauskunft gefunden und diese dadurch gefährdet würden. Oft wird über solche Anträge nicht sofort entschieden, da noch fehlende Unterlagen nachgereicht oder weitere Nachforschungen angestellt werden müssen. In diesen Fällen gibt es zurzeit unterschiedliche Praktiken:

- Es wird eine vorläufige Auskunftssperre, teilweise befristet für drei Monate, bewilligt, ohne jedoch die Meldebehörde des letzten Wohnortes davon zu unterrichten.
- Es wird eine Auskunftssperre vorläufig in das eigene Melderegister eingetragen; Betroffene erhalten davon jedoch keine Kenntnis.
- Es wird bis zur endgültigen Entscheidung des Antrages nichts veranlasst.

Der Gesetzgeber hat im Melderecht nichts zu einer vorläufigen Auskunftssperre geregelt. Abschließend normiert ist dagegen die Befristung der eigentlichen Auskunftssperre. Sie endet mit Ablauf des zweiten auf die Antragstellung folgenden Kalenderjahres. Eine zum Teil praktizierte formelle Befristung in einem vorläufigen Verfahren auf drei Monate ist dagegen nicht im Gesetz vorgesehen. Wird bei der Antragstellung die Notwendigkeit einer Auskunftssperre **schlüssig vorgetragen**, kann dies bis zur endgültigen Entscheidung nicht ohne Folgen für die Weiterverarbeitung der Meldedaten bleiben. In diesen Fällen sind zwingend die schutzwürdigen Interessen der Betroffenen nach dem Landesmeldegesetz (LMG) zu beachten. Folgende Maßnahmen kommen in Betracht:

- Bis zur Entscheidung ist der Antrag als vorläufige Auskunftssperre zu speichern, damit die schutzwürdigen Interessen der Betroffenen sichergestellt werden.
- Schriftliche und telefonische Auskunftsersuchen werden bis zur Entscheidung des Antrages zurückgestellt. Gegebenenfalls ist eine Zwischennachricht an die Auskunftssuchenden zu erteilen.
- In automatisierten Abrufverfahren sind die Fälle zu sperren und die Anfragen an die Meldebehörde weiterzuleiten. Auskunftssuchende erhalten den Hinweis, dass zurzeit eine Auskunft im automatisierten Verfahren nicht möglich ist und eine gesonderte Nachricht der Meldebehörde erfolgt.
- Die Meldebehörde des letzten Wohnortes muss von dem laufenden Antragsverfahren unterrichtet werden, um ebenfalls die erforderlichen Maßnahmen für ihren Bereich treffen zu können. Sie muss auch über die abschließende Entscheidung informiert werden.

- Die Betroffenen sind über das Veranlasste und den weiteren Verfahrensgang zu unterrichten.

Was ist zu tun?
Meldebehörden müssen bereits bei Anträgen auf Auskunftssperre die schutzwürdigen Interessen der Betroffenen beachten. Sie sollten ihre Verfahrenspraxis an den Vorschlägen des ULD ausrichten.

4.1.3 Überprüfung von Nebenwohnsitzen durch die Meldebehörde

Im Melderecht ist das An- und Abmelden von Nebenwohnsitzen nur unvollständig geregelt. Flächendeckende Kontrollen ohne konkreten Anlass sind nicht vorgesehen. Karteileichen sind damit fest vorprogrammiert.

Ein Einwohner kann nur einen Hauptwohnsitz, aber mehrere Nebenwohnsitze haben. Die Voraussetzungen für die An- und Abmeldung dieser Nebenwohnsitze sind im Gesetz **nicht eindeutig geregelt**. Dies hat offensichtlich zur Folge, dass in vielen Kommunen weit mehr Nebenwohnsitze angemeldet als vorhanden sind, weil die Betroffenen diese längst aufgegeben haben. Eine ähnlich große Zahl von Nebenwohnsitzen dürfte nicht angemeldet sein.

Meldebehörden wollen im Hinblick auf die offensichtlichen Mängel immer wieder flächendeckende Kontrollen durchführen. Solche Pläne sind jedoch weitgehend zum Scheitern verurteilt, weil das Meldegesetz eine Kontrolle von Amts wegen nur zulässt, wenn konkrete Anhaltspunkte für die Unrichtigkeit des Melderegisters im Einzelfall oder bei einer Vielzahl namentlich bezeichneter Einwohner vorliegen. Dies ist auch gut so: Mit der Anmeldung eines Nebenwohnsitzes sind keine weiteren rechtlichen Folgen in anderen Rechtsgebieten verknüpft. Vor diesem Hintergrund sollte geprüft werden, ob die Speicherung von Nebenwohnsitzen überhaupt noch sinnvoll ist. Wegen der hohen Fehlerquote ist der Datenbestand für alle Nutzenden inklusive Sicherheitsbehörden kaum verwendbar. Die derzeitige Praxis erzeugt einen nicht unerheblichen Verwaltungsaufwand. Mit dem **Verzicht auf die Speicherung des Nebenwohnsitzes** könnte ein echter Beitrag zur Entbürokratisierung der Verwaltung geleistet werden.

Was ist zu tun?
Der Gesetzgeber sollte die Speicherung des Nebenwohnsitzes im Melderegister mit dem Ziel überprüfen, ob hierauf verzichtet werden kann. Anderenfalls sollte ein Verfahren gewählt werden, das zu einem aussagekräftigen und verlässlichen Datenbestand führt.

4.1.4 Elektronische Passdatei bei den Meldebehörden noch nicht sicher

Die elektronische Übermittlung von Passdaten an die Bundesdruckerei veranlasste viele Meldebehörden, ihre Passdatei ausschließlich elektronisch zu führen. Die notwendigen Datensicherheitsmaßnahmen, die hierbei zu treffen sind, stehen noch aus.

Die Passdatei soll einen authentischen Nachweis über die tatsächlich ausgestellten Pässe leisten. Sie ist Grundlage für die Neuausstellung verlorener Pässe; zudem steht sie der Polizei für Fahndungszwecke zur Verfügung. An die **Richtigkeit und Unveränderbarkeit** der gespeicherten Daten sind deshalb höchste Ansprüche zu stellen. Nach Ausstellung eines Passes kann eine Fortschreibung erfolgen, eine rückwirkende Änderung darf aber nicht vorgenommen werden.

Die Erstellung der Passdatei erfolgt aus einer Funktion des Einwohnerinformationssystems der Meldebehörden. Die notwendigen Daten werden aus dem jeweiligen Personendatenbestand automatisiert in ein spezielles Formular übernommen, um das Passbild sowie die Unterschrift des Antragstellers ergänzt und für die elektronische Übermittlung der Daten an die Bundesdruckerei eingescannt. Die erfassten Daten werden in Papierform (zurzeit Originaldatei) und **in elektronischer Form als Passdatei** abgespeichert.

Die **Begutachtung** bei einer von uns beratenen Gemeinde brachte folgende Ergebnisse:

- Die für eine ordnungsgemäße automatisierte Datenverarbeitung vorgeschriebene Verfahrensdokumentation, Test und Freigabe konnten nicht nachgewiesen werden.
- Die Mitarbeiter der Meldebehörde mussten sich bei der Fachanwendung mit einem Benutzernamen und einem Passwort autorisieren, doch innerhalb der Fachanwendung hatten sie auch nach Ausstellung eines Passes noch Änderungsrechte. So konnte z. B. der Geburtsort eines Bürgers in einer bestehenden Passdatei problemlos geändert werden.
- In dem Fachverfahren wurde die Bearbeitung der Passdatei nicht ausreichend protokolliert. Es lag ein Bearbeitungsprotokoll für das gesamte Fachverfahren vor, aus dem allerdings nicht hervorging, aus welchem Grund ein bestimmtes Formular der Fachanwendung aufgerufen wurde und ob Daten hinzugefügt, geändert oder gelöscht wurden.
- Es wurde kein Verfahren zur Gewährleistung der Authentizität einer automatisiert gespeicherten Passdatei, die bei einem papierenen Passdateiblatt durch eine Unterschrift bzw. ein Namenskürzel gewährleistet wird, eingesetzt.

Sollen personenbezogene Daten **ausschließlich automatisiert** gespeichert werden, so muss neben der

- vollständigen Verfahrensdokumentation,
- Definition, Einführung und Kontrolle der allgemeinen Maßnahmen zur Datensicherheit und der besonderen Maßnahmen zur Datensicherheit beim Einsatz von automatisierten Verfahren und der
- revisionsfähigen Protokollierung (was, wann, durch wen und in welcher Weise gespeichert, verändert, übermittelt oder gelöscht wurde)

zusätzlich ein Verfahren zur **Gewährleistung der Authentizität** der gespeicherten Daten eingesetzt werden, das dem Stand der Technik entspricht. Diese „Nichtabstreitbarkeit", dass die Daten von dem entsprechenden autorisierten Sachbearbeiter erhoben und gespeichert wurden, kann z. B. durch eine digitale Signatur sichergestellt werden. Digitale Signaturen werden in Meldebehörden schon eingesetzt, z. B. um elektronische Passdateien an die Bundesdruckerei zu übermitteln.

Was ist zu tun?
Die Meldebehörden sollten ihre Originalpassdatei nur dann auf ein elektronisches Verfahren umstellen, wenn ein ausreichender Datensicherheitsstandard und die Authentizität der gespeicherten Daten gewährleistet sind. Digitale Signaturen sind hierfür aus heutiger Sicht ein geeignetes Mittel.

4.1.5 ostseecard*

Der Ostsee-Holstein-Tourismus e.V. hat federführend das Chipkartensystem ostseecard* eingeführt, mit dem eine Kurabgabe erhoben wird und zugleich Leistungspakete und Rabatte privater Anbieter angeboten werden. Bei wesentlichen Änderungen dieses vom ULD auditierten Systems wird eine Reauditierung erforderlich.

Bereits zum Zeitpunkt der Einführung der ostseecard* (27. TB, Tz. 9.2.1) war geplant, in der folgenden Saison das auditierte System weiterzuentwickeln. Wesentliche Änderungen haben zur Folge, dass eine **Reauditierung** notwendig ist. Andernfalls kann das Audit widerrufen werden.

Eine wesentliche geplante Änderung besteht in der Einführung eines Online-Meldescheins. Die Ausgabe der Chipkarte ist mit dem Ausfüllen des Meldescheins verbunden. Bisher musste dieser von der Besucherin und dem Besucher handschriftlich ausgefüllt und unterschrieben werden. Künftig soll das Ausfüllen über einen Online-Meldeschein durch den Vermieter vorgenommen werden können. Dieser kann zum Ausfüllen des Meldescheins auf seinem PC die in seinem Hotelsystem gespeicherten Daten verwenden. Der Meldeschein bedarf

nach dem Ausdruck nur noch einer handschriftlichen Unterschrift. Auf Wunsch des Gastes kann auf dem Meldeschein vermerkt werden, dass er der Speicherung seiner Adressdaten zustimmt, um mit Informationsmaterial beworben zu werden.

Die Reauditierung setzt eine **datenschutzfreundliche Lösung** der Neuerungen voraus. Daraus folgt, dass der Vermieter die Meldescheindaten nicht dauerhaft auf seinem lokalen PC speichern und den Gast mit Informationsmaterial bewerben darf, wenn er nicht tatsächlich hierzu freiwillig zugestimmt hat.

Was ist zu tun?
Weiterentwicklungen des Verfahrens ostseecard* sollten frühzeitig dokumentiert und mit dem ULD abgestimmt werden.

4.1.6 Mitarbeiter sind nicht nur Funktionsträger

Die aktuelle Rechtsprechung des Bundesverwaltungsgerichts stellt klar, dass die Verarbeitung von Daten der Mitarbeiter in dienstlichen Angelegenheiten auch deren Persönlichkeitsrecht beeinträchtigen kann.

Behörden und sonstige öffentliche Stellen sind juristische Personen, die erst über ihre Mitarbeiterinnen und Mitarbeiter handlungsfähig sind. Bei der Erfüllung dienstlicher Aufgaben kommt es in verschiedenen Konstellationen zur Nennung von Namen und weiteren Daten der Beschäftigten. Nicht einfach zu beantworten ist, welche datenschutzrechtlichen Anforderungen an die Verarbeitung dieser so genannten **Funktionsträgerdaten** zu stellen sind. Spätestens mit dem Urteil des Bundesverwaltungsgerichts über die Nutzung der Stasiabhörprotokolle des Altbundeskanzlers Helmut Kohl ist geklärt, dass bei solchen Mitarbeiterdaten das LDSG anwendbar ist.

Liegen keine speziellen Befugnisgrundlagen vor, so ist bei der Übermittlung der Mitarbeiterdaten nach dem LDSG zu prüfen, ob diese im Rahmen der Zweckbestimmung erforderlich ist, also der rechtmäßigen Erfüllung der durch Rechtsvorschrift zugewiesenen Aufgaben der Daten verarbeitenden Stelle dient. Zur rechtmäßigen Aufgabenerfüllung gehört, wenn die öffentlichen Stellen mit Außenwirkung tätig werden, für den Adressatenkreis erreichbar zu sein, da hinter der juristischen Person „Behörde“ immer konkrete Menschen stehen. Der **Dienstverkehr** erfordert die Bereitstellung der Mitarbeiterdaten im notwendigen Umfang – gegebenenfalls auch durch deren Veröffentlichung.

Zu den Funktionsträgerdaten sind in der Regel zu rechnen:

- Familiennamen,
- Vornamen,
- E-Mail-Anschriften,
- dienstliche Telefonnummern,

- Dienstadressen mit Zimmernummern und
- Organisationsbezeichnungen innerhalb der Verwaltungen, denen die Mitarbeiter angehören.

Bei der Prüfung der Frage der Außenwirkung ist vorrangig auf die so genannte Funktionsebene, d. h. auf die von den Mitarbeitern wahrzunehmenden Aufgaben abzustellen. Mitarbeiter der Leitungsebene oder mit der direkten Vertretung nach außen betraute Mitarbeiter, z. B. Pressesprecher, müssen eine Veröffentlichung ihrer funktionsbezogenen Daten **sogar im Internet** hinnehmen. In den anderen Fällen bedarf diese Form der Veröffentlichung der Einwilligung der Mitarbeiter. Bei Grenzfällen kann eine Widerspruchslösung gewählt werden, bei der die Mitarbeiter über Art und Umfang der geplanten Veröffentlichung und über die Möglichkeit, hiergegen zu widersprechen, aufgeklärt werden.

Ein Sonderfall der Internetveröffentlichung besteht, wenn die **Mitarbeiterdaten nicht suchfähig** bzw. verknüpfbar in einer dynamischen Datenbank enthalten sind, d. h., wenn zum Erhalt der gewünschten Informationen der Name von den Anfragenden manuell eingegeben werden muss. Da Suchmaschinen hierzu nicht in der Lage sind, können sie die Mitarbeiterdaten für eine Auswertung nicht erfassen. In diesen Fällen bestehen gegenüber der konventionellen Veröffentlichung im Internet keine zusätzlichen Risiken.

Bei der Übermittlung von Mitarbeiterdaten in **Papierform** sind die Erfordernisse des Dienstverkehrs vorrangig an den Bedürfnissen des Empfängerkreises auszurichten. Zweckbestimmungen sind für die jeweiligen Empfänger verbindlich. Werden z. B. dem Lieferanten einer Behörde die zuständigen Mitarbeiter der Geschäftsstelle benannt, darf er diese Daten nicht auf seiner Internethomepage veröffentlichen. Die übermittelnde Stelle hat die empfangende Stelle zu verpflichten, die Daten nur zu dem Zweck zu verwenden, zu dem sie ihr übermittelt wurden.

Ob der Dienstverkehr eine Verarbeitung von Mitarbeiterdaten erfordert, entscheidet im Rahmen der gesetzlichen Aufgaben der Behördenleiter über sein **Direktionsrecht**. Diese Entscheidungen sind unter Plausibilitätsgesichtspunkten überprüfbar; im Ergebnis bleibt dem Behördenleiter aber ein gewisser Beurteilungsspielraum hinsichtlich der gebotenen Präsentation in der Öffentlichkeit. Aus Gründen der Bürgerfreundlichkeit kann keine strenge Erforderlichkeit der Datenweitergabe verlangt werden; wohl ist eine Überprüfung auf Schlüssigkeit hin aber möglich.

Was ist zu tun?
Ein praxisgerechter Umgang mit Funktionsträgerdaten verlangt einen Ausgleich zwischen Transparenzanforderungen der Verwaltung und dem Schutz der Persönlichkeitsrechte der Bediensteten. Öffentliche Stellen sollten ihre Praxis auf dieser Grundlage überprüfen.

4.1.7 Das Interesse der Miteigentümer an einem Bauvorbescheid

In baurechtlichen Verfahren haben Miteigentümer das Recht auf Informationen, wenn deren öffentlich-rechtlich geschützten Belange berührt sind. Anderenfalls ist eine Datenübermittlung an sie ohne Einwilligung des Bauherrn unzulässig.

Eine Eingabe stellte uns vor die Frage: Darf eine Bauaufsichtsbehörde allen Miteigentümern einer Wohnungseigentümergemeinschaft den Bauvorbescheid eines der Miteigentümer übersenden? Generell gilt: Ja, wenn diese Datenübermittlungen zur rechtmäßigen Aufgabenerfüllung erforderlich sind; konkret: wenn der Bauvorbescheid **Drittwirkung** gegenüber den anderen Miteigentümern entfaltet, weil deren öffentlich-rechtlich geschützten Belange berührt sind. Nach der Landesbauordnung gilt übrigens Entsprechendes für die Beteiligung von Nachbarn.

Beim konkreten Bauvorbescheid war über eine besondere Auflage ein Rettungsweg aus dem Teileigentumsbereich des anderen Miteigentümers betroffen. Der Miteigentümer durfte nicht nur, sondern **musste unterrichtet** werden, damit der Bescheid ihm gegenüber Bestandskraft entwickeln konnte. Ohne eine solche Drittwirkung wäre die Datenübermittlung allerdings unzulässig gewesen.

Was ist zu tun?
Bauaufsichtsbehörden sollten vor der Unterrichtung von Miteigentümern über baurechtliche Entscheidungen sorgfältig prüfen, ob deren öffentlich-rechtlich geschützten Belange berührt sind. Ist dies nicht der Fall, muss vor einer Datenübermittlung die Einwilligung des Bauherrn eingeholt werden.

4.1.8 Das datenschutzgerechte Bürgerbüro

Durch zentrale Auskunfts- und Beratungsstellen kann innerhalb der Verwaltung die Bürgerfreundlichkeit verbessert werden. Die Vertraulichkeit der Datenverarbeitung bleibt dabei allerdings noch oft auf der Strecke.

Nach dem Umbau des Rathauses war das neu geschaffene Bürgerbüro einer Stadt gerade feierlich eingeweiht worden. Beim Architektenwettbewerb für den Umbau hatte offensichtlich keiner an den Datenschutz gedacht. Nur so erklärt sich, dass der Wartebereich für Besucher allenfalls zwei Meter von den Beratungsplätzen entfernt lag. Die vier vorhandenen Beratungsplätze befanden sich so nah beieinander, dass ein unbefugtes **Mithören der Gespräche** durch Dritte nicht verhindert werden konnte, wenn an den einzelnen Arbeitsplätzen gleichzeitig Publikumsverkehr stattfand.

Das Geld für den Umbau war inzwischen ausgegeben. Entsprechend schwer tat sich die Stadt bei unserer Forderung nach Änderung der Einrichtung des Bürgerbüros. Es gelang gleichwohl eine Lösung, bei der der Wartebereich räumlich

deutlich von den **Beratungsplätzen abgetrennt** wurde. Zwischen den Beratungsplätzen wurden provisorische Schallschutztrennwände aufgestellt. Nach Verabschiedung des nächsten Haushalts soll dem dann eine datenschutzgerechte Designerlösung folgen.

Was ist zu tun?
Unnötiger Zeit- und Kostenaufwand wird vermieden, wenn vor der Einrichtung eines Bürgerbüros sorgfältig die datenschutzrechtlichen Anforderungen geprüft und in die Planungen mit einbezogen werden. Wir stehen gern für eine fachliche Beratung zur Verfügung.

4.1.9 Personalräte interessieren sich für Eingruppierungsdaten

Personalräten steht nach dem Mitbestimmungsgesetz ein Initiativrecht bei Maßnahmen in personellen, sozialen, organisatorischen und sonstigen innerdienstlichen Angelegenheiten der Dienststelle zu. Informationswünsche dazu hat die Dienststelle zu erfüllen.

Bei einer Anstalt öffentlichen Rechts wollten der örtliche Personalrat und der Gesamtpersonalrat eine Namensliste aller Mitarbeiter erhalten mit Angaben zu Eingruppierung, Fallgruppe, Datum der letzten Höhergruppierung und Ähnliches. Diese Datenweitergabe bedarf einer ausreichenden Befugnisgrundlage; diese findet sich im **Mitbestimmungsgesetz**. Danach sind schriftliche Unterlagen und in Dateien gespeicherte Daten, über die die Dienststelle verfügt, dem Personalrat in geeigneter Weise zugänglich zu machen, soweit dies für die Erfüllung der Aufgaben des Personalrats erforderlich ist.

Personalräte sind nicht nur für die Beteiligung an einzelfallbezogenen Personalmaßnahmen einer Dienststelle zuständig. Sie haben auch ein eigenes **Initiativrecht** und können insoweit die Beratung über geplante Maßnahmen einfordern. Hierfür müssen sie unter Umständen über die Gesamtheit der Mitarbeiter informiert sein, einschließlich der Beurteilungsnoten und der Eingruppierung bei der Vergütung. Aus Datenschutzsicht ist es nicht zu beanstanden, wenn Dienststellen ihren Personalräten auf Anforderung regelmäßig einen zu definierenden „Grunddatensatz“ der Beschäftigten übermitteln. Bei örtlichen Personalräten ist darauf zu achten, dass diese nur Daten über solche Mitarbeiter erhalten, die in den jeweiligen Zuständigkeitsbereich fallen.

Was ist zu tun?
Dienststellen dürfen Personalräten die für die Ausübung ihres Initiativrechts erforderlichen Personaldaten übermitteln. Umfang und Verfahren sollten einvernehmlich, z. B. in einer Dienstvereinbarung, festgelegt werden.

4.1.10 Ärztliche Gutachten für Fachvorgesetzte

Fachvorgesetzte haben kein generelles Zugangsrecht zu Personalaktendaten. Die Personalverwaltung darf ihnen solche Daten nur zur Verfügung stellen, soweit es zur Ausübung der Aufsichtsfunktion im Einzelfall erforderlich ist.

Zwischen einem Mitarbeiter einer obersten Landesbehörde und seinem Dienstherrn bestanden Meinungsverschiedenheiten über die Pflichten im Arbeitsvertrag. Im Klageverfahren musste geklärt werden, ob die dem Mitarbeiter per Geschäftsverteilungsplan übertragenen Aufgaben zumutbar waren. Wegen geltend gemachter gesundheitlicher Beeinträchtigungen wurde vom Arbeitsgericht eine amtsärztliche Untersuchung veranlasst. Der Fachvorgesetzte erhielt das medizinische Gutachten von der Personalverwaltung in vollem Umfang zur Kenntnis, nicht nur einzelne Hinweise zur **Einsetzbarkeit am Arbeitsplatz**, sondern die Darstellung des Gesundheitszustandes des Betroffenen.

Fachvorgesetzte müssen selbstverständlich von Hinweisen Kenntnis erhalten, die bei der Aufgabenverteilung im Referat **im Rahmen der Leitungsfunktion** relevant sind. Das Personalreferat hat die dafür im Einzelfall erforderlichen Daten bereitzustellen. Fachvorgesetzte haben aber kein Recht auf darüber hinausgehende umfassende amtsärztliche Gutachten. Die Dienststelle sah ihren Fehler ein und hat sich bei dem Mitarbeiter entschuldigt.

Was ist zu tun?
Personalaktendaten dürfen an Fachvorgesetzte nur weitergegeben werden, soweit es zu deren Aufgabenerfüllung im Einzelfall erforderlich ist. Dies gilt sowohl für die Bereitstellung von Personaldaten in Akten als auch über automatisierte Verfahren.

4.1.11 Auch das Gemeindeprüfungsamt ist auskunftspflichtig

Erfolgt die Verarbeitung personenbezogener Daten zur Ausübung von Aufsichts- und Kontrollbefugnissen, so bleiben die Rechte der Betroffenen bestehen – auch gegenüber einem Gemeindeprüfungsamt.

Bei einer überörtlichen Prüfung stellte das Gemeindeprüfungsamt eines Kreises erhebliche Mängel im Bereich der Personalverwaltung einer Stadt fest. Ein inzwischen bei der Stadt ausgeschiedener **verantwortlicher Mitarbeiter** begehrte nun beim Gemeindeprüfungsamt Auskunft über seine Daten. Diese wurde ihm zunächst verweigert; es seien allenfalls so genannte Funktionsträgerdaten gespeichert. Die Daten beträfen ihn nicht als natürliche Person, sondern nur als Amtsträger, der in Vertretung für die Stadt als juristische Person gehandelt hat.

Bei unserer Kontrolle vor Ort stellten wir fest, dass das Gemeindeprüfungsamt sich wertend zu der persönlichen Verantwortlichkeit des Mitarbeiters, insbesondere zu Haftungsfragen und möglichen **disziplinarischen Konsequenzen**, geäußert hatte. Es ist klar, dass dies den früheren Mitarbeiter persönlichkeitsrechtlich betraf. Nach unserer Beanstandung erhielt er die gewünschten Informationen.

Dem Gemeindeprüfungsamt war offensichtlich auch nicht hinreichend klar, dass seine Kontrolltätigkeit nicht zu einer neuen Zweckbestimmung der erhobenen Daten führt. Deshalb sind z. B. Kopien aus Personalakten, die vom Gemeindeprüfungsamt zu Prüfungszwecken gefertigt und gespeichert werden, als Personalnebenakten zu werten und daher in das entsprechende Verzeichnis in die Personalgrundakte aufzunehmen. Die Betroffenen sind grundsätzlich zu unterrichten, wenn vom Gemeindeprüfungsamt Mängel bei der Personalverwaltung festgestellt werden, die sich auf ihr **Rechtsverhältnis als Bedienstete** auswirken.

Was ist zu tun?
Es besteht weiterhin Erörterungsbedarf in Bezug auf den Umgang der Gemeindeprüfungsämter mit Daten aus dem Bereich der Personalverwaltung. Deren Tätigkeit kann unmittelbar das Rechtsverhältnis der Betroffenen beeinflussen. Die Rechte der Betroffenen nach dem Personalaktenrecht müssen beachtet werden.

4.1.12 Zugriffsschutz auf automatisierte Personalaktendaten

Der Schutz von Personalaktendaten vor unbefugtem Zugriff Dritter muss auch in automatisierten Verfahren zur Personaleinsatzplanung und zur produktorientierten Arbeitszeiterfassung der Polizei gewährleistet sein. Mängel bei der Einführung des Verfahrens SP-Expert wurden schnell und unbürokratisch abgestellt.

Wir wurden darauf aufmerksam gemacht, dass das automatisierte Verfahren der Polizei zur produktorientierten Arbeitszeiterfassung und flexiblen Personaleinsatzplanung (SP-Expert) bei seiner Einführung trotz durchgeführter Tests und Freigabe Mängel aufwies. Jeder Mitarbeiter einer Polizeidienststelle konnte auf die **Arbeitszeitkonten** seiner Kolleginnen und Kollegen problemlos zugreifen. Aus entsprechenden Übersichten war erkennbar, welcher Mitarbeiter wann krank war, Urlaub hatte oder eine Kur machte.

Sowohl bei den Arbeitszeitdaten als auch bei den Details der Abwesenheit aus privaten Gründen handelt es sich um so genannte Personalaktendaten, die nach dem Beamtenrecht besonders vertraulich zu behandeln und vor unbefugter Einsicht zu schützen sind. Die Kollegen eines Mitarbeiters in einer Polizeidienststelle gehören insofern zum Personenkreis der Unbefugten. Das **Zugriffsrechtekonzept** sowie die Rechtevergabe mussten deshalb überarbeitet werden. Innerhalb kürzester Zeit – nach drei Wochen – wurden die notwendigen Korrekturen vorgenommen und damit die Voraussetzungen für einen rechtmäßigen Betrieb geschaffen. Die Polizei hat jedenfalls in diesem Fall ihre Leistungsfähigkeit in datenschutzrechtlicher Hinsicht eindrucksvoll unter Beweis gestellt.

Was ist zu tun?
Behörden sollten neue automatisierte Verfahren vor ihrem Echteinsatz sorgfältiger testen. Erweisen sich später dennoch Fehler, so müssen diese unverzüglich und konsequent beseitigt werden.

4.2 Polizeibereich

Das ULD berät die Polizeibehörden wie auch Bürgerinnen und Bürger in datenschutzrechtlichen Fragen und führt – als eine Kernaufgabe – Kontrollen durch, auch wenn dies für die Polizei nicht immer angenehm ist.

Bei den Datenschutzkontrollen wird geprüft, ob das Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung auch dann beachtet wird, wenn sie selbst von einer Erhebung oder Speicherung nichts wissen oder keinen Einblick in die polizeilichen Dateien erhalten dürfen. Das ULD kann solche Kontrollen **anlassunabhängig** durchführen. Oft wenden sich Bürgerinnen und Bürger an das ULD mit einer Kontrollbitte in ihrem konkreten Fall, etwa wenn sie sich nicht sicher sind, welche Daten die Polizei über sie erhoben hat oder speichert. Auch im Falle solcher **Eingaben** führen wir Kontrollen durch.

Im Berichtsjahr mussten leider **häufig Beanstandungen** wegen Verletzungen datenschutzrechtlicher Bestimmungen durch die Polizei ausgesprochen werden. Dabei handelte es sich durchaus um vermeidbare Fälle. Das Landeskriminalamt reagierte auf unsere schriftlichen Anfragen nicht oder nur nach übermäßiger Verzögerung. Beanstandet werden mussten auch gravierende materielle Verstöße, z. B. bei Fahndungsausschreibungen, der Speicherung von Versammlungsteilnehmern (Tz. 4.2.9) oder der Auskunftserteilung an Betroffene (Tz. 4.2.5). Bei den zwischenzeitlich implementierten beiden großen automatisierten Verfahren der Polizei des Landes Schleswig-Holstein – @rtus und INPOL Schleswig-Holstein (Tzn. 4.2.3 und 4.2.2) – sehen wir eine **stetige Annäherung** der beiderseitigen Positionen, wenngleich noch nicht in allen Fragen eine Lösung erreicht werden konnte. Ein wichtiges Zwischenergebnis ist, dass die Polizei die gesetzlich vorgesehene Protokollierung von Abrufen in diesen Verfahren verbessern will.

4.2.1 Neues Polizeirecht – mehr Daten von Unverdächtigen

Der Entwurf der Landesregierung für eine Novellierung des Landesverwaltungsgesetzes bedeutet eine grundsätzliche Wende im Polizeirecht. Die Polizei soll weitgehende Befugnisse im so genannten Gefahrenvorfeld erhalten und dabei Daten unverdächtiger Bürgerinnen und Bürger erfassen können, ohne dass diese hierfür einen konkreten Anlass geben.

Der Trend zur Erweiterung der Polizeibefugnisse auf das „**Vorfeld**“ mit der Datenspeicherung unabhängig vom Vorliegen einer konkreten Gefahrenlage oder einer Straftat bestand bundesweit. Doch sollte dieser Trend spätestens durch die Entscheidung des Bundesverfassungsgerichtes zum niedersächsischen Polizeigesetz, wo hierfür enge Grenzen gezogen werden, gestoppt sein. Schon bei der Entscheidung zum „Großen Lauschangriff“ hatte das Gericht klare Maßstäbe gesetzt (27. TB, Tz. 4.3.1). Doch werden diese Vorgaben von den Gesetzgebern vieler Länder ignoriert. Nun soll auch das Polizeirecht in Schleswig-Holstein grundlegend geändert werden, u. a. in folgenden Bereichen:

- präventive Telekommunikationsüberwachung,
- Bild- und Tonaufzeichnungen an öffentlich zugänglichen Orten,
- Kfz-Kennzeichenüberwachung,
- Erweiterte Kontrollbefugnisse bei Schleierfahndung und Identitätsfeststellung,
- Erweiterung der Generalermächtigung zur vorbeugenden Straftatenbekämpfung.

Beispiel für die uferlose Ausweitung von Tatbeständen ist die **Bild- und Tonaufzeichnung** in öffentlich zugänglichen Räumen. Diese Eingriffe sollen zukünftig bereits möglich sein, wenn „Tatsachen die Annahme rechtfertigen", dass „sich Gefahren für die öffentliche Sicherheit verfestigen". Von einer „moderaten Absenkung der Voraussetzungen" – so die Gesetzesbegründung – kann keine Rede sein. Was mit „Verfestigen" von Gefahren gemeint ist, ist weder dem Gesetz noch der Begründung zu entnehmen.

Es drängt sich daher die Vermutung auf, dass der Polizei an öffentlich zugänglichen Orten ein breiter Überwachungsteppich selbst mit Tonaufzeichnungen erlaubt werden soll, z. B. um Gespräche auf der Parkbank **ohne hinreichende rechtsstaatliche Hürden** zu belauschen. Dies rechtfertigt schlimmste Befürchtungen, dass die Freiheit zur unbefangenen Kommunikation zwischen den Menschen erschüttert wird.

Die Tatbestände sind oftmals unbestimmt gefasst und verstoßen gegen den Grundsatz der Verhältnismäßigkeit. Dies gilt auch für die neue **Kfz-Kennzeichenerfassung**. Alle Menschen, die eine überwachte Straße mit ihrem Fahrzeug benutzen, werden gescannt. Die Freiheit, sich unbeobachtet im Straßenverkehr zu bewegen, wird zum Lotteriespiel für den Bürger.

Neu eingefügt ins Polizeirecht wird die **Telekommunikationsüberwachung** zur Abwehr von Gefahren für Gesundheit und Leben. Juristisch betrachtet ist die Gesundheit z. B. bereits durch eine Ohrfeige in Gefahr. Erwägungen zur Verhältnismäßigkeit finden sich im Gesetzentwurf nicht. Eine verfassungsrechtlich notwendige Einschränkung des „Großen Lauschangriffs" aufgrund des zu weiten Begriffs der „Gesundheit" ist in dem Entwurf ebenfalls nicht vorhanden.

Die im Grundsatz zu begrüßenden Bemühungen zum **Schutz des Kernbereichs** privater Lebensgestaltung werden durch eine auf den ersten Blick „unscheinbare" Formulierung **vollständig entwertet**: Die Polizeibehörden sollen kernbereichsrelevante Gespräche erfassen dürfen, wenn dies im Wege einer automatisierten Aufzeichnung geschieht. Hierin muss geradezu eine Einladung an die Polizei zum verstärkten Technikeinsatz gesehen werden. Der Entwurf widerspricht insoweit den ausdrücklichen Vorgaben des Bundesverfassungsgerichts.

Die Regelungen zum Schutz des Kernbereichs sollten in einer vor die Klammer gezogenen Regelung **sämtliche heimlichen Ermittlungsmaßnahmen** betreffen. Neben der Telekommunikations- und der Wohnraumüberwachung sind alle vergleichbaren Maßnahmen, z. B. die Aufzeichnung des außerhalb von Wohnungen gesprochenen Wortes (z. B. Autofahrt, Parkbankgespräch), in den Kernbereichsschutz einzubeziehen. Dies wurde von der Konferenz der Datenschutzbeauftragten im Oktober 2005 in Lübeck bekräftigt.

www.datenschutzzentrum.de/material/themen/presse/20051028-dsbk-kernbereich.htm

> ***? Kernbereich privater Lebensgestaltung***
>
> *Bei heimlichen Beobachtungen durch staatliche Organe ist zur Wahrung der Menschenwürde stets ein unantastbarer Kernbereich privater Lebensgestaltung freizuhalten. Dieser unantastbare Kernbereich dient dem Schutz der Entfaltung des Menschen bei ihn betreffenden höchst persönlichen Angelegenheiten. Dieser Kernbereich ist nicht relativierbar. Das heißt: Auch überwiegende Interessen der Allgemeinheit können einen Eingriff nicht rechtfertigen.*
>
> *(Entscheidung des Bundesverfassungsgerichts zum „Großen Lauschangriff", 27. TB, Tz. 4.3.1).*

Der Gesetzentwurf enthält **auch positive Ansätze**. Erfreulich ist etwa, dass die Vollprotokollierung bei automatisierten Dateien ausdrücklich vorgesehen und damit einer alten Forderung des ULD nachgekommen wird (Tz. 4.2.4). Das ULD hat zu dem Gesetzentwurf eine ausführliche rechtliche Stellungnahme abgegeben.

www.datenschutzzentrum.de/polizei/stellungnahme-lvwg.htm

Was ist zu tun?
Sollte der Entwurf so Gesetz werden, ist zu erwarten, dass er im Fall einer verfassungsgerichtlichen Überprüfung aufgehoben wird. Er sollte daher nachgebessert werden.

Entschließung der 70. DSB-Konferenz vom 27./28.10.2005

Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen der Sicherheitsbehörden

Aus dem Urteil des Bundesverfassungsgerichts vom 27. Juli 2005 zur präventiven Telekommunikationsüberwachung nach dem niedersächsischen Polizeigesetz folgt, dass der durch die Menschenwürde garantierte unantastbare Kernbereich privater Lebensgestaltung im Rahmen aller verdeckten Datenerhebungen der Sicherheitsbehörden uneingeschränkt zu gewährleisten ist. Bestehen im konkreten Fall Anhaltspunkte für die Annahme, dass eine Überwachungsmaßnahme Inhalte erfasst, die zu diesem Kernbereich zählen, ist sie nicht zu rechtfertigen und muss unterbleiben (Erhebungsverbot). Für solche Fälle reichen bloße Verwertungsverbote nicht aus.

Die Gesetzgeber in Bund und Ländern sind daher aufgerufen, alle Regelungen über verdeckte Ermittlungsmethoden diesen gerichtlichen Vorgaben entsprechend auszugestalten.

Diese Verpflichtung erstreckt sich auch auf die Umsetzung der gerichtlichen Vorgabe zur Wahrung des rechtsstaatlichen Gebots der Normenbestimmtheit und Normenklarheit. Insbesondere im Bereich der Vorfeldermittlungen verpflichtet dieses Gebot die Gesetzgeber aufgrund des hier besonders hohen Risikos einer Fehlprognose, handlungsbegrenzende Tatbestandselemente für die Tätigkeit der Sicherheitsbehörden zu normieren.

Im Rahmen der verfassungskonformen Ausgestaltung der Vorschriften sind die Gesetzgeber darüber hinaus verpflichtet, die gerichtlichen Vorgaben im Hinblick auf die Wahrung des Verhältnismäßigkeitsgrundsatzes – insbesondere die Angemessenheit der Datenerhebung – und eine strikte Zweckbindung umzusetzen.

In der Entscheidung vom 27. Juli 2005 hat das Gericht erneut die Bedeutung der – zuletzt auch in seinen Entscheidungen zum „Großen Lauschangriff“ und zum Außenwirtschaftsgesetz vom 3. März 2004 dargelegten – Verfahrenssicherungen zur Gewährleistung der Rechte der Betroffenen hervorgehoben. So verpflichtet beispielsweise das Gebot der effektiven Rechtsschutzgewährung die Sicherheitsbehörden, Betroffene über die verdeckte Datenerhebung zu informieren.

Diese Grundsätze sind sowohl im Bereich der Gefahrenabwehr als auch im Bereich der Strafverfolgung, u. a. bei der Novellierung der §§ 100a und 100b StPO, zu beachten.

Die Konferenz der DSB erwartet, dass nunmehr zügig die erforderlichen Gesetzgebungsarbeiten in Bund und Ländern zum Schutz des Kernbereichs privater Lebensgestaltung bei allen verdeckten Ermittlungsmaßnahmen aufgenommen und die Vorgaben des Bundesverfassungsgerichts ohne Abstriche umgesetzt werden.

4.2.2 INPOL-SH

INPOL-SH wird nach wie vor ohne ausreichende Errichtungsanordnung betrieben. Das System ist für die Polizei des Landes Schleswig-Holstein ein unerlässliches System für eigene Zwecke und als Schnittstelle zu den gemeinsamen Dateien der Polizeien des Bundes und der Länder beim Bundeskriminalamt (INPOL-Zentral) unverzichtbar.

In einer **ausführlichen Stellungnahme** haben wir gegenüber dem Innenministerium die Mängel der Errichtungsanordnung zu INPOL-SH (27. TB, Tz. 4.2.4) aufgezeigt und Empfehlungen zur Mängelbeseitigung gegeben. Darauf erfolgte in einem Punkt eine Nachbesserung: Zugriffe auf den Datenbestand in INPOL sind zu protokollieren, um mögliche unberechtigte Abrufe im Nachhinein feststellen zu können. Diese Protokolldaten dürfen ausschließlich für Kontrollzwecke genutzt werden, also

- zur Datenschutzkontrolle, Datensicherheit und zur Sicherstellung des ordnungsgemäßen Betriebes der Datenverarbeitungsanlage und
- zur Ausübung von Aufsichts- und Kontrollbefugnissen durch Dienst- und Fachvorgesetzte.

Die Polizei wollte die **Protokolldaten** in INPOL-SH ursprünglich für sämtliche polizeilichen Zwecke, z. B. für Ermittlungszwecke, verwenden, was nach unserem Hinweis auf die Rechtslage zurückgenommen wurde. Die angesprochene Bestimmung in der Errichtungsanordnung hat das Innenministerium gestrichen; unsere Frage nach der bisherigen Nutzung der Protokolldaten blieb allerdings unbeantwortet.

Was ist zu tun?
Das Innenministerium bleibt aufgefordert, eine bewertbare Darstellung von INPOL-SH vorzulegen, um einen zielführenden Dialog fortsetzen zu können. Die Ziele einer rechtskonformen Errichtungsanordnung und eines datenschutzgerechten Verfahrens sind noch nicht erreicht.

4.2.3 @rtus

@rtus ist das Nachfolgesystem von COMPAS für die polizeiliche Vorgangsbearbeitung. Bei dem inzwischen in vielen Polizeidienststellen des Landes eingesetzten System sind so manche datenschutzrechtlichen Fragen noch ungeklärt.

Hinsichtlich der im letztjährigen Tätigkeitsbericht (27. TB, Tz. 4.2.5) unbeantworteten Fragen nach den tatsächlichen Zwecken des Verfahrens und – damit eng verbunden – der **rechtlichen Einordnung** besteht weiterhin keine Klarheit. In seiner ausführlichen Stellungnahme vom Februar 2005 auf eine Errichtungsanordnung mit Stand November 2004 hat das ULD Optimierungsmöglichkeiten aufgezeigt, was zu einer weiterentwickelten Version der gesetzlich zwingend vor-

geschriebenen Errichtungsanordnung führte. Bevor aber im Detail Präzisierungen erfolgen, muss klargestellt sein, dass die Strafprozessordnung neben dem Landesverwaltungsgesetz **nicht** anzuwenden ist. Konflikte birgt weiterhin die Frage der Zuständigkeit für eine neue Vorabkontrolle. Wir haben ebenso eine angemessene Protokollierung der Abrufe angemahnt.

Das Innenministerium betrachtet @rtus als Datei zum Zweck der Auskunftserteilung nach dem Landesverwaltungsgesetz. Es hält aber die Regelungen zum „automatisierten Abrufverfahren“ nicht für anwendbar. Unsere Forderung nach einer **Protokollierung** wurde dahin gehend aufgegriffen, dass eine Aufzeichnung der Zugriffe auf Dokumente „fremder“ Dienststellen implementiert werden soll. Ob dies ausreichend ist, werden wir erst nach Vorliegen der einschlägigen konsolidierten Konzepte beurteilen können.

Das System enthält als Funktionalität die Möglichkeit „horizontaler Blockverbünde“; diese soll – so das Innenministerium – jedoch nicht genutzt werden. Für das ULD stellt sich die Frage, welche **weiteren Funktionalitäten** bei @rtus bestehen, ohne dass diese in der Errichtungsanordnung transparent gemacht werden.

Weitere Fragen im Zusammenhang mit dem Wechsel von COMPAS auf @rtus harren noch auf eine Antwort:

- Wann wird COMPAS für den täglichen Betrieb abgeschaltet?
- Was geschieht mit den Daten von COMPAS? Werden sie migriert und somit Bestandteil von @rtus, oder bleiben sie gespeichert und werden weiter parallel genutzt?
- Gibt es bereits ein datenschutzkonformes Lösungskonzept beim Innenministerium oder beim Landespolizeiamt?

Was ist zu tun?
Nach der Vorlage der ersten Lösungsansätze sind die Konzeptunterlagen und die Errichtungsanordnung gemeinsam vom ULD und Innenministerium auf Schwachstellen zu untersuchen und die rechtlichen Fragen zu klären. Lösungen müssen gefunden werden, wie COMPAS datenschutzrechtlich korrekt abgeschaltet werden kann.

4.2.4 Protokollierung – eine unendliche Geschichte

Nicht protokollierte Verarbeitungsprozesse können nicht überprüft werden; die gespeicherten Daten verlieren ihre Authentizität. Die Verlässlichkeit von Informationen ist für alle Verarbeiter, insbesondere aber für Sicherheitsbehörden, von herausragender Bedeutung, da aufgrund der Informationen Entscheidungen getroffen werden, die Bürgerinnen und Bürger stark belasten können.

Wir fragen uns: Warum müssen Datenschützer für die Protokollierung kämpfen, die eigentlich im wohlverstandenen ureigenen Interesse der Daten verarbeitenden

Stelle liegen sollte? Die Protokollierung beschäftigt Datenschützer bereits, solange es sie gibt. Die Erwägungen zum Sinn der Aufzeichnungen über Zugriffe auf den Datenbestand und Veränderungen sind unverändert geblieben. Geändert haben sich die technischen Möglichkeiten und die Kostensituation für die erforderliche IT-Beschaffung. In früheren Jahren war Datenverarbeitung teuer und weniger leistungsfähig. Aus Datenschutzsicht geforderte Protokollierungen wurden wegen der Kosten für Speicherplatz als nicht praktikabel angesehen. Die Lösung in dieser Not und ein Schritt in die richtige Richtung war eine Teilprotokollierung – die Stichprobenaufzeichnung – von durchschnittlich jedem zehnten Abruf. Inzwischen ist eine **Vollprotokollierung** technisch und finanziell überhaupt kein Problem mehr, aber ...

Der vorliegende Referentenentwurf zur **Novellierung des Landespolizeirechts** (Tz. 4.2.1) berücksichtigt den technischen Stand und verzichtet auf das bisherige Regelungsmerkmal „stichprobenartig“: „Abrufe sind in überprüfbarer Form automatisiert zu protokollieren.“ Diese Änderung begrüßen wir ausdrücklich. Diese Einsicht wird nun hoffentlich die letzten Zweifler an der Notwendigkeit einer Vollprotokollierung überzeugen. Sie sollte schon in den Gesprächen über die Errichtungsanordnungen zu @rtus, INPOL-SH (Tzn. 4.2.3 und 4.2.2) und anderen Dateien zum Tragen kommen. Die Klärung der Details, insbesondere die Festlegung der Dauer und des Umfangs der Protokolldatenspeicherung, ist eine lösbare Aufgabe.

An der Schnittstelle von INPOL-SH zum **INPOL-Verbund beim BKA** erfolgt derzeit landesseitig keine Protokollierung. Das BKA protokolliert seinerseits die Abrufe von Daten des INPOL-Verfahrens nach bundesrechtlichen Bestimmungen. Die Landespolizei kann sich hier durch den Verweis auf die Bundesregelung nicht aus der Pflicht nach Landesrecht entziehen.

Was ist zu tun?
Die polizeilichen Bestrebungen zur Einführung einer umfassenden Protokollierung bei @rtus und bei INPOL-SH sollten konsequent weiterverfolgt werden.

4.2.5 Auskunftserteilung durch die Polizei

Eingaben bestätigen die Zweifel an der Richtigkeit von an Betroffene gegebenen Auskünften über Datenspeicherungen durch die Polizeibehörden des Landes.

Der Bundesbeauftragte für den Datenschutz stellte bei einer Kontrolle im Bundeskriminalamt (BKA) fest, dass die Polizei des Landes Schleswig-Holstein Daten über einen Petenten in den dort geführten Dateien gespeichert hatte, wovon das ULD in einer parallelen Prüfung vom Landeskriminalamt (LKA) nicht unterrichtet worden war. Eine Prüfung der Abteilung Staatsschutz des LKA zeigte, dass der Petent auch noch in zwei **weiteren automatisierten Dateien gespeichert** war, worüber wir auch keine Mitteilung vom LKA erhalten hatten. Unsere ursprüngliche Antwort an den Petenten war somit auch in diesem Punkte fehlerhaft. Wir mussten die unzutreffende Auskunftserteilung durch das LKA beanstanden.

In anderen Fällen monierten wir, dass unsere Auskunftsanfragen über **mehrere Monate vom LKA unbeantwortet** blieben. In einigen Fällen hatte das LKA nicht über bestehende Speicherungen von Polizeien anderer Länder oder des Bundes in Verbunddateien informiert, obwohl dies gesetzlich gefordert wird. Daher mussten wir das Innenministerium und LKA darauf hinweisen, dass

- Auskünfte über Datenspeicherungen bei örtlichen Polizeidienststellen vollständig sein müssen,
- Speicherungen in Dateien anderer Stellen der Landespolizei zu berücksichtigen sind,
- über interne Dateien des Landeskriminalamtes Auskunft erteilt werden muss,
- INPOL-Verbunddateien umfassend abgefragt werden müssen.

Wir haben Vorschläge für die **datenschutzkonforme Ausgestaltung des Auskunftsverfahrens** gemacht und unsere Unterstützung bei der Umsetzung angeboten. Leider wurde das Kooperationsangebot bisher nicht angenommen. Vielmehr teilte uns das LKA mit, es sehe ebenso wie das Innenministerium keine rechtliche Verpflichtung zur Auskunftserteilung über fremde Datenbestände. Hierzu sei man auch nicht berechtigt. Diese unserer Überzeugung nach falsche Ansicht führt dazu, dass Betroffene mit Erkenntnissen durch die Polizei konfrontiert werden, auf die die Polizei des Landes Zugriff hat, die aber bei einer Auskunftserteilung verschwiegen werden.

Das Bundesverfassungsgericht im Volkszählungsurteil:

„Als weitere verfahrensrechtliche Schutzvorkehrungen sind Aufklärungspflichten, Auskunftspflichten und Löschungspflichten wesentlich."

Zweifellos hat das Innenministerium die **Organisationshoheit** über die von ihm zu verantwortenden Verfahren. Dies ist aber kein Grund, Abläufe beizubehalten, die zwangsläufig immer wieder zu rechtswidrigen Auskunftserteilungen gegenüber Betroffenen führen. Unser Beratungsangebot besteht weiterhin.

Was ist zu tun?
Das Landeskriminalamt sollte im Eigeninteresse darauf bedacht sein, das Auskunftsverfahren gesetzeskonform zu gestalten. Das Vertrauen der Bürgerinnen und Bürger in die Arbeit der Polizei würde hierdurch gestärkt.

4.2.6 Rasterfahndung – nutzlos, aber verlängert

Nach den Terroranschlägen 2001 wurde die Rasterfahndung als Wunderwaffe gegen den Terrorismus angepriesen und auf Landesebene gesetzlich eingeführt, aber bis Ende 2005 befristet, um danach die gemachten Erfahrungen auszuwerten. Als die Frist plötzlich ablief, wurde die Gültigkeit der Regelung mit großer Eile trotz fehlender Bewährung verlängert.

Die Rasterfahndung betrifft fast ausschließlich die Daten völlig unbescholtener Bürgerinnen und Bürger. Die Befristung dieser Maßnahme zielte darauf ab, deren

Wirksamkeit zu überprüfen. Doch fand die **geforderte Evaluierung** in Schleswig-Holstein nicht statt und ist offenbar auch nicht mehr geplant. Über Medienberichte sind lediglich bundesweite Zahlen und Erfahrungen bekannt: „Demnach haben deutsche Fahnder über acht Millionen Datensätze ausgewertet – und nur ein einziges Ermittlungsverfahren gegen einen so genannten Terrorschläfer eingeleitet. Allerdings wurde dieses Verfahren auch schon eingestellt – ohne Erfolg."

Die Herausgabe eines internen, für die Innenministerkonferenz erstellten Papiers verweigert das Innenministerium dem ULD. Unseres Wissens enthält auch dieses Papier keine Gründe, an der äußerst aufwändigen, teuren und die Grundrechte massiv einschränkenden Maßnahme der Rasterfahndung festzuhalten. Vor diesem Hintergrund könnte die **Geheimniskrämerei des Innenministeriums** zu verstehen sein.

www.datenschutzzentrum.de/polizei/stellungnahme-rasterfahndung.htm

Was ist zu tun?
Die Rasterfahndung sollte abgeschafft werden.

4.2.7 Beobachtung von Versammlungen im Visier des ULD

Das ULD kontrollierte die Staatsschutzabteilung des Landeskriminalamts (LKA) im Zusammenhang mit der Sammlung von Daten über die Teilnahme an Demonstrationen.

Das Bundesverfassungsgericht hat im Volkszählungsurteil schon 1983 auf die gesellschaftlichen und rechtlichen Risiken einer Beobachtung, Speicherung und Nutzung der Daten von Demonstrationsteilnehmern hingewiesen. Bei unserer Kontrolle im LKA haben wir gravierende Defizite festgestellt und in den folgenden drei Fallkategorien **Beanstandungen** ausgesprochen:

- Das LKA hat die **erlaubte Teilnahme an Veranstaltungen** in – bereits aus anderen Gründen vorhandenen – Kriminalakten als so genannte „**Hinzuspeicherung**" erfasst. Die Polizei darf eine Kriminalakte nur anlegen, wenn im Falle von Straftaten eine Wiederholungsgefahr vorliegt und

Im Wortlaut: Volkszählungsurteil

„... Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. ..."

(BVerfGE 65, 1, 43)

die Speicherung zur Verhinderung von Wiederholungstaten geeignet ist. Hierfür bedarf es einer so genannten Negativprognose. Eine ergänzende Speicherung kann nur zulässig sein, wenn die zusätzlichen Daten selbst einen nachvollziehbaren **Straftatenbezug** aufweisen. Die Erfassung der – erlaubten – Teilnahme an Veranstaltungen in Personenakten läuft auf die Erstellung von Persönlichkeitsprofilen hinaus. Besonders im Hinblick auf die vom Grundgesetz geschützte Demonstrations- und Vereinigungsfreiheit und den für unsere Demokratie notwendigen Schutz weltanschaulicher und politischer Betätigungen ist nach unserer aktuellen Überzeugung das Hinzuspeichern zumeist unzulässig.

- Das Vorgangsbearbeitungssystem **COMPAS** läuft mit der allmählichen Einführung von @rtus aus (Tz. 4.2.3). Es wird im LKA noch mit den Funktionen Posteingangs- und Postausgangsbuch sowie Tagebuch genutzt. Dies ist im Grunde hinnehmbar. Es ist jedoch nicht nachzuvollziehen, weshalb dort keine Datensätze gelöscht werden können. Das LKA meinte, bei diesen Daten im Tagebuch handele es sich um Urkunden, die nicht gelöscht werden dürften. Mit dieser originellen, aber im Datenschutzrecht unbekannten Konstruktion ließen sich die gesamten gesetzlich vorgeschriebenen Löschungsregelungen aushebeln. Das dürfte auch das LKA nicht wollen. Nach Einführung des neuen Systems **@rtus** wird möglicherweise ein Teil der Daten für die Aufgabenerfüllung des LKA noch erforderlich sein, während der überwiegende Teil der gespeicherten personenbezogenen Daten löschungsreif ist: Es geht kein Weg daran vorbei, dass die COMPAS-Daten löschbar sein müssen und dann auch tatsächlich gelöscht werden.

- Das LKA betreibt automatisierte Dateien mit den Bezeichnungen „**Innere Sicherheit Schleswig-Holstein (ISSH)**“ und „**Warndatei Rechts**“ (Tz. 4.2.8). Darin werden neben Daten zu Personen und begangenen Straftaten, die dem „Kriminalpolizeilichen Meldedienst“ unterliegen, auch sonstige Erkenntnisse gespeichert, z. B. **Angaben zu Kfz-Haltern**, die ihr Fahrzeug in der Nähe von Veranstaltungen geparkt haben. Auch hier führt ein erlaubtes Verhalten zu nachhaltigen Datenspeicherungen in automatisierten Dateien, für die es keine rechtliche Grundlage gibt. Ein weiteres Problem ist, dass die Datei „ISSH“ ohne gültige Errichtungsanordnung geführt wird.

> ***Im Wortlaut: Art. 8 Grundgesetz***
>
> *(1) Alle Deutschen haben das Recht, sich ohne Anmeldung und Erlaubnis friedlich und ohne Waffen zu versammeln.*
> *(2) Für Versammlungen unter freiem Himmel kann dieses Recht durch Gesetz oder aufgrund eines Gesetzes beschränkt werden.*

In einer knappen E-Mail antwortete das LKA auf unsere Beanstandungen. Darin wurden hausinterne Prüfungen unter Beteiligung des Innenministeriums angekündigt. An COMPAS aber möchte das LKA keine Änderungen vornehmen. Die Staatsschutzabteilung will die gesetzliche **Löschungspflicht per Dienstanweisung** in den Griff bekommen, auf die wir mit Interesse warten.

Anlässlich der Beobachtung von **Demonstrationen gegen die Hartz-IV-Gesetze** baten wir das LKA im November 2004 um eine Stellungnahme. Selbst mehrfache Erinnerungen und die Androhung einer Beanstandung mit Fristsetzung veranlassten es nicht zur Antwort. Nachdem wir diese Auskunftsverweigerung im September 2005 beanstandeten, erhielten wir im Dezember eine uns wenig befriedigende Antwort.

Was ist zu tun?
Das Innenministerium ist gehalten, die zur Führung von Kriminalakten bestehenden Richtlinien zu überarbeiten. „Hinzuspeicherungen" und weitere darin vorgesehene Dateispeicherungen verletzen die Grundrechte und die Normen des Landesverwaltungsgesetzes.

4.2.8 Lageberichte – gute Kooperation mit der Polizei

Der behördliche Datenschutzbeauftragte einer Polizeidirektion fragte beim ULD zu den Datenschutzanforderungen bei periodisch erscheinenden Lageberichten der Staatsschutzabteilung einer Bezirkskriminalinspektion an. Die Bewertungen des ULD wurden als Grundlage für die behördeninterne Kontrolle verwendet – ein Musterbeispiel für effektive und sinnvolle Zusammenarbeit.

Die Lageberichterstellung erfolgte aufgrund einer Leitlinie des Innenministeriums aus dem Jahr 2000, die eine sehr **niedrige Verdachts- und Einschreitschwelle** vorsieht. Die Berichte enthalten neben Sachangaben auch namentlich genannte Personen, bei denen die Voraussetzungen für eine Speicherung in Kriminalakten nicht vorliegen. Dabei geht es in der Regel um Fälle kleinerer Kriminalität, z. B. Beschimpfungen bei Nachbarschaftsstreitigkeiten. Bei Lageberichten müssen zumindest die Voraussetzungen für eine Speicherung in Kriminalakten gegeben sein. Die Daten stammen aus Strafverfahren und werden für zukünftige Zwecke vorgehalten bzw. verteilt. Im konkreten Fall waren die Zweifel an der Zulässigkeit der Lageberichte berechtigt. Der behördliche Datenschutzbeauftragte steht nun mit der betreffenden Polizeidirektion zwecks datenschutzkonformer Gestaltung der Lageberichte im Dialog.

Die „**Warndatei Rechts**" des LKA und die dazu vorliegende Errichtungsanordnung können im Zusammenhang mit den Lageberichten gesehen werden. Das LKA reagierte auf unsere entsprechenden Empfehlungen leider erst auf unsere Beanstandung hin (Tz. 4.2.7). Es will nun die Hinweise des ULD unter Berücksichtigung der aktuellen Rechts- und Erlasslage prüfen. Die Errichtungsanordnung werde überarbeitet und die gespeicherten Daten entsprechend den Vorgaben überprüft. Das LKA will das Thema „Speicherung erlaubten Verhaltens" grundsätzlich aufbereiten. Wir sind gespannt.

Was ist zu tun?
Soweit Lageberichte personenbezogene Daten enthalten, sind die Vorschriften des Landesverwaltungsgesetzes über die Speicherung in polizeilichen Dateien strikt zu beachten. Die Angabe konkreter Beschuldigtennamen in Lageberichten sollten die Polizeibehörden vermeiden.

4.2.9 Fußball-WM 2006 führt zur Durchleuchtung

Die Fußballweltmeisterschaft bringt gleich zwei datenschutzwidrige Verfahren mit sich. Die Sicherheitsbehörden sollen in einem unzulässigen Akkreditierungsverfahren Mitarbeiter und freiwillige Helfer durchleuchten. Die Daten der Zuschauer werden beim Kartenkauf in einem heiklen Ticketingverfahren gecheckt.

2006 findet in Deutschland die Fußballweltmeisterschaft statt. Aktiv an der Durchführung dieser Veranstaltung werden – nach vorsichtigen Schätzungen der Veranstalter – ca. **250.000** Menschen beteiligt sein, die zu bestimmten nichtöffentlichen Bereichen der Stadien Zutritt erhalten. Diese sollen nun alle in einem **Akkreditierungsverfahren** auf ihre Zuverlässigkeit überprüft werden. Betroffen sind u. a. Journalisten, Sicherheitspersonal, Mitarbeiter von Hilfsorganisationen und Sanitätsdiensten, Personal im gastronomischen Bereich, Reinigungskräfte, Begleitpersonal sowie andere Servicebedienstete aller Sparten.

Hierbei ist ein umfassender Datenabgleich der betroffenen Personen mit den Beständen der Sicherheitsbehörden vorgesehen. **Landeskriminalämter** und Ämter für Verfassungsschutz sollen ein Votum zu jeder Person abgeben, das vom BKA gesammelt und dem DFB mitgeteilt wird. Dieses gemeinsam von Veranstaltern und Sicherheitsbehörden entwickelte Überprüfungsverfahren greift wegen folgender Mängel unzulässig in grundrechtlich geschützte Positionen der Betroffenen ein:

- fehlende gesetzliche Eingriffsgrundlage,
- Zweifel an der rechtlichen Wirksamkeit der eingeholten Einwilligungserklärungen,
- Zweifel an der Verhältnismäßigkeit der Überprüfung,
- Defizite beim Rechtsschutz und beim Auskunftsverfahren.

Eine **gesetzliche Grundlage** für das Verfahren existiert nicht. Das Sicherheitsüberprüfungsgesetz des Landes ist nicht einschlägig. Darüber hinaus sind Überprüfungsverfahren nicht möglich.

Die **Einwilligung** der Betroffenen kann daneben keine Grundlage sein, sie ist selbst in den gesetzlich geregelten Verfahren eine zusätzliche Verfahrensvoraussetzung. Im Akkreditierungsverfahren sollen die Arbeitnehmer gegenüber ihren Arbeitgebern eine Einwilligungserklärung abgeben. Aus Sorge um den Arbeitsplatz wird kaum jemand die Einwilligung verweigern. Von einer **freiwilligen** Einwilligung kann dann kaum gesprochen werden.

Zudem ist nicht ausreichend sichergestellt, dass die Einwilligung wirklich von der betroffenen Person stammt. Die Sicherheitsbehörden sollen sich mit der allgemeinen Aussage der Veranstalter begnügen, der jeweilige Arbeitgeber habe ihm gegenüber durch einen Mausklick im Internet bestätigt, dass der Betroffene eingewilligt habe. Damit erhalten das LKA und die Abteilung für Verfassungsschutz

keinen authentischen Nachweis, der die Urheberschaft der einwilligenden Person sicherstellt.

Die **Verhältnismäßigkeit** des Verfahrens ist ebenfalls nicht gewährleistet. Nicht nur die ungewöhnlich hohe Zahl der Betroffenen und eine offenbar sehr weite Ausdehnung der Sicherheitszonen machen stutzig. Das Verfahren kann in Einzelfällen bis zum Arbeitsplatzverlust führen. Sicherheitsbedenken, die zum Ausschluss von der WM führen, können schon durch eine den Verfassungsschutzbehörden bekannte frühere politische Betätigung oder durch eine reine Verdachtsspeicherung begründet sein. Ob Betroffenen die zugrunde liegenden Daten im Auskunftsverfahren bekannt werden und ob diese sich ausreichend dagegen wehren können, bleibt fraglich. Eine Anhörung im Verfahren ist nur sinnvoll, wenn die betroffene Person weiß, um welche Daten es geht.

Hier wird bundesweit ein unzulässiges Verfahren am Gesetzgeber vorbei etabliert. Die beteiligten Stellen schaffen so neue Eingriffsbefugnisse für die Sicherheitsbehörden auf der Basis zweifelhafter Einwilligungserklärungen der Betroffenen. Alle am Verfahren Beteiligten, auch das Land, setzen sich unnötigen **Prozess- und Schadenersatzrisiken** aus.

@ www.datenschutzzentrum.de/material/themen/divers/fussball.htm

Beim **Ticketingverfahren** ist grundsätzlich zu fragen, ob mit der Personalisierung der Eintrittskarten und mit Datenabgleichen überhaupt ein Sicherheitsgewinn erzielt werden kann. Die Veranstalter erheben in jedem Fall von den Fußballfans weit mehr Daten als notwendig. Die Stadionbesucher müssen zahlreiche persönliche Angaben machen, bis hin zur Lieblingsmannschaft und zur Personalausweisnummer. Die Eintrittskarten sind mit RFID-Chips versehen, die grundsätzlich eine Lokalisierung im Stadion ermöglichen. Die auf dem Chip gespeicherten Daten können jederzeit mit denen in einer Datenbank verknüpft werden, um einen direkten Personenbezug herzustellen.

@ www.datenschutzzentrum.de/allgemein/wmticket.htm

Die **Datenschutzbeauftragten des Bundes und der Länder** haben frühzeitig auf die Defizite des Akkreditierungsverfahrens und auch des Ticketingverfahrens hingewiesen. Die Veranstalter und Sicherheitsbehörden waren jedoch nicht zu grundlegenden Veränderungen der Verfahren bereit, sondern haben sich allenfalls auf kleine Zugeständnisse eingelassen, etwa beim Akkreditierungsverfahren auf eine Erweiterung der Datenschutzinformation. Wir haben den Landtag Schleswig-Holstein, das Landeskriminalamt und den Verfassungsschutz über unsere Datenschutzbedenken informiert.

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

Was ist zu tun?
Die Akkreditierung darf nicht ohne Rechtsgrundlage in einem zweifelhaften Verfahren betrieben werden. Zumindest dessen Umfang und Reichweite müssen eingeschränkt werden.

4.3 Justizverwaltung

4.3.1 Neuregelung der DNA-Analyse zur Strafverfolgung

Im November 2005 trat das Gesetz zur Novellierung der forensischen DNA-Analyse in Kraft, das den Anwendungsbereich dieses Instruments ausdehnt und den Richtervorbehalt schwächt.

Vor der Erhebung der genetischen Muster zur Speicherung in der BKA-Datei muss eine so genannte **Negativprognose** erfüllt sein, die in Zukunft leichter möglich ist. Die eingrenzenden Beispiele, wann eine Straftat von erheblicher Bedeutung vorliegt, wurden abgeschafft. Nach der Neuregelung ist zudem eine Speicherung in der DNA-Datei auch bei wiederholten Straftaten der einfachen und mittleren Kriminalität (z. B. Diebstähle) möglich.

Negativprognose:

1. *Straftat*
   a) *von erheblicher Bedeutung oder Wiederholung einer nicht erheblichen Straftat, wenn gleichwertig, oder*
   b) *Straftat gegen die sexuelle Selbstbestimmung*
2. *Gefahr der Wiederholung einer Straftat von erheblicher Bedeutung*

Der Richtervorbehalt wird dadurch geschwächt, dass die Ermittlungsbehörden die DNA-Probe nunmehr aufgrund einer bloßen **Einwilligung** der betroffenen Person nehmen und auswerten können. Im Strafverfahren befinden sich die Betroffenen in der Regel in einer **Drucksituation**, in der sie die Tragweite einer Entscheidung nicht überblicken. Damit ist die Freiwilligkeit solcher Einwilligungen zweifelhaft, was zur Unwirksamkeit im Einzelfall führen kann.

Mit der Einwilligung zur Speicherung in der DNA-Datei wird den Betroffenen abverlangt, sich selbst eine Negativprognose auszustellen: Wer zustimmt, bestätigt damit nicht nur, dass er durch ein schwer wiegendes kriminelles Verhalten Anlass für eine Speicherung gegeben hat, sondern auch, dass von ihm nach wie vor eine Wiederholungsgefahr ausgeht. Dies kommt einer **Selbstbezichtigung** gleich, die niemandem zuzumuten ist.

Betroffene können die erteilte Einwilligung widerrufen. Der **Widerruf der Einwilligung** muss sich nach unserer Rechtsauffassung auf die Speicherung in der DNA-Datei auswirken.


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

Was ist zu tun?
Die Vereinbarkeit der Regelungen mit unserer Verfassung ist fraglich. Ermittlungsbehörden müssen die Betroffenen vor der Einwilligung zumindest umfassend aufklären und dabei insbesondere auf die Freiwilligkeit der Einwilligung, die Widerrufsmöglichkeiten, die Speicherungsdauer und die Weitergabe der Daten hinweisen.

4.3.2 Warum waren Sie in der Nähe des Tatortes?

Die Ermittlungsbehörden führen zunehmend Funkzellenabfragen durch. Hierbei werden alle Personen erfasst, die mit ihrem Mobiltelefon zu einem bestimmten Zeitraum innerhalb eines bestimmten Bereiches um einen Tatort kommuniziert haben.

Von persönlich betroffenen Journalisten wurden wir über die Praxis einer **neuen Ermittlungsmethode** informiert: Nach einer Brandstiftung in Bad Segeberg und einem Mord bei Ödendorf waren diese ebenso wie hunderte anderer Handynutzer angeschrieben bzw. angerufen und zur Straftat befragt worden. Viele Betroffene hatten – nicht ganz zu Unrecht – den Eindruck, sie würden dieser schweren Straftaten verdächtigt.

Unsere Prüfung zeigte, dass die eingesetzte Ermittlungsmaßnahme und der Umgang mit den erhobenen Daten problematisch sind. Die **Abfrage der Handyverbindungsdaten** darf sich nach dem Gesetz nur gegen Personen richten, die konkret in einem Strafverfahren Beschuldigte sind oder die für einen Beschuldigten Nachrichten übermittelt haben. In beiden Fällen hatten die Strafverfolgungsbehörden die erfassten Personen jedoch als Zeugen vernommen.

So haben die Ermittler im Bad Segeberger Fall an 641 Betroffene Fragebögen mit Zeugenbelehrung versandt, in denen nach dem Aufenthaltsort in der Tatnacht und nach besonderen Wahrnehmungen gefragt wurde. Sie wurden darauf hingewiesen, eine Überprüfung habe ergeben, dass mit ihrem Handy in der genannten Zeit **in der Nähe des Tatortes telefoniert** wurde. Für die Betroffenen war nicht eindeutig klar, dass gegen sie kein Tatverdacht besteht. Die Aussageverweigerungsrechte von Beschuldigten gehen weiter als die von Zeugen. Wir haben beanstandet, dass die Betroffenendaten zur Zeugenbefragung genutzt wurden.

Die Regelung in der Strafprozessordnung mag wegen ihrer unklaren Formulierung zu einer extensiven Anwendung einladen. Dies legitimiert aber nicht den äußerst sensiblen Eingriff bei einer derart großen Zahl von Menschen. Die Funkzellenabfrage greift in das **Telekommunikationsgeheimnis zahlreicher unbescholtener Bürgerinnen und Bürger** ein. Unter Umständen können mehrere tausend Nutzer von Mobiltelefonen betroffen sein. Deshalb sollten die Strafverfolgungsbehörden von diesem Instrument nur in eng begrenzten Ausnahmefällen Gebrauch machen. Die Gerichte sind nach der Rechtsprechung des Bundesverfassungsgerichts aufgefordert, die Verhältnismäßigkeit der Anordnungen im Einzelfall aufgrund der Tatortfakten zu begründen. Bevor eine Ansprache als Beschuldigter erfolgt, muss die Konkretisierung des Verdachts erfolgt sein.

Was ist zu tun?
Der begonnene Dialog zwischen Staatsanwaltschaft und ULD sollte fortgesetzt werden, um klare Kriterien für den Umgang mit den erlangten Daten zu finden.

4.4 Verkehr

4.4.1 Bezahlung der Parkgebühren per Handy

In Deutschland ist bereits in verschiedenen Städten die Bezahlung von Parkgebühren über Handy möglich. Entsprechende Pläne gibt es auch in Schleswig-Holstein. Diese neuen Systeme werfen neue Datenschutzfragen auf.

Handybezahlsysteme ermöglichen den Kunden, hier den Kraftfahrern, bargeldlos über eine monatliche oder sonstige Abbuchung per **Kreditkarte oder Einzugsermächtigung** Kosten oder Gebühren zu begleichen. Die jeweilige Kommune schließt einen Vertrag mit einem Systembetreiber ab, in dem sich dieser verpflichtet, das System zu installieren, die Parkgebühren einzuziehen und diese an die Kommune abzuführen.

Der Benutzer muss sich zunächst bei dem Systembetreiber anmelden und hierbei seine Adressdaten, Kontodaten, Kfz-Kennzeichen und Handyrufnummer angeben. Er erhält daraufhin eine **Identifikationsnummer**, die er an oder in seinem Auto sichtbar anbringen muss. Möchte der Nutzer den Service in Anspruch nehmen, teilt er der Betreibergesellschaft über sein Handy telefonisch oder per SMS mit, wo und wie lange er parken möchte. Möchte die Gemeinde ihrerseits prüfen, ob ein parkendes Fahrzeug sich angemeldet hat, fragt der Kontrolleur bei der Betreiberfirma elektronisch nach, indem er sich identifiziert und dann unter Angabe der Identifikationsnummer Auskunft über die Registrierung und die gewählte Parkdauer des Parkenden erhält.

Datenschutzrechtlich ist von Bedeutung, dass die **Kommune** für die Datenverarbeitung **verantwortlich** bleibt. Beauftragt eine Gemeinde einen Dritten mit der Abwicklung und mit dem Inkasso von Parkgebühren, handelt dieser als Auftragsdatenverarbeiter. Daraus folgt, dass die Vorschriften des Landesdatenschutzgesetzes anzuwenden und die Grenzen der Auftragsdatenverarbeitung zu beachten sind:

- Die Beauftragung eines privaten Dritten mit der Abwicklung von Parkgebühren kann nicht dazu führen, dass das **öffentlich-rechtliche Verhältnis**, das zwischen dem Nutzer und der Kommune bei Inanspruchnahme öffentlicher Parkplätze entsteht, verändert wird. Durch eine privatrechtliche Vereinbarung kann eine öffentliche Forderung nicht zu einer zivilrechtlichen gemacht werden. Ausstehende Parkgebühren müssen daher mit den Mitteln des öffentlichen Rechts eingezogen bzw. geahndet werden.
- Dem Betreiber als Auftragnehmer ist es nicht gestattet, mit der Registrierung die Einwilligung in die Beschaffung von Informationen über die **Kreditwürdigkeit** einzuholen.

- Anlässlich der Registrierung beim Betreiber werden personenbezogene Daten der Nutzer verarbeitet. Diese Daten unterliegen der **Zweckbindung**. Die erhobenen Daten dienen ausschließlich der Überwachung der Parkzeiten und der Bezahlung der Parkgebühren. Eine Verwendung zu anderen Zwecken ist nicht gestattet.
- Der Betreiber hat alle technischen und organisatorischen Maßnahmen nach aktuellem Stand der Technik zur Sicherung der Daten vor **unberechtigter** Kenntnisnahme und Veränderungen zu treffen.

Was ist zu tun?
Die Gemeinden sollten bei der Beauftragung von Dritten mit der Abwicklung der Bezahlung von Parkgebühren über das Handy darauf achten, dass die Voraussetzungen und Grenzen der Auftragsdatenverarbeitung eingehalten werden.

4.4.2 Videoüberwachung in öffentlichen Verkehrsmitteln

In Schleswig-Holstein haben einige Verkehrsgesellschaften damit begonnen, ihre Busse mit Videoüberwachungsanlagen auszustatten. Damit soll dem zunehmenden Vandalismus Einhalt geboten werden.

Verkehrsunternehmen wollen den zunehmenden **Vandalismus** in ihren Bussen mit Videoüberwachungstechnik eindämmen – auch in Schleswig-Holstein. Videoüberwachung ist in öffentlich zugänglichen Räumen, soweit erforderlich, zur Ausübung des Hausrechts zulässig, wenn nicht schutzwürdige Belange Betroffener überwiegen. Busgesellschaften sind überzeugt, dass eine Verminderung der Sachbeschädigungen durch Videoüberwachungsmaßnahmen möglich sei. Von einem Unternehmen wurde zunächst nur zu Testzwecken ein videoüberwachtes Fahrzeug eingesetzt; dabei wurde ein Rückgang der Sachbeschädigung fast auf null festgestellt.

Wir dringen aber darauf, dass zumindest der Fahrgastbereich hinter dem Fahrer **frei von Videoüberwachung** gehalten wird. So erhalten Fahrgäste die Möglichkeit, überwachungsfrei befördert zu werden. Außerdem erwarten wir flankierend organisatorische Maßnahmen, z. B. schriftliche Regelungen, für welchen Zeitraum das Bildmaterial gespeichert wird und welche Personen Zugang hierzu bekommen. Zwei vom ULD beratene Verkehrsunternehmen speichern das Bildmaterial für maximal 48 Stunden und bleiben damit unter der zulässigen Höchstgrenze von sieben Tagen, ohne dass Sicherheitseinbußen zu befürchten wären.

Was ist zu tun?
Videoüberwachung sollte als Eingriff in die Persönlichkeitsrechte der Betroffenen nur als letztes Mittel eingesetzt werden. Eine datenschutzfreundliche Gestaltung bedeutet kurze Speicherfristen, die Information der Betroffenen durch ausreichend große Hinweisschilder und die Erkennbarkeit der verantwortlichen Stelle.

4.4.3 Zentralisierung beim Kraftfahrt-Bundesamt führt zu Konflikten

Die bisher bei den Straßenverkehrsbehörden der Kommunen gespeicherten Daten sollen zukünftig ausschließlich beim Kraftfahrt-Bundesamt gespeichert werden. Dort liegen dann auch die Originaldatenbestände und nicht mehr nur „Abbilder".

Führerscheindaten, Kfz-Zulassungsinformationen und die Daten über die Berufskraftfahrer sollen nach dem Willen des Gesetzgebers zukünftig nur noch zentral auf den Rechnersystemen des Kraftfahrt-Bundesamtes (KBA) in Flensburg gespeichert werden. Alle in Deutschland für die Ausgabe von Führerscheinen, Fahrerkarten und Kfz-Zulassungspapieren zuständigen Stellen sollen Speicherungen, Änderungen und Löschungen direkt **online in Flensburg** vornehmen können.

Die Datenbestände, die bisher beim KBA nur zu Abrufzwecken vorgehalten wurden, bekommen dadurch eine neue Qualität. Die Originaldatenbestände bei der dezentralen Datenhaltung lagen jeweils bei den **zuständigen örtlichen Behörden**. Ein elektronischer Zugriff hierauf durch andere Stellen war nicht möglich. Die Verantwortlichkeit für die Authentizität und die Richtigkeit der Informationen lag bei den örtlichen Behörden. Nunmehr erhalten prinzipiell alle Fahrerlaubnisbehörden in Deutschland einen Vollzugriff auf die Daten von ca. 60 Millionen Führerscheininhabern. Dadurch stellen sich völlig neue Fragen hinsichtlich der Datensicherheit bei der Online-Kommunikation und der Sicherstellung der Aktualität, der Richtigkeit und der Nachvollziehbarkeit dieser Informationen.

War bisher das KBA für die dort gespeicherten Informationen verantwortlich und die örtlichen Behörden für die bei ihnen gespeicherten Daten, so stellt sich die rechtliche Situation nunmehr anders dar: Die beim KBA gespeicherten Daten sind von den zuständigen lokalen Stellen jetzt nicht nur abruf-, sondern auch veränderbar. Sie teilen sich die Verantwortlichkeiten mit dem KBA für die so genannten **Verbunddateien**.

Eine Folge ist, dass die Datenschutzbeauftragten der Länder und des Bundes nun gemeinsam die datenschutzrechtlichen Probleme analysieren. Ärgerlich ist, dass die sich ergebenden rechtlichen und technischen Fragestellungen durch den Bundesgesetzgeber nicht vollständig bedacht wurden: Wer ist für was **verantwortlich**? An wen können sich die Betroffenen wenden? Wie erfolgt die Abstimmung bei Konflikten? ... Gesucht sind pragmatische praktische Lösungen.

Was ist zu tun?
Es besteht erheblicher Handlungsbedarf, die rechtlichen und technischen Auswirkungen durch die Zentralisierung der Kfz-Datenbestände zu klären. Beides – Funktionalität und Datenschutz – müssen gewährleistet bleiben.

4.4.4 Protokollierungslücken bei der Polizei erleichtern unberechtigte ZEVIS-Abrufe

Die Polizei ist immer noch nicht in der Lage, sicher nachzuvollziehen, welche Mitarbeiter das Zentrale Verkehrsinformationssystem (ZEVIS), mit dem Kfz-Halterdaten beim Kraftfahrt-Bundesamt abgerufen werden können, genutzt haben.

Die Eingabe eines Petenten ließ vermuten, dass ein Polizeibeamter aus privaten Gründen eine Halterdatenabfrage beim KBA durchgeführt hat. Eine Überprüfung der Protokolldaten ergab tatsächlich eine Halterdatenabfrage zu dem Kfz-Kennzeichen des Petenten. Die weitergehenden Recherchen zeigten dann aber, dass nicht nachvollzogen werden konnte, welche Person diese Abfrage tätigte. Bereits im Jahre 1998 hatten wir aufgrund eines ähnlichen Vorfalles die Polizei aufgefordert, sicherzustellen, dass Datenabfragen über das ZEVIS-Abrufsystem, die ausschließlich aus dienstlichem Anlass erfolgen dürfen, **revisionssicher dokumentiert** werden müssen, um feststellen zu können, welche Person den jeweiligen Abruf durchführt (21. TB, Tz. 4.2.7). Damals erklärte die Polizei ihre Verfahrensvorkehrungen für völlig ausreichend und ignorierte offensichtlich unsere Hinweise und Verbesserungsvorschläge. Der Bundesgerichtshof hat klargestellt, dass unberechtigte ZEVIS-Abfragen kriminelles Handeln darstellen. Wir gehen nicht davon aus, dass Derartiges durch organisatorisches und technisches Unterlassen von der Polizei gedeckt werden soll. Wir vermuten, dass die bekannt gewordenen Fälle nur die Spitze des Eisberges sind.

Was ist zu tun?
Durch Änderung der Verfahrensvorkehrungen muss nachvollzogen werden können, welcher Polizist wann zu welchem Zweck welche ZEVIS-Daten abgerufen hat.

4.5 Soziales

4.5.1 Hartz IV

Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden – so ist das Sozialgeheimnis gesetzlich verankert! Das müssten auch die Arbeitsgemeinschaften bzw. Jobcenter, die Agenturen für Arbeit und die für eine selbstständige Aufgabenwahrnehmung optierenden Kommunen beachten.

Wir berichteten darüber, dass das Sozialgeheimnis bei der Zusammenlegung von Arbeitslosen- und Sozialhilfe oft nicht beachtet wurde (27. TB, Tz. 4.6.1). Ein Jahr danach hat sich nicht viel verbessert – im Gegenteil:

- **Datenschutzgerechte Gestaltung von Antragsvordrucken und Ausfüllhinweisen**

Die Kritik an ihrem 16-seitigen Antragsvordruck war so laut, umfangreich und berechtigt, dass die Bundesagentur für Arbeit (BA) ihre Fehler einräumte und

(Nach-)Besserung gelobte. Gemeinsam mit den Datenschutzbeauftragten des Bundes und der Länder wurden die Vordrucke und Ausfüllhinweise überarbeitet. Wer diese neuen Vordrucke, die bisher aber noch nicht zur Verfügung stehen, verwendet und die Ausfüllhinweise beachtet, der braucht nur wirklich zulässige Fragen beantworten.

Leider haben die BA und die Arbeitsgemeinschaften (ARGEn) bislang nicht überzeugend dargelegt, wie sichergestellt wird, dass zukünftig ausschließlich datenschutzgerecht gestaltete Vordrucke und entsprechende Ausfüllhinweise eingesetzt werden. Nur wenn die Vordrucke zusammen mit den Ausfüllhinweisen verwendet werden, sind Hilfe Suchende ausreichend informiert und in der Lage, die wirklich erforderlichen Angaben zu machen („Paketlösung“).

- **Anforderung von Kontoauszügen**

Bei der Bearbeitung von Anträgen auf Arbeitslosengeld II wird die Vorlage von Kontoauszügen gefordert, mal nur der letzte, mal die der letzten drei oder auch sechs Monate. Manchmal werden Kopien zur Akte genommen; nur gelegentlich wird den Hilfe Suchenden erlaubt, einzelne persönliche Buchungspositionen zu schwärzen. Fast nie erfährt der Betroffene, warum er überhaupt die Kontoauszüge vorlegen soll.

Bei Hilfe Suchenden entsteht der Eindruck, dass bei der Anforderung von Kontoauszügen weites Ermessen und Willkür der einzelnen Sachbearbeiter herrscht. Tatsächlich darf die Aufforderung zur Vorlage von Kontoauszügen nur erfolgen, wenn dies im konkreten Fall erforderlich ist. Dem Hilfe Suchenden muss erläutert werden, was anhand der Kontoauszüge geprüft werden soll. Grundsätzlich dürfen Kontoauszüge nur eingesehen, aber nicht in Kopie zur Akte genommen werden. Der Hilfe Suchende hat das Recht, in begrenztem Umfang einzelne Buchungstexte zu schwärzen.

Da klare Vorgaben der BA fehlen, haben wir gemeinsam mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit und anderen Landesbeauftragten unter

www.datenschutzzentrum.de/material/themen/kontoaus.htm

Hinweise zur datenschutzgerechten Anforderung von Kontoauszügen veröffentlicht.

- **Datenschutzgerechte Gestaltung der eingesetzten EDV-Verfahren (A2LL, coArB ...)**

Arbeitslose müssen intimste Fragen nach Schulden-, Ehe- oder Suchtproblemen beantworten. Wichtig sind daher effektive Sicherungen, um die erhobenen, oft sehr sensiblen persönlichen Daten zu schützen. Schon in unserem letzten Tätigkeitsbericht schilderten wir, dass verschiedene Fachverfahren der BA, z. B. A2LL und coArb, alles andere als datenschutzgerecht gestaltet sind.

Eine allein erziehende Mutter aus dem Ruhrgebiet erzählte ihrem Sachbearbeiter, dass sie den Kindesvater nicht kenne. Das Kind sei Ergebnis einer flüchtigen Bekanntschaft bei einem Fußballspiel des FC Schalke 04 gegen den HSV. Der Sachbearbeiter fertigte ordnungsgemäß einen Vermerk, ergänzt um einige zynische Anmerkungen zur Lebensführung der Hilfe Suchenden. Dieser Vermerk wurde nicht in einer Papierakte abgeheftet, sondern – der modernen Technik sei Dank – im Verfahren coArb niedergelegt, auf das bundesweit über 40.000 Mitarbeiterinnen und Mitarbeiter der BA und der ARGEn Zugriff haben. Nur wenige Tage später kursierte dieser Vermerk zur allgemeinen Belustigung durch die gesamte Republik. Auch in Schleswig-Holstein war die Mutter bald der „Witz des Tages“ und kam so zu zweifelhaftem Ruhm. Der Fall zeigt, wie wichtig effektive technische Schutzmaßnahmen wären.

Die BA und die ARGEn verstehen sich offenbar als eine große Familie, in der es keine Geheimnisse gibt. Daten, die in ihre EDV-Verfahren eingegeben werden, stehen bundesweit allen Anwendern zur Verfügung. Die Verfahren sehen überwiegend keine ausreichenden Löschmöglichkeiten vor. Lesende Zugriffe einzelner Mitarbeiter werden nicht protokolliert.

Vertraulich wurde uns geschildert, dass Mitarbeiter von der BA und den ARGEn die Verfahren zu privaten Zwecken nutzen. Im Handumdrehen und ohne Entdeckungsrisiko können Informationen für Familien- oder Nachbarschaftsstreitereien besorgt werden.

Dieser Zustand ist unhaltbar. Bereits im November 2004 beanstandete der Bundesbeauftragte für den Datenschutz das Fehlen eines ausreichenden Berechtigungs- bzw. Löschungskonzeptes sowie das Fehlen einer Protokollierung der Zugriffe auf Sozialdaten durch die Mitarbeiter.

Geändert hat sich seitdem fast nichts. Die BA spielt offenbar auf Zeit und lässt die ARGEn mit den Problemen alleine. Einzelne ARGEn sind offenbar stärker am Schutz der Rechte der Betroffenen interessiert. Sie reagierten auf die Missstände und speichern ihre Unterlagen wieder in Papierform, um das Vertrauen der Hilfe Suchenden nicht vollends zu verlieren.

- **Datenschutzgerechte Migration der Daten beim Einsatz neuer Verfahren (VAM/VerBIS)**

Die BA vertröstet die Betroffenen damit, dass neue Verfahren wie z. B. VAM/VerBIS entwickelt würden, die allen datenschutzrechtlichen Anforderungen gerecht werden sollen. Die Datenschutzbeauftragten des Bundes und der Länder haben ihre Mitarbeit wiederholt angeboten.

Selbst wenn in der Zukunft neue, datenschutzgerecht gestaltete Verfahren eingesetzt würden, sollten die BA und die ARGEn nicht bei null anfangen. Die Migration der Daten muss datenschutzgerecht erfolgen. Es kann nicht angehen, dass – wie bislang von der BA geplant – völlig veraltete Daten von Bürgerinnen und Bürgern, die irgendwann einmal Kontakt zur BA hatten, ungeprüft in die neuen Verfahren überspielt werden.

- **Datenschutzgerechte Gestaltung der telefonischen Befragung durch die BA: „Datenabgleich durch Vivento“**

Im Sommer 2005 beauftragte die BA das Callcenter von T-Systems „Vivento Customer Services“ mit einer telefonischen Überprüfung von Hilfeempfängern. Ziel sei die „Intensivierung der vermittlerischen Bemühungen“ bzw. die „Bereinigung des statistischen Datenmaterials“. Den Hilfe Suchenden sei es freigestellt, an der Befragung teilzunehmen. Die Betroffenen schilderten jedoch, dass sie massiv unter Druck gesetzt worden seien. Wer nicht antwortete, dem sei mit Leistungskürzung gedroht worden. Offenbar wurden nicht nur die Betroffenen nicht bzw. nicht ausreichend informiert. Auch einzelne ARGEn hatten keine Kenntnis darüber, wie die BA deren Kunden befragte.

Der Bundesbeauftragte für den Datenschutz forderte von der BA ein datenschutzgerechtes Verfahren; insbesondere sollten die Angerufenen vorab schriftlich auf die vorgesehenen Anrufe hingewiesen werden. Der Vorstandsvorsitzende der BA erklärte dazu lapidar, eine Vorabinformation der Betroffenen sei nicht möglich.

Wurde als Anlass für die Befragung zunächst noch die Verstärkung der Vermittlungsaktivitäten genannt, so hieß es im Oktober 2005 bereits, dass das Ergebnis dieser telefonischen Befragung ein deutliches Zeichen dafür sei, dass mit einer Missbrauchsquote „von sicherlich über 10 Prozent“ zu rechnen sei, so der stellvertretende Verwaltungsratsvorsitzende der BA laut Presse. Wer wiederholt nicht ans Telefon ging oder die telefonische Befragung ablehnte, wurde als potenzieller Betrüger eingestuft. Und das, obwohl die Beantwortung der Fragen ausdrücklich freiwillig erfolgen sollte.

Die offenbar unzulänglichen Ergebnisse der schlecht vorbereiteten und rechtlich zweifelhaften Telefonaktion passten scheinbar gut in das Bild, das offizielle Stellen zu dieser Zeit zeichneten: Es wurde der Eindruck erweckt, die immensen Kosten für das Arbeitslosengeld II würden vor allem durch massenhaften Missbrauch und weniger durch echte Bedürftigkeit verursacht. Ein zweifelhafter Höhepunkt war ein so genannter Report des Bundesministeriums für Wirtschaft und

Arbeit, veröffentlicht im Oktober 2005, in dem an ausgewählten Einzelfällen der umfangreiche Missbrauch der Leistungen belegt werden sollte. Nicht gerade von Unvoreingenommenheit zeugte die Sprache dieses Machwerks, sogar von Parasiten war die Rede.

Gleichwohl wurde diese Art des telefonischen Marketings bei der BA wohl als Erfolg angesehen. Im November 2005 wurden wir über ein neues Konzept zur Einrichtung eines „Contact Centers SGB II“ unterrichtet, welches die feste Installation eines Callcenters als Kontaktstelle zu den Hilfe Suchenden vorschlug. Allerdings warf dieses Konzept mehr Fragen auf, als es Lösungen enthielt.


www.datenschutzzentrum.de/material/themen/presse/20051028-dsbk-alg2-telefonbefragung.htm

- **Durchführung von Hausbesuchen**

Hausbesuche sind datenschutzrechtlich nicht grundsätzlich unzulässig. Aufgrund ihres für den Betroffenen besonders belastenden Charakters sind jedoch strenge Anforderungen zu stellen (23. TB, Tz. 4.7.3).

Dass dringender Klärungsbedarf besteht, zeigt die Vielzahl von Eingaben. Eine allein erziehende Mutter klagte, dass zwei ihr unbekannte Außendienstmitarbeiter – ohne sich auszuweisen – ihre Wohnung besichtigen wollten. Für den Fall, dass sie den Hausbesuch verweigern würde, sei ihr eine Leistungskürzung wegen fehlender Mitwirkung angedroht worden. So ließ sie die Mitarbeiter in ihre Wohnung, zeigte alle Räume und begehrte auch nicht auf, als im Schlafzimmer die Kleiderschränke geöffnet und ihre Wäsche begutachtet wurde. Noch Wochen nach dem Hausbesuch wusste sie nicht, warum sie überhaupt Besuch vom Amt bekommen hatte. In einem anderen uns bekannten Fall wurde in Abwesenheit der Eltern ein minderjähriges Kind befragt. Auch von einer heimlichen Observation wurde uns berichtet.

Wiederholt wurde die BA darauf hingewiesen, dass verantwortungsvolles Handeln gefordert ist. Ein strukturiertes Konzept mit Kriterien, wann und wie Hausbesuche vorzunehmen sind, wurde den Datenschutzbeauftragten aber bislang nicht vorgelegt.

Die im Zuge der Missbrauchskampagne im Oktober 2005 gemachte Ankündigung der BA, „über 400 neue Außendienstmitarbeiter“ einzustellen, verwundert. Sollen Beamte der BA aus Nürnberg zukünftig Wohnungen z. B. auch in Schleswig-Holstein durchsuchen?

- **Meldung der Krankenkasse an BMWA**

Dass die BA und manchmal leider auch das Bundesministerium für Wirtschaft und Arbeit (BMWA) über das Ziel hinausschossen, zeigt sich an einem Beispiel: Im März 2005 forderte der Staatssekretär des BMWA die gesetzlichen Krankenkassen auf, Versicherte, die ALG II beziehen, zu kontrollieren. Medizinische

Daten über Erkrankungen sollten dem BMWA gemeldet werden, um die Arbeitsfähigkeit einzelner Hilfeempfänger prüfen zu können.

Das BMWA ist weder Aufsichtsbehörde über landesunmittelbare Krankenkassen, noch darf es Kenntnis haben von den Leistungsfällen. Sensibelste Gesundheitsdaten, die, wenn überhaupt, lediglich die ARGEn benötigen, sollten im Ministerium gesammelt werden. Die AOK Schleswig-Holstein folgte unserer Empfehlung und kam der Aufforderung des BMWA nicht nach.

- **Diskretion und Vertraulichkeit**

In jeder Bank fordert ein Schild die Kunden auf, einen Diskretionsabstand einzuhalten, damit Gespräche vertraulich, also ohne Zuhörer, geführt werden können – eigentlich eine Selbstverständlichkeit. Aber offenbar nicht für jede ARGE.

Betroffene schilderten uns wiederholt, dass bereits in den Eingangsbereichen Fragen zur Schul- und Berufsausbildung oder zu gesundheitlichen Problemen beantwortet werden müssten, auch wenn in der Schlange der Wartenden die Nachbarn große Ohren bekommen. Größere Büros werden genutzt, um zeitgleich mehrere Hilfe Suchende zu bedienen. Türen zwischen den Büroräumen seien ausgehängt. Der Datenschutz bleibt hierbei schon mal auf der Strecke. Mal ehrlich: Wer würde Fragen zu eigenen familiären Problemen wahrheitsgemäß und umfassend beantworten, wenn der Nachbar zuhört?

- **Klärung der rechtlichen Stellung der Arbeitsgemeinschaften (ARGEn)**

Es ist schon lange kein Geheimnis mehr, dass bei der Zusammenlegung von Arbeitslosen- und Sozialhilfe der Datenschutz sträflich vernachlässigt wurde, weshalb sich die Datenschutzbeauftragten über Arbeitsmangel nicht beklagen können. In vielen Fällen ist es erforderlich, offene Fragen vor Ort in den ARGEn zu prüfen.

Die BA und auch das BMWA meinen nach wie vor, dass nicht geklärt sei, ob der Bundesbeauftragte oder die Landesbeauftragten für die Kontrollen zuständig sind, und irren sich: Die ARGEn sind eigenverantwortliche Daten verarbeitende Stellen, die uneingeschränkt der Kontrolle der Landesbeauftragten für den Datenschutz unterliegen. Bei einer Vorortkontrolle waren wir dann mit einer absurden Situation konfrontiert: In die Einzelakten aus Papier wurde uns Einblick gewährt, nicht aber in die zum Gesamtvorgang gehörenden elektronischen Datensätze, ebenso wenig in die Software, in allgemeine Arbeitsmaterialien und selbst nicht in ausgedruckte Screenshots, die unserer Kenntnisnahme dadurch entzogen wurden, dass sie vor der Prüfung in der Akte zusammengeklammert wurden.

In einer auf Bundesebene eingesetzten Arbeitsgruppe arbeitet das ULD gemeinsam mit Vertretern des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz Berlin, Brandenburg und Nordrhein-Westfalen an einer Lösung dieser Probleme. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt öffentlich gefordert – zuletzt anlässlich ihrer Sitzung im

Oktober 2005 in Lübeck –, die gravierenden Mängel beim Arbeitslosengeld II zu beseitigen.

www.datenschutzzentrum.de/material/themen/presse/20051028-dsbk-alg2.htm

Das ULD ist sich seiner Kontroll- und Prüfaufgabe bewusst. Verstöße von ARGEn gegen datenschutzrechtliche Vorschriften wurden in den letzten Monaten konsequent förmlich beanstandet und das Landesministerium als Fachaufsicht unterrichtet. Dieses Vorgehen zeigt Wirkung. In Schleswig-Holstein nehmen die ARGEn ihre Datenschutzverantwortung gegenüber den Hilfe Suchenden zunehmend wahr und suchen in vielen Fragen den Rat des ULD. Dieser konstruktive Dialog wird uns aber auch künftig nicht von Einzel- und Querschnittskontrollen abhalten.

Was ist zu tun?
Die Bundesagentur für Arbeit, das Bundesarbeitsministerium und die sonstigen verantwortlichen Stellen sind verpflichtet, bei der Gewährung von Leistungen nach den Vorschriften des Sozialgesetzbuches II (Arbeitslosengeld II) den Sozialdatenschutz zu beachten.

4.5.2 JobCard-Verfahren – wer ist vertrauenswürdig?

Die bundesweite Einführung des JobCard-Verfahrens ist ein Stück näher gerückt. Die von den Datenschutzbeauftragten geltend gemachten Bedenken bestehen jedoch fort.

Ähnlich wie bei der elektronischen Gesundheitskarte (Tz. 4.6.1) kommt beim JobCard-Verfahren (27. TB, Tz. 2.3) nicht einer Chipkarte die zentrale Bedeutung zu, sondern dem geplanten mächtigen Hintergrundsystem. Die Chipkarte, die künftig jeder Beschäftigte erhalten soll, spielt erst bei der Datennutzung eine Rolle. Datenschutzrechtlich entscheidend ist die umfassende Speicherung aller **Einkommensdaten von allen Arbeitnehmern**, von denen – was heute schon absehbar ist – nur ein geringer Bruchteil tatsächlich benötigt werden wird, denen aber zugleich ein gewaltiges Missbrauchsrisiko innewohnt. Die Einkommensdaten sollen in einer Vielzahl von staatlichen Verfahren, insbesondere im Sozialbereich, genutzt werden können.

Bisher besteht ein Problem darin, dass die eigentlich zur Bereitstellung dieser Daten im herkömmlichen Format verpflichteten Arbeitnehmer ihrer Verpflichtung oft nur unzureichend nachkommen. Oft können sie diese Pflicht nicht mehr erfüllen, z. B. weil das Unternehmen als Arbeitgeber gar nicht mehr existiert. Dies kann für die Betroffenen nachteilige Folgen haben,

wenn sie nicht nachweisen können, dass bestimmte **soziale Leistungsvoraussetzungen**, wie z. B. Beschäftigungszeiten, vorlagen.

Die Kritik der Datenschutzbeauftragten des Bundes und der Länder richtet sich primär gegen die Speicherung von sensiblen Datenmassen, von denen zumindest teilweise erkennbar ist, dass sie nie gebraucht werden. Diese **Vorratsdatenspeicherung** beträfe die überwiegende Zahl von Beschäftigten, die zu keinem Zeitpunkt einen Antrag auf soziale Leistungen stellen, wozu die vorgehaltenen Daten über das Arbeitsverhältnis genutzt werden könnten. Nach der derzeitigen Planung wäre eine legale Nutzung für andere Zwecke als die Ausstellung von Bescheinigungen über das Arbeitsverhältnis ausgeschlossen. Doch befürchten die Datenschutzbeauftragten nicht nur den illegalen Missbrauch der künftig gespeicherten Daten. Es gibt Grund zu der Annahme, dass – wenn einmal diese riesige Datenbank vorhanden ist – der Gesetzgeber den Begehrlichkeiten hieran für weitere Zwecke nachgeben wird.

Trotz dieser grundsätzlichen Bedenken hatten die Datenschutzbeauftragten praktische Vorschläge für technische Sicherungen gemacht. Wir schlugen vor, in einem Gutachten zu prüfen, ob sich eine so genannte Ende-zu-Ende-Verschlüsselung der fraglichen Datensätze der Arbeitnehmer realisieren ließe. Nach dem von den Datenschützern vorgeschlagenen Konzept sollte ein **asymmetrisches Verschlüsselungsverfahren** angewandt werden. Der Arbeitgeber würde mit dem öffentlich verfügbaren Schlüssel des Arbeitnehmers den Datensatz verschlüsseln, bevor dieser an die speichernde Stelle im JobCard-Verfahren übermittelt wird. Dadurch wären die Daten sowohl auf dem Übermittlungsweg als auch für die Betreiber des Servers, auf dem sie gespeichert werden, nicht im Klartext lesbar. Die Lesbarkeit könnte nur vom Versicherten selbst wiederhergestellt werden, der die Daten im Einzelfall – und soweit dies für die Ausstellung bestimmter Bescheinigungen erforderlich wäre – mit seinem privaten Schlüssel dechiffriert.

Dieses Modell der Datenschutzbeauftragten wurde tatsächlich durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) einer **Machbarkeitsprüfung** unterzogen. Daraus ergab sich, dass nur schwer zu lösende Problemkonstellationen entstehen können. Es müssten zusätzliche Anforderungen an die Signaturkarte gestellt werden, die im Signaturgesetz, dem die Karte genügen soll, so nicht vorgesehen sind. Weitere Fragen tauchen auf, wenn die Nutzung der Daten nicht mehr erfolgen kann, weil der Arbeitnehmer seine Karte verliert oder diese aus irgendwelchen Gründen nicht lesbar ist. Zudem bereitet die dauerhafte Speicherung von mit asymmetrischen Verfahren signierten bzw. verschlüsselten Daten nach wie vor im Grundsatz Probleme, da die zur Verschlüsselung verwendeten Schlüssel lediglich einen beschränkten Gültigkeitszeitraum (zurzeit drei Jahre) haben. Dies hätte zur Folge, dass die gesamten Daten in regelmäßigen Abständen umgeschlüsselt werden müssten, was die aktive Teilnahme der Beschäftigten voraussetzt: Die vielen Millionen Beschäftigten müssten alle drei Jahre ein Serviceterminal aufsuchen, um ihre Daten umzuschlüsseln. Diese Argumente führten dazu, dass das Verfahren der Ende-zu-Ende-Verschlüsselung im Kontext der JobCard verworfen wurde.

Die grundsätzlichen Bedenken der Datenschutzbeauftragten liegen weiterhin auf dem Tisch: Ist es verhältnismäßig, eine so große Zahl von Daten Betroffener zu speichern, bei denen absehbar ist, dass die Speicherung für sie selbst keinerlei Relevanz haben wird? Die Bundesregierung sagte zu, eine solche verfassungsrechtliche Prüfung vorzunehmen. Egal wie diese Prüfung ausgehen wird, es muss über zusätzliche Sicherheitsmechanismen nachgedacht werden. Ein Vorschlag der Datenschutzbeauftragten des Bundes und der Länder geht dahin, die Datenhaltung und das operative Geschäft im JobCard-Verfahren jeweils bei unterschiedlichen Stellen anzubinden. Die Datenspeicherung sowie die vorgesehene Ver- bzw. Entschlüsselung bei der Speicherung bzw. bei berechtigten Abrufen der Daten sollte bei einer **unabhängigen Vertrauensstelle** erfolgen. Ein Zugriff auf die Daten könnte so nur durch das Zusammenwirken der operativ mit dem JobCard-Verfahren betrauten Stelle und der vertrauenswürdigen Stelle realisiert werden; es wäre ein funktionelles Vieraugenprinzip gewährleistet.

Darüber hinaus bedarf es der Verbesserung der **Transparenz** für die Betroffenen. Diesen sollte jederzeit die Möglichkeit gegeben werden, abzurufen, welche ihrer Daten gespeichert sind und welche Übermittlungen zur eigenen Person stattgefunden haben.

Was ist zu tun?
Das JobCard-Verfahren harrt immer noch einer sorgfältigen verfassungsrechtlichen Prüfung. In keinem Fall genügen die bisher vorgesehenen verfahrensmäßigen Sicherungen. Es bietet sich die Trennung zwischen operativer Stelle und einem unabhängigen Datentreuhänder an.

4.6 Schutz des Patientengeheimnisses

4.6.1 Die elektronische Gesundheitskarte kommt – nur wann und wie?

Durch Festlegung technischer Standards ist die elektronische Gesundheitskarte ein gutes Stück weitergekommen. Das Datenschutzniveau konnte gewahrt werden trotz mancher Versuche, die klaren gesetzlichen Vorgaben auf technischem Wege einzuschränken.

Seit 2002 (24. TB, Tz. 4.8.2) berichtet das ULD regelmäßig über die Fortschritte bei der Einführung der elektronischen Gesundheitskarte. Dabei ist zwischen der regionalen und der nationalen Ebene zu unterscheiden. In der Region Flensburg ist aus dem dortigen regionalen Praxisnetz das Projekt der **Gesundheitskarte Schleswig-Holstein** entstanden (25. TB, Tz. 4.8.2; 26. TB, Tz. 4.7.6).

Auf Bundesebene war für Anfang 2006 die Einführung einer verpflichtenden elektronischen Gesundheitskarte (eGK) für jeden gesetzlich Versicherten vorgesehen. Dieser ehrgeizige Zeitplan war nicht einzuhalten, doch wird die eGK kommen. Die Grundlage dafür findet sich in einer Vorschrift des fünften Teils des Sozialgesetzbuches, die in vorbildlicher Weise die Autonomie der Patienten umzusetzen versucht. Dem Inhaber der neuen Karte wird danach die Möglichkeit gegeben, selbst zu bestimmen, welche Akteure im Gesundheitswesen welche

Informationen über ihn zur Kenntnis bekommen. Nun besteht die äußerst komplexe Aufgabe, die gesetzlichen Vorgaben in technische Standards umzusetzen: Die Chipkarte mit dem Namen „elektronische Gesundheitskarte“ ist dabei nur ein Instrument (neudeutsch: Token), das in einem **umfassend vernetzten medizinischen Informationssystem** – der so genannten Telematikinfrastruktur – zur Steuerung von Kommunikationsprozessen dient.

Im ersten Quartal 2005 wurden erste Spezifikationen für die technischen Elemente der Telematikinfrastruktur sowie für die Karte selbst vorgestellt. Eine extra hierfür geschaffene Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (**Gematik**) wurde vom zuständigen Bundesministerium für Gesundheit mit der weiteren Fortschreibung der Spezifikationen sowie der nachfolgenden Realisierung beauftragt. Die Gematik wird getragen von den Spitzenorganisationen des deutschen Gesundheitswesens: den Spitzenverbänden der Krankenkassen, der Kassenärztlichen Bundesvereinigung, der Kassenzahnärztlichen Bundesvereinigung, der Bundesärztekammer, der Bundeszahnärztekammer, der Deutschen Krankenhausgesellschaft, den entsprechenden Verbänden und Spitzenverbänden der Apotheker.

Offensichtlich wegen widerstreitenden Interessen der unterschiedlichen an der Gematik beteiligten Stellen kam es zu Schwierigkeiten bei der Fortschreibung der Spezifikationen. Aus Datenschutzsicht bedenklich war, dass technische Standards, die dazu dienen, das **Selbstbestimmungsrecht der Versicherten** auf der Karte umzusetzen, von der Gematik in fortgeschriebener Version der Spezifikationen plötzlich infrage gestellt wurden. Die Datenschutzbeauftragten des Bundes und der Länder unterstützten daher eine Weisung des Bundesgesundheitsministeriums an die Gematik, deren Ziel es ist, die Rechte der Betroffenen bei der Fortentwicklung der technischen Standards und Spezifikationen zu sichern. Die Ende 2005 veröffentlichte erste offizielle Version der technischen Standards enthielt die zur Realisierung des Selbstbestimmungsrechts der Betroffenen erforderlichen Elemente.

Als nächste Schritte bei der Einführung der eGK sind Tests in acht Regionen vorgesehen, u. a. in der **Region Flensburg**. Damit wird die bundesweite eGK mit der „Gesundheitskarte Schleswig-Holstein“ vorbereitet. Gerade im schleswig-holsteinischen Projekt wurden Datenschutzaspekte bisher ernst genommen und umgesetzt.

Bei der Erprobung in den Testregionen werden die **Datenschutzbeauftragten** auf Bundes- und Landesebene eingebunden sein. Das ULD setzt sich im Rahmen des schleswig-holsteinischen Projektes dafür ein, dass bei den weiteren Spezifikationen und Konkretisierungen der Technik ein datenschutzfreundlicher Weg beschritten wird. Alle Beteiligten müssen sich darüber im Klaren sein, dass es angesichts der

Komplexität und des umfassenden Charakters des Vorhabens entscheidend ist, ein valides Konzept aufzubauen und zu realisieren, was Vorrang vor einer schnellen Einführung haben muss.

Selbstbestimmung über die eigenen medizinischen Informationen fordert unter den Bedingungen der Telematikinfrastruktur von den Betroffenen eine erhebliche **Medien- und Technikkompetenz**. Die technische Realisierung genügt nicht. Vielmehr müssen auch Hilfen, insbesondere in Form von Beratung und konkreten Handreichungen für die Versicherten, zur Verfügung gestellt werden. Besonders wichtig ist dies für ältere Menschen, denen oft der intuitive Zugang zur Informationstechnik fehlt.

www.datenschutzzentrum.de/somak/somak05/somak05_gundermann.pdf
www.datenschutzzentrum.de/vortraege/050510_weichert_bsi.htm

Was ist zu tun?
Bei der Einführung der elektronischen Gesundheitskarte muss dem Datenschutz und der Autonomie der Patienten die gleiche Bedeutung beigemessen werden wie den Zielen der Kosteneinsparung und des Effizienzgewinns. Nur ein nachhaltiges und von den Nutzern akzeptiertes System wird erfolgreich sein.

4.6.2 popgen: Forschungsdaten für Generationen

Das in Schleswig-Holstein betriebene Projekt „popgen“ ist das ehrgeizigste seiner Art in Deutschland zum Aufbau einer Biobank. Nach längerem Diskussionsprozess mit dem ULD wurde eine datenschutzkonforme Verfahrensgestaltung erreicht. Ein Datenschutz-Audit ist angedacht.

Der Begriff „Biobank“ bezeichnet die Sammlung von biologischen Proben, aus denen sich die genetische Disposition ihrer Träger erkennen lässt. Zwischen Nord- und Ostsee soll mit dem Projekt „popgen“ die **größte derartige Sammlung in Deutschland** aufgebaut werden. Sie dient dazu, festzustellen, ob genetische Dispositionen im Zusammenhang mit bestimmten Erkrankungen eine Rolle spielen. Langfristig verspricht man sich davon bessere Möglichkeiten der Früherkennung und eventuell Heilung.

Personen, die von bestimmten Krankheiten betroffen sind, werden gebeten, an dem Projekt teilzunehmen. Dazu muss eine Blutprobe abgegeben werden. Aus dieser Probe wird dann in der Universitätsklinik die DNA, also die Erbsubstanz der Patienten ermittelt. Diese Probe wird für die gesamte Projektlaufzeit, vorgesehen sind 30 Jahre, gespeichert. Die **genetischen Muster der Erkrankten sollen mit einer Kontrollgruppe abgeglichen** werden, die möglichst dem Durchschnitt der Bevölkerung in Schleswig-Holstein entsprechen soll. Zu diesem Zweck werden zufällig ausgewählte Personen vom Projekt angeschrieben und um Mitwirkung als Spender von genetischem Material für die Kontrollgruppe gebeten. Die Daten dazu werden aus den Melderegistern des Landes erhoben. Wer an dem Projekt nicht teilnehmen möchte, wird lediglich ein zweites Mal angeschrieben,

danach werden seine Daten komplett gelöscht. Auch nach Abgabe einer Probe werden die Identitätsdaten der Mitglieder der Kontrollgruppe in der Datenbank gelöscht. Damit ist für die Kontrollgruppe sichergestellt, dass es sich um anonymisierte Daten handelt. Allerdings könnte die genetische Probe selbst der Person wieder zugeordnet werden, wenn sie mit einer anderen Probe desselben Individuums verglichen würde.

Die wissenschaftliche Forschung im Rahmen des Projektes „popgen“ wird sich mit bestimmten Sequenzen des Genoms beschäftigen und festzustellen versuchen, ob ein Zusammenhang zwischen bestimmten genotypischen Erscheinungen und Erkrankungshäufigkeiten oder Variationen bestehen. Dazu wollen die Wissenschaftler die DNA der Patientengruppe mit der DNA der Kontrollgruppe vergleichen, um **charakteristische genetische Besonderheiten** aufzuspüren.

Die Untersuchung der DNA muss so erfolgen, dass eine unmittelbare Identifikation des Spenders aus der Patientengruppe ausgeschlossen ist. Dazu sind im Projekt verschiedene **Mechanismen der Pseudonymisierung** vorgesehen. Im Zusammenspiel garantieren diese Mechanismen, dass keine Beeinträchtigungen für das Persönlichkeitsrecht bei der Teilnahme an dem Projekt erfolgen. Eine entsprechende Feststellung konnte das ULD nach Vorlage der vollständigen Unterlagen und genauer Erläuterung bzw. Anpassung des Verfahrens im Januar 2006 treffen.

Um die Datenschutzkonformität umfassend zu dokumentieren und ein nachhaltiges Datenschutzmanagementsystem im Projekt zu verankern, ist vorgesehen, dass ein **förmliches Datenschutz-Audit** für das Projekt durchgeführt werden soll.

Was ist zu tun?
Der Aufbau von Forschungsbiobanken kann in einer Weise realisiert werden, dass die Datenschutzrechte der Betroffenen gewahrt bleiben. Forscher sollten sich dazu mit den Datenschutzbehörden abstimmen und die entsprechenden Verfahren zertifizieren bzw. auditieren lassen.

4.6.3 Neuerungen beim Krebsregister

Der Informationsfluss bei der Meldung von Krebserkrankungen zum Landeskrebsregister soll sich ändern. Die Datenschutzrechte der Betroffenen konnten gewahrt bleiben.

Das schleswig-holsteinische Krebsregister wurde 1997 unter intensiver Mitarbeit des Landesbeauftragten für den Datenschutz konzipiert und aufgebaut. Es soll sämtliche im Lande auftretenden Fälle von Krebserkrankungen erfassen, um Auswertungen vornehmen zu können, die Hinweise geben, wie Krebserkrankungen effektiver verhindert und behandelt werden können (19. TB, Tz. 4.8.1). Die Daten werden durch die Ärzte angeliefert, die neu diagnostizierte Fälle zu melden haben. Bisher hatten die von der Krankheit betroffenen Patientinnen und Patienten die Wahlmöglichkeit zwischen einer **namentlichen und einer anonymen Meldung**.

Im ersten Fall wurde die so genannte Vertrauensstelle mit Informationen über die Krankheit und identifizierenden Angaben der Betroffenen versorgt. Bei der Vertrauensstelle wurden dann die identifizierenden Angaben abgetrennt; diese Daten bleiben ohne Bezug zu den Krankheitsdaten dort gespeichert. Die epidemiologischen Daten, also Informationen über die jeweilige Erkrankung, werden zur Registerstelle weitergeleitet und bei dieser gespeichert. Dort liegt kein unmittelbarer Personenbezug der Krankheitsdaten vor. Bei der anonymen Meldung handelte es sich tatsächlich um ein Pseudonymisierungsverfahren. Anstelle eines Namens wurde lediglich ein Zahlencode nach einer bestimmten Codierungstabelle an die Vertrauensstelle geliefert.

Durch die flächendeckende Einführung des **Mammografie-Screenings** (Tz. 4.6.4) wurde eine Verfahrensänderung erforderlich, da hierbei kontrolliert werden soll, ob diese Maßnahme den gewünschten Erfolg bringt. Dazu ist eine Rückmeldung vom Krebsregister vorgesehen: Es soll erfasst werden, ob es eine signifikant hohe Anzahl von Krebserkrankungen gibt, die auftreten, obwohl die betroffenen Frauen regelmäßig an den Screening-Untersuchungen teilgenommen haben. Auf der Grundlage dieser Erfahrungen will man das Screening verbessern.

Dies machte die Änderung des Krebsregistergesetzes notwendig. Wesentlicher Bestandteil ist eine so genannte **Kontrollnummer**, die mit einem bestimmten geheim gehaltenen Algorithmus aus den Namen der Betroffenen errechnet wird. Eine direkte Rückidentifizierung des Namens aus dem errechneten Code ist ausgeschlossen. Der geheime Algorithmus zur Berechnung der Kontrollnummern wird der zentralen Stelle beim Mammografie-Screening zur Verfügung gestellt. Diese berechnet für sämtliche Teilnehmerinnen der Screening-Untersuchungen die jeweiligen Kontrollnummern und teilt dann der zentralen Mammografie-Stelle mit, ob Krankheitsfälle für die betreffenden Nummern gemeldet wurden. Voraussetzung für diese Rückmeldung aus dem Krebsregister ist die Einwilligung der Betroffenen, die zu Beginn der Screening-Untersuchung eingeholt wird.

Zwecks Berechnung der Kontrollnummern müssen künftig mindestens vorübergehend bei der Vertrauensstelle des Krebsregisters sämtliche Patientinnen mit Krebserkrankungen namentlich erfasst werden. Deshalb wird es künftig keine anonymen Meldungen mehr geben. Gleichwohl bleibt den Betroffenen ein **Wahlrecht**; sie können einwilligen, dass ihre Daten mit Namensbezug für Forschungszwecke zur Verfügung stehen. Ohne diese Einwilligung werden die Identitätsdaten der Patientinnen, also insbesondere Name und genaue Adresse, bei der Vertrauensstelle nach kurzer Zeit gelöscht. Es kommt folglich dort zu keiner länger andauernden Speicherung der identifizierenden Angaben.

Das Gesetz sieht außerdem einige Erleichterungen für bestimmte Verwendungen der Krebsregisterdaten für Forschungszwecke vor. Durch die bundesweit im Einsatz befindlichen einheitlichen Kontrollnummern wird eine **repräsentative Forschung** über Schleswig-Holstein hinaus möglich. Gesundheitsdaten über Krebserkrankungen sind hochsensibel. Nach der Neudefinition des Informationsflusses im Krebsregisterverfahren bleibt es die zentrale Aufgabe für die beteiligten Institutionen, durch die erforderliche Sorgfalt das Patientengeheimnis der Betroffenen zu wahren.

Was ist zu tun?
Der Beachtung der Datensicherheitsmaßnahmen bei Vertrauensstelle und Registerstelle im Krebsregister kommt künftig eine noch größere Bedeutung zu. Die noch nicht bestimmte zentrale Stelle im Mammografie-Screening-Verfahren wird eine ebensolche Sorgfalt an den Tag legen müssen.

4.6.4 Herausforderung: Flächendeckendes Mammografie-Screening

Im Kampf gegen den Brustkrebs wird mit flächendeckenden Reihenuntersuchungen von Frauen in einer bestimmten Altersgruppe ein neues Kapitel aufgeschlagen. Vertrauen in den Datenschutz ist für viele eine entscheidende Teilnahmebedingung.

Nach einem fraktionsübergreifenden Beschluss des Bundestages aus dem Jahr 2002 soll ein flächendeckendes Screening-Programm für **Frauen zwischen 50 und 69 Jahren** durchgeführt werden, um Brustkrebserkrankungen möglichst frühzeitig zu erkennen (Mammografie-Screening). Die Spitzenverbände der Krankenkassen und die Kassenärztliche Bundesvereinigung erarbeiteten Krebsfrüherkennungsrichtlinien für dieses Verfahren. Danach werden alle Frauen der betroffenen Altersgruppe alle zwei Jahre schriftlich zu einer Untersuchung eingeladen. Die dort hergestellten Diagnoseaufnahmen werden durch zwei Ärzte unabhängig voneinander begutachtet; damit wird die Zuverlässigkeit des Befundes erhöht. Das Ergebnis wird den Betroffenen mitgeteilt. Um die Qualität des Verfahrens zu sichern, soll auch eine Rückkopplung vom Krebsregister des Landes Schleswig-Holstein erfolgen. So kann man erfahren, ob ohne Befund im Screening untersuchte Patientinnen danach an Krebs erkrankten. Diese Informationen werden im Krebsregister gespeichert.

Dieses Verfahren bringt eine umfangreiche Verarbeitung sensibler Daten mit sich. Dies beginnt mit der Erfassung der Frauen, die unter die Kriterien für die Einladung fallen. Die Einladung sowie weitere Aufgaben werden jeweils landesweit von einer so genannten **zentralen Stelle** wahrgenommen. Diese erhält die Daten über die einzuladenden Frauen von dem örtlich zuständigen Melderegister. Die Daten dürfen nur für den Zweck der Durchführung des Screenings verwendet werden. Dazu gehört ein erstes Anschreiben an die zu der Zielgruppe gehörenden Frauen und eine Erinnerung, wenn keine Rückmeldung erfolgt. Hierfür ist es erforderlich, dass die zentrale Stelle mit der so genannten Screeningeinheit Daten austauscht. Die Screening-Einheit ist die Stelle, bei der die Untersuchung selbst durchgeführt wird.

Die Krebsfrüherkennungsrichtlinien sehen einige datenschutzfachliche Sicherungen vor. Details sind aber der konkreten Ausgestaltung vorbehalten. Dazu gehört die Frage, welche Organisation die Aufgaben der zentralen Stelle übernimmt. Diese Stelle übernimmt eine hohe Verantwortung, nicht nur im Hinblick auf gesundheitspolitische Fragestellungen, sondern auch bezüglich der Daten, zu denen solche über den Gesundheitszustand gehören.

Es bedarf eines Landesgesetzes als Rechtsgrundlage für derartige medizinische Reihenuntersuchungen. Dieses so genannte **Reihenuntersuchungsgesetz** (RUG), an dessen Entstehungsprozess das ULD beteiligt ist, liegt als Entwurf vor.

Auf der Grundlage des RUG soll eine **Verordnung** erlassen werden, in der die zentrale Stelle bestimmt wird und einige ihrer Aufgaben beschrieben werden. Wir verlangten nachdrücklich eine klare Festlegung zu dieser zentralen Stelle. Die Stelle, der die operativen Aufgaben durch Gesetz übertragen werden, darf diese nicht an dritte Stellen delegieren. Für Schleswig-Holstein sind als zentrale Stelle der Medizinische Dienst der Krankenversicherungen und die Kassenärztliche Vereinigung im Gespräch. Diese Institutionen haben jedenfalls viel Erfahrung im Umgang mit sensitiven medizinischen Daten.

Was ist zu tun?
Die bisherige vorbildliche Einbindung des ULD bei der Weiterentwicklung und Umsetzung des Verfahrens des Mammografie-Screenings und die Berücksichtigung des Datenschutzes durch die Beteiligten muss beibehalten werden.

4.6.5 Verkürzung der Aufbewahrungsfrist von Patientenakten auf zehn Jahre

In Kliniken wurden Patientenakten üblicherweise 30 Jahre aufbewahrt, obwohl die Berufsordnungen der Ärztekammern nur eine Aufbewahrungspflicht von zehn Jahren vorsehen. Nachdem die regelmäßige Verjährungsfrist im Zivilrecht statt bisher 30 nur noch drei Jahre beträgt, können Patientenakten bereits nach zehn Jahren vernichtet werden.

Die Schuldrechtsreform macht es möglich: Überquellende Archive können bereinigt werden. Eine Klinik plante ihr Archiv baulich und organisatorisch umzugestalten und fragte uns: Wohin mit den Unmengen von Patientenakten, die eigentlich keiner mehr braucht? Die **Berufsordnung der Ärztekammer** Schleswig-Holstein sieht, ebenso wie entsprechende Vorschriften in anderen Bundesländern, eine Aufbewahrungspflicht von zehn Jahren vor. Diese Frist ist von Arztpraxen und Kliniken gleichermaßen einzuhalten. Nur in wenigen Bereichen gilt eine längere gesetzliche Aufbewahrungsfrist, so z. B. nach der Strahlenschutz- bzw. der Röntgenverordnung eine Frist von bis zu 30 Jahren.

Die in der Vergangenheit übliche Aufbewahrung von 30 Jahren wurde damit begründet, dass die Verjährung zivilrechtlicher Ansprüche erst nach diesem Zeitraum eintrat. Nach der **Schuldrechtsreform** des Jahres 2002 gilt nunmehr eine regelmäßige Verjährungsfrist von drei Jahren. Diese Frist gilt auch für Ansprüche, die vor 2002 entstanden sind.

Eine über die jetzt maßgebliche Aufbewahrungsfrist von zehn Jahren hinausgehende Speicherung von Patientendaten kann jedoch in bestimmten Behandlungsbereichen **aus medizinischer Sicht** sinnvoll und erforderlich sein, etwa bei Erbkrankheiten, psychischen Störungen oder Transplantationen. Gleichwohl darf auch in diesen Fällen die Erforderlichkeit einer über zehn Jahre hinausgehenden

Aufbewahrung nicht pauschal angenommen werden. Es bedarf vielmehr einer Prüfung im Einzelfall. Entsprechende Regelungen enthält unsere Musterarchivordnung, die wir veröffentlicht haben unter

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

Was ist zu tun?
Daten von Patienten, deren Behandlung abgeschlossen ist, unterliegen der ärztlichen Schweigepflicht und dem Datenschutz. Kliniken müssen Regelungen zur ordnungsgemäßen Führung ihres Archivs erlassen. Dabei ist grundsätzlich eine Aufbewahrungsfrist von zehn Jahren festzulegen. Eine längere Aufbewahrung ist nur noch in begründeten Fällen erforderlich.

4.6.6 Besuch vom Pflegeberater der AOK

Pflegebedürftige Menschen freuen sich meist über Besucher in ihrer Wohnung. Das ist aber kein Grund, dass die AOK als Pflegekasse einfach mal so vorbeischaut.

Eine ältere, allein stehende Dame erzählte ihrem Pflegedienst ganz aufgeregt von einem Telefonanruf. Der Anrufer habe sich als Mitarbeiter der AOK ausgegeben und wollte sie zu Hause besuchen. Ganz allein sollte sie jemanden in ihr Haus lassen. Die Dame hatte Angst. Der Pflegedienst argwöhnte, dass dieser Hausbesuch wohl eher dazu dient, seine Arbeit zu kontrollieren. Beide stellten uns die gleiche Frage: Dürfen Pflegeberater der AOK **Hausbesuche** durchführen?

Die AOK des Landes hat bereits Anfang 2004 Pflegeberater eingestellt. Diese ausgebildeten Altenpflegerinnen und -pfleger sollen Pflegebedürftige, die Leistungen von der Pflegekasse bei der AOK erhalten, und deren Angehörige in Fragen zur häuslichen Pflege beraten. Schließlich gehöre, so die AOK, die Beratung von Versicherten zu ihren Aufgaben. Die Pflegeberatung sei lediglich ein Angebot, das den Versicherten alle Möglichkeiten der Pflegeversicherung aufzeigen soll. Es gehe **nicht um Kontrolle, sondern um Hilfe**. Häufig würden Versicherte nicht alle bzw. nicht die richtigen Pflegeleistungen in Anspruch nehmen.

Die Beratung vor Ort als Hausbesuch sei am sinnvollsten. Der Pflegeberater der AOK schaue sich nicht nur die Wohnung an, sondern auch gleich noch die Pflegedokumentation des Pflegedienstes. So hätte schon vielen geholfen werden können. Mal empfehle man, eine Türschwelle zu beseitigen, damit das Leben im Rollstuhl leichter wird. Mal gebe es praktische Tipps für die Angehörigen, wie eine pflegebedürftige Person am einfachsten aus dem Bett zu heben sei. Nebenbei riet man den Versicherten aber auch, bestimmte Leistungen der Pflegedienste nicht in Anspruch zu nehmen, da diese doch eher überflüssig seien. Die Kasse **spart diese Ausgaben** und reduziert den Umsatz der Pflegedienste. Diese befürchten aber auch, dass derartige Kontrollen das Vertrauen der Pflegebedürftigen beeinträchtigen.

Die AOK ist kein Unternehmen wie jedes andere. Als gesetzliche Krankenkasse bzw. Pflegekasse hat sie einen gesetzlichen fest definierten Auftrag, der den äußeren Rahmen ihrer Datenverarbeitung setzt, welcher nicht eigenmächtig erweitert werden kann. Ein Blick ins Gesetz zeigt schnell, dass eine Pflegeberatung vorgesehen ist, aber nicht durch die Kasse selbst, sondern durch einen neutralen Pflegedienst bzw. einer neutralen Pflegefachkraft. Der Hintergrund ist klar: **Beratung und Kontrolle** sollen strikt voneinander getrennt sein. Eine Pflegekasse muss zwangsläufig auch aufs Geld schauen. Dies kann einer sinnvollen Beratung entgegenstehen.

Die AOK selbst hat nur einen **allgemeinen Beratungsauftrag**. Hierfür kann sie ausgebildete Fachkräfte einstellen. Sie darf allgemein, z. B. in ihren Mitgliederzeitschriften, auf dieses Angebot hinweisen. Jeglicher Druck der Pflegekasse, eine derartige Beratungsleistung wahrzunehmen, ist unzulässig. Erst wenn ein Versicherter selbst aktiv wird und die Beratung ausdrücklich einfordert, darf die Kasse diese durchführen. Wünscht der Versicherte einen Hausbesuch, dann ist auch dies möglich. Eine Einsichtnahme in die Pflegedokumentation kommt nur in Betracht, wenn dies für die Durchführung der Beratung unabdingbar ist und der Versicherte sich damit aus freien Stücken einverstanden erklärt hat.

Was ist zu tun?
Pflegeberatung hat grundsätzlich von Pflegediensten bzw. besonderen Pflegefachkräften zu erfolgen. Lediglich im Rahmen des allgemeinen Beratungsauftrages darf eine Pflegekasse Beratungen anbieten. Eine Beratung kann nur dann erfolgen, wenn der Versicherte von sich aus diese ausdrücklich einfordert.

4.6.7 Pflegedienste: Welches Datenschutzrecht gilt?

Ambulante bzw. stationäre Pflegedienste müssen als nichtöffentliche Stellen den dritten Abschnitt des Bundesdatenschutzgesetzes beachten, darüber hinaus aber auch die Vorschriften zum Patientengeheimnis.

Das Strafgesetzbuch stellt Ärzte, Zahnärzte, Apotheker und **Angehörige eines anderen Heilberufs**, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert, unter Strafe, wenn diese das Patientengeheimnis verletzen.

Andere Heilberufe im Sinne des Strafgesetzbuches sind solche, deren Abschlüsse in Heilberufegesetzen geregelt sind, so z. B. im Gesetz über die Berufe in der Krankenpflege bzw. im Gesetz über die Berufe in der Altenpflege. **Kranken- oder Altenpflegerinnen und -pfleger** – ob nun angestellt oder selbstständig tätig – müssen also die Vorschriften zum Patientengeheimnis, oft auch als ärztliche Schweigepflicht bezeichnet, beachten. Bei Verletzung droht den Mitarbeiterinnen und Mitarbeitern der Pflegedienste eine Gefängnisstrafe von bis zu zwei Jahren.

Ambulante und stationäre Pflegedienste verfügen über zum Teil sensibelste soziale, biografische und medizinische Informationen ihrer Pflegebedürftigen. Diese

Daten unterliegen zu Recht den strengsten datenschutzrechtlichen Anforderungen. Pflegedienste müssen auch unter bestimmten Bedingungen einen **betrieblichen Datenschutzbeauftragten** bestellen. Findige Unternehmer nutzten diese Situation und verschickten Werbebriefe, in denen sie damit drohen, dass die Aufsichtsbehörde – also das ULD – bei Nichtbeachtung Geldbußen von bis zu 25.000 Euro verhängen würde.

Wir erhielten viele Anrufe von besorgten Pflegediensten.

- Welche Daten dürfen in der Pflegedokumentation gespeichert werden?
- Wie schütze ich meine Daten vor dem Zugriff Unbefugter?
- Dürfen Daten von Pflegebedürftigen elektronisch gespeichert und per E-Mail verschickt werden?
- Welche Daten darf ein Pflegedienst einer Pflegekasse übermitteln?
- Welche Rechte hat der Medizinische Dienst der Krankenversicherungen (MDK)?

Im vergangenen Jahr haben verschiedene Verbände wie z. B. der Bundesverband privater Anbieter sozialer Dienste e.V. (bpa) oder der Deutsche Paritätische Wohlfahrtsverband (DPWV) erkannt, wie wichtig die Beantwortung derartiger **Fragen für die tägliche Arbeit** in den Pflegediensten ist, und gehandelt. Gemeinsam mit der DATENSCHUTZAKADEMIE Schleswig-Holstein wurden Fortbildungsveranstaltungen für die Mitglieder organisiert, die sich großer Nachfrage erfreuten.

Was ist zu tun?
Die notwendigen Kenntnisse für Kranken- oder Altenpflegerinnen und -pfleger in ambulanten oder stationären Pflegediensten vermittelt die DATENSCHUTZAKADEMIE Schleswig-Holstein durch gezielte Fortbildungen.

4.6.8 Kostensenkung bei den Krankenkassen – nicht um jeden Preis

Disease-Management-Programme dienen nicht nur der Optimierung der Behandlung von chronisch Kranken, sondern auch der Kostensenkung bei den gesetzlichen Krankenkassen. Wie können nun die Versicherten zur Teilnahme bewegt werden? Unzulässig ist es jedenfalls, dazu Daten von den behandelnden Ärzten zu erheben, wie es im Berichtszeitraum in Schleswig-Holstein vorkam.

Die Patienten profitieren von Disease-Management-Programmen (DMP) dadurch, dass deren Behandlung an bestimmten Standards ausgerichtet und der Erfolg überprüft wird. Aber auch die Krankenkassen ziehen hieraus ihren Nutzen, da für DMP besondere Mittel zur Verfügung stehen. Die Kassen haben ein erhebliches Interesse daran, neue Patienten für DMP anzuwerben. Dazu dürfen die Krankenkassen die Patienten unmittelbar anschreiben und auf diese Programme hinweisen. Dies halten einige Kassen jedoch offenbar nicht für ausreichend. Sie wendeten sich **unmittelbar an die behandelnden Ärzte** und baten diese, bestimmte Patienten auf die Teilnahme am DMP anzusprechen oder dies gar nahe zu legen.

Die Kassenärztliche Vereinigung Schleswig-Holstein (KV SH) schilderte uns die Praxis einer großen, bundesweit tätigen Angestelltenkrankenkasse. Den Ärzten wurden ausführliche so genannte **Potenziallisten** zugesandt. Darin wurden Mitglieder der fraglichen Kasse aufgeführt, die bei dem Arzt in Behandlung waren, mit Versicherungsnummer, Name, Vorname, Geburtsdatum und einigen weiteren Schlüsseldaten. Dazu zählten auch die Anzahl der aufgesuchten Hausärzte sowie teilweise einige Informationen zu Erkrankungen. Die Ärzte wurden gebeten, in dieser Liste eine Rückmeldung an die Kasse einzutragen einschließlich der vermuteten Bereitschaft oder Eignung der Patienten zur Teilnahme am DMP. Wollte der Arzt ankreuzen, dass eine Teilnahme ausscheidet, so sollte er auch den Grund dafür angeben. Als Antwortmöglichkeit wurde vorgegeben, die Erkrankung läge nicht vor, die Diagnose sei zwar richtig, die DMP-Einschreibekriterien seien aber nicht erfüllbar, oder eine abweichende Erkrankung läge vor.

Damit versuchte die fragliche Krankenkasse Daten über die Patienten beim Arzt zu erheben. Der Patient sollte nicht unterrichtet werden. Für diese Erhebung von Daten, die der **ärztlichen Schweigepflicht** unterliegen, gibt es keine Rechtsgrundlage und keine Rechtfertigung. Wir haben daher über die KV SH den Ärzten dringend davon abgeraten, die entsprechenden Listen an die Krankenkasse ausgefüllt zurückzusenden. Anderenfalls könnten sich die Ärzte wegen des Verstoßes gegen das Patientengeheimnis strafbar machen. Wir unterrichteten außerdem den Bundesbeauftragten für Datenschutz und Informationsfreiheit über den Vorgang. Dieser ist zuständig für die Einhaltung der datenschutzrechtlichen Vorschriften bei der fraglichen Krankenkasse.

Was ist zu tun?
Die Ärzte im Land sollten sorgsam auf den Schutz der Daten ihrer Patienten achten, auch und gerade vor unberechtigten Begehrlichkeiten mancher Krankenkasse. Deren Anfragen sind nicht in jedem Fall zulässig.

4.7 Wissenschaft und Bildung

4.7.1 Kindertageseinrichtungen kooperieren mit Grundschulen

Die Zusammenarbeit zwischen Kindertageseinrichtungen und Grundschulen soll nach den Vorstellungen des Bildungsministeriums verbessert werden. Dabei darf der Start ins Schulleben nicht sofort durch elterliches Misstrauen und durch Vorurteile belastet werden.

Im Oktober 2004 gab das Bildungsministerium Empfehlungen zur Zusammenarbeit zwischen Kindertageseinrichtungen und Grundschulen heraus. Danach sollten die Kindertageseinrichtungen die Entwicklungen der Kindergartenkinder **in sozialer, sprachlicher und motorischer Hinsicht** beobachten, die Ergebnisse personenbezogen schriftlich dokumentieren und diese Dokumentationen den Grundschulen vor der Einschulung zur Verfügung stellen. Diese Daten sollten der Leitung der Grundschule im Einschulungsverfahren als Hilfestellung dienen und zugleich eine individuelle Förderung des Kindes in den ersten Grundschuljahren erleichtern.

An den Datenschutz wurde dabei vom Ministerium überhaupt nicht gedacht. Erst durch unsere Nachfragen stellte man fest, dass es für diese personenbezogene Zusammenarbeit keine gesetzliche Grundlage gibt und daher die Einwilligung der Eltern erforderlich ist. Wir haben gemeinsam mit dem Bildungsministerium ein amtliches Muster einer solchen **Einwilligungserklärung** erstellt. Die Schulen wurden angewiesen, personenbezogene Daten von den Kindertageseinrichtungen über die einzuschulenden Kinder nur zu erheben, wenn ihnen eine solche Einwilligungserklärung vorliegt. Dieses Verfahren ist nicht nur rechtlich geboten, sondern auch pädagogisch sinnvoll: Die Eltern werden eingebunden. Deren Verweigerung kann Anlass sein, mit diesen über die Einschulung zu sprechen.

4.7.2 Videoüberwachung an Schulen

Haben Schulen disziplinarische Schwierigkeiten mit den Schülerinnen und Schülern, so denken sie nicht nur an pädagogische, sondern auch an technische Lösungen, z. B. an den Einsatz von Videotechnik.

Die Forderung nach mehr Videoüberwachung an Schulen wird angesichts von Meldungen über Vandalismus und Gewalttätigkeiten auch in unserem Land immer wieder erhoben. Das ULD wird damit von verschiedenen Seiten konfrontiert: von Eltern, von den Schulleitungen und nicht zuletzt auch von Politikern. Dabei steht nicht nur die Sicherheit im Raum, sondern auch die Sorge, dass der Einsatz dieser Überwachungstechniken Gewöhnungseffekte auslöst und Probleme verdeckt, statt diese transparent zu machen. Videoüberwachung löst keine persönlichen oder sozialen Konflikte und baut keine Aggressionen ab. Daher dringen wir darauf, bei einem vermeintlichen Bedarf erst einmal gemäß dem Gebot des Schulgesetzes nach **anderen Lösungen** zu suchen.

Im Wortlaut: § 4 Schulgesetz

Der Auftrag der Schule wird bestimmt durch das Recht des jungen Menschen auf eine seiner Begabung, seinen Fähigkeiten und seinen Neigungen entsprechende Erziehung und Ausbildung sowie durch die staatliche Aufgabe, die einzelnen Schülerinnen und Schüler auf ihre Stellung als Bürgerinnen und Bürger mit den entsprechenden Rechten und Pflichten vorzubereiten. Es ist die Aufgabe der Schule, die geistigen, seelischen und körperlichen Fähigkeiten des jungen Menschen unter Wahrung des Gleichberechtigungsgebots zu entwickeln. Zum Bildungsauftrag der Schule gehört die Erziehung des jungen Menschen zur freien Selbstbestimmung und Achtung anders Denkender, zum politischen und sozialen Handeln und zur Beteiligung an der Gestaltung der Arbeitswelt und der Gesellschaft im Sinne der freiheitlichen demokratischen Grundordnung.

Wir haben uns in wenigen **Ausnahmefällen** davon überzeugen lassen, dass der Einsatz von Videokameras in der Schule gerechtfertigt sein kann. Dies gilt für den Objektschutz, insbesondere zur Nachtzeit. Auch mögen die Vorteile zur Sicherung eines ausschließlich als Fahrradkeller genutzten Raumes gegenüber den nachteiligen Wirkungen des Videoeinsatzes überwiegen.

Generell sollte es aber das gemeinsame Anliegen aller Beteiligten sein, dass die Schule ein Raum der selbstbestimmten Entfaltung ist und nicht der anonymen technischen Kontrolle. In keinem Fall akzeptabel wäre es, wenn aus Sicherheitsgründen der Unterricht überwacht würde.

Was ist zu tun?
Videoüberwachung hat an Schulen grundsätzlich nichts zu suchen. Sollte in Einzelfällen ein Bedarf gesehen werden, so steht das ULD zur Beratung gerne bereit.

4.8 Steuerverwaltung

4.8.1 Verfassungsbeschwerde: Kontenabruf

Die Kontenabfrage wurde im April 2005 in Betrieb genommen. Die Zweifel an der Verfassungsgemäßheit des Verfahrens sind bisher nicht ausgeräumt worden.

Schon im letzten Jahr forderten wir eine Überprüfung und Überarbeitung des **Gesetzes zur Förderung der Steuerehrlichkeit** (27. TB, Tz. 4.9). Durch dieses Gesetz erhalten Finanzbehörden und Sozialämter, BAföG-Stellen, Arbeitsagenturen sowie weitere Sozialleistungsträger die Befugnis, auf die Stammdaten von sämtlichen ca. 50.000.000 Bankkonten und Wertpapierdepots in Deutschland in automatisierter Form zuzugreifen. Die Kreditinstitute sind verpflichtet worden, eine entsprechende Datei vorzuhalten. Abrufbar sind die Adresse, das Geburtsdatum sowie die Nummer sämtlicher Bankkonten, Wertpapierdepots und Bausparverträge bei allen Instituten sowie Datum von Eröffnung und Abschluss der Konten. Auf die Kontenstände und Bewegungen kann auf diese Weise nicht zugegriffen werden.

Durch das Gesetz wird in mehrfacher Weise unverhältnismäßig in das Recht auf informationelle Selbstbestimmung der Betroffenen eingegriffen:

- Das **Gebot der Normenklarheit** ist verletzt. Eine Behörde wird nach dem Gesetz zur Kontenabfrage ermächtigt, wenn sie ein Gesetz anwendet, das „an Begriffe des Einkommenssteuergesetzes“ anknüpft, und wenn eigene Ermittlungen der Behörde angeblich nicht zum Ziel geführt haben oder keinen Erfolg versprechen. Es ist für den Bürger überhaupt nicht ersichtlich, welche Behörden unter welchen Voraussetzungen zur Abfrage tatsächlich berechtigt sind.
- Das verfassungsrechtliche **Gebot der Transparenz** ist verletzt. Der Betroffene erhält von Abfragen keine Kenntnis, es sei denn, es werden weitere Ermittlungen direkt bei ihm aufgrund des Abrufes getätigt.
- Das Gesetz verstößt gegen das **Gebot der Zweckbindung**. Bankdaten werden für Zwecke der Besteuerung und für die Berechnung von Sozial- und staatlichen Leistungen genutzt. Diese Zweckänderung muss jedoch im konkreten Einzelfall durch überwiegende Gemeinwohlbelange gerechtfertigt sein. Dies ist hier schon fraglich, weil das Vertrauensverhältnis zur Bank erheblich beein-

trächtigt ist. Hinzu kommt, dass die Kontendaten über die Finanzbehörden abgefragt werden und an die anderen Behörden zur Berechnung der sozialen Leistungen weitergereicht werden, mit denen die Finanzbehörden sonst nichts zu tun haben. Die zweckwidrige Nutzung von Daten unter dem Steuergeheimnis, durch das Steuerehrlichkeit gewährleistet werden soll, kann nicht im Interesse der Finanzverwaltung liegen.

Über Beschwerden gegen das Gesetz wird das **Bundesverfassungsgericht** voraussichtlich im Jahr 2006 entscheiden. Dieses hatte sich bereits kurz vor In-Kraft-Treten des Gesetzes im April 2005 mit der Kontenabfrage im vorläufigen Rechtsschutzverfahren zu befassen. Es hatte abzuwägen, ob die Nachteile, die durch einen rechtswidrigen Eingriff in die Persönlichkeitsrechte Dritter entstehen, schwerer wiegen als der Schaden, der entstünde, wenn das Verfahren rechtmäßig wäre und nicht eingesetzt werden würde.

In Erwartung dieser einstweiligen Anordnung sah sich das Bundesfinanzministerium gezwungen, einen **Anwendungserlass** zur Konkretisierung des Gesetzes herauszugeben. Dieser sieht u. a. vor, dass

- ein Abruf der Kontenstammdaten nur anlassbezogen und zielgerichtet und unter Bezugnahme auf eindeutig bestimmte Personen zulässig ist,
- die Betroffenen in verschiedenen Verfahrensstadien zu benachrichtigen sind,
- im Bereich der Sozialverwaltung, die über das Finanzamt Zugriff auf die Kontendaten erhalten werden, Einschränkungen gelten,
- ein Kontenabruf als nicht zulässig gilt, wenn es zur Aufklärung des Sachverhaltes ein ebenso geeignetes, aber für den Betroffenen weniger belastendes Beweismittel gibt, etwa die Auskunft durch den Betroffenen.

Allein diese Nachbesserungen per Erlass haben bewirkt, dass das Bundesverfassungsgericht das Kontenabfrageverfahren **vorläufig zugelassen** hat. Es betonte, dass der Ausgang des Beschwerdeverfahrens offen sei. Mögliche Mängel des Gesetzes würden durch den Anwendungserlass „derart abgemildert, dass eine einstweilige Anordnung durch das Bundesverfassungsgericht vor der Entscheidung über die Verfassungsbeschwerden nicht geboten“ sei. Dessen ungeachtet kann ein Erlass ein Gesetz nicht verfassungskonform machen. Die Konkretisierungen des Erlasses müssten in das Gesetz aufgenommen werden. Davon ist aber derzeit keine Rede mehr. Das ULD vertritt darüber hinaus die Ansicht, dass das Verfahren insgesamt in unverhältnismäßiger Weise in das Recht auf informationelle Selbstbestimmung eingreift. Darüber wird das Gericht **im Hauptsacheverfahren entscheiden**.

4.8.2 Einsicht in Steuerakten für Betroffene

Noch immer enthält die Abgabenordnung keinen Rechtsanspruch auf Akteneinsicht für Betroffene. Noch immer verweigert die Finanzverwaltung ihren Steuerbürgerinnen und Steuerbürgern systematisch das diesen verfassungsrechtlich zustehende Recht auf informationelle Selbstbestimmung.

Wieder einmal wurde das Ersuchen eines Betroffenen um Einsicht in seine Steuerakte mit der Begründung abgelehnt, in der Abgabenordnung gäbe es keinen Anspruch auf Akteneinsicht im steuerlichen Verwaltungsverfahren (27. TB, Tz. 4.9.1). Diese zweifellos formal richtige Feststellung ändert nichts daran, dass der Steuerpflichtige einen **verfassungsrechtlichen Anspruch** auch gegenüber dem Finanzamt auf Kenntnis hat, wer was wann und bei welcher Gelegenheit über ihn weiß. Mindeststandard ist die Gewährung von Akteneinsicht nach pflichtgemäßem Ermessen, wobei die Interessen der Behörde gegen die Belange des Betroffenen abzuwägen sind.

Uns gegenüber legte der Betroffene nicht nur ein allgemein persönliches, sondern ein besonderes **rechtliches Interesse** an der Akteneinsichtsgewährung schlüssig dar. Offensichtlich sollte die Frage der Steuerpflicht seiner Aufwandsentschädigung auch mit Wirkung für die Vergangenheit neu bewertet werden. Diese war mehr als ein Jahrzehnt lang als steuerfrei anerkannt worden. Zur Verfolgung seiner Ansprüche wollte der Betroffene nun prüfen, ob und wie intensiv seine Angaben in den vergangenen Jahren überprüft worden waren. Das Finanzamt hielt generell und grundsätzlich dagegen, es müsse prüfen, ob ein Geheimhaltungsinteresse Dritter beeinträchtigt sein könne; gegebenenfalls müssten das gesamte Kontrollmaterial, behördeninterne Vermerke, Anweisungen und Ähnliches aus den Akten entfernt werden, was zu einem **erheblichen Verwaltungsaufwand** der Behörde führe.

Die Beurteilung der **Geheimhaltungsinteressen** Dritter sowie des Verwaltungsaufwands darf nicht abstrakt generell erfolgen, sondern muss sich auf den konkreten Einzelfall beziehen. Belange Dritter waren nicht einmal im Ansatz erkennbar. Auch war nicht ersichtlich, weshalb es erforderlich sein sollte, das gesamte Kontrollmaterial, behördeninterne Vermerke, Anweisungen und Ähnliches aus den Akten zu entfernen. Eine Gefährdung des Ermittlungsinteresses der Finanzbehörde durch die Gewährung der Akteneinsicht konnte damit jedenfalls nicht verbunden sein. Das Finanzamt ließ sich endlich erweichen und gewährte die erbetene Akteneinsicht.

Was ist zu tun?
Finanzbehörden müssen ihre bürgerfeindliche Praxis ändern, auch wenn die Abgabenordnung nicht geändert wird. Sie dürfen Akteneinsichtsbegehren nach pflichtgemäßem Ermessen nur ablehnen, wenn die Durchführung des Besteuerungsverfahrens tatsächlich gefährdet wäre oder konkrete Geheimhaltungsinteressen Dritter entgegenstehen.

4.8.3 Grundsteuerdaten für den ehrenamtlichen Bürgermeister

Viele Kommunen vermuten, dass die Einheitswerte für die Bemessung der Grundsteuer nicht mehr den aktuellen Verhältnissen vor Ort entsprechen. Eine Überprüfung dieser Werte durch ehrenamtliche Bürgermeister ist allerdings kein zulässiges Mittel zur Verbesserung der Einnahmesituation der Gemeinden.

Ein ehrenamtlicher Bürgermeister erbat von seiner Amtsverwaltung eine komplette Liste aller Grundsteuerpflichtigen seiner Gemeinde mit genauer Angabe der Lage des jeweiligen Grundstücks und des Steuerbetrags. Diese Liste sollte ihm zur Einschätzung einer sachgerechteren Besteuerung im Interesse des Gemeindehaushalts dienen. Der Bürgermeister meinte, dass insbesondere bei älteren Gebäuden, die später – teilweise auch ohne Baugenehmigungserfordernis – aus- bzw. umgebaut worden sind, eine **ungerechte Besteuerungslage** entstanden sei. Die Ursache vermutete er in durch das Finanzamt nicht aktualisierten Messbeträgen – die Grundlage für die Berechnung der Grundsteuer.

Die Gemeindeordnung enthält zwar ein allgemeines Auskunfts- und Akteneinsichtsrecht für kommunale Mandatsträger, dieses steht jedoch bei der Weitergabe personenbezogener Daten unter dem Vorbehalt der Erforderlichkeit zur rechtmäßigen Erfüllung der durch Rechtsvorschrift zugewiesenen **Aufgaben der empfangenden Stelle**. Die begehrten Informationen mussten also in einem funktionalen Zusammenhang zur konkreten Aufgabenerfüllung des Mandatsträgers stehen.

Zur generellen Beurteilung der Einnahmesituation der Gemeinde im Rahmen der Vorbereitung auf die Haushaltsplanberatungen hätten allgemeine Angaben zum Haushaltsvollzug des Vorjahres sowie gegebenenfalls anonymisierte Daten mit Hinweisen zu den Veränderungen gegenüber den Vorjahren ausgereicht. Der Bürgermeister begehrte die Daten, die zudem dem Steuergeheimnis unterliegen, aber wohl zur **Kontrolle der konkreten Grundsteuermessbeträge**. Für diese Aufgabe war nun der Bürgermeister beim besten Willen nicht zuständig, weshalb sein Auskunftsersuchen abgelehnt werden musste.

Was ist zu tun?
Amtsverwaltungen müssen vor der Weitergabe personenbezogener Daten an kommunale Mandatsträger im Rahmen ihrer Auskunfts- und Akteneinsichtsrechte sorgfältig prüfen, ob die begehrten Daten in einem funktionalen Zusammenhang zur konkreten Aufgabenerfüllung der Mandatsträger stehen.

5 Datenschutz in der Wirtschaft

5.1 Kontrollen bei der Wohnungswirtschaft

Im Verlauf des Jahres wurden insgesamt vierzehn Unternehmen der schleswig-holsteinischen Wohnungswirtschaft einer Querschnittsprüfung unterzogen. Wir wollten vor allem wissen, in welchem Umfang das von den Medien viel beschworene Thema der so genannten Mietnomaden tatsächlich existiert und wie die Unternehmen mit den Daten von Mietinteressenten verfahren.

Wenig Schmeichelhaftes ergab die Prüfung für die gewerbliche Wohnungswirtschaft bei den allgemeinen Datenschutzanforderungen (26. TB, Tz. 5.7; 27. TB, Tz. 5.2). Den Unternehmen sind teilweise sehr umfangreiche und auch sensitive Mieterinformationen anvertraut. Wir stellten zum Teil erhebliche materielle wie **formelle Missstände** fest. Bei der Bestellung betrieblicher Datenschutzbeauftragter, der Erstellung von Verfahrensverzeichnissen oder der Verpflichtung der Mitarbeiter auf das Datengeheimnis gab es teilweise absolute Fehlanzeigen und regelmäßig große Defizite. Die Verträge mit Auftragsdatenverarbeitern entsprachen praktisch alle nicht den gesetzlichen Anforderungen.

Auch bei der Prüfung der konkreten **Verarbeitung von Mieterdaten** gab es zahlreiche Beanstandungen: So wird nicht hinreichend zwischen den für die Vertragsanbahnung erhobenen Daten und den später im Stammdatensatz des Mieters aufzunehmenden Daten unterschieden. Die umfangreichen Informationen zu Mietinteressenten aus dem Bewerbungsfragebogen oder die Auskünfte von Auskunfteien dürfen nur in den späteren Mieterdatensatz übernommen werden, soweit dies unbedingt erforderlich ist. Informationen zu abgelehnten Mietinteressenten sind umgehend zu löschen. Und auch für die Daten der Mieter gilt: Diese dürfen grundsätzlich nicht länger gespeichert werden, als der Mietvertrag andauert.

Abgesehen von einer einzigen Ausnahme unterhielten alle geprüften Unternehmen geschäftliche **Verbindungen mit Auskunfteien**. Diese werden zur Bonitätsprüfung von Mietinteressenten und teilweise bei Zahlungsproblemen mit Mietern eingeschaltet. In zwei Fällen war den Wohnungsunternehmen die Möglichkeit eingeräumt, eigene Einmeldungen, z. B. von säumigen Mietern, vorzunehmen und über die Auskunftei so genannte weiche Mieterdaten (z. B. eine offene Handyrechnung) zu beziehen. In allen anderen Fällen beschränkte sich die Datenübermittlung mit Auskunfteien ausschließlich auf so genannte harte Daten. Darunter sind Informationen über Mietinteressenten zu verstehen, die im Rahmen eines unabhängigen gerichtlichen Verfahrens festgestellt wurden (z. B. Klagen nach Räumungsurteil, Einträge aus Schuldnerverzeichnissen).

Das Anmieten von Wohnraum ist ein **existenzielles menschliches Bedürfnis**. Dies darf nicht schon dadurch infrage gestellt werden, dass jemand – aus welchen Gründen auch immer – seine Handyrechnung nicht bezahlt hat. Vage Vermutungen oder einzelne unbezahlte Rechnungen dürfen nicht dazu führen, dass es zur Ausgrenzung kommt. Daher beanstandeten wir die Beschaffung von weichen Negativdaten ebenso wie von weniger gewichtigen harten Negativdaten, die

keinen direkten Bezug zur Wohnungswirtschaft haben. In diesen Fällen fehlt es an dem für die Zusammenarbeit mit Auskunfteien grundsätzlich nachzuweisenden kreditorischen Interesse. Vermietung mag für den Vermieter in mancher Hinsicht ein Risikogeschäft sein; mit klassischer Kreditgewährung hat es nichts zu tun. Vermieter verfügen über zahlreiche andere Möglichkeiten, sich vor möglichen Ausfällen des Mietzinses und Schäden zu schützen, z. B. durch Kautionen oder die Nutzung des Vermieterpfandrechts.

Auf das in den Medien breit diskutierte Problem der **Mietnomaden** angesprochen, verneinten sämtliche Unternehmen eine erhebliche betriebswirtschaftliche Relevanz. Vielmehr wurde gegenüber dem ULD betont, dass es einzelne Fälle der mutwilligen Anmietung und Zerstörung der Mietsache stets gegeben habe und es zum Geschäft gehöre, für diese Fälle eine – insgesamt als gering zu bezeichnende – Rücklage zu bilden.

Was ist zu tun?
Vor allem bei kleinen und mittleren Unternehmen besteht ein riesiger Nachholbedarf in Sachen Datenschutz. Das Vertrauen der Mieter darf angesichts der erhobenen und vorhandenen sensitiven Daten und der auf Dauer angelegten Vertragsverbindung nicht überstrapaziert werden. Die Gefahr von unerquicklichen Auseinandersetzungen sollte und kann vermieden werden.

5.2 Das Data Warehouse bei der Internetbank

Eine bereits im Jahr 2004 begonnene Prüfung einer großen Internetdirektbank wurde fortgeführt. Während die formalen Anforderungen des BDSG weitestgehend eingehalten wurden, zeigten sich teilweise gravierende Mängel im Umgang mit den Kundendaten. Einige Ergebnisse haben grundlegende Bedeutung auch für andere Kreditunternehmen.

Die geprüfte Bank unterhält ein so genanntes Data-Warehouse-System. Diese Datenbankanwendung erlaubt es, den gesamten Kundendatenbestand einschließlich der Kontensalden gezielt auszuwerten, insbesondere auch zu **Marketingzwecken**. Die aus diesen Informationen gezogenen Schlüsse steuern die Werbeansprache. Mit extern angekauften Informationen zum Wohnumfeld der Kunden wird der Datenbestand angereichert. Mit den erstellten sensitiven Kundenprofilen wird entschieden, ob und – wenn ja – welche Produkte beim einzelnen Kunden beworben werden sollen.

Der Einsatz von Data-Warehouse-Systemen stellt erhebliche Gestaltungsanforderungen an die verantwortlichen Unternehmen. Gerade weil die Systeme der Zusammenführung von zu ganz unterschiedlichen Zwecken gesammelten Daten dienen, ist der zentrale Datenschutzgrundsatz der Zweckbindung betroffen. Außerdem werden Profile möglich, die zu einem **weitgehenden Persönlichkeitsbild** der betroffenen Kunden führen. Das ULD hat die Einbeziehung von soziodemografischen Daten und die fehlende gesonderte Information der Kunden über den Einsatz des Systems beanstandet.

Das Unternehmen führt ein **Scoring bei Kreditantragstellern** durch. Dabei werden allgemeine statistische Annahmen zur Zahlungsfähigkeit und Zahlungswilligkeit mit konkret vorliegenden Informationen über den Antragsteller abgeglichen. Hierbei werden viele Informationen, z. B. auch der Familienstand und das Alter der Antragsteller, zu einer Art Schulnote gebündelt, die bei der Antragsbearbeitung zu Schlechterstellungen führen kann. Diese Note wird Score genannt. Ein schlechter Scorewert kann zur Ablehnung des Kreditantrages führen. Die Betroffenen werden über die Durchführung des Bewertungsverfahrens nicht informiert. Das ULD hat die Einbeziehung von Familienstand und Alter in das Scoring als nicht relevante Merkmale beanstandet (Tz. 8.8).

Die Internetbank speichert sämtliche **Nutzungsdaten der Webseitenbesucher**, die so genannten Logdaten einschließlich der IP-Adresse, bis zu sechs Monate lang. Dies gilt nicht nur für Vertragskunden, sondern auch für Interessenten. Als Zweck wurde pauschal auf die Beweissicherung und die Verfolgung von Internetkriminalität verwiesen. Die unverhältnismäßige Speicherdauer wurde von uns als Verstoß gegen die Löschpflicht der nicht unmittelbar zu Abrechnungszwecken erforderlichen Nutzungsdaten beanstandet. Auch für Internetbanken gilt: Die beim Betrieb von Internetseiten anfallenden und grundsätzlich personenbeziehbaren Nutzerdaten sind in der Regel unverzüglich zu löschen, wenn der Besuch der Webseite beendet ist. Eine längere Speicherung – auch zu sonstigen Zwecken – setzt die Einwilligung der informierten Nutzer voraus.

Was ist zu tun?
Unternehmen müssen beim Betrieb eines Data Warehouse beachten, dass bestimmte Daten überhaupt nicht der Auswertung zugeführt werden dürfen, z. B. Gesundheitsdaten oder konkrete Transaktionsdaten von Bankkunden. Die Kunden sind über den Einsatz der Systeme zu informieren. Einer Einbeziehung der eigenen Daten zu Werbezwecken können Betroffene jederzeit widersprechen. Bei der Speicherung von Internetnutzungsdaten sind der Erforderlichkeitsgrundsatz und das Prinzip der Datensparsamkeit zu beachten.

5.3 Bank pfeift auf Datenschutz

Ausgerechnet bei Banken, von denen Kunden zu Recht Vertraulichkeit und besondere Vorkehrungen für den Schutz ihrer Daten erwarten, sind immer wieder gravierende Datenschutzmängel festzustellen. Bei einer umfassenden Prüfung einer Volks- und Raiffeisenbank traten massive Mängel in nahezu allen Bereichen zutage. Offenbar hatte man sich bislang noch nie mit den Datenschutzanforderungen befasst.

Es konnte keine gesetzlich geforderte Verfahrensübersicht vorgelegt werden. Als Ersatz wurden uns Auszüge aus einem Verfahrensverzeichnis des Rechenzentrums der Bank bzw. des Verbandes präsentiert. Die Auftragsdatenverarbeitungsverhältnisse waren **nicht dokumentiert**, die nötigen Organisations- und Handlungsanweisungen für die in Betrieb befindlichen Videokameras auch nicht. Auf Nachfrage konnte der betriebliche Datenschutzbeauftragte zu fast keinem der im

Hause im Einsatz befindlichen automatisierten Verfahren eine Stellungnahme abgeben. Bei der zweitägigen Prüfung vor Ort war es dem Unternehmen auch nicht möglich, entsprechend kompetente Ansprechpartner zur Verfügung zu stellen.

Eine stichprobenartige Einsichtnahme in die Kundendatenbank zeigte, dass über Kreditkunden ohne deren Wissen **Persönlichkeitsbewertungen** erstellt und abgespeichert waren mit Angaben zu Ruf, Ansehen und Lebensstil, Zielstrebigkeit und Zuverlässigkeit. Hierbei konnten die Sachbearbeiter Noten auf einer Skala von eins bis sechs vergeben.

Wir haben das Unternehmen aufgefordert, ein **ordnungsgemäßes Datenschutzmanagement** aufzusetzen. Die Zustände stellten einen schweren Managementfehler dar. Dessen Bereinigung wird einen großen zeitlichen und hohen finanziellen Aufwand und viel Nacharbeit kosten. Zwischenzeitlich hat das Unternehmen signalisiert, grundlegende Maßnahmen zum Schutz der Daten ihrer Kundinnen und Kunden vornehmen zu wollen.

Was ist zu tun?
Das ULD wird die allmähliche Umsetzung der datenschutzrechtlichen Anforderungen begleiten und kontrollieren.

5.4 Lichtspiele, Video und Attrappen

Das ULD prüfte die Zentrale eines bundesweit tätigen Kinounternehmens mit dem Schwerpunkt Videoüberwachung.

Das vom ULD geprüfte Unternehmen betreibt Kinos in Schleswig-Holstein und in anderen Bundesländern. Nach unseren Feststellungen wurden Videokameras innerhalb der Filmtheater an vielen Orten installiert – im Bereich der Kinokassen, vor einem Sicherheitsraum, in dem die Kasseneinnahmen abgerechnet und gelagert wurden, in den Bar- und Restaurationsbereichen. Neben funktionsfähigen Kameras kommen auch Attrappen zum Einsatz. Nicht alle überwachten Räumlichkeiten waren mit den erforderlichen Hinweisschildern ausgestattet.

Unsere Prüfung beschränkte sich auf die Häuser im Zuständigkeitsbereich des ULD. Es konnte aber mit dem Unternehmen Einigkeit erzielt werden, dass die Ergebnisse auf alle Häuser des Konzerns übertragen werden. Folgende **Grundsätze zur Videoüberwachung** wurden erarbeitet:

- Jede Videoüberwachung, die zur Wahrnehmung des Hausrechts durchgeführt wird, unterliegt dem **Erforderlichkeitsprinzip**.
- Es muss in jedem Einzelfall ein **berechtigtes Interesse** für konkret festgelegte Zwecke bestehen (z. B. Verhinderung von Diebstahl oder Vandalismus).

- Die **schutzwürdigen Interessen** der Betroffenen sind in jedem Einzelfall zu beachten. Das berechtigte Interesse des Unternehmens muss gegenüber den Betroffeneninteressen überwiegen.
- Es ist eine periodische **Risikoanalyse** (z. B. alle sechs Monate) durchzuführen, wobei die tatsächlich eingetretenen Schäden in die Entscheidung, ob eine Videoüberwachung fortgesetzt wird, einzubeziehen sind.
- Für jeden überwachten Bereich sind aussagekräftige **Hinweisschilder** in Augenhöhe zu installieren. Sie können aus einem Text oder einem Piktogramm bestehen und dürfen nicht zu klein sein. Die Schilder müssen jedem Betroffenen ins Auge fallen.
- Bei Zuordnung der Bilddaten zu einer bestimmten Person ist die gesetzlich geforderte **Benachrichtigungspflicht** zu beachten.
- Die **Aufbewahrung** von gespeicherten Videoaufnahmen ist auf wenige Kalendertage zu beschränken (z. B. drei Tage).
- **Attrappen** sind so zu behandeln wie echte Kameras. Das bedeutet, dass in jedem Fall die gleichen Konsequenzen zu ziehen sind (Prüfung der Erforderlichkeit, Zulässigkeit, Hinweispflicht).
- In **Intimzonen** (z. B. Toiletten oder Umkleideräumen) ist eine Videoüberwachung in jedem Fall unzulässig (auch keine Attrappen).
- Die Beobachtung von **Kassenbereichen** und Abrechnungsräumen, in denen mit hohen Bargeldbeträgen umgegangen wird, kann bei Einhaltung aller sonstigen Voraussetzungen (Einzelfallprüfung, Hinweisschilder, Risikoanalyse, Speicherungsdauer) in der Regel als zulässig angesehen werden. Die Mitarbeiterinnen und Mitarbeiter sind ausreichend zu informieren. Gegebenenfalls ist der Betriebsrat zu beteiligen. Eine dauerhafte Erfassung der Arbeitsbereiche (Bar, Tresen, Verkaufsstände, Kasse) sollte unterbleiben.
- Reine **Freizeitbereiche** (Bars, Sitzgruppen, Foyer, Aufenthaltsräume) dürfen nicht überwacht werden. Hier überwiegt das Persönlichkeitsrecht der Betroffenen.
- So genannte „**Dome-Kameras**“ sind nur in absoluten Ausnahmefällen zulässig und unterliegen wegen ihrer universellen Technik einer besonders strengen Erforderlichkeitsprüfung.
- Die Beobachtung der **Gebäudeaußenwände** ist nur bei tatsächlich eingetretenen Beschädigungen zulässig. Dabei darf von öffentlichen Wegen und Bürgersteigen nur ein schmaler Streifen von maximal einem Meter erfasst werden.

Was ist zu tun?
Die aufgeführten Grundsätze sollten nicht nur bei Kinos Anwendung finden, sie können auf andere Unternehmen, die Videotechnik einsetzen, übertragen werden.

5.5 Das schnelle Anschmieren übers Internet?

Warndateien und Internetpranger aus den unterschiedlichsten Bereichen „beleben“ das Internet. Datenschutzrechtlich sind diese zumeist nicht in Ordnung.

Dem ULD wurde das Geschäftsmodell einer Warndatei für **Autovermieter und Gebrauchtwagenkäufer** vorgelegt. Dieses zielte darauf ab, die Autovermietungen als Vertragsnehmer zu gewinnen. Diese sollten schlechte Erfahrungen mit Kfz-Mietern an die Warndatei melden: mit Angaben zum Zahlungsverhalten, zu Führerschein und Personalausweis sowie zum Fahrzeug bis hin zur Fahrgestellnummer. Der Zugriff auf diese Daten sollte auch für Privatkunden geöffnet werden, die einen Gebrauchtwagen kaufen möchten. Die Betreiber hatten sich zunächst über die Datenschutznotwendigkeit eines solchen Vorhabens gar keine Gedanken gemacht. Zwischenzeitlich liegt ein überarbeitetes Modell zur Prüfung vor.

In einem anderen Fall war die Errichtung einer Website zur **Bewertung von Vermietern** geplant. Angesichts der bekannten Mieterwarndateien (27. TB, Tz. 5.2) sollte hier der Spieß umgedreht und erstmals Mietern und Mietinteressenten ein Forum geboten werden, schlechte Erfahrungen mit Vermietern und Hausverwaltungen in Form eines Schulnotensystems an eine im Internet abrufbare Datenbank zu melden. Für **Internetpranger**, bei denen Personen oder Personengruppen eine öffentliche Bewertung durch einen offenen Kreis von Bewertern hinnehmen müssen, ist die gesetzlich geforderte Abwägung zwischen den möglicherweise berechtigten Interessen an der Information der Öffentlichkeit und dem Grundrecht der Betroffenen auf informationelle Selbstbestimmung zumeist nicht möglich. Im konkreten Fall waren keine Vorkehrungen für die Richtigkeit der Angaben vorgesehen. Das Recht der betroffenen Vermieter auf Schutz ihrer Persönlichkeit wäre bei dem uns vorgelegten Geschäftsmodell auf der Strecke geblieben.

Was ist zu tun?
Personenbezogene Warndateien sind meldepflichtige Verfahren. Wenn für bestimmte Branchen Warndateien zur Bonitätsprüfung von Kunden geplant sind, muss ein kreditorisches Interesse der beteiligten Unternehmen bestehen. Angebote mit Bewertungen von Einzelpersonen machen eine besonders sorgfältige Vorabprüfung notwendig.

5.6 Einzelfälle

5.6.1 Wahlwerbung – Spiel mit dem Feuer

Mitglieder eines größeren Verbandes wandten sich an uns, weil sie Werbung für die im vergangenen Jahr stattgefundenen Landtagswahlen erhielten: Ein Landtagsabgeordneter hatte sie in einem nicht als Werbepost gekennzeichneten Schreiben persönlich angeschrieben. Unter Verweis auf die **gemeinsame Verbandsmitgliedschaft** warb er für seine Wiederwahl. Die Angeschriebenen fühlten sich

dadurch teilweise belästigt und betonten, den Abgeordneten nicht persönlich zu kennen. Der Abgeordnete trug vor, er habe die Namen der Angeschriebenen seinen persönlichen Aufzeichnungen entnommen. Teilweise habe es sich auch um besonders engagierte Personen des Verbandes gehandelt, die ihm Dritte entsprechend benannt hätten. Wir konnten nicht feststellen, dass der Verband offiziell die Mitgliedsdaten weitergegeben hatte. Für die zu Werbezwecken und ohne Kenntnis der Betroffenen erfolgte Datenerfassung gab es keine Rechtsgrundlage, weshalb wir den Vorgang beanstanden mussten. Beim Anschreiben war zudem der gesetzlich geforderte Hinweis auf die jederzeitige Möglichkeit des Widerspruchs gegen weitere Werbung versäumt worden.

Was ist zu tun?
Wahlwerbung unterfällt dem Bundesdatenschutzgesetz. Bürgerinnen und Bürger reagieren sensibel, mitunter allergisch auf persönlich adressierte Werbepost. Politiker sollten nur Personen anschreiben, von deren Einverständnis sie ausgehen können. In den Schreiben ist ein Hinweis auf die Widerspruchsmöglichkeit gegen weitere Werbung aufzunehmen.

5.6.2 Zeitungsanzeige – Stammdatensatz zehn Jahre gespeichert

Ein Bürger ärgerte sich: Er behauptete, jahrelang keine Anzeigen bei einer Zeitung mehr aufgegeben zu haben. Dennoch konnten die Mitarbeiter der Servicestelle seinen vollständigen Stammdatensatz samt Kontonummer aufrufen.

Die Recherchen des ULD ergaben, dass der betroffene Bürger entgegen seiner Behauptung bei der Zeitung weitere Anzeigen aufgegeben hatte. Doch veranlasste uns der Fall, grundsätzlich tätig zu werden. Die Zeitung meinte unterschiedslos alle **Abo- und Anzeigenkunden** für mindestens zehn Jahre speichern und diese Daten allen Servicemitarbeitern im operativen System abrufbar zur Verfügung stellen zu dürfen. Wir mussten die Zeitung darauf hinweisen, dass der gegenwärtige Zustand rechtswidrig ist.

Stammdaten der Kunden können grundsätzlich nur so lange gespeichert bleiben, wie eine vertragliche Verbindung besteht, die abgewickelt werden muss. Auch die Daten von Anzeigenkunden sind nach Abwicklung des Zahlungsvorganges zu löschen. Nach Schaltung einer Anzeige kann allenfalls für einen gewissen Zeitraum eine weitere Speicherung hingenommen werden, um weitere Aufträge schneller zu erfassen oder Werbeansprachen vorzunehmen. Danach sind die Daten für den Zugriff aus dem operativen System zu sperren. Widerspricht ein Kunde der weiteren Speicherung seiner Daten in diesem Zeitraum, so sind die Daten sofort zu sperren. Lediglich **Aufbewahrungspflichten** nach der Abgabenordnung oder dem Handelsgesetzbuch können es rechtfertigen – dann aber zweckgebunden –, die Daten über einen Zeitraum bis zu zehn Jahren zu speichern. Diese Pflicht betrifft aber nicht alle Daten, sondern nur wenige Transaktionsdaten.

Unternehmen tun sich auch finanziell keinen Gefallen, ausufernd veraltete Kundendaten zu führen. Dies hat **Einschränkungen der wirtschaftlichen Nutzbar-**

keit der Datenbestände zur Folge. Das Zeitungsunternehmen hat mittlerweile zugesagt, ihre Datenbank gemäß den datenschutzrechtlichen Vorgaben verbraucherfreundlich zu gestalten.

Was ist zu tun?
Das Speichern von Kundendaten bedarf einer Rechtsgrundlage. Mit einem gezielten Datenschutzmanagement können Unternehmen zu den üblichen Vertragstypen und Datensätzen klare Festlegungen zu Zugriffsbefugnissen, Lösch- und Sperrfristen vornehmen, die im automatisierten Verfahren umzusetzen sind. Softwareprodukte, die eine entsprechende Umsetzung nicht zulassen, sollten von vornherein gemieden werden.

5.6.3 Mehr Transparenz bei Zeitungszustellungen

Der Versuch einer Zeitungsleserin, Probleme mit ihrem Abonnement aufzuklären, brachte zutage, dass ihre Zeitung über ihre Lesegewohnheiten bezüglich anderen Zeitungen bestens Bescheid wusste.

Die verunsicherte Kundin befürchtete, dass bei der Zeitung ein umfassendes Profil ihrer **Lesepräferenzen und Gewohnheiten** vorliegt. Es zeigte sich, dass der Zeitungsverlag den Vertrieb seiner eigenen – ausschließlich regional angebotenen – Produkte über eine wirtschaftlich eng verbundene, aber rechtlich selbstständige Gesellschaft abwickelt. Diese Gesellschaft bearbeitet auch Kundenanfragen zu anderen, insbesondere überregionalen Tageszeitungen und führt für diese die Zustellung durch. Die Kundendatenbank des Unternehmens enthält eine Übersicht über alle für die jeweiligen Kunden vertriebenen Eigen- und Fremdprodukte.

Komplexe Vertriebs- und Zustellungssysteme erfordern Datenübermittlungen zwischen rechtlich selbstständigen Zeitungs- oder Verlagshäusern und zusätzlich eigens gegründeten Zustellgesellschaften. Der Kunde kennt zumeist nur den Verlag der von ihm abonnierten Zeitung. Regelmäßig werden aber, wenn keine postalische Zustellung erfolgt, auch Zustellgesellschaften eingesetzt. Zwecks Zustellung werden die Kundendatensätze dorthin übermittelt. Dies darf aber nicht hinter dem Rücken der Betroffenen erfolgen. Das Datenschutzrecht verlangt, dass – je nach vertraglicher Konstruktion und übertragener Aufgabe – entweder die Zeitung selbst oder die Zustellgesellschaft die Kunden über die stattfindenden Datenübermittlungen **zu informieren** hat. Denn jeder soll grundsätzlich wissen können, wer was wann über ihn weiß. Erfolgt eine rechtlich privilegierte Auftragsdatenverarbeitung, so kann im Einzelfall die Pflicht zur Mitteilung entfallen. Das Unternehmen sagte zu, sowohl seine Eigenkunden als auch die Fremdkunden über das Verfahren und die Beteiligten zu informieren.

Was ist zu tun?
Transparenz über Unternehmenskooperationen fördert das Kundenvertrauen in den sorgsamen Umgang mit deren Daten. Werden in einer Kundendatenbank personenbezogene Daten zu unterschiedlichen Zwecken verarbeitet, so sind diese räumlich oder zumindest technisch getrennt zu speichern.

5.6.4 Übermittlung von Mieterdaten

Es ist eine gängige Praxis, dass Wohnungs- und Versorgungsunternehmen Rahmenverträge hinsichtlich der Wärmeversorgung schließen. Für die Übermittlung von Mieterdaten zwischen den Unternehmen bedarf es einer rechtlichen Grundlage in den jeweiligen Mietverträgen.

Die Rahmenverträge zwischen Wohnungs- und Versorgungsunternehmen enthalten zumeist **Datenübermittlungsklauseln** zulasten der Mieter. Im Falle eines Mieterwechsels teilt das Wohnungs- dem Versorgungsunternehmen schriftlich die neue Anschrift des bisherigen Mieters und den Namen des neuen Mieters mit, ohne dass diese davon Kenntnis erlangen. Dies ist unzulässig. Es ist nicht zu bestreiten, dass an der praktizierten Verfahrensweise ein nachvollziehbares Interesse besteht. Für die Abgabe einer wirksamen Einwilligungserklärung fehlt es im Zusammenhang mit der Anmietung einer Wohnung und der damit verbundenen Inanspruchnahme von Leistungen eines Versorgungsunternehmens zumeist an der Freiwilligkeit. Ein Widerruf der Einwilligung ließe sich kaum umsetzen.

Formulierungsvorschlag:

Bei Abschluss des Mietvertrages ist der Vermieter berechtigt, folgende personenbezogene Daten: Name, Vorname, Anschrift, Wohnungsbezeichnung, beheizte Wohnfläche und Bezugsdatum an den im Mietvertrag genannten Betreiber ausschließlich zum Zwecke der Erstellung der jeweiligen Abrechnung zu übermitteln.

Bei Beendigung des Mietvertrages ist der Vermieter berechtigt, zum Zwecke der Abwicklung der Schlussrechnung die neue Anschrift des Mieters zu erheben. Ausschließlich für diesen Zweck ist die Übermittlung der Anschrift an das im Mietvertrag genannte Versorgungsunternehmen zulässig.

Aus Datenschutzsicht ist es daher erforderlich, den Betroffenen im Interesse vertraglicher Transparenz umfassend über den Umfang und den Zweck der beabsichtigten Verarbeitung seiner personenbezogenen Daten zu unterrichten. Wir haben daher vorgeschlagen, künftig einen entsprechenden **Passus in die Mietverträge** aufzunehmen. So werden die Mieter bereits bei Abschluss eines Mietvertrages über die sie betreffenden geplanten Datenverarbeitungsvorgänge informiert.

Was ist zu tun?
Wohnungsunternehmen, die Rahmenverträge über die Wärmeversorgung geschlossen haben, müssen in die Verträge mit ihren Mietern einen Passus aufnehmen, der die Datenübermittlung an das Versorgungsunternehmen erlaubt.

5.6.5 Bin ich denn blöd? Fremde Daten auf meinem neuen PC!

Der Kunde einer bundesweit tätigen Elektronikhandelskette staunte nicht schlecht: Gerade hatte er sich einen vermeintlich nagelneuen PC gekauft, da fand er auf der Festplatte hochbrisante personenbezogene Daten eines Unbeteiligten, u. a. private Fotos, Bewerbungsschreiben und Lebensläufe.

Der Käufer nahm mit dem offensichtlich Betroffenen Telefonkontakt auf und erfuhr, dass dieser kurz vor dem PC-Kauf einen Laptop zur Reparatur abgegeben hatte. Der ebenfalls informierte Elektronikmarkt forderte den Kunden zur sofortigen Löschung der fremden Daten auf und drohte widrigenfalls mit **gerichtlichen Schritten**. Der Kunde war sich der Schwächen der normalen Löschfunktion seines PCs durchaus bewusst und bat in seiner Not das ULD um Hilfe.

Unsere Nachfrage bei der Handelskette ergab, dass der Kunde einen **preisreduzierten Vorführrechner** erworben habe, der über längere Zeit in den Verkaufsräumen des Elektronikmarktes für alle Kundinnen und Kunden zugänglich gewesen sei. Plausibel hörte sich diese Darstellung nicht an. Letztlich war der Vorfall wegen fehlender Dokumentation nicht aufklärbar. Fakt war lediglich, dass ein PC verkauft worden ist, auf dem sich sensible Daten eines Dritten befanden, die kaum jemand freiwillig anderen Menschen offenbart.

Der Elektronikmarkt wurde im Rahmen unserer Beanstandung aufgefordert, bei der Reparatur von beschriebenen Datenträgern Maßnahmen zur Verhinderung unbeabsichtigter Datenübermittlungen zu treffen. Es muss durch **technisch-organisatorische Maßnahmen** sichergestellt werden, dass nur Rechner mit unbeschriebenen Festplatten verkauft werden. Den aufmerksamen Kunden verwiesen wir auf frei zugängliche Software, mit deren Hilfe eine vollständige und datenschutzgerechte Datenlöschung möglich ist.

Was ist zu tun?
Unternehmen, die Rechner reparieren und warten, müssen Maßnahmen ergreifen, um zu verhindern, dass fremde Sicherungsdatenbestände in die Hände anderer Kunden geraten.

5.6.6 „Familienstammbaum“ im Internet

Der Ersteller eines großen Familienstammbaumes stellte die personenbezogenen Daten von ca. 10.000 „Angehörigen“ aus drei Generationen ins Internet.

Über Internetrecherchen fand er weitere „Familienmitglieder“, die er über die Aufnahme in den Familienstammbaum informierte. Ein vermeintliches Familienmitglied widersprach der Veröffentlichung im Internet. Zwar wurde ihm die Löschung zugesagt, jedoch passierte nichts. Der Verantwortliche machte technische Probleme geltend. Unsere weitere Prüfung ergab, dass in mehreren Fällen keine wirksamen **Einwilligungen für die Veröffentlichung** im Internet vorlagen.

Die Einstellung der personenbezogenen Daten im Internet erfolgte somit unbefugt und wurde beanstandet. Da dem Verantwortlichen der Nachweis über das Vorliegen der anderen Einwilligungserklärungen nicht möglich war, verzichtete er schließlich konsequenterweise auf die Veröffentlichung von Stammbaumdaten der lebenden Personen im Internet.

Was ist zu tun?
Vor der Veröffentlichung personenbezogener Daten Dritter im Internet ist grundsätzlich in jedem Einzelfall eine Einwilligung einzuholen. Der Verantwortliche einer im Internet zur Verfügung gestellten Datenbank hat zu gewährleisten, dass eine ordnungsgemäße Datenverarbeitung personenbezogener Daten erfolgt.

5.7 Bußgelder – manchmal sind sie unvermeidbar

In der Regel zeigen Unternehmen großes Entgegenkommen und Verständnis für Forderungen, Hinweise und Ratschläge des ULD zur Verbesserung des Datenschutzes. Immer wieder sind aber, vor allem bei vorsätzlichen erheblichen rechtswidrigen Geschäftspraktiken, einzelne Bußgeldverfahren notwendig.

Für die Sachverhaltsermittlung einer Datenschutzaufsichtsbehörde unverzichtbar ist die im Gesetz eindeutig geregelte Pflicht zur **Auskunftserteilung**. Nur mit ihr ist es oft möglich, für betroffene Bürgerinnen und Bürger die faktischen Umstände aufzuklären. Reagiert ein Unternehmen nicht auf unsere Anfragen, und dies mehrfach und trotz Fristsetzung, dann müssen wir ein Bußgeld verhängen – so geschehen anlässlich eines Verdachts unerlaubter Telefonwerbung.

Sieben gleichartig gelagerte Bürgereingaben waren die Grundlage für die Einleitung eines noch andauernden Bußgeldverfahrens. Die Betroffenen erhielten personalisierte Gewinnmitteilungen für die Teilnahme an einem Gewinnspiel. Keiner von ihnen hatte an dem genannten Gewinnspiel teilgenommen oder von dem Unternehmen gehört. Dennoch lagen dem Unternehmen zum Teil Geburtsdaten, Kontonummern und Telefonnummern der Betroffenen vor. Bei einer Prüfung vor Ort konnte man uns die Herkunft der Datensätze nicht vollständig und plausibel erklären. Der Geschäftsführer gab allerdings zu, Teile der **eine halbe Million Personen umfassenden Adressdatenbank** bereits vor Jahren ohne Wissen der Betroffenen aus einem mittlerweile insolventen Unternehmen eingebracht zu haben. Zwischenzeitlich teilte das Unternehmen mit, nach einem Namenswechsel nun jegliche Geschäftstätigkeit eingestellt zu haben. Der Verdacht der vorsätzlichen unbefugten Verarbeitung nicht allgemein zugänglicher Daten ist damit nicht vom Tisch.

Trotz wiederholter Beanstandung und entgegen der schriftlichen Zusage des verantwortlichen Betreibers kam es in einem anderen Fall durch einen offensichtlich uneinsichtigen Hausbesitzer zur erneuten **unbefugten Videoüberwachung** eines öffentlichen Gehweges. Nach dem Einspruch gegen den Bußgeldbescheid liegt die Sache mittlerweile beim Amtsgericht zur Entscheidung.

5.8 Arbeitnehmerdatenschutz

5.8.1 Heimliches Fernwartungstool – der Feind auf meinem Rechner

Stellen Sie sich vor, Ihr Chef könnte jeden noch so kleinen Schritt, den sie an Ihrem Rechner tun, vollständig nachvollziehen. Fernwartungstools bieten dazu alle Möglichkeiten.

Ein Mitarbeiter eines mittelständischen Industrieunternehmens entdeckte rein zufällig, dass über Nacht auf seinem Arbeitsplatz-PC ein Softwareprogramm installiert worden war. Das eingesetzte Produkt ermöglicht innerhalb des Netzwerks den Echtzeitfernzugriff auf sämtliche Dateien des Rechners bis hin zur Beobachtung der jeweiligen Aktivitäten des Nutzers (Tastatureingaben, Internetnutzung usw.). Die Recherche des Betriebsrates ergab, dass auch alle anderen Rechner des Unternehmens betroffen waren. Offenbar hatte der für die EDV zuständige Geschäftsführer des Unternehmens in einer **Nacht- und Nebelaktion** das Programm installiert, ohne die Mitarbeiter zu informieren.

Der Einsatz von Fernwartungstools oder Spyware im Unternehmen ermöglicht die **lückenlose Überwachung der Bediensteten**. Wegen des hohen Eingriffspotenzials müssen mindestens die nachfolgenden datenschutzrechtlichen Vorgaben beachtet werden:

- Die betroffenen Mitarbeiter müssen über den Einsatz eingehend und vorab informiert werden.
- Die Zwecke der Nutzung der Software (z. B. Inventarisierung, Lizenzmanagement, Softwareinstallation) sollten in einer Betriebsvereinbarung hinreichend konkret und abschließend festgelegt werden. Der Einsatz für Verhaltens- und Leistungskontrollen sollte ausdrücklich ausgeschlossen werden.
- Konkret erfolgende Rechnerzugriffe mithilfe des Tools sollten stets in Absprache und mit Vorankündigung bei den betroffenen Mitarbeitern erfolgen. Diese sollten den Zugriff selbst abbrechen können.
- Die Nutzung des Programms durch die Administration ist laufend zu protokollieren. Die Zugriffsberechtigungen für die Nutzung des Programms sollten schriftlich festgelegt werden.

5.8.2 Immer wieder Ärger mit Personalfragebögen

Eine Bewerberin für einen Arbeitsplatz bei einer Handelskette ärgerte sich über den Umfang und den Inhalt eines Personalfragebogens. Nachdem sie ihre Bewerbung zurückgezogen hatte, bat sie uns um eine datenschutzrechtliche Überprüfung.

Der Personalfragebogen der Handelskette beinhaltete in der Tat eine Vielzahl von Fragen persönlichen Inhalts. Deren Bezug zum konkreten Arbeitsplatz war nicht immer erkennbar. Hier einige Beispiele:

- Die Frage nach den **Verwandtschaftsverhältnissen** der Bewerber zu bereits im Unternehmen angestellten Personen ist nur dann zulässig, wenn es um besondere Vertrauensstellungen geht oder Ehegatten oder Verwandte in einem Konkurrenzunternehmen beschäftigt sind und Gefahren bezüglich der Wahrung von Betriebsgeheimnissen bestehen.

- Fragen nach dem Verlauf eines **früheren** bzw. dem Bestehen eines **gegenwärtigen Arbeitsverhältnisses** sind grundsätzlich zulässig. Dies gilt jedoch nicht für konkrete Fragen nach den Modalitäten der Kündigung des bisherigen Arbeitsverhältnisses sowie nach dem Grund des Stellenwechsels. Einzelheiten der Kündigung der letzten Position stehen in keinem inhaltlichen Zusammenhang mit dem Beginn des neuen Arbeitsverhältnisses.

- Generelle Fragen nach **Nebentätigkeiten** sind datenschutzrechtlich unzulässig, da diese zumindest teilweise die engeren persönlichen Verhältnisse der Bewerber betreffen. Die Rechtsprechung verneint eine generelle Pflicht zur Auskunft über Nebentätigkeiten. Entsprechende Nachfragen können unter Umständen nach Abschluss des Arbeitsvertrages erfolgen; Anzeige- und Genehmigungspflichten sind möglich.

- Zwei Antidiskriminierungsrichtlinien der Europäischen Union sowie entsprechende Vorschriften des Sozialgesetzbuches schließen eine Benachteiligung **schwerbehinderter Beschäftigter** aus. Es ist erforderlich, dass die Beantwortung von Fragen nach der Schwerbehinderung eines Bewerbers als **freiwillig** gekennzeichnet wird.

- Die Frage nach einem **Rentenbezug** durch den Bewerber mag zwar relevant für die sozialversicherungstechnische Beitragsabrechnung sein, sie ist jedoch zum Zeitpunkt der Bewerbung datenschutzrechtlich nicht notwendig und daher unzulässig. Steuerliche und sozialversicherungsrechtliche Fragen werden erst nach Abschluss des Arbeitsvertrages relevant.

- Eine pauschale Abfrage von **Vorstrafen** ist unzulässig. Diese Frage darf nur bei der Besetzung bestimmter Arbeitsplätze gestellt werden (z. B. für Kassierer und Geldboten). Das Fragerecht beschränkt sich dann aber auf bestimmte, für die konkrete Position relevante Vorstrafen. Bei der Formulierung der Frage nach einer Vorstrafe muss dies hinreichend deutlich zum Ausdruck kommen.

Die Handelskette hat nach eingehender Beratung die Vorschläge des ULD umgesetzt und ihren Personalfragebogen inzwischen an die rechtlichen Anforderungen angepasst.

Was ist zu tun?
Die Unternehmen der Privatwirtschaft sollten die durch die arbeitsgerichtliche Rechtsprechung geformten Grundsätze des Fragerechts des Arbeitgebers bei Personaleinstellungen ernst nehmen.

6 Systemdatenschutz

6.1 Der Datenschutzzyklus

Ob Landes- oder Kommunalverwaltung – die Begleitung und Beratung von Einzelprojekten des E-Government gehört zu unserem täglichen Geschäft. Ziel ist eine datenschutzkonforme und sichere Datenverarbeitung in den Verwaltungen im Interesse der Beschäftigten sowie der Bürgerinnen und Bürger durch frühestmögliche Beratung und Unterstützung der Verantwortlichen.

Unser Augenmerk liegt dabei sowohl auf der Gestaltung und Konfiguration der eingesetzten Informationstechnik als auch auf den organisatorischen Rahmenbedingungen der Anwendungen und Fachverfahren. Es genügt nicht, Anforderungen zu formulieren; diese müssen auch in die Verfahren und die Organisation implementiert werden. Die steigende Nachfrage zeigt, dass wir mit unserem kooperativen Ansatz richtig liegen. Die Korrektur eines gravierenden Konzeptfehlers in einem Fachverfahren ist erheblich aufwändiger als die Berücksichtigung und Implementierung der Datenschutzanforderungen bereits von der **Planungsphase** an. Mit fortschreitender Entwicklung des E-Government gewinnen Standardprodukte und -verfahren eine immer größere Bedeutung. Wo immer es möglich ist, konzentrieren wir unsere Beratungsressourcen auf datenschutzrelevante Standardverfahren, von denen zu erwarten ist, dass sie in Zukunft in vielen Verwaltungen von Bedeutung sein werden. Dies gilt für Verfahren der IT-Basisinfrastruktur wie auch für Anwendungen der Fachverfahren. Ein Beispiel ist unsere Veröffentlichung „Datenschutzanforderungen an Dokumentenmanagementsysteme“ (Tz. 6.6), die aus einem intensiven Beratungsprozess mit dem Finanzministerium entstanden ist. Deren Ergebnisse stehen unmittelbar auch anderen Behörden zur Verfügung. Natürlich beraten wir ebenso bei Fragen, die im laufenden Betrieb eines Verfahrens auftauchen.

> ***Im Wortlaut: § 4 Abs. 2 LDSG***
>
> *Produkte, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde, sollen vorrangig eingesetzt werden.*

Konzeption und damit auch die Beratung werden erleichtert, wenn die Verwaltungen auf Produkte zurückgreifen, deren Grundeinstellungen (englisch: „default“) bereits in einem Verfahren überprüft und in Form eines **Datenschutz-Gütesiegels** bestätigt wurden. Das Landesdatenschutzgesetz setzt explizit auf diesen Vereinfachungsmechanismus. Von Jahr zu Jahr erweitert sich das Angebot der mit einem Datenschutz-Gütesiegel versehenen Produkte (Tz. 9.2).

Standardverfahren sind wichtig. Von nicht geringerer Bedeutung ist die datenschutzkonforme Implementierung der Verfahren in konkreten Anwendungsbedingungen. Im Regelfall ist dies keine Hexerei. Die Praxiserfahrungen zeigen aber, dass die Tücken im Detail liegen: bei der Planung und Umsetzung, bei der Organisation des Datenschutzmanagements durch die Formulierung der Dienstanweisungen, bei der Mitbestimmung, bei der Erstellung des Berechtigungskonzeptes,

bei der Festlegung der Verwendungszwecke, bei der Speicherung und Löschung der anfallenden Protokolldaten ... Mit dem **Datenschutz-Audit** hat der Gesetzgeber ein Instrument entwickelt, mit dem die verantwortlichen Stellen ihr Datenschutzkonzept einschließlich der Implementierung von automatisierten Verfahren überprüfen lassen können (Tz. 9.1).

Proaktiver Datenschutz kann **Kontrollen vor Ort** nicht völlig ersetzen. Nicht jede Verwaltung ist bereit oder in der Lage, einen ordnungsgemäßen Zustand ihrer Datenverarbeitung zu gewährleisten. Mit Kontrollen vor Ort werden die Säumigen gemahnt, und das ULD wird in die Lage versetzt, die Praxis vor Ort kennen zu lernen und daraus Hilfestellungen zu entwickeln. Es nützt wenig, eine Lawine an Beanstandungen loszutreten, wenn es an konzeptionellen und **pragmatischen Hilfestellungen** fehlt. Hilfen sind unsere Informationen, unsere Beratung, die Schulung von IT-Verantwortlichen und Datenschutzbeauftragten über die DATENSCHUTZAKADEMIE. Es ist für uns eine permanente Herausforderung, dieses Angebot zu verbessern.

Vom **Datenschutzzyklus** sprechen wir, um das ULD-Angebot über die gesamte Prozesskette der Entwicklung des E-Government zu verdeutlichen: von der frühzeitigen **Konzeptberatung**, der Unterstützung der Beschaffung durch geprüfte, mit einem **Gütesiegel** versehene Produkte, der **Auditierung** ihrer Implementierung im Rahmen eines Datenschutzmanagements und schließlich auch der Instrumente der **Datenschutzkontrolle** vor Ort und der **Schulung** der verantwortlichen Mitarbeiter.

Was ist zu tun?
Die für die Einführung von IT-Verfahren Verantwortlichen sollten sich vom ULD frühzeitig bei ihren IT-Vorhaben beraten lassen.

6.2 Datenschutzkonformes Projektmanagement

Es sollte eigentlich kein Geheimnis sein: Datenschutz setzt eine Ordnung der Datenverarbeitung voraus. Das Datenschutzgesetz spricht ausdrücklich von der „Ordnungsmäßigkeit der Datenverarbeitung". Geordnet und geklärt sein müssen die Ziele, die rechtlichen Voraussetzungen und die Maßnahmen der Datensicherheit. Zur Ordnung gehören Tests, die Freigabe sowie eine Dokumentation des Verfahrens.

Um IT-Verfahren im E-Government erfolgreich einführen zu können, bedarf es technischer wie organisatorischer Kompetenz. Der Erfolg beginnt mit der **Projektierung**. Die Umsetzung der Anforderungen des Datenschutzes und der Datensicherheit muss bei der Implementierung und dann beim Betrieb folgen. Immer wieder werden wir mit automatisierten Verfahren konfrontiert, in denen die Ziele, Schritte und Voraussetzungen nur unzureichend formuliert und dokumentiert sind. Kurz: Das Projektmanagement funktioniert nicht oder nur unzureichend. Die Folgen sind, dass Zeitpläne nicht eingehalten werden, wichtige Anforderungen der Datensicherheit nicht beachtet oder vergessen werden und teurer Nachbesserungsbedarf entsteht.

Für die **Projektphasen** formuliert die Datenschutzverordnung eindeutige Vorgaben, über die Planung und Einführung automatisierter Verfahren strukturiert und die Ordnungsmäßigkeit der Datenverarbeitung gewährleistet werden sollen:

- **IT-Konzept**

„Wenn ich nicht weiß, was ich erreichen will, brauche ich erst gar nicht anfragen." Das IT-Konzept ist der Ort, an dem der **Zweck des Verfahrens** und seine **technisch-organisatorischen Vorgaben** zu beschreiben sind. Diese Anforderungen gehören auch zu den Grundvoraussetzungen jeder Mittelbewirtschaftung. Verblüffend ist, dass dennoch manch ein Projekt in Schleswig-Holstein nur auf der Grundlage von Überschriften, grafischen Skizzen und Powerpoint-Präsentationen geplant und durchgeführt zu werden scheint.

> ***Im Wortlaut: § 4 DSVO***
>
> *Zum Nachweis der Zweckbestimmung des automatisierten Verfahrens (...) sind die technischen und organisatorischen Vorgaben für die Verarbeitung sowie die erzielbaren Ergebnisse in einem informationstechnischen Konzept zu beschreiben.*

- **Sicherheitskonzept**

Es wäre verantwortungslos, IT-Projekte ohne eine Risikoabschätzung unter den Gesichtspunkten des Datenschutzes und der Datensicherheit vorzunehmen. Es ist mittlerweile eine schmerzliche Erfahrung, dass Informationstechnik nicht nur die Effizienz des Verwaltungshandelns erhöhen kann, sondern auch die **Verletzlichkeit der öffentlichen Verwaltung** und der ihr anvertrauten Rechtsgüter. Der Vertrauensverlust in die Funktionsfähigkeit der öffentlichen Verwaltung wäre verheerend, wenn die Daten der Bürgerinnen und Bürger wegen unterlassener Sicherheitsmaßnahmen ungeschützt frei verfügbar wären. Ein Sicherheitskonzept ist nicht nur aus Gründen des Datenschutzes geboten, sondern auch aus Gründen der Rechtmäßigkeit des Verwaltungshandelns sowie der Wirtschaftlichkeit.

> ***Im Wortlaut:***
> ***§ 5 Abs. 2 Satz 1 LDSG***
>
> *Es sind die **technisch-organisatorischen Maßnahmen** zu treffen, die nach dem Stand der Technik und der **Schutzbedürftigkeit** der Daten erforderlich und angemessen sind.*

Im Sicherheitskonzept sind die erforderlichen **technisch-organisatorischen Maßnahmen** darzustellen, mit denen die Risiken für eine unsichere Verarbeitung der personenbezogenen Daten minimiert werden. Es setzt voraus, dass die Schutzbedürftigkeit der Daten und die sich aus den konkreten Verarbeitungsbedingungen ergebenden Umstände analysiert und bewertet werden. Es besteht demnach aus zwei Teilen:

- Um den **Schutzbedarf** der Daten zu ermitteln, ist zu erarbeiten und darzustellen, welche Risiken sich für die personenbezogenen Daten aus den konkreten technisch-organisatorischen Verarbeitungsbedingungen ergeben. Voraussetzung ist die Klärung der rechtlichen Rahmenbedingungen des konkreten Verfahrens.

- Die im Anschluss an die Ermittlung des Schutzbedarfes zu erarbeitenden und zu dokumentierenden **technisch-organisatorischen Maßnahmen** müssen geeignet sein, die im ersten Schritt ermittelten Risiken angemessen zu minimieren. Sie müssen dem Stand der Technik entsprechen.

Konkrete Hilfestellungen und weitere Informationen befinden sich in der Datenschutzverordnung sowie in dem von uns herausgegebenen **backUP-Magazin 1: IT-Sicherheitskonzepte**.

Im Wortlaut:
§ 6 Abs. 1 Satz 1 DSVO

*Auf der Grundlage des Verfahrenszweckes (§ 4 DSVO) hat die Daten verarbeitende Stelle in einem **Sicherheitskonzept** darzustellen, welche technischen und organisatorischen Maßnahmen unter Berücksichtigung der tatsächlichen örtlichen und personellen Gegebenheiten getroffen wurden, um die Anforderungen der §§ 5 und 6 LDSG zu erfüllen.*

- **Verfahrenstest**

Bevor automatisierte Verfahren mit personenbezogenen Daten in den Produktivbetrieb gehen, müssen die eingesetzten **Programme und die im Sicherheitskonzept festgelegten Maßnahmen getestet** werden. Gemäß der Datenschutzverordnung sind die Testmaßnahmen und Ergebnisse sowie die bei den Tests eingesetzten informationstechnischen Geräte und Programme zu protokollieren. Der Verzicht auf Tests ist fahrlässig. Fehlende Dokumentationen der Tests fallen auf die Verantwortlichen zurück. Mit ihnen kann der Nachweis geführt werden, dass das automatisierte Verfahren vor seiner Freigabe nach allen Regeln der Kunst geprüft wurde.

- **Freigabe**

Im Wortlaut: § 5 Abs. 2 Satz 2 LDSG

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

Die Freigabe markiert die Grenze zwischen Planung und Einführung (der Projektphase) sowie dem Produktivbetrieb. Sie erfolgt durch die jeweilige Dienststellenleitung oder eine ausdrücklich befugte Person. Mit der Freigabe übernimmt die **Leitung der Dienststelle** die Verantwortung für die Ordnungsmäßigkeit der Verarbeitung personenbezogener Daten. Dieser Verantwortung kann sie nur gerecht werden, wenn für sie die Dokumentation des Verfahrens überprüfbar ist. Aus diesem Grund schreibt die Datenschutzverordnung ausdrücklich vor, dass die Dokumentation „für sachkundige Personen in angemessener Zeit nachvollziehbar“ sein muss. Freizugeben sind übrigens nicht nur automatisierte Verfahren, die das erste Mal eingesetzt werden, sondern auch ihre späteren Änderungen.

- **Dokumentation**

Zur Ordnungsmäßigkeit der Datenverarbeitung gehört die Dokumentation des automatisierten Verfahrens. Sicher: Die meisten Techniker „schrauben“ lieber an ihren Rechnern, als dass sie Dokumentationen erstellen. Aber: Eine vollständige

Dokumentation ist unabdingbar, um die **Sicherheit und Verfügbarkeit der eingesetzten Verfahren** zu gewährleisten. Im Schadensfall, bei einem Personalwechsel, einer Änderung des Verfahrens oder einem Systemwechsel müssen die Verantwortlichen und die von ihnen beauftragten Personen die erforderlichen Unterlagen über die Funktionsweise des Systems zur Hand haben. Die Dokumentation umfasst die Informationen über den Zweck und die Beschreibung des Verfahrens, das Sicherheitskonzept, die durchgeführten Tests sowie die Freigabe.

Was ist zu tun?
Die Ordnungsmäßigkeit der Datenverarbeitung beginnt bereits mit der Phase der Planung eines automatisierten Verfahrens. Sie erfordert ein IT-Konzept, ein Sicherheitskonzept, die Durchführung von Tests, eine Freigabeentscheidung durch die Dienststellenleitung sowie eine Dokumentation. Dies sind die Mindestanforderungen an die Durchführung von IT-Projekten.

6.3 Von Piloten und anderen Geisterfahrern

Als „Piloten“ sind dem ULD automatisierte Verfahren vorgestellt worden, für die keine Freigabe erfolgt war, geschweige denn die Voraussetzungen hierfür erfüllt waren. Gleichwohl wurden bereits personenbezogene Daten wie in einem produktiven Betrieb verarbeitet.

Vielleicht sind die hohe Komplexität und ein unangemessener Zeitdruck die Gründe, dass uns Projekte als bloßer Pilotbetrieb vorgestellt wurden, die aber tatsächlich bereits im Produktivbetrieb mit personenbezogenen Daten liefen – so geschehen etwa bei der Einführung von Voice-over-IP in drei Landesbehörden oder bei der Vertrauensstellung des Active Directory Schleswig-Holstein/Hamburg. Die äußerst dürftige Konzeptlage wurde mit dem Hinweis gerechtfertigt, man sei ja noch dabei, die erforderlichen Unterlagen zu erarbeiten. Derartige Verzögerungen sind – bei allem Verständnis für die Nöte von Projektverantwortlichen – **eindeutige Grenzen** gesetzt, wenn personenbezogene Daten verarbeitet werden (24. TB, Tz. 7.2).

Ein Pilotbetrieb

- setzt eine nach Beginn und Ende **vorab zeitlich begrenzte Laufzeit** voraus,
- muss in einem **IT-Konzept** beschrieben sein,
- bedarf eines **Sicherheitskonzeptes**, das sich aber auf einen beschränkten Funktionsumfang des Piloten beschränken kann,
- bedarf der **Freigabe** durch die Dienststellenleitung bzw. der von ihr beauftragten Person,
- bedarf einer fortlaufenden **Auswertung**, deren Ergebnisse und Schlussfolgerungen am Ende des Pilotbetriebes zusammengefasst werden.

Entweder ein Verfahren ist gut durchdacht und konzipiert, dann wird sich auch der Aufwand zur Erstellung der Konzeptlage in Grenzen halten, oder aber wesentliche

Fragen der Datensicherheit sind noch nicht geklärt, dann wird sich der Pilotbetrieb für die Daten der Betroffenen eher als eine Risikoerhöhung als eine Minimierung darstellen. Bei Unklarheiten stehen wir zur Beratung zur Verfügung.

Was ist zu tun?
Die Bezeichnung eines automatisierten Verfahrens als Pilot befreit die Verwaltungen nicht von der Verpflichtung, die Vorgaben der Datenschutzverordnung zu beachten.

6.4 Sicherheitskonzept à la BSI-Grundschutz?

Das Datenschutzrecht erfordert bei automatisierten Verfahren die Erstellung eines Sicherheitskonzeptes. Wir wurden gefragt, ob mit der Befolgung der Vorgaben des „BSI-Grundschutzes“ das Nötigste für den Datenschutz geleistet sei.

Im Sicherheitskonzept nach der Datenschutzverordnung (DSVO) sind die erforderlichen **technisch-organisatorischen Maßnahmen** darzustellen, mit denen die Risiken bei der Datenverarbeitung minimiert werden. Das Sicherheitskonzept setzt eine **Analyse der Schutzbedürftigkeit** der Daten unter den konkreten Verarbeitungsbedingungen des automatisierten Verfahrens voraus (Tz. 6.2). Verbleibenden Risiken muss unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes begegnet werden.

In letzter Zeit wurden uns mehrfach Unterlagen als Sicherheitskonzept vorgelegt, in denen **formularmäßig Sicherheitsmaßnahmen** beschrieben wurden, die sich an dem IT-Grundschutzhandbuch (IT-GSHB) des Bundesamts für Sicherheit in der Informationstechnik (BSI) orientierten. Diese Dokumente sind nahezu ausnahmslos mit einer Programmunterstützung (Grundschutztool – GS-Tool) erstellt.

Das IT-Grundschutzmodell des BSI verfolgt einen anderen Ansatz als die DSVO. Statt auf die Sicherheitsbedürfnisse eines konkreten Verfahrens einzugehen, wird ein mehrstufiger Ansatz zur Herstellung eines einheitlichen Sicherheitsniveaus gewählt. Durch „Summenbildung“ aller Einzelmaßnahmen wird dann ein erreichtes Grundschutzniveau dokumentiert.

Ein Sicherheitskonzept nach der DSVO verlangt mehr als eine listenartige Erfassung von Einzelmaßnahmen. Im Sicherheitskonzept müssen Aussagen über die Qualität und Ausgestaltung der Sicherheitsmaßnahmen getroffen werden, die auf den Schutzbedarf einer konkreten Anwendung zielen. Die DSVO erfordert also gegenüber dem GS-Tool eine **größere Präzision**. Das GS-Tool kann für die Gewinnung technisch-organisatorischer Maßnahmen eine gute Hilfestellung bieten, ersetzt aber nicht die von der DSVO geforderte analytische Arbeit.

Außerdem gilt: **IT-Grundschutz ist mehr** als die Generierung von Sicherheitsmaßnahmen nach dem GS-Tool und bedarf einer intensiven Schulung. IT-Grundschutz verlangt die Einführung und Anwendung eines kompletten IT-Manage-

mentprozesses. Erst durch das Ausrichten der eigenen IT-Sicherheitsorganisation nach dem vom BSI vorgeschlagenen Aufbau und den Abläufen lassen sich die im BSI-Grundschutzhandbuch definierten Ziele auch erreichen.

Was ist zu tun?
Das GS-Tool des BSI bietet eine gute Hilfestellung, um Sicherheitsmaßnahmen zu generieren. Es ersetzt aber nicht die Analyse des Schutzbedarfes eines konkreten Verfahrens und die Anpassung der einzelnen Maßnahmen auf die konkrete Situation.

6.5 Datenschutzgerechte Protokollierung

Es entspricht guter Praxis sowie dem Datenschutzrecht, dass die Aktivitäten der Systemadministratoren zu protokollieren und diese zu kontrollieren sind. Systemseitig zu protokollieren ist auch die Nutzung der Anwender der Fachverfahren. Die Revisionsfestigkeit der Aktivitäten „am Herzen der IT-Systeme“ ist von zentraler Bedeutung. Die Protokollierung des Verhaltens von Nutzern und Systemadministratoren muss den Grundregeln des Arbeitnehmerdatenschutzes genügen.

Gestaltende Zugriffe auf Betriebssysteme und Anwendungsprogramme sind nur den dazu berechtigten **Systemadministratoren** erlaubt. Ihre Aktivitäten sind zu protokollieren und die Protokolle zu kontrollieren. Näheres regelt die Datenschutzverordnung.

Im Wortlaut: § 6 Abs. 2 LDSG

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

Protokolliert werden systemseitig auch die Aktivitäten der Nutzer, insbesondere wenn ein Verfahren ausschließlich elektronisch durchgeführt wird. Im Regelfall sind dies die **Beschäftigten** in den Verwaltungen. Das Datenschutzrecht verlangt, dass bei der Protokollierung die Grundsätze der Datensparsamkeit und der Zweckbindung beachtet werden müssen. Eine Protokollierung der Nutzeraktivitäten darf nur den Zwecken der Datensicherheit dienen, nicht einer Verhaltens- oder Leistungskontrolle. Die Protokollierung dient dem Nachweis, dass nur die berechtigten Personen Daten verarbeiten, dagegen nicht der Feststellung, wann ein Beschäftigter bei der Arbeit Pausen eingelegt hat.

Im Wortlaut: § 23 Abs. 2 LDSG

Daten von Beschäftigten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach den §§ 5 und 6 gespeichert oder in einem automatisierten Verfahren gewonnen werden, dürfen nicht für Zwecke der Verhaltens- oder Leistungskontrolle ausgewertet werden.

Die Protokollierung ist gegenüber dem Fachverfahren ein **eigenständiges Verfahren**. Deren Gegenstand sind nicht die personenbezogenen Daten des Fachver-

fahrens, sondern die des Administrators oder des Anwenders des Fachverfahrens. Manches wäre einfacher, wenn die Fachverfahren nach einem einheitlichen Standard protokollieren würden. Leider ist dies nicht der Fall. Die Fachverfahren werfen zumeist unterschiedliche Sets von Protokolldaten aus. Daher müssen für jedes Verfahren für die Protokollierung die Zwecke festgelegt werden. Nötig ist die Abgrenzung von anderen Verfahren und ein eigenes Sicherheitskonzept für die Protokolldaten. Im Einzelnen sind folgende Entscheidungen zu treffen:

- Wer ist für die Aufbereitung zuständig?
- Wie werden die Protokolldaten aufbereitet?
- Auf welchem Rechner werden die Protokolldaten gespeichert?
- Wer ist für die Auswertung zuständig?
- Zu welchem Zweck darf eine Auswertung erfolgen?
- Welche Daten sind für die Auswertung erforderlich?
- Werden die Protokolldaten nach Auswertungszweck differenziert aufbereitet?
- Wird eine Pseudonymisierung von Protokolldaten durchgeführt?

Eine Protokollierung umfasst im Kern **drei Bestandteile**:

- Zeitstempel,
- Aktion,
- die den Protokolleintrag auslösende und beteiligte Instanz.

Die Instanz kann eine Maschine, eine Applikation oder ein Mensch sein.

Damit eine Protokollierung sinnvoll geprüft werden kann, müssen ihre Einträge richtig sein, d. h., das Verfahren muss **vertrauenswürdig** sein. So einfach sich dies anhört, so anspruchsvoll ist die sicherheitstechnische Umsetzung und Bewertung: Um den richtigen Zeitpunkt zu protokollieren, könnte man sich z. B. auf die Systemzeit des Rechners beziehen, auf dem die Protokollierung erfolgt. Man kann sich aber auch auf die Zeit aus einem Zeitstempeldienst innerhalb des Rechenzentrums oder auf einen kommerziellen Zeitstempeldienst aus dem Internet stützen, der eine signierte Zeit anliefert. Korrekt und aussagekräftig müssen auch die Informationen sein, die in den Protokolleintrag geschrieben werden. Die Instanz, die die Aktion ausgelöst hat, muss zweifelsfrei festzustellen sein.

Die Protokolldatei muss dem schreibenden Zugriff der Systemadministratoren entzogen sein. Sollen Protokolldaten aussagekräftige Informationen über Systemaktivitäten bieten, müssen **Manipulationen ausgeschlossen** werden. Diese Vorkehrungen schützen auch die Systemadministratoren vor unberechtigten Verdächtigungen. Eine manipulationsresistente Protokollierung ist gleichwohl leichter gefordert als umgesetzt: Nach unseren Recherchen genügen weder Windows 2003 Server noch syslog-Architekturen auf UNIX-Servern diesen Anforderungen.

Was ist zu tun?
Die Protokollierung sollte auf dedizierte und mandantenfähige Protokollserver ausgelagert werden, um eine datensparsame, aussagekräftige und revisionssichere Protokollierung und deren Kontrolle zu gewährleisten.

6.6 Dokumentenmanagementsystem elektronischer Akten

Welche Vorteile Dokumentenmanagementsysteme auch immer bieten, es handelt sich aus Datenschutzsicht um mächtige Instrumente. Sie ermöglichen eine umfassende Erfassung und Kontrolle der Tätigkeit der Beschäftigten. Dokumentenmanagementsysteme bedürfen einer datenschutzkonformen Gestaltung.

Im Zuge der Entscheidung für ein bestimmtes Produkt als Dokumentenmanagementsystem für Landesbehörden begleiten wir das zuständige Finanzministerium, in dem eine Pilotanwendung des Produktes VISkompakt an einigen Arbeitsplätzen installiert ist. Ein Ergebnis der Beratung ist ein Arbeitspapier, das unter dem Titel „**Datenschutzanforderungen an Dokumentenmanagementsysteme**“ von unserer Webseite abgerufen werden kann.

 www.datenschutzzentrum.de/e-government/anforderungen-dms.pdf

Drei gestaltungsbedürftige **Themen** sind herauszuheben:

- das Einscannen von Papierunterlagen,
- die Regelung der Zugriffsberechtigungen,
- die Regelung der Protokollierung.

Das **Einscannen** eines Papiers ist ein regelungsbedürftiger Arbeitsprozess. In einer Dienstanweisung sollte festgelegt werden, welche Dokumente nicht eingescannt und damit elektronisch verfügbar und bearbeitbar gemacht werden dürfen. Beschränkungen unterliegen z. B. als Verschlusssachen gekennzeichnete Dokumente. Auch bei Daten, die dem Sozialgeheimnis, dem Personalaktengeheimnis oder anderen Amts- oder Berufsgeheimnissen unterliegen, ist Zurückhaltung angeraten. Gewährleistet werden muss die Übereinstimmung der gescannten Kopie mit dem Papieroriginal, damit nicht unrichtige Daten in den elektronischen Arbeitsprozess Eingang finden.

Eine zentrale Funktion haben die Festlegungen, die in einem differenzierten Rollenkonzept getroffen werden, wer über welche **Zugriffsrechte** auf Dokumente bzw. Objekte verfügt. VISkompakt identifiziert z. B. als Objekttypen den Aktenplan, die Akte, den Vorgang, das Dokument, die Adresse. Folgende Rollen, an denen unterschiedliche Zugriffsrechte haften, kennt dieses System: Applikationsadministrator, Posteingang, Sachbearbeiter, Führungskraft. Als Operationen, mit denen Objekte behandelt werden, sind vorgegeben: Anlegen, Ändern, Lesen, Löschen, Suchen, Rechtesetzen, Umprotokollieren, Reorganisation, Stellvertretung. Mit diesen drei Dimensionen lässt sich eine Matrix anlegen, in der transpa-

rent, funktional und datenschutzgerecht festgelegt wird, welche Rolle welche Art der Operation auf welches Objekt anwenden darf. Ferner ist zu definieren, welche Rollen einer Person zugewiesen werden dürfen und welche nicht.

Die neue Qualität eines Dokumentenmanagementsystems besteht darin, dass die Tätigkeiten der Beschäftigten automatisiert und im Detail erfasst und ausgewertet werden können. Diese **Protokollierungen** lassen sich in drei Kategorien gliedern:

- **Metadaten** bezeichnen Eigenschaften des Dokuments.
- **Vorgangsdaten** informieren über den Workflow in der (Sub-)Organisation.
- **Logdaten** liefern Informationen über die Eigenschaften des technischen Zustands der Applikation bzw. des Betriebssystems und der Netzanbindung.

Jede Kategorie ergibt für sich und erst recht in der Kombination eine brisante Sammlung an Informationen über die Leistung und das Verhalten der Beschäftigten. Aus diesem Grund ist besondere Sorgfalt auf die Gewährleistung der Datensparsamkeit und der Zweckbindung dieser Informationen zu legen.

Was ist zu tun?
Die Beachtung unserer „Datenschutzanforderungen an ein Dokumentenmanagementsystem“ verhindert Ärger mit den Bediensteten und dem ULD.

6.7 Clearingstellen sind nur eine Übergangslösung

Vom 1. Januar 2007 an muss die Übermittlung der elektronischen Rückmeldung im Meldewesen zwischen den Meldeämtern nach bundeseinheitlichen Vorgaben funktionieren. Die Kommunikation zwischen den Meldeämtern soll über eine Vermittlungsstelle („Clearingstelle“) erfolgen.

In der Landesmeldeverordnung ist festgelegt, dass die Datenübermittlungen zwischen den Meldeämtern im Verfahren der Rückmeldung über eine zentrale Vermittlungsstelle erfolgen muss. Diese wird auch als **Clearingstelle** bezeichnet. Die Aufgabe wurde dataport übertragen. Sie wird von Hamburg und Schleswig-Holstein gemeinsam betrieben, weswegen wir in enger Abstimmung mit unseren Hamburger Datenschutzkollegen vorgehen.

Der kritische Punkt des Konzeptes der Clearingstelle ist, dass die Meldedaten – einschließlich sensibler Angaben wie z. B. zur Religionszugehörigkeit – erst in der Clearingstelle in das **Übermittlungsformat OSCI-Transport** übersetzt werden. Begründet wird die Notwendigkeit einer Clearingstelle damit, dass man den Meldeämtern die Einhaltung der vorgeschriebenen Übermittlungsformate nicht zutraue. Die Clearingstelle müsse Korrekturfunktionen übernehmen,

indem sie z. B. Inkompatibilitäten der Formate behebe oder zur richtigen Übermittlung Routinginformationen für die Adressierung einer Nachricht auslese. Mittelfristig soll die Clearingstelle als Datendrehscheibe wohl auch für andere Datenübermittlungen zumindest innerhalb des Landes genutzt werden.

Eine Vermittlungsstelle wäre an sich nicht notwendig, denn der in Deutschland allgemein anerkannte Standard OSCI-Transport ermöglicht eine gesicherte Übermittlung von der einen Meldebehörde zur anderen. Genau zu diesem Zweck ist dieser Standard mit Steuermitteln entwickelt worden und hat europaweit eine Vorbildfunktion. OSCI-Transport orientiert sich an dem in der Wirtschaft weit verbreiteten Modell der **Ende-zu-Ende-Sicherheit**. Mittlerweile wird auch nicht mehr bestritten, dass praktisch alle in Schleswig-Holstein eingesetzten Meldefachverfahren diesen Standard beherrschen.

Der von der Konferenz der Innenminister eingesetzte Arbeitskreis I hat die Clearingstellen zur Abwicklung der Rückmeldung nur für eine **Übergangszeit** vorgesehen und sich in einem Beschluss vom November 2002 dafür ausgesprochen, Clearingstellen nur dort, wo es notwendig ist, einzusetzen und den Standard OSCI-Transport verbindlich vorzuschreiben. In einem späteren Beschluss vom März 2003 heißt es, „auf jedem Kommunikationsweg (d. h. auch landesintern)“ sei das gleiche Sicherheitsniveau einzuhalten.

Nach Auffassung der Konferenz der Datenschutzbeauftragten, die hierzu am 16. Dezember 2005 eine Entschließung gefasst hat, entspricht der Standard OSCI-Transport dem **Stand der Technik**, weil er eine Ende-zu-Ende-Sicherheit und damit rechtsverbindliche Transaktionen unmittelbar zwischen den beteiligten Kommunikationspartnern ermöglicht. Clearingstellen können nur eine Übergangslösung sein.

Für unsere datenschutzrechtliche Bewertung der Clearingstelle wird es maßgeblich auf die in dem **Sicherheitskonzept** getroffenen und implementierten organisatorischen und technischen Maßnahmen ankommen, die das Risiko eines unbefugten Zugriffs oder einer technischen Fehlschaltung auf die Meldedaten minimieren. Das Sicherheitskonzept liegt uns noch nicht vor.

www.datenschutzzentrum.de/material/themen/presse/20051216-dsbk-osci.html

Was ist zu tun?
Mit OSCI-Transport steht ein datenschutzkonformer Standard für eine Ende-zu-Ende-Verschlüsselung zwischen Behörden zur Verfügung. Clearingstellen sind nur ein Notbehelf für eine Übergangszeit.

6.8 Gewusst wo – im Geodatenserver

Die allgemeine Verfügbarkeit von raumbezogenen Daten der öffentlichen Vermessungs- und Liegenschaftskataster (Geobasisdaten) wurde in den letzten Jahren verstärkt vorangebracht. Aus Datenschutzsicht ist von Bedeutung, ob und inwieweit durch hochauflösendes Karten- und Fotomaterial und räumlich zugeordnete Datenbankinformationen ein Personenbezug hergestellt werden kann.

Raumbezogene Entscheidungen und Handlungen von Wirtschaft und Verwaltung sollen vereinfacht und zugleich der Service für Bürger, Unternehmen und Verwaltungsangehörige verbessert werden. Diese Ziele verfolgen Schleswig-Holstein und Hamburg gemeinsam mit dem Projekt **Geodatenserver**. Der Geodatenserver soll die Basisdaten der Kataster- und Vermessungsämter und die Geofachdaten beteiligter Behörden über standardisierte Dienste bündeln und sie der Verwaltung, aber auch der Wirtschaft und den Bürgerinnen und Bürgern zur Verfügung stellen. Über das Internet können dann zukünftig die Einsatzleitstellen der Polizei, der Feuerwehr und der medizinischen Rettungsdienste ebenso mit Geoinformationen versorgt werden wie die Bürger und Unternehmen.

Geoinformationen können sowohl aus Landkarten verschiedener Auflösungen als auch aus entzerrten Luftbildern (Orthofotos) sowie Satelliten- und Navigationsdaten bestehen. Durch das Übereinanderlegen verschiedener Karten („Verschneiden“) kann die Informationsdichte in einer Art optisch-statistischem Verfahren deutlich erhöht werden. Erleichtert wird das Verschneiden durch den Standard des Open Geo Spatial Consortium (OGC), der die Datennutzung über das Internet ermöglicht. Werden diese Informationen mit soziodemografischen Informationen über kleine Räume wie Straßen, Plätze oder Wohnblocks aus anderen Quellen zusammengeführt, so können kleinräumige Informationscluster erzeugt werden, mit deren Hilfe sich Zusatzinformationen über einzelne Adressen gewinnen lassen. Mit Zusatzinformationen angereicherte Geodaten sind z. B. für den Adresshandel wertvoll, wenn sie qualitative Ansatzpunkte für eine gezielte Werbung ermöglichen. Umgekehrt ist das Interesse der betroffenen Eigentümerinnen und Eigentümer oder Bewohnerinnen und Bewohner evident, ohne ihr Einverständnis

Im Wortlaut: § 13 Abs. 3 VermKatG

Folgende Personen und Stellen können personenbezogene Daten einsehen und entsprechende Auskünfte und Auszüge erhalten:

1. *Eigentümerinnen und Eigentümer sowie Inhaberinnen und Inhaber grundstücksgleicher Rechte über die sie betreffenden Liegenschaften,*
2. *Personen und Stellen, die ein berechtigtes Interesse darlegen,*
3. *Vermessungsstellen sowie Notarinnen und Notare, soweit dies zur rechtmäßigen Erfüllung ihrer Aufgaben erforderlich ist, und*
4. *gebietsdeckend für ihren Zuständigkeitsbereich die Behörden und sonstigen öffentlichen Stellen sowie diejenigen nichtöffentlichen Stellen, die leitungsgebundene Ver- und Entsorgungsleistungen erbringen, soweit es zur rechtmäßigen Erfüllung ihrer Aufgaben erforderlich ist.*

nicht zum Ausforschungsobjekt, zur Handelsware oder zum Adressaten gezielter Werbemaßnahmen zu werden.

Für die datenschutzrechtliche Bewertung ist zwischen den Informationen zu unterscheiden, die über den Geodatenserver selbst verfügbar sind, und den Informationen, die von Dritten mit anderen Geo- oder Adressinformationen verschnitten werden können. Für die Veröffentlichung von Informationen aus dem Geodatenserver gilt das Vermessungs- und Katastergesetz (VermKatG). Danach erhalten z. B. Notarinnen und Notare oder Energieversorger für ihre spezifischen Zwecke einen privilegierten **Informationszugang**. Sonstige Dritte dürfen personenbezogene Informationen aus dem Liegenschaftskataster nur bekommen, wenn sie ein berechtigtes Interesse darlegen. Die Eigentümer erhalten als Betroffene Einsicht in den sie betreffenden Teil des Liegenschaftskatasters.

Die Bereitstellung von personenbezogenen Geoinformationen zum Abruf ist eine Übermittlung im Sinne des Datenschutzrechts. Die Empfänger dieser Daten müssen von dem Betreiber des Geodatenservers verpflichtet werden, die Daten nur zu dem Zweck zu verwenden, zu dem sie ihnen übermittelt worden sind. Der **Verwendungszweck** richtet sich nach dem dargelegten berechtigten Interesse.

Im Wortlaut: § 15 Abs. 2 LDSG

Die übermittelnde Stelle hat die empfangende Stelle zu verpflichten, die Daten nur zu dem Zweck zu verwenden, zu dem sie ihr übermittelt wurden.

Mit dem geplanten Geodatenserver werden nicht nur Verwaltungsinformationen zugänglich gemacht. Zugleich soll eine Plattform für die **Bezahlung** für Informationsprodukte eingerichtet werden, die auch für andere Zwecke eingesetzt werden kann. Diese Zahlungsfunktion muss datenschutzkonform gestaltet sein, zumal die Nutzer dieser Plattform Informationen wie Bankverbindungen im Fall der Einwilligung zum Lastschrifteinzug oder Angaben ihrer Kreditkartennummer anvertrauen. Die rechtlichen Anforderungen hierfür ergeben sich aus dem Teledienstedatenschutzgesetz.

Was ist zu tun?
Technik und Ablauforganisation des geplanten Geodatenservers sowie die Paymentplattform bedürfen einer datenschutzkonformen Gestaltung, damit dieser bei Betroffenen wie Nutzern die notwendige Akzeptanz findet.

6.9 IP-Telefonie

Aufgrund eines Kabinettsbeschlusses werden in den Landesbehörden die Endgeräte für die Sprachtelefonie ausgetauscht. Damit bietet das Finanzministerium Internettechnologie beim Telefonieren bis zum Schreibtisch des einzelnen Behördenmitarbeiters.

Der Beschluss ist gefasst, aber das **Sicherheitskonzept** ist noch in Arbeit. Dies ist kein guter Zustand. Uns stellen sich ungeachtet der administrativen Vorteile einer

zentralen Steuerung der Sprachtelefonie durch das Finanzministerium einige noch zu beantwortende Fragen. Zentraler Gesichtspunkt ist, dass administrative Zugriffe vonseiten des Finanzministeriums, seiner Auftragnehmer und Unterauftragnehmer auf das jeweilige Endgerät nicht die Verantwortung der einzelnen Behörde für die Datensicherheit des eigenen Netzes infrage stellen dürfen.

Was ist zu tun?
Systementscheidungen ohne eine vorherige Sicherheitsbetrachtung sind ein riskantes Unterfangen. Wir empfehlen, künftig die Anforderungen des Datenschutzes und der Datensicherheit als Kriterien in die Ausschreibung aufzunehmen.

6.10 Fusionen und Kooperationen von Verwaltungen

Im Zuge der Verwaltungsreform steht die Zusammenlegung der Informationstechnik unterschiedlicher Verwaltungen auf der Agenda. In welcher Rechtsform auch immer die Verwaltung effizienter werden soll, die Beachtung des Datenschutzes bleibt gesetzliche Pflicht und Verpflichtung gegenüber den Bürgerinnen und Bürgern.

Die Informationstechnik in Kommunen kann unterschiedlich als eine gemeinsame Aufgabe gestaltet und organisiert werden: als Zweckverband, als Verwaltungsgemeinschaft, durch Nutzungsvereinbarung oder durch Bildung gemeinsamer Kommunalunternehmen. Welchen Weg die Verantwortlichen unter politischen und wirtschaftlichen Gesichtspunkten auch immer wählen, es bedarf ungeachtet der zahlreichen Rechtsfragen **der sorgfältigen Planung und eines strukturierten Vorgehens**, wenn unterschiedliche IT-Infrastrukturen und Fachverfahren unter einem Dach zusammengeführt werden sollen. Bei den Kooperationen dürfen die Verantwortlichkeiten nicht verwischt werden. Von praktischer Bedeutung ist vor allem das Instrument der Auftragsdatenverarbeitung, zu dem wir im 27. Tätigkeitsbericht (Tz. 6.1) detaillierte Handlungsempfehlungen gegeben haben. Bei Zweifelsfragen beraten wir gerne.

Was ist zu tun?
Fusionen oder Kooperationen bei der Informationstechnik unterschiedlicher Verwaltungen bedürfen der sorgfältigen Planung, eines strukturierten Vorgehens und der Beachtung der datenschutzrechtlichen Vorgaben.

6.11 SOHO in landesweiten IT-Konzepten

Aktuelle Informationstechnik für kleine Büros und Heimnetzwerke ist oft günstig und leistungsfähig. Lässt sich diese preiswerte Technik für große IT-Projekte nutzen, ohne dass Datensicherheit und Datenschutz auf der Strecke bleiben?

Für den Bereich der ambitionierten Heimanwender oder für kleine Büroumgebungen (SOHO steht für Small Office Home-Office) existieren leistungsfähige und vor allem preiswerte Informations- und Kommunikationskomponenten (IuK), die auf den ersten Blick die gleichen **Leistungsmerkmale** anbieten wie Lösungen für den professionellen Bereich. Doch fehlen diesen Komponenten häufig Funktionalitäten, die für den professionellen Einsatz zwingend nötig sind:

- zentrales Management einer Vielzahl gleichartiger Geräte,
- erweiterte Sicherheitsfunktionen zur Integration in große IT-Umgebungen,
- Auslegung der Hardware auf einen Rund-um-die-Uhr-Betrieb,
- Skalierbarkeit für zukünftige Einsatzszenarien.

Im Rahmen eines IT-Großprojektes des Landes stießen wir auf Planungen für ein am Netzwerk anzuschließendes Speichergerät (NAS Devices – **Network Attached Storage**). Derartige Geräte haben den Vorteil, dass sie klein, günstig und flexibel sind und viele Daten speichern können. Bei einer intensiven Prüfung erwies sich, dass deren Einsatz die Nutzung in der landesweit vernetzten Umgebung eingeschränkt hätte, da die Geräte nicht die zentrale Authentifizierung des Landes über das Active Directory unterstützen. Zudem fehlten Schnittstellen, um die für den Einsatz erforderliche Zahl dieser Geräte – mehrere hunderte – zentral zu managen. Die Projektleitung hat sich nach unserer Beratung entschlossen, auf eine andere, mit den landesweiten IT-Standards vereinbare Lösung zu setzen.

Was ist zu tun?
Bevor SOHO-Geräte in großen Netzwerken eingesetzt werden, muss geprüft werden, ob sie allen Ansprüchen genügen. Besonders zu achten ist auf die Kriterien Skalierbarkeit, zentrales Management, erweiterte Sicherheitsfunktionen sowie die Integration in die landesweite IT-Umgebung.

6.12 Kontrollen vor Ort – ausgewählte Ergebnisse

Flächendeckende Routineüberprüfungen im kommunalen Bereich bringen häufig **keine spektakulären Ergebnisse**. Oft ist schon nach kurzer Gesprächsdauer erkennbar, welchen Stellenwert Datenschutz und Datensicherheit in der Organisation einnehmen und ob bzw. welche technisch-organisatorischen Maßnahmen ergriffen wurden.

6.12.1 Ein geschulter Datenschutzbeauftragter ist ein Gewinn

Die Bestellung von Datenschutzbeauftragten führt in der Regel zu einer deutlichen Erhöhung des Datenschutz- und Datensicherheitsniveaus in den Verwaltungen.

> ***Im Wortlaut: § 10 Abs. 1 LDSG***
>
> *Die Daten verarbeitende Stelle kann schriftlich eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten bestellen ...*

Tendenziell positive Prüfungsergebnisse ergaben sich bei den Organisationen, in denen engagierte Datenschutzbeauftragte und/oder Systemverantwortliche tätig sind. Bereits mit der **Bestellung eines Datenschutzbeauftragten** signalisiert eine Stelle ihre grundsätzliche Bereitschaft, dem Schutz und der Sicherheit der Daten der Bürgerinnen und Bürger einen hohen Stellenwert einzuräumen: Es spielt eine große Rolle, ob der behördliche Datenschutzbeauftragte nur eine „Feigenblattfunktion“ erfüllt oder ob er seine Rolle ernsthaft ausübt.

- Ist für die Behördenleitung die **Einhaltung der datenschutzrechtlichen Vorschriften** ein Anliegen, so ist die Beauftragung einer Mitarbeiterin oder eines Mitarbeiters hilfreich, der dies unterstützt und überprüft. Viele neu bestellte Datenschutzbeauftragte haben die Schulungen der DATENSCHUTZAKADEMIE besucht; so können wir damit rechnen, dass wir ein in den Grundzügen einheitliches Vorgehen in der Organisation antreffen.
- In der Regel wirkt der Datenschutzbeauftragte bei der Erstellung und Führung der von der Datenschutzverordnung (DSVO) geforderten **Dokumentationen** mit und **überwacht** die datensicherheitstechnischen Maßnahmen innerhalb der Organisation. Seine Beteiligung gewährleistet, dass wir eine anforderungsgerechte Dokumentation nach der DSVO vorfinden.
- Viele Datenschutzbeauftragte sensibilisieren die Mitarbeiter am PC-Arbeitsplatz in Bezug auf Datenschutz und Datensicherheit und führen eigene **Schulungen** durch. Nach unserer Erfahrung ist die Datensicherheit in den Verwaltungen deutlich höher, in denen derartige Schulungen stattfinden.
- Der Datenschutzbeauftragte und der Systemverantwortliche sind während einer Prüfung direkte **Ansprechpartner**, begleiten die Prüfung und können bei eventuell vorgefundenen Mängeln vor Ort beratende Hilfe von den Prüfern in Anspruch nehmen.

> ***Im Wortlaut:***
> ***§ 10 Abs. 2 Satz 1 LDSG***
>
> *Die oder der behördliche Datenschutzbeauftragte muss die erforderliche Sachkunde und Zuverlässigkeit besitzen.*

Wir können immer dann eine gute Umsetzung der datenschutzrechtlichen und datensicherheitstechnischen Vorgaben feststellen, wenn die Systemadministratoren eine **Datenschutzschulung** mit einem hohen Praxisanteil z. B. bei der DATENSCHUTZAKADEMIE besucht haben. Es macht einen deutlichen

Unterschied, ob ein Systemadministrator ein IT-System nur technisch beherrscht oder ob er zusätzlich datensicherheitstechnische Aspekte in das System integrieren kann.

Wir ermöglichen, dass Systemadministratoren Seminare mit einem **Zertifikat** abschließen können. Die Fortbildung qualifiziert die Teilnehmer, ein IT-System von der Konzeption bis zum praktischen Betrieb unter Beachtung der datenschutzrechtlichen und datensicherheitstechnischen Hintergründe zu planen und zu verwalten. Auch in diesem Jahr konnten wir wieder sieben Zertifikate verleihen.

Was ist zu tun?
Die Bestellung eines behördlichen Datenschutzbeauftragten erleichtert der Verwaltung die Integration der Datenschutzanforderungen in die Verwaltungspraxis. Der Besuch von Fort- und Weiterbildungsveranstaltungen z. B. an der DATENSCHUTZAKADEMIE erhöht das Datenschutzniveau in den Verwaltungsorganisationen.

6.12.2 Gemeindeverwaltung Flintbek

Bei der routinemäßigen Überprüfung der Gemeindeverwaltung Flintbek fielen uns die umfangreiche und übersichtliche Dokumentation und die datenschutzkonforme Umsetzung der im Sicherheitskonzept geforderten Sicherheitsmaßnahmen für die PC-Arbeitsplätze positiv auf.

Der IT-Leiter der Gemeinde Flintbek hat ein besonderes **Verfahren zur Protokollierung im Vertretungsfall** erstellt: Bei Abwesenheit des IT-Leiters dokumentieren die vertretenden Administratoren die durchgeführten Systemarbeiten in so genannten Vertretungsbögen. Bei komplexen Aufgaben und Problemen können sie eine vom IT-Leiter erstellte Dokumentation heranziehen. Sie beschreibt alle anfallenden Systemarbeiten und Systeminformationen mit konkreten Anweisungen für ein Schritt-für-Schritt-Vorgehen.

Die Gemeindeverwaltung setzt das Serverbetriebssystem Windows 2000 ein. Die Systemadministratoren hatten den Windows 2000-Sicherheitskurs der DATENSCHUTZAKADEMIE besucht und die wichtigsten der dort vermittelten Struktur- und Konfigurationsvorschläge im Bereich des Verzeichnisdienstes umgesetzt. Die Sicherheitspolicy sowie die Absicherung der PC-Arbeitsplätze erfolgte über die **Gruppenrichtlinien**. Dennoch hat das ULD einige Mängel gefunden. Drei davon sind in der Prüfungspraxis häufig vorzufinden:

- Auf dem Domänencontroller befanden sich Benutzerkonten mit administrativen Rechten für den **Fernzugriff zu Wartungszwecken**. Die Nutzung dieser Konten und die damit verbundenen Möglichkeiten zum externen Zugriff auf die Datenbestände waren den Verantwortlichen nicht ausreichend bekannt. Eine Dokumentation der Rechte und der Funktionalität dieser Benutzerkonten stellte der externe Dienstleister der Gemeindeverwaltung nicht zur Verfügung. Für die Fernwartung sollte ein gesondertes Benutzerkonto erstellt werden, das aber erst vor Beginn der Fernwartung freigeschaltet werden darf und nach der Benutzung

deaktiviert werden muss. Ein Zugriff des externen Dienstleisters auf personenbezogene Daten sollte z. B. durch Protokollierung und Beobachtung während der Fernwartung unterbunden werden.

- An einem **öffentlich zugänglichen Netzwerkdrucker** wurden die ausgedruckten Dokumente nicht zeitnah von den Mitarbeitern abgeholt. So konnten personenbezogene Daten Unbefugten zur Kenntnis gelangen. Sind keine baulichen Sicherungen möglich, so muss organisatorisch geregelt werden, dass die Ausdrucke sofort am Drucker abzuholen sind. Diese Regelung sollte in die Dienstanweisung aufgenommen und den Mitarbeitern bekannt gemacht werden. Kombinierte Druck-, Fax- und Kopiergeräte bieten häufig die Funktionalität, dass der Ausdruck einer Datei erst dann gestartet wird, wenn der Mitarbeiter am Drucker eine persönliche PIN eingibt.
- Die Entsorgung von **personenbezogenem Papiermüll** durch einen externen Dienstleister war vertraglich nicht geregelt. Die Gemeindeverwaltung musste diesen Vertrag mit dem aktenvernichtenden Betrieb erst nachfordern. Ein solcher Vertrag muss das Verfahren der Aktenvernichtung detailliert beschreiben; die Gemeindeverwaltung muss kontrollieren können, dass die personenbezogenen Daten gemäß ihren Anweisungen vernichtet werden.

Was ist zu tun?
Zur Datenschutzorganisation gehört die Absicherung des internen Netzes für den Fall der Fernwartung, die Beschränkung des Zugangs zu öffentlichen Netzdruckern sowie die vertragliche Ausgestaltung des Auftragsverhältnisses mit dem Unternehmen, das die Datenträger entsorgt.

6.12.3 Amtsverwaltung Hohner Harde

Die Amtsverwaltung Hohner Harde hatte sich vor einigen Jahren durch uns sicherheitstechnisch beraten lassen. Ergebnis dieser Beratung war eine ausführliche Dokumentation der Datenverarbeitungsabläufe, die während der durchgeführten Prüfung positiv aufgefallen ist. Mit der Bestellung der drei Systemadministratoren zu Datenschutzbeauftragten wählte die Amtsverwaltung eine interessante, gleichwohl problematische Lösung.

Prüfungen enden nur selten ohne Beanstandungen und einen Katalog mit Vorschlägen zur Beseitigung der Mängel. Ein aufgeführter Mangel spiegelt eine ungewöhnliche Situation wider: Die Amtsverwaltung hat alle **drei Systemadministratoren zu Datenschutzbeauftragten** bestellt. Diese Konstellation ist aus folgenden Gründen zu kritisieren:

- Wenn die Datenschutzbeauftragten zugleich die Aufgabe der Systemadministration wahrnehmen, kann die Ausübung des Amtes zu **Konflikten** mit anderen dienstlichen Aufgaben führen.

Im Wortlaut:
§ 10 Abs. 2 Satz 1 LDSG

Die oder der behördliche Datenschutzbeauftragte muss die erforderliche Sachkunde und Zuverlässigkeit besitzen. Sie oder er darf durch die Bestellung keinem Konflikt mit anderen dienstlichen Aufgaben ausgesetzt sein.

- Der Datenschutzbeauftragte sollte **zentraler Ansprechpartner** in Datenschutzfragen sowohl für die Amtsleitung als auch für die Beschäftigten sein. Sind mehrere Datenschutzbeauftragte bestellt, gibt es für die Leitung und die Beschäftigten mehrere Ansprechpartner. Das kann dazu führen, dass die einzelnen Datenschutzbeauftragten Sachverhalte unterschiedlich bewerten.
- Bei der Bestellung von drei Datenschutzbeauftragten muss sichergestellt werden, dass sich jeder Datenschutzbeauftragte die notwendige **technische und rechtliche Sachkunde** in Form von Schulungen aneignet und in ausreichendem Umfang von anderen Aufgaben freigestellt wird, um das Amt ordnungsgemäß wahrzunehmen.

Daher sollte **nur ein Mitarbeiter als Datenschutzbeauftragter** bestellt werden. Im Hinblick auf die Größe der Amtsverwaltung schlugen wir vor, dass ein Mitarbeiter aus der Gruppe der Systemadministratoren das Amt des behördlichen Datenschutzbeauftragten übernimmt und dieser nach seiner Stellenbeschreibung von den Aufgaben als Systemadministrator entbunden wird. Im Interesse der Nutzung seines technischen Fachwissens soll er in Ausnahmefällen (Krankheit, Urlaub) vertretungsweise administrative Aufgaben wahrnehmen können.

Was ist zu tun?
Die Bestellung eines fachkundigen Datenschutzbeauftragten ist ausreichend. Systemadministratoren dürfen wegen des möglichen Interessenkonfliktes nicht zu Datenschutzbeauftragten bestellt werden.

7 Neue Medien

7.1 Nutzerdaten in Internetforen ausgooglen

Internetforen sind beliebte Plattformen, um Meinungen und Lebenshilfen zu unterschiedlichsten Themen auszutauschen. Mit der Wahl eines Pseudonyms gehen viele Nutzer verständlicherweise davon aus, dass ihr wirklicher Name für Dritte unbekannt bleibt, wenn sie sich etwa mit ihren Sorgen, Nöten oder Leidenschaften in einem Forum offenbaren.

So ging es einem Petenten, der sich für ein Internetforum für allein erziehende Eltern angemeldet hatte. Er war umso erstaunter, als er mithilfe der Suchmaschine Google seinen eigenen Namen recherchierte und einen Link zu seinem **kompletten Anmeldeprofil** in dem besagten Forum fand. Es enthielt nicht nur seinen Namen, sondern auch noch weitere Informationen.

Aus der Stellungnahme des Anbieters wurde deutlich, dass die Profilinformationen in Google aufgrund einer **Fehlkonfiguration** der Forensoftware aufgenommen worden waren. Google basiert auf Listen, die durch so genannte Bots erstellt werden. Bots sind Programme, die von einer Webseite ausgehen, den Links auf dieser und weiteren Seiten folgen und diese dann indizieren. Weil ein Zugriffsschutz fehlte, war diese Suche auch über die Profilseiten möglich.

Für den Betroffenen ergab sich nun das Problem, nicht nur die aktuellen Google-Einträge für die Zukunft zu beseitigen, sondern auch seinen Eintrag aus dem Google-Archiv **löschen** zu lassen. Um eine solche Löschung hat sich der Forenbetreiber nach Aufforderung durch uns – mittlerweile erfolgreich – bemüht. Für eine Reihe weiterer Betroffener sind die Löschungen noch nicht abgeschlossen. Für den Betroffenen bleibt das ungute Gefühl, möglicherweise noch in anderen Internetarchiven gelistet zu sein.

Was ist zu tun?
Webanbieter sind verpflichtet, die Pseudonyme ihrer Nutzer wirksam zu schützen. Nutzer sollten sich bei Angaben zu ihrer Person auf das unbedingt erforderliche Maß beschränken, wenn sie einen Internetdienst nutzen.

7.2 Schnell mal surfen über fremde Funknetzwerke

Wer mit dem Notebook mit WLAN-Adapter durch die Stadt geht, der findet eine Menge drahtloser Datennetze. Manche dieser Netze sind vor Zugriffen Dritter geschützt, andere sind frei zugänglich. Eine häufig reisende Petentin stellte uns die Frage, ob sie ein solches fremdes Netzwerk nicht zum Abruf der eigenen E-Mails oder zum Surfen im Internet nutzen könne.

Die Nutzung offen zugänglicher, **nicht verschlüsselter Accesspoints** als Internetzugang wird – auch im Hinblick auf die zunehmende Verbreitung von pauschalisierten Abrechnungen (Flatrates) – wohl keine Straftat darstellen. Die konkrete Nutzung des Internets kann jedoch anders zu beurteilen sein. Darüber hinaus wirft die Nutzung fremder Accesspoints als Internetzugang auch datenschutzrechtliche Fragen auf.

Nutzt ein Dritter einen Accesspoint für den Internetzugang, so ist er in der Regel im Internet unter einer **IP-Adresse** unterwegs, die dem Accesspoint-Betreiber zugewiesen wurde. Die IP-Adresse ist zumindest für den Internetzugangsanbieter des Accesspoint-Betreibers ein personenbezogenes Datum, das Datenschutz genießt. Daher bedarf die Nutzung des Accesspoints einer Einwilligung des Accesspoint-Betreibers. Denkbar ist außerdem eine Erlaubnis durch eine Rechtsvorschrift.

Eine **Einwilligung** des Accesspoint-Betreibers ist nur anzunehmen, wenn der Zugangspunkt zu einem der Öffentlichkeit angebotenen Funknetzwerk gehört (z. B. öffentliche Hotspots großer Internetprovider) oder die Kennung des Zugangspunktes eine Freigabe des Nutzers ausdrücklich erkennen lässt (z. B. „Öffentliches Funknetzwerk“, „Come in“ usw.). Bei anderen Kennungen, insbesondere auch werkseitigen Standardeinstellungen wie „default“, liegt keine datenschutzrechtliche Einwilligung vor.

Als **Erlaubnisregelung** kommt allenfalls die Generalklausel in Betracht, die eine Interessenabwägung zwischen dem berechtigten Interesse des Nutzers und dem schutzwürdigen Interesse des Accesspoint-Betreibers vorsieht. Eine solche Zulässigkeit kann jedenfalls nicht pauschal angenommen werden. Der Nutzer kann nicht davon ausgehen, dass ihm die Internetnutzung über ein ungeschütztes fremdes Funknetzwerk erlaubt ist.

Für Betreiber von Funknetzwerken hat die Arbeitsgemeinschaft Technik der Datenschutzbeauftragten des Bundes und der Länder eine „**Orientierungshilfe WLAN**“ herausgegeben:


www.lfd.saarland.de/dschutz/OHWLAN.pdf

Weitere Informationen zur Konfiguration der Verschlüsselung drahtloser Netzwerke finden sich unter:


www.datenschutzzentrum.de/material/tb/tb27/kap10.htm#105

Was ist zu tun?
Reisende sollten fremde WLAN nur nutzen, wenn der Betreiber kenntlich gemacht hat, dass er eine Nutzung durch Dritte akzeptiert. Accesspoint-Betreiber sollten ihre Netzwerke sichern, wenn sie keine Nutzung ihres Internetzugangs durch Dritte wünschen.

7.3 Rundfunkgebührenbefreiung: Ein Fall für den Bürokratieabbau

Wer von der Rundfunkgebühr befreit werden will, muss als Antragsteller die Voraussetzungen seiner Befreiung belegen. Nach dem Rundfunkgebührenstaatsvertrag muss der Antragsteller den entsprechenden Bescheid über den Bezug von Sozialleistung im Original oder in beglaubigter Kopie vorlegen.

Der Rundfunkgebührenstaatsvertrag verpflichtet zur Vorlage des Bescheides über den Bezug einer Sozialleistung, wenn man eine Befreiung von der Rundfunkgebühr erreichen will. Betroffen sind z. B. die Bezieher von Sozialhilfe, Arbeitslosengeld oder Berufsausbildungsförderung. Die Sozialleistungsbescheide enthalten in der Regel Angaben über alle **Voraussetzungen des Leistungsbezuges**, also Angaben zur Person, zu den persönlichen Lebensumständen, zu den Einkommensverhältnissen, eventuell auch Angaben über Dritte im Haushalt des Antragstellers sowie sonstige, z. B. unterhaltspflichtige Personen. Manche Bescheide umfassen knapp 20 Seiten. Die Gebühreneinzugszentrale (GEZ) befreit Antragsteller meistens nur für kurze Zeiträume von der Rundfunkgebühr. Viele Sozialleistungsbezieher empfinden die Pflicht zur Vorlage derart vieler Daten als unverhältnismäßige Schikane. Von Datenschutzrelevanz ist, dass bei der GEZ zentral eine gewaltige Menge von Sozialdaten zusammenkommt, die zur Gebührenbefreiung nicht notwendig sind. Im Jahr 2004 wurden z. B. ca. 3,5 Millionen Befreiungsbescheide erteilt.

Ein datensparsameres Verfahren drängt sich geradezu auf: Eine **formlose Bescheinigung** über die Tatsache des Bezuges einer Sozialleistung mit einem Stempel der bescheidenden Stelle wäre völlig ausreichend. So einfach war das Verfahren auch in der Vergangenheit, bis der Gesetzgeber es änderte. Die GEZ bekäme die Urkunde einer öffentlichen Stelle zum Nachweis der Voraussetzungen einer Gebührenbefreiung vorgelegt. Der Aufwand für die Beglaubigung der Bescheide entfiele und selbst der Aufwand der Sozialleistungsbehörden hielte sich in Grenzen. Doch dies wäre wohl ein zu vernünftiges Verfahren: Die bisherigen Verhandlungen sind gescheitert, weil sich die Sozialleistungsbehörden die **Kosten für die Bestätigungen** von der GEZ bezahlen lassen wollten. Die GEZ weigerte sich und verwies auf die Rechtslage, und dies, obwohl der Verwaltungsaufwand für die Entgegennahme der zum Teil umfassenden Bescheide weitaus größer ist als die einfacher Bestätigungen. Hier ist Bürokratieabbau angesagt. Nun liegt der Ball wieder beim Gesetzgeber, also bei den Landtagen.

Was ist zu tun?
Der Gesetzgeber sollte die Sozialleistungsbehörden verpflichten, den Leistungsempfängern eine einfache Bestätigung über den Bezug von Sozialleistungen automatisch mit dem Bescheid auszuhändigen, damit sie diese ihrem Antrag auf Befreiung von der Rundfunkgebühr beilegen können.

8 Modellprojekte zum Datenschutz

8.1 Erfolge im Innovationszentrum ULD-i

Das Innovationszentrum Datenschutz & Datensicherheit (ULD-i) unterstützt die Wirtschaft darin, Datenschutz und Datensicherheit als Wettbewerbsvorteil und Alleinstellungsmerkmal einzusetzen. Nach dem Datenschutz-Gütesiegel ist das ULD-i der zweite neue strukturelle Ansatz des ULD zur Stärkung der Wirtschaft.

Datenschutz-Gütesiegel können erst sehr spät in den Prozess der Produktentwicklung einfließen, nämlich nicht vor der endgültigen Fertigstellung und Markteinführung. Unternehmen und Wissenschaft sollten aber schon während des **Entwicklungsprozesses** datenschutzgerechter Produkte unterstützt werden. Genau dies ist die Idee des Innovationszentrums Datenschutz & Datensicherheit. 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.

Die Nachfrage nach solchen Angeboten aus der Wirtschaft ist zunehmend. Das Ministerium für Wissenschaft und Verkehr des Landes Schleswig-Holstein hat Datenschutz und Datensicherheit als einen zentralen **Wachstumsbereich für die Wirtschaft** in Schleswig-Holstein identifiziert. Eine vom Ministerium in Auftrag gegebene Studie bestätigt diese Einschätzung und bescheinigt dem Bereich Datenschutz und Datensicherheit ein hohes Innovationspotenzial.

Von der Projektidee bis zum Projektstart ist es zumeist ein langer Weg. Doch nach dem Start des ULD-i kann inzwischen über erfolgreich platzierte Projekte berichtet werden. Das ULD-i hat zwei Projekte im schleswig-holsteinischen **Förderprogramm e-Region PLUS** in der ersten Vergaberunde bei der Antragstellung mit seinem Know-how unterstützt. Eines der Projekte wurde ausgewählt und gehört zu den insgesamt fünf Projekten, die seit dem Sommer 2005 gefördert werden. Auch in der zweiten Vergaberunde erhielt eines der vom ULD-i betreuten Projekte den Zuschlag. Das ULD-i versteht sich vorrangig als Serviceangebot für die regionale Wirtschaft; es pflegt aber Kontakte zu Wirtschaft und Wissenschaft im gesamten Bundesgebiet.

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 Datenschutzgerechtes Identitätsmanagement

8.2.1 Mit PRIME-Prototypen in die Zukunft

Das EU-Projekt PRIME hat Halbzeit. In dem Vierjahresprojekt entwickeln die 20 Partner Anwendungsszenarien und Prototypen, mit denen Nutzer mithilfe von selbstbestimmtem Identitätsmanagement ihre Datenschutzrechte leichter und effektiver wahrnehmen können sollen. Erste Prototypen wurden im Hinblick auf die Erfüllung der Datenschutzanforderungen untersucht.

PRIME steht für Privacy and Identity Management for Europe (27. TB, Tz. 8.2.1). Im Gegensatz zu einem „Network of Excellence“, wie es FIDIS (Tz. 8.2.2) darstellt, werden bei PRIME **Prototypen von Identitätsmanagementsystemen** entwickelt. Neben einem integrierten Prototyp, der die allgemeinen Möglichkeiten des selbstgesteuerten Identitätsmanagements aufzeigt, geht es insbesondere um folgende drei Applikationen:

- Beim **E-Learning**-Prototyp werden Lösungen entwickelt, die die Teilnahme an Lehrveranstaltungen anonym bzw. unter Pseudonym ermöglichen – unter Einbeziehung von Lerngruppen. Dabei werden auch pädagogische Zielsetzungen verfolgt, etwa dass die Angst vor vermeintlich „dummen“ Fragen abgebaut wird.
- Beim Prototyp zu **Location Based Services** werden Verfahren entwickelt, mit denen Handydienste datenschutzfreundlich genutzt werden können, die auf die aktuelle örtliche Position des Nutzers abstellen. Z. B. kann ein Pollenwarner den Nutzer informieren, dass er in eine Gegend mit einer hohen Pollenbelastung kommt, auf die er persönlich besonders stark allergisch reagiert.
- Beim dritten Prototyp geht es um **Airport Security**. Die Lösungen sollen dem Fluggast das Einchecken und die Bewegung zum und auf dem Flughafen erleichtern, ohne dass hierbei der gläserne Fluggast entsteht.

? PRIME

Das Ziel von PRIME ist es, Lösungen zu erforschen und zu entwickeln, die es den Menschen ermöglichen, selbst die Kontrolle über ihre Privatsphäre im Cyberspace zu übernehmen.

PRIME wird seit dem Start am 1. März 2004 im Rahmen des 6. Europäischen Forschungsprogramms „Technologien für die Informationsgesellschaft“ gefördert (27. TB, Tz. 8.2.1). Partner sind Industrieunternehmen und Forschungseinrichtungen aus dem In- und Ausland: IBM Belgien als Projektkoordinator, IBM 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 am Main (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).

Unsere Aufgaben liegen in der rechtlichen und insbesondere datenschutzrechtlichen Begleitung, der Erarbeitung von speziellen Kriterien für datenschutzfreundliche Lösungen, der Mitentwicklung und Gestaltung von Nutzungsoberflächen sowie der Öffentlichkeitsarbeit für das Gesamtprojekt. Uns obliegt seit kurzem die Administration der offiziellen PRIME-Website und damit die Außenpräsentation des Projekts. Die Prototypen haben wir mit Blick auf unsere Erfahrungen mit dem Datenschutz-Gütesiegel evaluiert (Tz. 9.2.5); außerdem haben wir Hinweise für die weitere Entwicklung gegeben. Zusammen mit unserem Unterauftragnehmer W3C (WWW-Konsortium) treiben wir darüber hinaus die Standardisierung im Bereich des datenschutzfreundlichen Identitätsmanagements voran.

Was ist zu tun?
Bei den nächsten Versionen der bei PRIME zu entwickelnden Prototypen sind die Datenschutzanforderungen weiter zu optimieren. Wir werden aktiv in die weitere Forschung bis hin zur Programmierung eingreifen. Organisationen, die Bedarf an datenschutzfördernden Identitätsmanagementlösungen haben, können und sollten sich mit den PRIME-Partnern in Verbindung setzen.

Weitere Informationen zum Projekt befinden sich im Internet unter:

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

8.2.2 FIDIS – das Expertennetzwerk zur Identität

Wie sieht Identität in der Zukunft aus? Im Projekt FIDIS, das von der EU innerhalb des 6. Forschungsrahmenprogramms gefördert wird, liegen inzwischen die ersten Ergebnisse in Form von Studien, Berichten und Zeitschriftenartikeln vor.

Im Projekt „FIDIS – Future of Identity in the Information Society“ arbeiten wir mit weiteren 23 Partnern aus 12 Ländern zusammen in einem so genannten „**Network of Excellence**“ (27. TB, Tz. 8.2.2). Ergebnisse des Projektes sind europäische Studien, Berichte und Artikel zu verschiedenen Aspekten von Identität, Identifizierung und Identitätsmanagement, die unter www.fidis.net oder in Fachzeitschriften publiziert werden. Wir vertreten dabei mit unterschiedlichen fachlichen Perspektiven grundsätzliche und angewandte Aspekte des Datenschutzes.

Die Arbeit im Projekt ist in **Arbeitspaketen** organisiert. In acht dieser Arbeitspakete sind wir aktiv eingebunden, in weiteren übernehmen wir „Reviews“ zur Qualitätssicherung. Das Arbeitspaket, das sich mit Techniken zum Identitätsmanagement und zur Identifizierung auseinander setzt, wird von uns koordiniert. Einige Resultate aus dem vergangenen Jahr stellen wir hier kurz vor:

- In einer Studie wurden eine Kategorisierung und ein Überblick über bestehende **Identitätsmanagementsysteme** erarbeitet. 60 existierende Systeme wurden

hierbei untersucht. Ein Großteil dieser Systeme ist in der FIDIS-Datenbank (http://fidis.net) zu Identitätsmanagementsystemen detailliert beschrieben.

- Eine weitere Studie befasst sich mit **PKI (Private Key Infrastructure) und Biometrie**. In dieser Studie werden die bestehenden Probleme dieser Technologien bezogen auf IT-Sicherheit und Datenschutz analysiert und Lösungsvorschläge vorgestellt. Die Artikel-29-Datenschutzgruppe der EU verweist auf diese Studie und bezieht die dortigen Ergebnisse in eigene Arbeiten zu Biometrie ein. Ferner dienten die Studie sowie ergänzend recherchierte Hintergrundinformationen zum Thema PKI und elektronische Signaturen als Referenzinformationen für die Bewertung der für Schleswig-Holstein geplanten Konzepte zur Einführung der Verwaltungs-PKI.

- Im Rahmen der Sommerakademie 2005 zum E-Government wurden deutsche und internationale Aspekte zu **digitalen Ausweisen** diskutiert. Im FIDIS-Netzwerk begann im Berichtsjahr die Arbeit an einer Studie zum Thema öffentliche Chipkartensysteme und digitale Ausweise zur Identifizierung (**eIDs**). Neben dem europäischen Reisepass wird auch das Pilotprojekt zur Gesundheitskarte in Flensburg behandelt werden.

- In den USA sind **Identitätsbetrug und Identitätsdiebstahl** mittlerweile ein großes Problem; auch in Europa gibt es mehr und mehr Geschädigte. FIDIS hat sich des Themas angenommen und dazu einen Bericht herausgegeben. Neben einer Kategorisierung unterschiedlicher Formen des Identitätsbetrugs wurden vor allem die Bedeutung von geeigneter Authentifizierung/Autorisierung für die Prävention von Identitätsbetrug herausgestellt und konkrete Vorschläge erarbeitet, wie Identitätsmanagementsysteme unter Berücksichtigung des Datenschutzes diesbezüglich optimiert werden können.

- Eine Reihe von Studien wurden zum Thema **Profiling** erarbeitet. Neben den eingesetzten Techniken und Anwendungsbeispielen standen dabei die Umsetzung von europäischem Datenschutzrecht und die Auswirkung von Profiling auf die Demokratie im Mittelpunkt. Das erworbene technische Hintergrundwissen wurde und wird im ULD für die Scoring-Studie (Tz. 8.8) und für die Evaluation von Scoring-Systemen in der Finanzwirtschaft in Schleswig-Holstein eingesetzt. Eine weitere Untersuchung beschäftigt sich mit Profiling als Hintergrundtechnik bei ubiquitärem Computing. Hier gab es bezogen auf zukünftige Technologien wie z. B. RFID eine Zusammenarbeit mit dem Projekt TAUCIS (27. TB, Tz. 8.6).

- Zwei weitere Studien wurden zum Thema **Interoperabilität** erstellt. In diesem Zusammenhang konnte auch das Projekt „Gesundheitskarte Schleswig-Holstein“ in Zusammenarbeit mit dem Ministerium für Soziales, Gesundheit, Familie, Jugend und Senioren Schleswig-Holstein in eine der beiden Studien aufgenommen werden. Das Ergebnis dieser Untersuchung ist, dass sehr wenige, vor allem nicht technische Aspekte über den Erfolg oder das Scheitern von Projekten mit hohen Anforderungen an Interoperabilität entscheiden. Schlüsselfaktoren sind der Aufbau von Vertrauen zum Endnutzer durch gute Kommunikationspolitik, Nutzungsfreundlichkeit und Einhaltung geltender Datenschutzbestimmungen.

8.3 RISER (Registry Information Service on European Residents)

Die europäische Melderegisterauskunft RISER ist der erste E-Government-Dienst für grenzüberschreitende Meldeauskünfte in Europa. Unsere Aufgabe ist die datenschutzgerechte Gestaltung des Verfahrens. Die Gutachter der EU haben die erste Phase des Projektes als „ausgezeichnet“ bewertet.

Unter dem Namen RISER (Registry Information Service on European Residents) arbeitet ein **internationales Konsortium** aus Irland, Österreich, Polen und Deutschland an der Vermittlung offizieller Melderegisterauskünfte in Deutschland und Österreich (27. TB, Tz. 8.5). In einem Folgeprojekt RISERac wird der Dienst nun auf Estland, Polen und Ungarn ausgedehnt. Das Projekt wird von der Europäischen Kommission im Rahmen des eTen-Programms gefördert.

Zielkunden von RISER sind Unternehmen und Bürger. Registrierten Kunden bietet der Dienst einen einheitlichen Zugang zu einer sehr heterogenen und unübersichtlichen Melderegisterlandschaft in Europa. Über das Serviceportal können Meldeanfragen als Datei- oder Einzelanfrage über das Internet an die zuständige Meldebehörde weitergeleitet werden. RISER übernimmt dabei die **Funktion eines Zustellers**.

Im Mittelpunkt unserer Arbeit für RISER steht dessen datenschutzgerechte Gestaltung. Die Adressdaten aus den Anfragen dürfen nicht zentral gespeichert und es darf **kein zentrales europäisches Melderegister** aufgebaut werden. In Richtlinien zur Datensicherheit und zum Datenschutz und in Musterverträgen wurden die Anforderungen konkretisiert. Zugriffs- und Kontrollrechte werden ebenso geregelt wie die Besonderheiten des jeweiligen nationalen Melde- und Datenschutzrechtes.

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 Standards OSCI-Transport gestaltet sich hingegen schwieriger, da er bei den Meldebehörden noch wenig zum Einsatz kommt.

Nach dem guten Start in Deutschland und Österreich wurde RISER im Mai 2005 vom eTen-Programm als Projekt des Monats ausgezeichnet. Als Finalist wurde RISER im „Good Practice Projects“-Wettbewerb mit „The Best 2005“ der Europäischen Kommission prämiert. Im November 2005 konnte sich das Projekt auf dem Stand der Europäischen Kommission auf der E-Government-Ministerkonferenz in Manchester präsentieren. Ende des Jahres wurde RISER zum **zweitbesten eTen-Projekt des Jahres 2005** gewählt.


www.datenschutzzentrum.de/riser/

Was ist zu tun?
RISER muss auf der Grundlage europäischer Vorgaben die Anforderungen des Melde- und Datenschutzrechts aller Mitgliedsländer erfüllen, um europaweit als Vermittler von Melderegisterauskünften seinen Dienst datenschutzgerecht anbieten zu können.

8.4 AN.ON

AN.ON entwickelt sich weiter: neue, schnelle Mixrechner, mehr Nutzer, neue Funktionen, verbesserte Benutzungsoberfläche und Anbindung an den internationalen Anonymisierungsdienst TOR.

Bereits in früheren Tätigkeitsberichten (27. TB, Tz. 8.3) wurde über das seit Anfang 2001 bei uns in Kooperation mit der Technischen Universität (TU) Dresden, der Universität Regensburg, der Humboldt-Universität Berlin und der Freien Universität Berlin durchgeführte und vom **Bundesministerium für Wirtschaft und Arbeit** geförderte Projekt „AN.ON – Anonymität online“ berichtet. Die Förderung läuft nach aktuellem Stand bis März 2006.

Die von der TU Dresden entwickelte (Client-)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 der Verwendung von JAP wird der Kontakt zu den Webservern nicht, wie normalerweise üblich, unmittelbar aufgenommen, sondern für den Nutzer unsichtbar über eine Kette von Anonymisierungsservern (so genannte Mixserver) geleitet. Diese sorgen dafür, dass niemand Kenntnis von der IP-Adresse des Nutzers erlangen kann. Hierin besteht die Besonderheit des AN.ON-Dienstes gegenüber anderen Anonymisierungsdiensten. Der AN.ON-Dienst garantiert im Rahmen der geltenden Gesetze Anonymität nicht nur gegenüber dem Anbieter der angesurften Webseiten sowie dem eigenen Serviceprovider, sondern auch gegenüber den Betreibern des Anonymisierungsdienstes selbst.

Mittlerweile betreibt das ULD zwei eigene **Mixserver**:

- einen in den Räumlichkeiten der TU Dresden, der sich physikalisch getrennt von den anderen dortigen Servern in einem speziellen PC-Tresor befindet, der lediglich von unseren Mitarbeitern geöffnet werden kann, sowie
- einen Server bei einer professionellen Hosting-Firma; die hierüber aufgebaute Kaskade wird mittlerweile von ca. 1000 Nutzern gleichzeitig eingesetzt und erzeugt etwa 5 TBytes Übertragungsvolumen im Monat (das entspricht dem Umfang von über 8000 voll beschriebenen CD-ROMs (à 650 MB).

Von den Projektpartnern wurde der AN.ON-Dienst erweitert und mit interessanten **neuen Funktionen** ausgestattet:

- Mit der „**Forward-Funktion**“ kann jeder JAP-Nutzer mittels eines Klicks seinen Internetzugang für andere als Zugangspunkt ins Internet von außen freigeben. Dies dient dazu, Internetnutzern aus Staaten, die nur einen eingeschränkten Zugriff auf das Internet zulassen, die unzensierte Nutzung zu ermöglichen. Da somit praktisch hinter jeder IP-Adresse ein Zugangspunkt zum Internet bestehen kann, ist es kaum noch möglich, diese manuell zu sperren.
- Die JAP-Software kann nun auch für den Zugriff auf den internationalen Anonymisierungsdienst **TOR** genutzt werden, der ähnlich wie das Mixsystem von AN.ON arbeitet. Allerdings kann bei TOR jeder individuell einen entsprechenden Anonymisierungsserver betreiben, der automatisch in das Netz aufgenommen wird.

Im Jahr 2005 wurden zahlreiche **Artikel** unter Mitarbeit von allen AN.ON-Projektpartnern veröffentlicht, wie z. B. in den „Datenschutz Nachrichten“, „Mac Life“ oder auch „Capital“. Des Weiteren haben wir **Vorträge und Präsentationen** zu AN.ON beim Heise-Forum auf der CeBIT 2005 in Hannover, auf den Mediatagen Nord, bei IQPC, marcusevans, an der FH Kiel und an der Universität Kiel gehalten.

Auch 2005 lag eine unserer Hauptaufgaben im Rahmen des AN.ON-Projektes darin, **Anfragen von Strafverfolgungsbehörden und Privatleuten** nach Informationen über Nutzer des AN.ON-Dienstes zu beantworten. Hierbei mussten wir stets die Auskunft geben, dass derartige Daten bei unserem Anonymisierungsdienst im Einklang mit dem Recht nicht vorliegen und damit auch nicht herausgegeben werden können.

Im Mai 2005 erging gegen die Mixbetreiber des AN.ON-Dienstes durch die Staatsanwaltschaft München eine **Eilanordnung** zur Protokollierung der Zugriffe auf näher bestimmte Internetadressen. Zur Vermeidung der Probleme, die mit dem BKA-Fall aufgekommen waren (27. TB, Tz. 8.3; 26. TB, Tz. 8.3), fanden mehrere Gespräche zwischen uns und dem Bayerischen Landeskriminalamt und der Staatsanwaltschaft München statt. Die Überwachung der Internetadressen wurde gesetzesgemäß nach Eingang der Anordnung umgehend von uns und den Projektpartnern implementiert. Da die Anordnung mehrere juristische und technische Unzulänglichkeiten aufwies, wurde kurz darauf von uns eine Gegenvorstellung an die Staatsanwaltschaft München und das Amtsgericht München geschickt. Insbesondere wurde neben einigen formalen Aspekten die Eilbedürftigkeit, die eine Anordnung durch die Staatsanwaltschaft ohne Einbeziehung des eigentlich zuständigen Richters notwendig machte, bezweifelt. Im Ergebnis erfolgte keine Bestätigung der Eilanordnung durch einen Richter, sodass die Überwachung der Internetadressen umgehend wieder abgeschaltet werden konnte und musste. Die Stellungnahme der Staatsanwaltschaft München auf die Gegenvorstellung steht noch aus.

Weitere Informationen zum Projekt befinden sich im Internet unter:

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

Die Beschlüsse auf EU-Ebene zur **Einführung einer Vorratsdatenspeicherung** (Tz. 11.1) können, wenn sie in nationales Recht umgesetzt werden, Auswirkungen auf den AN.ON-Dienst haben. Es ist zu erwarten, dass die hier zum Einsatz gebrachte Technologie in Drittstaaten eingesetzt wird, wodurch die Ziele der Vorratsdatenspeicherung vereitelt werden könnten. Demgegenüber dürfte ein Dienst, der einerseits Internetnutzern nach der heutigen Rechtslage Anonymität im Internet zusichern kann, der sich zugleich aber den nationalen Anforderungen einer gesetzeskonformen Strafverfolgung stellt, aus rechtsstaatlicher Sicht die bessere Alternative sein.

Was ist zu tun?
Der Nutzer ist bei der effektiven Wahrnehmung seines gesetzlich garantierten Rechts auf Anonymität im Internet zu unterstützen. Ziel ist es, weitere Betreiber von Mixservern zu gewinnen und die Infrastruktur auszubauen. Im Kontakt zu den Strafverfolgungsbehörden sind weiterhin gemeinsame Lösungen gegen Internetkriminalität zu suchen.

8.5 SpIT-AL – billig telefonieren ohne Werbung

Das Versenden von E-Mails kostet heute fast nichts mehr. Kehrseite des günstigen Preises ist eine gewaltige Flut unerwünschter Werbe-E-Mails. Auch die Telefonkosten fallen dank des zunehmenden Angebots von Internettelefonie. Damit steigt das Risiko, dass auch unlautere Werbetreibende diesen Verteilungskanal nutzen und Anschlussinhaber mit Anrufen z. B. von Sprachcomputern belästigen.

Lösungen für dieses Problem erarbeiten wir gemeinsam mit der Firma TNG – The Net Generation AG aus Kiel in dem Projekt „Spam over Internet Telephony (SpIT) Abwehr-Lösung“, kurz: SpIT-AL. Das Projekt wird vom e-Region-PLUS-Programm des Landes Schleswig-Holstein über Mittel der Europäischen Union gefördert. Ziel des bis Ende 2006 laufenden Projektes ist die Entwicklung eines datenschutz- und telekommunikationsrechtlich einwandfreien **SpIT-Filters**, der es dem Nutzer von Internettelefonie technisch ermöglicht, belästigende Anrufe von unlauteren Werbetreibenden abzuweisen. Unsere Aufgabe ist die rechtliche Begleitung und Begutachtung. Wir werden dabei auf unsere Erfahrungen aus abgeschlossenen und noch laufenden Projekten in den Bereichen des Erreichbarkeits- und Identitätsmanagements und der datenschutzfreundlichen Technikgestaltung zurückgreifen.

Nach der Konzeption und Labortests soll im Rahmen des Projektes ein einsatzfähiger Prototyp entwickelt werden, der Nutzern zu Testzwecken zur Verfügung gestellt wird. Die Ergebnisse aus diesem Probeeinsatz fließen in die Verbesserung des Prototyps ein, der zum marktfähigen Produkt weiterentwickelt werden soll. Das Resultat wird nach Projektende im Rahmen einer **Open-Source-Software** der Allgemeinheit zur Verfügung gestellt.

Was ist zu tun?
Neue Kommunikationstechnologien und Geschäftsmodelle schaffen neue Herausforderungen für die Rechte ihrer Nutzer. Durch eine bedienerfreundliche Technikentwicklung soll die Akzeptanz hierfür erhöht werden.

8.6 Ubiquitäres Computing: Wenn Dinge sich über Menschen unterhalten

Von ubiquitärem Computing sprechen wir, wenn Gegenstände des Alltages mit kleinsten Prozessoren ausgestattet werden, die mit anderen Gegenständen über Sensoren und Lesegeräte Informationen austauschen. Anwendungen des UbiCom können das Leben erleichtern, wenn sie uns z. B. Entscheidungen abnehmen. Sie können aber zum Problem werden, wenn in den Hintergrundsystemen der Lesegeräte umfassende Nutzungsprofile ohne Wissen und Zustimmung der Betroffenen entstehen.

Ubiquitäre Anwendungen sind z. B. Häuser, in denen sich die Heizung automatisch auf Ihre **Bedürfnisse** einstellt, wenn Sie den Raum betreten, Räume, in denen Ihre Lieblingsmusik erklingt, wenn Sie abends von der Arbeit kommen, in denen die Kaffeemaschine anspringt, wenn Ihr Wecker morgens klingelt, und Kühlschränke, die im Supermarkt Butter und Milch selbst bestellen, wenn diese zur Neige gehen. Warum auch nicht, wenn es der Besitzer wünscht und es ihm das Leben erleichtert ...

Ebenso gut können Sie aber auch z. B. einen Mantel mit einem eingenähten oder eingewebten Prozessor gekauft und mit Ihrer EC-Karte bezahlt haben. Jedes Mal, wenn Sie nun ein Geschäft dieser Ladenkette betreten, werden Sie individuell als Person erkannt und begrüßt, aber auch Ihr Weg in dem Geschäft wird von Ware zu Ware nachvollzogen. Was nehmen Sie in die Hand, was legen Sie wieder zurück, wo verweilen Sie wie lange? Von einem anonymen Einkauf kann keine Rede mehr sein. Im Gegenteil: Das Ziel dieser Maßnahmen ist es, Ihr **Verhalten zu analysieren** und gezielt durch Ansprache und Werbung darauf zu reagieren.

Und nicht nur das, die Ladenkette installiert ihre Sensoren bereits an der Schaufensterscheibe und erkennt und erfasst Sie über Ihren Mantel, obwohl Sie nur an dem Ladengeschäft vorbeischlendern. Das Kaufprofil wird also ergänzt um ein Nutzungsprofil, dieses um ein Interessenprofil und schließlich ein Bewegungsprofil … Diese Profile werden umso umfassender, je mehr Daten aus unterschiedlichen Geschäftsbeziehungen z. B. über eine Kundenkarte zusammengeführt werden können. Die dadurch gewonnenen **Konsumentenprofile** stehen zur Verfügung, um für Zwecke der gezielten Werbung, vor allem aber der Verhaltenssteuerung verwendet werden zu können.

Ob diese Entwicklung beängstigend oder faszinierend ist, hängt nicht zuletzt von der Entwicklung der Technik, ihren Kosten, dem Erfolg der jeweiligen Geschäftsmodelle und damit maßgeblich auch von der **Akzeptanz** der Nutzer und Betroffenen ab. Informationstechnik kann gestaltet werden, also kann der Datenschutz auch bereits in der Konzeptionsphase berücksichtigt werden. Empirische Untersuchungen zeigen, dass viele Nutzer keine Probleme mit einer neuen Technik

haben, wenn sie ihnen Vorteile bietet. Die grundlegende Zustimmung kippt jedoch schnell in Ablehnung um, wenn die Menschen erkennen müssen, dass sie heimlich erfasst, ausgelesen und gesteuert werden sollen.

Mit der Studie TAUCIS – der Name steht für „Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung“ – untersuchen wir zusammen mit unserem Projektpartner, dem Institut für Wirtschaftsinformatik der Humboldt-Universität Berlin, die **Folgen und Gestaltungsmöglichkeiten** des ubiquitären Computing. Auftraggeber ist das Bundesministerium für Bildung und Forschung (BMBF), das mit dieser Untersuchung die Rahmenbedingungen innovativer Technologien besser erkennen will. Die Studie wird in diesem Frühjahr dem Auftraggeber übergeben.

www.datenschutzzentrum.de/taucis/
www.taucis.de

Was ist zu tun?
Technische Innovationen leben von der Akzeptanz der Nutzer und Betroffenen. Hersteller und Anwender des ubiquitären Computing sollten im Interesse des eigenen Geschäftserfolges die Betroffenen über die Zwecke der Erhebung und Verarbeitung ihrer Daten informieren und deren Zustimmung einholen.

8.7 Privacy4DRM

Inhaber von Urheber- und Verwertungsrechten an digitalen Inhalten beklagen finanzielle Einbußen durch unzulässiges Kopieren von Musik- oder Filmdateien. Durch den Einsatz technischer Schutzmechanismen, so genannter Digital-Rights-Management-Systeme, sollen die Nutzenden zum Erwerb einer Lizenz veranlasst werden. Dabei können umfangreiche Konsumprofile über die Nutzung der geschützten Inhalte entstehen, die von den Anbietern ausgelesen und kontrolliert werden.

Das ULD hat gemeinsam mit zwei Projektpartnern ausgewählte Systeme des Digital Rights Management (DRM) auf ihre Nutzerfreundlichkeit und ihre Datenschutzkonformität hin untersucht, um ein Anforderungsprofil für ein **nutzer- und datenschutzkonformes DRM** zu entwickeln. Wir nennen das Konzept Privacy4DRM (4 steht für englisch: „for“). Unsere Partner waren das Fraunhofer-Institut für Digitale Medientechnologie (IDMT) und die Technische Universität in Ilmenau, Auftraggeber war das Bundesministerium für Bildung und Forschung (BMBF). Die Studie wurde in der Zeit von Oktober 2004 bis Mai 2005 erstellt.

Zwischen dem Recht der Urheber bzw. der Verwerter und den Rechten der Nutzer muss ein vernünftiger Kompromiss gefunden werden. Unsere Analyse zeigt, dass die derzeitige Praxis die Nutzer erheblich benachteiligt. Teilweise erfolgt eine exzessive Ausforschung, die den Inhabern der digitalen Rechte nicht wirklich nützt: Der Missbrauch der digitalen Rechte wird nicht zurückgedrängt, wohl aber sind die Nutzer der DRM-Systeme verärgert, und dies oft aus gutem Grund. Über DRM-Systeme wird das **Nutzungsverhalten heimlich ausgeforscht** und die

Nutzung der käuflich erworbenen Rechte behindert. Mittlerweile gibt es hierfür viele Beispiele. Kaum war unsere Studie veröffentlicht, kamen der Anbieter SONY und wenige Wochen später der iTUNES von Apple wegen heimlicher Ausforschungen der Kundinnen und Kunden ins Gerede. Niemand ist begeistert, wenn er z. B. für viel Geld ein Lexikonprogramm ersteht, das wegen des restriktiven DRM nur von einem Familienmitglied am häuslichen PC genutzt werden kann.

Hier tut Umdenken Not. Der Vorschlag unserer Studie an die Inhaber der digitalen Rechte lautet: „Machen Sie den **Nutzer zu Ihrem Partner**. Räumen Sie ihm umfassende Rechte der Verwertung ein, und verzichten Sie auf seine Kontrolle." Nur unter diesen Voraussetzungen werden DRM-Systeme auf Akzeptanz stoßen. Dieser widersprüchlich klingende Appell ist – wie unsere Studie zeigt – real umsetzbar; er findet bei Teilen der Musikindustrie positive Resonanz. So stellte der Verband unabhängiger Tonträgerunternehmen, Musikverlage und Musikproduzenten e.V. (VUT) in der Kampagne „respect the music" Anfang 2006 fest: „DRM und Kopierschutz sind nicht die Lösung des Problems der Musikindustrie. So wie diese Techniken bislang gestaltet werden, helfen sie eher, auch noch den letzten ‚ehrlichen' Musikkäufer zu verprellen und in die Piraterie zu treiben."

Die Studie Privacy4DRM ist in einer Lang- und Kurzfassung veröffentlicht unter

www.datenschutzzentrum.de/privacy4DRM

Was ist zu tun?
Systeme zum Schutz digitaler Rechte müssen und können nutzerfreundlich und datensparsam gestaltet sein. Dies fördert die Akzeptanz der Kunden. Das verlorene Vertrauen der Kunden kann über die unabhängige Zertifizierung datensparsamer DRM-Systeme mit einem Datenschutz-Gütesiegel wiederhergestellt werden.

8.8 Kredit-Scoring – das große Unbekannte

Das ULD erstellte im Auftrag des Bundesverbraucherministeriums ein Gutachten zum Kredit-Scoring – einem ebenso umstrittenen wie unbekannten und publikumsträchtigen Thema. Das Gutachten legt große Datenschutzvollzugsdefizite offen.

Das ULD plagt sich schon seit längerem mit dem Kredit-Scoring herum. Es war Gegenstand von Bankenprüfungen (Tz. 5.2) und von Eingaben und beschäftigt seit Jahren den Düsseldorfer Kreis – den Zusammenschluss der deutschen Datenschutzaufsichtsbehörden. Praktisch **nichts ist hier unstreitig**. Es war daher mehr als nahe liegend, dass sich das ULD um einen ausgeschriebenen Gutachtenauftrag bemühte, der genau um dieses Thema kreiste: „Scoring-Systeme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher". Wir konnten mit den uns zur Verfügung gestellten Mitteln eine umfassende tatsächliche und rechtliche Bestandsaufnahme vornehmen.

Wir führten eine **Fragebogenaktion** bei 500 Kreditinstituten durch. Der Rücklauf von nur 29 Anworten gibt einen Hinweis darauf, dass die Thematik aus Sicht der Kreditinstitute entweder nicht für wichtig angesehen wird oder diese hierzu keine Auskunft geben wollen. Die Antworten gaben dennoch einen Eindruck über die Vielfalt der in Deutschland verwendeten Systeme des Kredit-Scoring.

Der Schwerpunkt unserer Untersuchung liegt im **Datenschutzrecht**. Der Rückgriff auf allgemeine gesetzliche Befugnisnormen genügt zur Rechtfertigung des Kredit-Scoring in der Regel nicht. Vielmehr bedarf es einer ausdrücklichen Legitimation im Kreditvertrag oder durch eine Einwilligung. Zentraler Aspekt für die Zulässigkeit der Verfahren ist, dass die verwendeten Merkmale eine direkte Relevanz für die Bonitätsbewertung und keine diskriminierende Wirkung haben. Beim Einsatz von externem Scoring, also bei der Durchführung des Scorings durch spezialisierte Unternehmen, müssen zusätzliche rechtliche Anforderungen erfüllt sein, da diese Unternehmen keinen direkten Kontakt zum Verbraucher haben. Bei der Verwendung des Scores bei der Kreditvergabe ist das Verbot automatisierter Entscheidungen zu beachten.

Beim Kredit-Scoring finden in der Praxis vielfältige **Beeinträchtigungen der Verbraucherinteressen** statt. Je nach Verfahren werden **Merkmale** einbezogen, deren Aussagekraft für die Bewertung der Kreditwürdigkeit fragwürdig ist: Adresse, Alter, Geschlecht, Staatsangehörigkeit, Familienstand, Zahl der Kreditanfragen. Zwar weisen diese mathematisch-statistisch eine Signifikanz für die Prognose des Kreditverhaltens auf, nicht hinreichend berücksichtigt werden jedoch mögliche individuelle Abweichungen bei den Betroffenen oder gar diskriminierende Wirkungen.

Zu wünschen übrig lässt auch die **Transparenz**. Dies gilt für die Einbeziehung dieser Methode der Datenverarbeitung in die Vertragsgestaltung, die öffentlich zugängliche Information hierüber wie auch die individuelle – teilweise kostenpflichtige – Auskunftserteilung gegenüber den betroffenen Verbrauchern. Die Pflichten zur Benachrichtigung und zur Auskunftserteilung werden derzeit noch nicht ausreichend beachtet. Es besteht eine Pflicht zur unentgeltlichen Auskunftserteilung über die Scores, über die verwendeten Daten sowie über die wesentliche Merkmalsgewichtung.

Verblüffend war für uns, dass es zur Verbesserung des Verbraucherschutzes und des Datenschutzes beim Kredit-Scoring kaum neuer **gesetzlicher Regelung** bedarf. Die bestehenden Regelungen ermöglichen weitgehend einen angemessenen Interessenausgleich. Das Problem für die Verbraucher besteht im großen Vollzugsdefizit der bestehenden Normen.

Was ist zu tun?
Zum Abbau des Vollzugsdefizits sind Maßnahmen auf verschiedenen Ebenen möglich: Die Entwicklung von „Best Practice“ durch die Kreditwirtschaft selbst, eine verbesserte Beratungs- und Aufklärungstätigkeit vor allem durch die Verbraucherzentralen und eine verstärkte Kontrolle durch die Datenschutzaufsichtsbehörden.

8.9 Das Virtuelle Datenschutzbüro boomt

Das Virtuelle Datenschutzbüro konnte gegenüber dem Vorjahr die Zugriffszahlen mehr als verdoppeln und erfreut sich damit steigender Beliebtheit. Mit Sachsen-Anhalt sind nun alle Landesbeauftragten für den Datenschutz Projektpartner.

Das Internetportal des Virtuellen Datenschutzbüros bündelt die Ressourcen und das Fachwissen von Datenschutzbeauftragten durch deren Mitarbeit als Projektpartner. Es bietet Bürgerinnen und Bürgern bei ihren Fragen zu Datenschutzrecht und -technik eine kompetente Anlaufstelle. Im deutschsprachigen Raum ist das Virtuelle Datenschutzbüro seit langem die stark frequentierte **erste Anlaufstelle** im Internet rund um den Datenschutz. Eine große Anzahl der Nutzerinnen und Nutzer gelangt über die Suchmaschine Google zu www.datenschutz.de, zunehmend auch aus Österreich und aus der Schweiz.

Neben der Information über die Seiten der per Virtuellem Datenschutzbüro verlinkten Online-Ressourcen, erreichbar u. a. über eine eigene Suchmaschine oder ein Schlagwortsystem, können Interessierte über die Adresse info@datenschutz.de auch **E-Mail-Anfragen** stellen. Dieser zunehmend in Anspruch genommene Service gibt Hilfe bei konkreten persönlichen Datenschutzproblemen. Eigene **Mailinglisten** dienen als weiteres Instrument der Informationsgewinnung und des Austausches. Datenschutzinteressierte Fachleute und Laien diskutieren insbesondere über die jedermann frei zugängliche, offene und unmoderierte vpo-datenschutz-list aktuelle Fragen.

Neben dem Landesdatenschutzbeauftragten von Sachsen-Anhalt konnte das Virtuelle Datenschutzbüro im Jahr 2005 auch die Stabsstelle für Datenschutz Liechtenstein als **neuen Projektpartner** gewinnen und damit die internationale Verzahnung und Ausrichtung des Informationsangebots stärken. Für dieses Jahr hoffen wir, dass sich weitere internationale Datenschutzbehörden als Partner anschließen.

Seit August 2004 ist die Anzahl der **Kooperationspartner** von 34 auf 42 gestiegen. Nach wie vor erreichen das Virtuelle Datenschutzbüro regelmäßig Anfragen von interessierten Unternehmen oder Personen, die sich so inhaltlich am Virtuellen Datenschutzbüro beteiligen und das Informationsangebot bereichern wollen. Im Interesse von Gleichbehandlung und Klarheit wollen wir in diesem Jahr die Geschäftsordnung des Virtuellen Datenschutzbüros überarbeiten, um genauere Anforderungen für eine Partnerschaft und das Aufnahmeverfahren festzulegen. Das Virtuelle Datenschutzbüro ist als erste Online-Anlaufstelle für Datenschutzfragen nicht mehr wegzudenken.

Was ist zu tun?
Die redaktionellen und finanziellen Beiträge aller Partner dürfen nicht nachlassen, um das hohe Niveau und den guten Ruf des Virtuellen Datenschutzbüros weiter auszubauen.

9 Audit und Gütesiegel

Audit und Gütesiegel sind **neue freiwillige Instrumente des präventiven Datenschutzes**, die an unterschiedlichen Objekten ansetzen und sich gegenseitig ergänzen. Das Gütesiegel bestätigt die Datenschutzkonformität eines Produktes, während mit dem Audit eine datenschutzkonforme Implementierung automatisierter Verfahren geprüft und bestätigt wird. In beiden Bereichen eines proaktiven Datenschutzes sind erhebliche Aktivitäten und Erfolge zu verzeichnen.

9.1 Datenschutz-Audit konkret

Mit dem Datenschutz-Audit verfügt das ULD über ein modernes und leistungsfähiges Instrument des präventiven Datenschutzes. In dem Auditverfahren können öffentliche Stellen ihr **Datenschutzkonzept** durch das ULD prüfen und beurteilen lassen. Das bei einem positiven Ergebnis verliehene Auditzeichen bestätigt nicht nur der Verwaltung, sondern auch den betroffenen Bürgerinnen und Bürgern, dass sich die Investition in den Datenschutz in Form von Sicherheit und Qualität ausgezahlt hat. Das ULD hat bereits 12 Auditierungen erfolgreich abgeschlossen. Sieben weitere Audits sind derzeit in Bearbeitung.

9.1.1 Landesnetz Schleswig-Holstein

Damit die Daten im landesweiten E-Government „laufen“ können, werden Landesbehörden und Kommunen über das Landesnetz miteinander verbunden. Als Basisinfrastruktur des E-Government bedürfen Datenschutz und Datensicherheit des Landesnetzes großer Aufmerksamkeit. Das vom Finanzministerium für das Landesnetz beauftragte Auditverfahren ist noch nicht abgeschlossen.

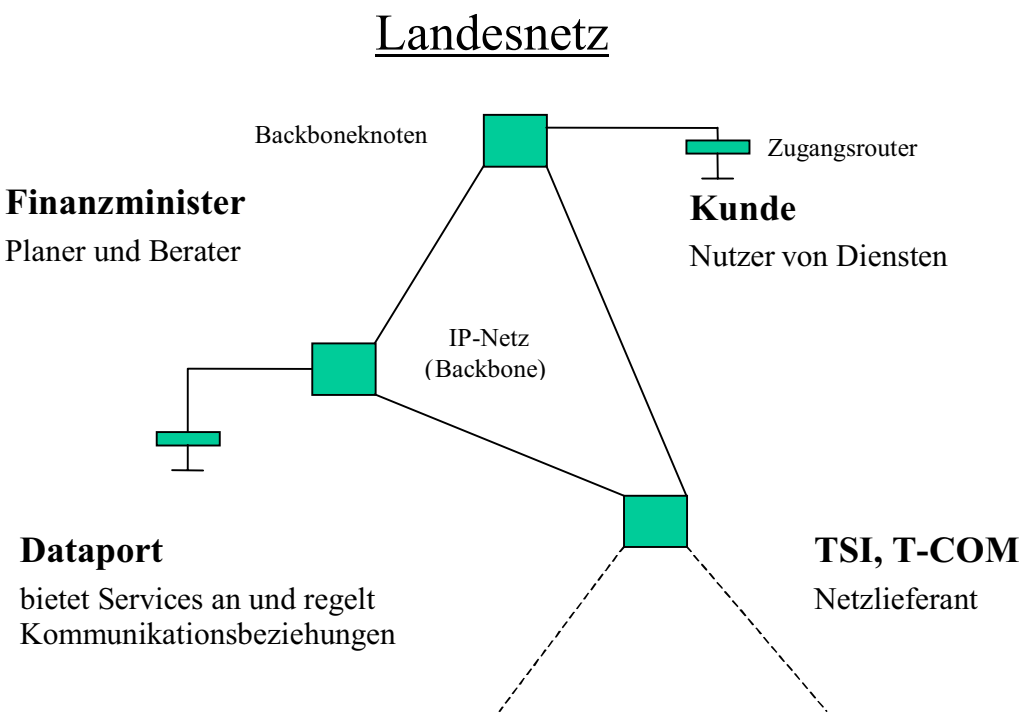
Nach der E-Government-Vereinbarung des Landes Schleswig-Holstein und der kommunalen Spitzenverbände steht das Landesnetz Schleswig-Holstein (LN) auch den Kommunen zur Verfügung. Als **Datendrehscheibe** erfüllt das LN eine zentrale datenschutzrelevante Funktion für das E-Government. Die Bürgerinnen und Bürger dürfen erwarten, dass ihre Daten nur dann über das LN übermittelt werden, wenn es auch sicher ist. Das Sicherheitsniveau muss von den an das LN angeschlossenen Behörden beurteilt werden können. Nur so können sie feststellen, ob und welche weiteren Sicherheitsmaßnahmen erforderlich sind.

Zum besseren Verständnis skizzieren wir einige wesentliche Punkte zur **Struktur des LN**:

- Betreiber des LN ist das Finanzministerium, das mit der T-Systems International (TSI) – heute T-Systems Enterprise (TSE) – über die Bereitstellung von

Netzkapazitäten einen Vertrag geschlossen hat. Da die TSE selbst keine Netze besitzt, kauft sie die Netzleistungen bei Dritten wie z. B. der T-Com ein.

- Das LN basiert technisch auf einer Verknüpfung von Datenleitungen, die nicht nur von LN-Benutzern in Anspruch genommen werden.
- Als Dienstleister des Finanzministeriums stellt dataport die Anschlüsse zur Verfügung und übernimmt die Administration der Kommunikationsbeziehungen.
- Der Datentransport über das Landesnetz wird nicht statisch festgelegt, sondern in Abhängigkeit von der Auslastung und Verfügbarkeit der Leitungen gesteuert. Das LN ist also ein „virtuelles“ Netz für den Datentransport.
- Das LN stellt Funktionen zur Verfügung, die den Datentransport benutzerbezogen kennzeichnen (MPLS-Technologie), sodass jeder Benutzer einer bestimmten Gruppe zugeordnet werden kann.
- Der Transport von Daten erfolgt im LN grundsätzlich unverschlüsselt. Der Benutzer kann aber veranlassen, dass eine Verschlüsselung im Bereich des LN optional aktiviert wird.
- Unter Sicherheitsaspekten ist die Benutzung des LN wie der Anschluss an ein sonstiges externes Netz zu betrachten.
- Über das LN wird auch die Sprachkommunikation der Landesbehörden übertragen.



Aus technischer Sicht besteht das LN aus den Systemkomponenten (Backbone) der TSE bzw. der T-COM bis hin zum **Übergaberouter**. Für die Datensicherheit dieser Komponenten ist das Finanzministerium verantwortlich. Auf dem Überga-

berouter werden nicht nur die Kommunikationsbeziehungen, sondern auch die Sicherheitsregeln definiert, die das interne Netz eines Benutzers vor Angriffen aus dem externen Landesnetz oder Fehlkonfigurationen schützen sollen. Die Sicherheit der internen Netze der Benutzer wird also durch die Sicherheitseinstellungen auf dem Übergaberouter maßgeblich beeinflusst. In der Regel sind jedoch dem Benutzer die jeweils aktuellen Einstellungen auf dem Übergaberouter weder bekannt noch von ihm zu beeinflussen.

Um ihrer Verantwortung für die Sicherheit der Daten in ihrem internen Netz gerecht werden zu können, installieren Benutzer des LN nicht selten zwischen ihrem internen Netz und dem Landesnetz eine in ihrer Verfügungsgewalt stehende **Firewall**. Auf diese Weise schotten sich diese Stellen gegenüber dem LN ab, dessen sicherheitsrelevante Einstellungen sie nicht beeinflussen können, die aber erheblichen Einfluss auf die Sicherheit ihres internen Netzes haben können. Diese Vorgehensweise ist konsequent, solange sich die Schnittstelle zwischen Übergaberouter und internem Netz nicht angemessen sicher für den Kunden darstellt (27. TB, Tzn. 9.2.2 und 9.2.4).

Um den Benutzern bzw. Kunden des LN eine ausreichende Transparenz über die Funktionen und die Sicherheit des LN zu vermitteln, erstellt dataport im Auftrag des Finanzministeriums eine **Generaldokumentation** zur aktuellen Netzinfrastruktur. Eine weitere „Baustelle“ der Verantwortlichen ist das **Sicherheitskonzept** des LN, das auf wesentliche Sicherheitsfragen noch Antworten liefern muss. Erst nach Abschluss dieser Vorarbeiten kann die Begutachtung mit dem Audit abgeschlossen werden.

Was ist zu tun?
Generaldokumentation und Sicherheitskonzept für das LN sollten zeitnah fertig gestellt werden. Die Benutzer bzw. Kunden müssen gegen unzulässige Zugriffe aus dem LN auf ihr eigenes internes Netz wirksam geschützt werden.

9.1.2 SAP R/3-Modul Kosten- und Leistungsrechnung

Mit dem Einsatz der Kosten- und Leistungsrechnung kann die Wirtschaftlichkeit des Verwaltungshandelns überprüft und beeinflusst werden. Das komplexe Verfahren wird derzeit im Auftrag des Finanzministeriums einem Audit unterzogen.

Ein Kernelement der Verwaltungsmodernisierung ist die flächendeckende Einführung der Kosten- und Leistungsrechnung (KLR**)** in den Landesbehörden mithilfe der Software SAP R/3. Das Verfahren KLR befindet sich bereits in vielen Landesbehörden im Einsatz. Dieses **SAP R/3-Verfahren** ist eines der größten Fachverfahren der Landesverwaltung Schleswig-Holstein. Es wird in über 200 Landesbehörden mit mehr als 2000 Benutzern eingesetzt. Die Daten der einzelnen Landesbehörden werden zentral auf Rechnern des Dienstleisters dataport verarbeitet. Dataport ist nicht nur für den Betrieb zuständig, sondern auch für die Entwicklung und Programmpflege des SAP R/3-Verfahrens.

Das Finanzministerium hat als verantwortlicher Betreiber des Verfahrens das ULD mit der Auditierung der KLR beauftragt. Gegenstand des Audits ist der datenschutzrechtlich und sicherheitstechnisch ordnungsgemäße Einsatz der KLR unter dem Management des Finanzministeriums. Um die **Anforderungen des Datenschutzes und der Datensicherheit** beim Betrieb des Verfahrens zu gewährleisten, ist eine Reihe von technischen und organisatorischen Sicherheitsmaßnahmen umzusetzen. Noch steht das Auditverfahren am Anfang.

Was ist zu tun?
Aufgrund seiner Komplexität bedarf SAP R/3 der Einrichtung eines verantwortungsvollen Sicherheitsmanagements, damit die Ordnungsmäßigkeit der Datenverarbeitung dauerhaft gewährleistet werden kann.

9.1.3 Das „EAGFL-G“ des Landwirtschaftsministeriums

Das Ministerium für Landwirtschaft, Umwelt und ländliche Räume hat bei der Durchführung von Ausgleichszahlungen EU-Vorschriften zu beachten, die einen erhöhten Sicherheitsstandard für den Einsatz von IT-Systemen vorgeben. Im Rahmen eines Audits stellt sich das Ministerium den neuen EU-Anforderungen.

Nach der gemeinsamen Agrarpolitik der Europäischen Union (EU) gibt es einen Europäischen Ausrichtungs- und Garantiefond für die Landwirtschaft (EAGFL), aus dem **Ausgleichszahlungen** in Milliardenhöhe für Landwirte geleistet werden. Die Kommission der Europäischen Gemeinschaft erlässt für eine ordnungsgemäße Abwicklung dieser Finanzmittel Verordnungen, die von den einzelnen Bundesländern einzuhalten sind.

Anträge für eine Fördermaßnahme werden in Schleswig-Holstein hauptsächlich von den Ämtern für ländliche Räume bearbeitet. Die Zahlungen werden dann von einer Zahlstelle im Landwirtschaftsministerium durchgeführt und verbucht. Für die Verwaltung der Datenbestände wurde länderübergreifend ein **Zahlungsinformationssystem für Agrarfördermittel (ZIAF)** entwickelt, wodurch die Bearbeitung der Antragsabwicklung einheitlich gestaltet ist.

Das Landwirtschaftsministerium hat für den Betrieb des Verfahrens **dataport** beauftragt; die Applikation und die Datenbestände werden dort verwaltet. Darüber hinaus wurde dataport länderübergreifend die Entwicklung einiger Programmteile übertragen.

Die Kommission der Europäischen Gemeinschaft hat im März 2005 ihre Kriterien für eine ordnungsgemäße Abwicklung der Finanzmittel mit einer neuen Verordnung verschärft. Die Zahlstellen der einzelnen Bundesländer haben ab 2008 für

die Sicherheit der Informationssysteme einen international anerkannten Standard anzuwenden. Für die Umsetzung der Verordnung haben sich die Bundesländer auf die Anwendung des **IT-Grundschutzhandbuchs** des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verständigt. Die Bundesländer beginnen jetzt, die für die Abwicklung der Zahlungen eingesetzten IT-Systeme zu untersuchen und sie an die neuen Sicherheitsbestimmungen anzupassen.

In Schleswig-Holstein hat das Landwirtschaftsministerium das ULD bei der Umsetzung der Verordnung um Unterstützung gebeten. Im Rahmen eines **Audits** wird zunächst eine umfassende Bestandsaufnahme der technischen und organisatorischen Gegebenheiten durchgeführt. Sich ergebender Anpassungsbedarf soll umgesetzt werden. Es soll ein Sicherheitsmanagement aufgebaut werden, um den vorgegebenen Sicherheitsstandard zur Abwicklung der Zahlungen langfristig aufrechtzuerhalten. Mit der Anwendung des BSI-Grundschutzhandbuchs erfolgt eine IT-Strukturanalyse, eine Schutzbedarfsfeststellung sowie die Modellierung der IT-Sicherheitsmaßnahmen. Ziel der Auditierung ist es, dem Ministerium zu bescheinigen, dass die geforderten EU-Kriterien erfüllt sind und zugleich eine ordnungsgemäße Datenverarbeitung im Sinne des Landesdatenschutzgesetzes vorliegt.

Was ist zu tun?
Das Landwirtschaftsministerium hat rechtzeitig begonnen, die Sicherheitsaspekte für ihr Zahlungsinformationssystem an die EU-Verordnung anzupassen. Die für Schleswig-Holstein entwickelte Sicherheitspolicy kann auch anderen Bundesländern bereitgestellt werden.

9.1.4 Kommunale IT-Standards (KITS)

Das Kommunale Forum für Informationstechnik der Kommunalen Landesverbände in Schleswig-Holstein (KomFIT) hat mit den „Kommunalen IT-Standards“ (KITS) ein Standardsystemkonzept der Bürokommunikation für den IT-Einsatz im kommunalen Bereich entwickelt. Das ULD prüft die Datenschutzkonformität des KITS in einem Auditverfahren.

Bereits 1999 hat das KomFIT eine erste Version eines **Standardsystemkonzeptes für die Bürokommunikation** in Kommunalverwaltungen entwickelt. 2002 wurde das Konzept aktualisiert und erweitert. In der aktuellen Version definiert KomFIT eine standardisierte Umgebung sowohl für zentrale Komponenten wie einen Verzeichnisdienst und Mechanismen für den E-Mail-Austausch als auch für dezentrale Komponenten wie die Ausgestaltung der Softwareumgebung auf einem Standard-PC oder einem verwaltungsinternen Fileserver.

Die Auditierung eines **IT-Standards** für die Bürokommunikation von Verwaltungen hat für den Datenschutz eine große Bedeutung. Erfüllt bereits der IT-Standard grundlegende Anforderungen des Datenschutzes nicht, so wird seine Implementierung in der Fläche großen Schaden anrichten. Wird aber umgekehrt ein IT-Standard bereits datenschutzgerecht formuliert und zudem nach den Regeln der Tech-

nik sauber implementiert, so kann im Interesse der Betroffenen ein Höchstmaß an Datenschutz und Datensicherheit erreicht werden. Natürlich wird das Ergebnis der Auditierung Einfluss auf die Motivation der Entscheidungsträger in den Kommunen Schleswig-Holsteins haben, KITS in ihren Verwaltungen zur Verarbeitung der Daten der Bürgerinnen und Bürger einzusetzen.

Die zu KITS gehörenden zentralen Komponenten werden in der Verantwortung des Finanzministeriums betrieben. Dieses hat **dataport** mit der Durchführung des Betriebs der zentralen Infrastruktur beauftragt. Die Auditierung von KITS bezieht daher die Bedingungen dieser **Auftragsdatenverarbeitung** mit ein. Schwerpunkte des Audits werden sein:

- Untersuchung der Datenschutzaspekte im KITS-Konzept,
- Prüfung der vertraglichen Vereinbarungen zwischen den Beteiligten auf ihre Datenschutzkonformität,
- Implementierung des Standards in den zentralen Komponenten wie dem Active Directory,
- Umsetzung des Standardsystemkonzepts in einer Beispielkommune.

Was ist zu tun?
Standardkonzepte für mehrere Verwaltungen sollten bereits während der Konzeptionsphase vom ULD begleitet werden, was deren Implementierung stark vereinfacht.

9.1.5 Kreisnetz Nordfriesland

Die Kreisverwaltung Nordfriesland hat für die Umsetzung ihrer E-Government-Projekte ein eigenes Kreisnetz geschaffen. Um datenschutzrechtlich und sicherheitstechnisch gegenüber ihren Kommunen vorbildlich zu sein, will sie ihr Kreisnetz im Rahmen eines Audits durch das ULD begutachten lassen.

Der Kreis Nordfriesland und die ihm angehörigen Kommunalverwaltungen sind seit Anfang 2004 elektronisch miteinander vernetzt. Durch die Verbindung zum Landesnetz Schleswig-Holstein und zum Internet wird eine umfassende regionale E-Government-Infrastruktur aufgebaut. Fachverfahren der Kommunen werden nach und nach im **Servicebereich der Kreisverwaltung** zentralisiert. Die sich daraus ergebenden vielschichtigen Veränderungen der IT-Systeme und die von der Kreisverwaltung für ihre Kommunen angebotenen technischen Dienstleistungen werden im Rahmen eines Audits untersucht.

Zusammen mit der Datenschutzbeauftragten und dem IT-Leiter der Kreisverwaltung wurden folgende **Maßnahmen** festgelegt:

- Bestandsaufnahme der IT-Organisation,
- Festlegung der Datenschutzziele,

- Erstellung fehlender Dokumentationsunterlagen,
- Erarbeitung von Dienstleistungsverträgen,
- Beseitigung technischer und organisatorischer Schwachstellen,
- Einrichtung eines Datenschutzmanagementsystems,
- Sensibilisierung der Mitarbeiter durch Schulungsmaßnahmen,
- Begutachtung durch das ULD.

Die Kreisverwaltung wird mit der datenschutzkonformen Gestaltung ihres Kreisnetzes einen Sicherheitsstandard festlegen, der **Maßstab** für die Netze anderer Kreisverwaltungen sein kann.

Was ist zu tun?
Als Dienstleistung für kreisangehörige Gemeinden und Ämter müssen Kreisnetze die Anforderungen des Datenschutzes erfüllen. Auditverfahren sind insofern hilfreich.

9.1.6 Stockelsdorf: Interne Datenverarbeitung und Internetanbindung

Audits gibt es nicht nur für Großprojekte – ganz im Gegenteil: Gerade für kleinere Gemeinden kann sich die konzeptionelle Unterstützung sowie die spätere Begutachtung durch das ULD lohnen. Die Gemeinde Stockelsdorf macht vor, wie es gehen könnte.

Das ULD hilft mit seinem Know-how bei der Analyse der Datenverarbeitung und ihrer datenschutzgerechten Strukturierung. Dies ist ein einmaliger Aufwand, der die Gemeinde entlastet und sich für die Zukunft auszahlt: So lässt die Gemeindeverwaltung Stockelsdorf ihre **interne Datenverarbeitung sowie ihren Internetanschluss** auf die Konformität mit den datenschutzrechtlichen Vorgaben in einem Auditverfahren überprüfen. Nach einer Bestandsaufnahme vor Ort haben der Datenschutzbeauftragte und der Administrator der Gemeinde Optimierungsmöglichkeiten für die interne automatisierte Datenverarbeitung erarbeitet. Durch eine gute Arbeitsplanung und die Beratung durch das ULD ist die datenschutzkonforme Restrukturierung der internen Datenverarbeitung und der Internetanbindung bereits auf einem guten Weg.

Was ist zu tun?
Kleine und mittlere kommunale Verwaltungen können mit einer Auditierung ihrer Datenverarbeitung bei guter Vorbereitung und Arbeitsplanung zügig und ohne hohe Aufwände zu einem erfolgreichen Ergebnis kommen.

9.1.7 Konzept für pharmakogenetische Forschung

Die Universität Kiel hat im Auftrag des Pharmakonzerns Schering AG ein Konzept für die Lagerung, Verwaltung und wissenschaftliche Auswertung von genetischen und klinischen Daten in der pharmakogenetischen Forschung erstellt. Den ersten Teil des Konzepts haben wir im Jahr 2003 auditiert. Anfang 2006 konnten wir auch die Fortsetzung des Konzepts mit einem Audit auszeichnen.

> ***? Pharmakogenetische Forschung***
>
> *Pharmakogenetische Forschung hat zum Ziel, den Einfluss genetischer Faktoren bei der Reaktion von Patienten auf Arzneimittel zu erforschen und die Ergebnisse für die Entwicklung und die Verabreichung von Arzneimitteln zu nutzen.*

Im ersten Teil dieses Konzepts ging es um die Schaffung einer wichtigen Grundlage für die pharmakogenetische Forschung: die pseudonyme Einlagerung von Blut- und Gewebeproben. Der zweite Teil des Konzepts befasst sich mit der Durchführung der Forschung selbst. Im Mittelpunkt steht die Frage der **Zusammenführung der genetischen und der klinischen Daten** eines Teilnehmers. Es gilt zu verhindern, dass bei diesem Prozess die nach der ersten Phase des Konzepts pseudonymisierten genetischen Informationen durch die hinzukommenden klinischen Daten wieder der Person des Teilnehmers zugeordnet werden können.

> ***? Genetische und klinische Daten***
>
> *Genetische Daten werden durch eine Analyse der DNA ermittelt, die wiederum aus Blut- oder Gewebeproben der Teilnehmer gewonnen wird. Klinische Daten sind in einer klinischen Studie erhobene medizinische Daten, z. B. Befunde, Laborergebnisse, Geburtsdatum, Gewicht und Größe. Im Rahmen einer solchen Studie lassen sie direkte Rückschlüsse auf die Person des Teilnehmers zu.*

Dazu werden in den klinischen Datensätzen Informationen, die eine persönliche Zuordnung erlauben (z. B. Namen oder Geburtsdaten), gelöscht. Neben diesem Reinigungsprozess ist ein so genannter **Feed-back-Prozess** Gegenstand des Audits: Auf Wunsch eines Teilnehmers an dem Forschungsprogramm kann dieser zusammen mit einem Arzt seines Vertrauens über Erkenntnisse zu seiner persönlichen genetischen Veranlagung informiert werden. Dazu müssen die pseudonymisierten genetischen Informationen wieder dem Teilnehmer zugeordnet werden. Mithilfe eines Verschlüsselungsverfahrens kann das Konzept sicherstellen, dass innerhalb der Forschungsstelle niemand zugleich Teilnehmerinformationen und genetische Informationen kennt. Der Teilnehmer und sein Arzt können nur gemeinsam auf die genetischen Informationen zugreifen.

Ein dritter Schwerpunkt des Audits ist ein **Anonymisierungsprozess** für sonstige **interessierte Forschungsstellen**, die anonymisierte Gewebeproben und dazugehörige klinische Daten zur Verfügung gestellt bekommen. Da diese nicht an die speziellen Datenschutzmaßnahmen des Konzeptes gebunden sind, dürfen sie nur

Proben und Daten ohne Personenbezug erhalten. Hierfür werden mindestens acht Datensätze zusammengefasst; dieser Datenbestand wird nur mit einem Teil der Gewebeproben, die zu den aggregierten Datensätzen gehören, herausgegeben. Eine 1:1-Zuordnung zwischen Gewebeproben und klinischen Daten ist so nicht mehr möglich.

Was ist zu tun?
Das Auditverfahren zeigt, dass ein datenschutzgerechter Umgang mit genetischen Daten und Probenmaterial möglich und praktikabel ist. Ähnliche Forschungsvorhaben können sich an diesem Konzept orientieren.

9.2 Datenschutz-Gütesiegel

9.2.1 Abgeschlossene Gütesiegelverfahren

Im Berichtszeitraum konnte zahlreichen Produkten ein Datenschutz-Gütesiegel verliehen werden. Es wurden 12 Produkte erstmalig zertifiziert. Zwei weitere Produkte wurden nach Fristablauf der ersten Zertifizierung in einem vereinfachten Verfahren rezertifiziert.

Dank der Förderung durch das EU-Programm „e-Region“ (27. TB, Tz. 9.1.1) konnte das ULD seine Zertifizierungsdienstleistungen in der Startphase gebührenfrei erbringen. Obwohl inzwischen für die Durchführung des Gütesiegelverfahrens den Produktanbietern Kosten entstehen, reißt die Nachfrage nicht ab. Das steigende Interesse der Hersteller, eine Zertifizierung auch ohne finanzielle Zuschüsse durchzuführen, belegt die **Notwendigkeit des Angebotes** von Datenschutzzertifikaten für die Wirtschaft.

Im Einzelnen wurden folgende Produkte zertifiziert:

- PrimeSharing TeamDrive, Version 1.1, ein Kollaborationstool für den Fernzugriff mehrerer Benutzer auf einen verschlüsselten Datenbestand zur gemeinsamen Bearbeitung von Dokumenten,
- CC DMS, Version 2.2, ein Dokumentenmanagement- und Archivsystem für öffentliche Verwaltungen, das die elektronische Ablage und Verwaltung von Dokumenten ermöglicht,
- MESO Internetauskunft, Version 1.2, eine internetbasierte Anwendung für Meldebehörden, die Daten aus dem Melderegister für die Behördenauskunft oder für die einfache Melderegisterauskunft zur Verfügung stellt,
- e-NFS, Version 1.0, eine webbasierte Anwendung zur Erhebung und Verarbeitung der Daten von Teilnehmern an berufsvorbereitenden Bildungsmaßnahmen,
- Verfahren der Akten- und Datenträgervernichtung, Stand: Oktober 2005, ein Verfahren zur Vernichtung von Akten und Datenträgern durch die Lutz von Wildenradt GmbH im Auftrag für öffentliche und nichtöffentliche Stellen,

- TurboMed.Net, Version 1.0, eine Kommunikationslösung zum verschlüsselten Austausch von Nachrichten und Patienteninformationen zwischen Ärzten über das Internet,
- MBS-easy, Version 3.6.0.0, eine Softwareapplikation für die Aufnahme, weitere Verarbeitung und Verwaltung von digitalen ärztlichen Diktaten durch Schreibkräfte oder durch ein Spracherkennungsprogramm.

Darüber hinaus wurden fünf Produkte zertifiziert, die als Branchenlösung für Industrie- und Handelskammern zentral bei einem IT-Dienstleister der IHK, der IHK GfI, gehostet und zur Verfügung gestellt werden. Im Einzelnen sind dies:

- Erweiterte Verwaltungsanwendung – EVA, Version 2.05, Modul FiDa (Firmendaten), ein Informationssystem für die Verarbeitung von Stammdaten der IHK-Mitgliedsunternehmen,
- Erweiterte Verwaltungsanwendung – EVA, Version 2.05, Modul Beruf, ein Modul zur Unterstützung der Wahrnehmung der gesetzlichen Aufgaben der Industrie- und Handelskammern in der Berufsausbildung,
- die drei Module IHK SELEROM (Version 1.2), IHK SELEInfo (Version 2004) und IHK SELEInfoPlus (Version 5.0), die das Produkt EVA ergänzen und als Selektionsverfahren den Abruf, die Auswahl und den Export von Daten aus dem Datenbestand der Industrie- und Handelskammern auf DVD, im Extranet sowie im Intranet der Industrie- und Handelskammern ermöglichen.

Im Rezertifizierungsverfahren wurden die folgenden Produkte in einem vereinfachten Verfahren (27. TB, Tz. 9.1.4) erneut überprüft und zertifiziert:

- e-pacs Speicherdienst, Version 3.0, eine Lösung für die elektronische externe Archivierung von Röntgenbildern und anderen patientenbezogenen medizinischen Daten, und
- ein Verfahren der Vernichtung von Akten und Mikroformen der Firma AVZ im Auftrag für öffentliche und nichtöffentliche Stellen, das Akten und Mikroformen in verschlossenen Containern der Vernichtung zuführt.

Einen Gesamtüberblick über alle zertifizierten und rezertifizierten Produkte enthält das **Register auf unserer Homepage**, das auch auf die Kurzgutachten mit den Ergebnissen der Prüfung und mit näheren Erläuterungen zu den Produkten verweist.

www.datenschutzzentrum.de/guetesiegel/register.htm

Auch im letzten Jahr erreichten uns viele Anfragen von Herstellern, die wir – oft zu unserem Bedauern – wegen fehlender rechtlicher Voraussetzungen **zurückweisen** mussten. Dazu gehörte z. B. der Betrieb von Webportalen, Datenschutzliteratur sowie Online-Schulungen datenschutzrechtlicher Inhalte. Einigen Angeboten mangelte es an der Produkteigenschaft im Sinne der Datenschutzverordnung: Sie hatten zwar Berührungspunkte mit dem Datenschutz, verarbeiteten selbst aber

weder personenbezogene Daten, noch unterstützten sie auf technische Weise eine sichere Datenverarbeitung. Andere Anfragen hatten die Zertifizierung eines datenschutzgerechten Verfahrensablaufs einer nichtöffentlichen Stelle zum Gegenstand. Diese können wir **mangels einer rechtlichen Grundlage** nicht zertifizieren. Immer noch nicht ist die Ankündigung des Bundesgesetzgebers umgesetzt, ein Bundesdatenschutzauditgesetz zu erlassen (27. TB, Tz. 9.1.6). So schön es sein mag, dass das ULD bisher auch von der Privatwirtschaft als wichtiger Datenschutzzertifizierungspartner angesprochen wird, so ärgerlich ist es, dass wir den offensichtlich bestehenden Bedarf selbst nicht stillen können und ein Bundesgesetz nicht in Aussicht steht.

Was ist zu tun?
Die Ausarbeitung eines Bundesdatenschutzauditgesetzes ist überfällig.

9.2.2 Überarbeitung der Regelungen für das Zertifizierungsverfahren

Gütesiegelverfahren sind nichts Statisches. Laufend sind Anpassungen an die Änderungen der rechtlichen und technischen Gegebenheiten nötig. Dabei fließen die Erfahrungen aus bisherigen Zertifizierungen ein.

Im vergangenen Jahr haben wir die Regelungen für das Zertifizierungsverfahren an **aktuelle Entwicklungen** angepasst. Dies betraf neben den Regeln für die Anerkennung von Sachverständigen (Tz. 9.2.4) den Anforderungskatalog, der die Prüfpunkte bei der Begutachtung eines Produktes vorgibt. Der Katalog wurde in Teilen **umstrukturiert und gestrafft**, was die Prüfung der Zulässigkeit der Datenverarbeitung vereinfacht. Einige Prüfkriterien wurden im Katalog deutlicher als bisher hervorgehoben. Dies betraf die Zulässigkeit und die technische Sicherheit von Abrufverfahren und so genannten Gemeinsamen Verfahren, die im letzten Jahr verstärkt Gegenstand von Zertifizierungsverfahren waren.

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

In fast allen Produkten werden **Protokolldaten** aus Gründen der Datensicherheit und der Revision verarbeitet. Diese unterliegen selbst strengen datenschutzrechtlichen Anforderungen wie Zweckbindung, Zugriffsbeschränkungen und Löschungsverpflichtungen, die im Gütesiegelverfahren überprüft werden. Da diese Prüfung durch die Sachverständigen immer wieder unzureichend war und häufiger Nachfragen durch uns bedurften, haben wir die Anforderungen an Protokolldaten in einem speziellen **Anforderungsprofil** zusammengestellt, um die Prüfung zu erleichtern.

Anfragen zum Gütesiegelverfahren zeigten uns, dass der genaue Ablauf des Zertifizierungsverfahrens für Hersteller im Detail nicht ganz einfach nachzuvollziehen

ist. Wir haben daraufhin unsere Webseite auf einzelne Nutzergruppen zugeschnitten und in einem Dokument speziell die für **Hersteller** notwendigen Informationen zusammengefasst.

9.2.3 Umfrage zu den Erfahrungen der Hersteller zertifizierter Produkte

Gut zwei Jahre nach der ersten Verleihung eines Gütesiegels wollten wir von den Empfängern der bis dahin 20 vergebenen Gütesiegel über eine an die Hersteller gerichtete Fragebogenaktion erfahren, wie sich diese in der Praxis ausgewirkt haben.

Ungefähr die Hälfte der Herstellerunternehmen hat sich an unserer Umfrage beteiligt. Zwei Drittel der Hersteller haben die **Auswirkungen der Zertifizierung** für ihr Produkt als **sehr positiv** angegeben; für mehr als die Hälfte der Unternehmen ist es nach erfolgter Zertifizierung einfacher geworden, Aufträge in ihrem Bereich zu erhalten. Ein Großteil der befragten Hersteller bietet ihr Produkt bzw. ihre IT-Dienstleistung sowohl für die Verwaltung als auch für die Privatwirtschaft, teilweise sogar schwerpunktmäßig für Letztgenannte, an. Auffällig ist, dass die Erfahrungen im Bereich der Verwaltung und in der Privatwirtschaft gleich sind. Als erfolgreichste Branche für den Einsatz zertifizierter Produkte hat sich der Medizinbereich herausgestellt. Hier haben die Hersteller durch das Gütesiegel teilweise erhebliche Erleichterungen und Steigerungen bei dem Absatz ihrer Produkte erzielen können. Für ein Drittel der Hersteller hat sich die Zertifizierung ihres Produktes nur geringfügig ausgewirkt. Vielfach konnte sich dieses wegen anderer Kriterien, hauptsächlich aufgrund des Preises, trotz Zertifizierung nicht gegen Konkurrenzprodukte durchsetzen.

Wir baten die Hersteller um ihre Einschätzung zu den **Gründen**, weshalb sich in ihrem Fall das Gütesiegel nicht positiv auf die Vermarktung des Produkts ausgewirkt hat. Am häufigsten wurde angegeben, dass das Datenschutz-Gütesiegel einen zu starken Regionalbezug habe. Als weiterer Grund wurde die fehlende Bekanntheit des Instruments des Gütesiegels und des ULD als Zertifizierungsstelle genannt. Nur in Einzelfällen wurde angegeben, die Kunden seien an Datenschutz und Datensicherheit nicht interessiert oder die Tatsache der konkreten Produktzertifizierung sei diesen nicht bekannt. Die Antwortmöglichkeit „Fehlendes Vertrauen in die Zertifizierung und in das ULD“ wurde von keinem Hersteller angekreuzt.

Wir haben die Hersteller sowohl nach ihren **Erwartungen**, die sie mit der Zertifizierung verbunden hatten, als auch danach gefragt, in welchem Maß diese Erwartungen tatsächlich eingetreten sind. In erster Linie haben die Hersteller eine **Verbesserung ihrer Marktposition** und der Akzeptanz bei den Kunden erwartet. Bei genau zwei Dritteln der Hersteller sind die hohen Erwartungen in der Praxis tatsächlich eingetreten. Ein Drittel der Hersteller konnte jedoch nur geringe Auswirkungen des Gütesiegels auf die Marktposition bzw. die Akzeptanz des Produkts verzeichnen. Betrachtet man die Hersteller einzeln für sich, wird deutlich, dass überwiegend die anfänglichen Erwartungen erreicht oder sogar übertroffen wurden.

Nach **Kritik und Verbesserungsvorschlägen** gefragt, haben die Hersteller am häufigsten die Aufforderung zu stärkerer Information der Verwaltung und der Privatwirtschaft über das Gütesiegel, zertifizierte Produkte und über die Wichtigkeit von Datenschutz gestellt. In einem Fall wurde darauf hingewiesen, dass das Gütesiegel bei Ausschreibungen nicht das alleinige Vergabekriterium und der Preis meist von höherer Bedeutung sei. Positiv wurde von zwei Herstellern geäußert, durch die Zertifizierung habe das Unternehmen ein Alleinstellungsmerkmal für ihr Produkt erhalten und so zahlreiche Aufträge bekommen können.

9.2.4 Sachverständige

Drei Jahre nach Beginn des Verfahrens belegen die Zahlen der Neuanträge ein stetes Interesse an der Akkreditierung als Datenschutzsachverständiger beim ULD.

Die Begutachtung von IT-Produkten im Zertifizierungsverfahren erfolgt durch externe Sachverständige. Personen oder Prüfstellen, die ihre Fachkunde im Bereich Recht und/oder Technik sowie Unabhängigkeit und Zuverlässigkeit nachweisen, können auf Antrag bei uns als Sachverständige oder sachverständige Prüfstellen anerkannt werden. Einhergehend mit dem wachsenden Angebot und der Nachfrage nach Beratungsdienstleistungen im Datenschutz nimmt auch das **Interesse an einer Akkreditierung** beim ULD als Nachweis der Fachkunde zu. Die für eine beratende Tätigkeit im Datenschutz, etwa als betrieblicher Datenschutzbeauftragter, geforderte Fachkunde ist jedoch nicht identisch mit den Anforderungen an eine Akkreditierung als Sachverständiger für das Gütesiegel. Die Akkreditierung setzt neben einer einschlägigen rechtlichen oder technischen Ausbildung eine mindestens dreijährige berufliche Erfahrung im Datenschutz voraus. Kenntnisse und Fähigkeiten sind über den betrieblichen Bereich hinaus auch im öffentlichen Sektor gefordert. Einigen Interessenten mussten wir von einer Antragstellung abraten, da zumeist wegen geringer beruflicher Erfahrungen keine Aussicht auf eine Anerkennung bestand.

- **Anerkennungen im Berichtszeitraum**

Im Berichtszeitraum haben wir fünf Anträge auf Anerkennung erhalten und auch **fünf Sachverständige anerkannt**. Unter diesen ist eine Sachverständige für die Bereiche Recht und Technik; ein Sachverständiger wurde für den Bereich Technik und drei Sachverständige wurden für den Bereich Recht akkreditiert. Drei Anträge, teilweise noch aus dem Vorjahr, waren nicht erfolgreich: Zwei der Anträge wurden von den Antragstellern zurückgenommen, einen Antrag haben wir abgelehnt.

- **Überarbeitung der Regelungen für die Anerkennung**

Für die Anerkennung von Sachverständigen haben wir im Jahr 2002 umfangreiche Regelungen erstellt, die die Voraussetzungen für die Anerkennung sowie Pflichten bei der Ausübung der Sachverständigentätigkeit benennen. Diese Regelungen wurden von uns anhand der umfangreichen zwischenzeitlich gesammelten praktischen Erfahrungen **auf den Prüfstand gestellt**. Der Informations- und der Pflichtenkatalog für Sachverständige wurden überarbeitet.

Die umfangreichste Änderung gab es bei den Anforderungen an die **Fachkunde** für Technik und Recht. Diese beiden Bereiche wurden angeglichen, indem für jeden Bereich jeweils drei gleichartige Stufen des Fachkundenachweises formuliert wurden. Die einzelnen Anforderungen in diesen Stufen wurden präzisiert und auf die tatsächlichen Ausbildungsmöglichkeiten in beiden Bereichen angepasst.

Wir haben zwei Regelungen zur Unabhängigkeit des Sachverständigen aus dem Katalog herausgenommen, da sie sich als nicht praxisgerecht erwiesen. Dies betrifft zum einen das in der ersten Fassung enthaltene Verbot für den Sachverständigen, **technische Einrichtungen des Auftraggebers** für die Begutachtung zu nutzen. Zum anderen ist das Verbot einer **Beteiligung** des angestellten Sachverständigen an dem **Gewinn seines Arbeitgebers** entfallen. Während die ursprüngliche Fassung die Koppelung des Einkommens eines angestellten Sachverständigen an die Zahl und das Ergebnis seiner Gutachten verbot, ist nunmehr lediglich die Koppelung an das Ergebnis der Sachverständigengutachten untersagt. Außerdem ist die Pflicht zur Vorlage eines Auszugs aus dem Gewerbezentralregister entfallen. Es erfolgten Klarstellungen hinsichtlich der zulässigen Organisationsformen von Prüfstellen sowie der Werbung und Haftung von Sachverständigen.

9.2.5 Gütesiegel und PRIME

Im Projekt PRIME werden Prototypen eines Identitätsmanagementsystems entwickelt. Das ULD begleitet das Projekt in datenschutzrechtlicher Hinsicht. Dazu gehört auch eine Prüfung der Prototypen nach Gütesiegelkriterien.

> ***? Common Criteria (CC)***
>
> *Bei den CC handelt es sich um eine international abgestimmte Grundlage für die Prüfung und Bewertung der Sicherheitseigenschaften von Produkten und Systemen der Informationstechnik, die auch bei der Entwicklung und Beschaffung anwendbar sein kann.*

Bei der Entwicklung der Prototypen (Tz. 8.2.1) werden auch Aspekte der **Qualitätssicherung** beachtet. Dabei geht es nicht nur um die Beachtung von Datenschutz- und Datensicherheitskriterien, vielmehr werden im Rahmen einer Evaluation die Gesichtspunkte der IT-Sicherheit und des Datenschutzes auch an etablierten Kriterien gemessen. Für die Prüfung der IT-Sicherheit werden die Common Criteria (CC) verwendet. Zur Datenschutzprüfung sollen u. a. die Kriterien des Datenschutz-Gütesiegels eingesetzt werden. Diese sind im Projekt PRIME nicht unmittelbar anwendbar: Sie bilden das Datenschutzrecht von Schleswig-Holstein ab, das für die Behörden des Landes gilt. Der Prototyp des Projekts PRIME wendet sich aber an Verbraucher und Firmen in der gesamten EU. Daher haben wir den **Anforderungskatalog des Gütesiegels** übersetzt und an den Aufbau und die Formulierungen der EU-Datenschutzrichtlinie angepasst. Diese „EU-Version“ deckt die Anforderungen der EU-Datenschutzrichtlinie ab und kann auch in anderen internationalen Projekten, z. B. im Projekt RISER (Tz. 8.3), als Prüfschema verwendet werden. Die Prototypen wurden während der Entwicklungsphase nach den Anforderungen des angepassten Anforderungskataloges geprüft.

Was ist zu tun?
Die bisher gewonnenen Erfahrungen sind bei den weiteren Entwicklungsschritten zu berücksichtigen und bei der Produktgestaltung umzusetzen.

9.2.6 Europäische Aktivitäten im Gütesiegelbereich

Nicht nur in Deutschland gibt es Regelungen für Audit und Gütesiegel, sondern auch in Frankreich. Eine Delegation der Französischen Datenschutzkommission (Commission Nationale de l'Informatique et des Libertés, CNIL) besuchte im Januar 2006 das ULD, um sich über das schleswig-holsteinische Verfahren und über Erfahrungen mit dem Gütesiegel zu informieren.

Das **französische Datenschutzgesetz**, das – anders als die deutschen Regelungen auf Länder- und Bundesebene – für alle Behörden und Firmen in ganz Frankreich gilt, sieht die Zertifizierung von datenschutzkonformen Produkten und Verfahren vor. Während in Deutschland auf Bundesebene (27. TB, Tz. 9.1.6) und in den meisten Ländern solche Umsetzungen noch ausstehen, wird in Frankreich an den konkretisierenden Regelungen gearbeitet. Der Besuch der Delegation hatte den Zweck, möglichst viele Informationen und Erfahrungen aus der Praxis zu sammeln, um diese in die französische Verordnung einfließen zu lassen. Am Dialog mit den französischen Kollegen nahmen auch ein schleswig-holsteinischer Hersteller eines zertifizierten Produktes und ein Sachverständiger teil, die über Aufwand und Nutzen der Zertifizierung aus erster Hand berichten konnten.

Bei dem Informationsbesuch wurden auch **zukünftige Kooperationsmöglichkeiten** erörtert. Erstes Ziel ist ein europaweiter Austausch zur Gültigkeit von Zertifizierungen durch gegenseitige Anerkennung. Langfristig kommt auch – einhergehend mit der Weiterentwicklung der nationalen Erfahrungen – ein europäisches Gütesiegel in Betracht.

Was ist zu tun?
Der Bundesgesetzgeber sollte sich mit dem Bundesdatenschutzauditgesetz beeilen und sich so an die Spitze der europäischen Entwicklung setzen.

10 Aus dem IT-Labor

10.1 Kreditkarten im Internet – Risiko ohne Grenzen?

Online-Shopping ist „in". Immer mehr Internetnutzer entdecken die Vorzüge von Warenbestellungen per Internet. Dabei kommt neben der Überweisung vor allem die Kreditkarte als Zahlungsmittel zum Einsatz. Wie im realen Leben lässt sich die Gefahr eines möglichen Missbrauchs der Kreditkartendaten nicht vollständig abwenden, durch Beachtung einfacher Regeln aber vermindern.

Wer bei einem Online-Händler mit einer Kreditkarte zahlen möchte, muss seinen Namen angeben, die Kartennummer, deren Ablaufdatum sowie die dreistellige Kartenprüfnummer. Mit diesen Informationen kann der Händler die Abbuchung des Kaufbetrages veranlassen. Allerdings kann er mit diesen Daten – zumindest theoretisch – **jederzeit Abbuchungen in beliebiger Höhe** vornehmen. Eine zusätzliche Authentifizierung, etwa durch eine Unterschrift, findet nicht statt.

Bankenvertreter bestätigen, dass Kundinnen und Kunden generell keine Möglichkeit haben, sich gegen derartigen Missbrauch zu schützen, und raten, Kreditkartendaten nur **vertrauenswürdigen Online-Händlern** zu übermitteln. Dies ist allerdings leichter gesagt als getan. Vertrauenswürdigkeit ist im Internet schwer zu vermitteln und leicht vorzutäuschen. Das Risiko unrechtmäßiger Abbuchungen ist den Kreditkartenunternehmen bewusst. Erklärt der Kunde an Eides statt, dass er eine geleistete Zahlung nicht autorisiert hat, und kann der Händler diese Autorisierung nicht belegen, so erhält der Kunde das Geld mit der nächsten Abrechnung zurück, so die Deutsche Bank. Um Ärger mit der Kreditkarte im Internet vorzubeugen, ergeben sich folgende Grundsätze:

- Online-Shopping per Kreditkarte niemals in einem Internetcafé abwickeln. Die Rechner dort sind nicht vertrauenswürdig: Tastatureingaben können leicht mitgeschnitten werden, sodass die Kreditkartendaten in fremde Hände gelangen können.
- Auf die Zahlung per Kreditkarte sollte im Internet so weit wie möglich verzichtet werden.
- Wird per Karte gezahlt, sollten unbedingt Ausdrucke der Transaktion angefertigt werden, eventuell versehen mit ergänzenden Kommentaren. So kann später besser belegt werden, wo welche Käufe getätigt worden sind und wo nicht.
- Wird eine Online-Zahlung durchgeführt, sollte dies nur über eine SSL-gesicherte Verbindung geschehen, zu erkennen an einer Webadresse beginnend mit „https://...".

Allerdings ist das Risiko nicht auf die Online-Welt beschränkt. Wer **im Restaurant** mit Kreditkarte zahlt, gibt die Karte in der Regel kurze Zeit aus der Hand. Kreditkarten- und Kartenprüfnummer können auch hier entwendet, d. h. abgeschrieben werden. Kreditkarten sind konzeptionell nur sehr schwach gegen Missbrauch geschützt.

Was ist zu tun?
Der sorgfältige Blick auf die Kartenabrechnung bleibt das einzige Mittel, um Missbrauch aufzudecken. Wirklich vorbeugen kann man nicht.

10.2 Per E-Mail zu fremden Bonusmeilen

Bei Anmeldeverfahren von Online-Diensten sollte auf die korrekte Schreibweise der eigenen Mailadresse geachtet werden. Im schlimmsten Fall kann ein fremder Nutzer auf die Kosten eines anderen diesen Dienst nutzen. Anmeldeverfahren sollten über eine Bestätigungsmailfunktion verfügen.

Im Juli 2005 häuften sich in einem elektronischen Postfach des ULD **Bestätigungsmails** für die Anmeldung an einem Bonusmeilenprogramm einer Fluggesellschaft. Zwei Dinge waren verwunderlich: Zum einen hatte sich kein Mitarbeiter bei einem solchen Programm angemeldet, zum anderen gingen die Mails allesamt an die Adresse „datenschutz@datenschutz.de“. Die Domain www.datenschutz.de inklusive der dazugehörigen Mailadressen wird zwar vom ULD verwaltet, diese Adresse ist jedoch keinem realen Mailkonto zugeordnet. Nachrichten an solche unbekannten Adressen landen in einem separaten, übergreifenden Posteingang, so auch die Anmeldebestätigungen der Fluggesellschaft.

Eine falsch angegebene Mailadresse ist nicht ungewöhnlich, eine derartige Häufung mit immer derselben Adresse hingegen schon. Auf der Webseite der Fluggesellschaft sahen wir uns die Anmeldeseite für Teilnehmer des Bonusprogramms an. Hier muss man sich mit Nutzernamen und Passwort authentifizieren. Es existiert eine Schaltfläche für vergessene Passwörter. Deren Betätigung generiert ein neues Passwort, das automatisch an die hinterlegte Mailadresse gesendet wird, in diesem Falle an uns. Innerhalb weniger Minuten erhielten wir so Zugang zum Bonusmeilenkonto. Eine Rücksprache mit dem Datenschutzbeauftragten der Fluggesellschaft ergab, dass die Konten alle von einer einzigen Person angelegt worden waren, vermutlich mit der **Absicht der Übervorteilung**.

Der Fall zeigt: Bei der Anmeldung bei Internetdiensten sollte sorgfältig auf die Schreibweise der eigenen Mailadresse geachtet werden. Ein Tippfehler führt im günstigsten Fall dazu, dass Mails des Seitenbetreibers nicht zugestellt werden und im Nirvana landen. Im schlimmsten Fall jedoch werden die **Mails an fremde Personen ausgeliefert**. Sind dann keine weiteren Sicherungsmaßnahmen vorgesehen, steht dem Nutzer der falschen Adresse mitunter der gesamte Dienst offen.

Das Problem lässt sich relativ leicht dadurch lösen, dass bei der Anmeldung eine **Bestätigungsmail** generiert wird. Diese muss der Nutzer beantworten, bevor sein

Account freigeschaltet wird. Mit diesem Verfahren wird sichergestellt, dass der Anzumeldende wirklich im Besitz der eingegebenen Mailadresse ist. So werden Nutzer und Diensteanbieter vor Tippfehlern geschützt. Wer übrigens unbedingt eine nicht existierende Mailadresse angeben möchte, sollte eine Adresse der Domain example.com verwenden. Diese ist Testzwecken vorbehalten und kann nicht registriert werden. Mailadressen wie z. B. niemand@example.com landen zuverlässig im digitalen Nirgendwo und nicht im Postfach unbedarfter E-Mail-Nutzer.

10.3 Erste Lösungen für anonymes Logging umgesetzt

Das ULD betreute zusammen mit der Universität Regensburg eine wissenschaftliche Arbeit, welche die Entwicklung eines Logfile-Anonymisierers zum Ziel hatte. Dieser wie auch andere Produkte zur Anonymisierung von Logfiles bedürfen der kritischen Betrachtung.

Die Problematik des anonymen Loggings beschäftigt das ULD weiterhin (27. TB, Tz. 10.9). Logfiles können als eine klassische Form der „Vorratsdatenspeicherung“ angesehen werden. Es handelt sich um von einem Programm erstellte Dateien, in der **Datenverarbeitungsereignisse** dokumentiert werden. Es kommt grundsätzlich nicht darauf an, mit welchem Dienst (z. B. Webserver, Firewall, Proxy) ein Logfile erstellt wird und welche Art von sensiblen Daten es zu anonymisieren gilt. Vorgegeben ist nur, dass die Logfiles im Textformat geschrieben werden. Im Interesse der Datensparsamkeit ist ein Tool wünschenswert, welches durch Eingabe eines beliebigen Logformates und dessen zu anonymisierenden Daten auf jede Art Logfile anwendbar ist.

Grundsätzlich sind zwei Zeitpunkte der Anonymisierung möglich: Das Anonymisieren eines bereits geschriebenen Logfiles sowie die Anonymisierung schon während des Schreibvorgangs. Letzteres ist vorzuziehen, da hier sensible Daten gar nicht erst in Klarschrift abgelegt werden. Als Anforderung an den Anonymisierer selbst soll grundsätzlich gelten, dass dieser die personenbezogenen Merkmale zu anonymisieren hat, ohne dabei die **Nutzung der Logdaten** für die üblichen Analysetools unnötig zu erschweren oder sogar zu verhindern. Was hilft eine Anonymisierung der Logdaten, wenn sie später keine Aussagekraft mehr besitzen?

Diese Gratwanderung zwischen vollständiger Anonymisierung und Sicherung umfangreicher Auswertbarkeit versuchen die **am Markt befindlichen Tools** auf unterschiedliche Weise zu meistern. Anonlog z. B. eignet sich für das nachträgliche Anonymisieren von Webserver-Logfiles, wobei sensible Daten durch Wörterbucheinträge ersetzt werden. Beim Lundin Firewall Anonymisierer ist eine solche Ersetzung auch in Echtzeit möglich. Das Problem bei der Ersetzungsmethode ist die Tabelle, die jedem sensiblen Datum einen Wörterbucheintrag zuordnet. Solange dieser nicht gelöscht oder überschrieben wird, ist das „anonymisierte“ Logfile nur schwach pseudonymisiert. Wird er zu schnell überschrieben, ist eine Verkettbarbeit der Logfile-Einträge nur noch beschränkt möglich.

Das Tool Pseudo/CoRe verwendet ein **kryptografisches Verfahren**, wobei auch an eine Reidentifikation gedacht ist, um eventuelle Angreifer eines Systems lokalisieren zu können. Pseudo/Core versucht den Spagat zwischen Anonymisierung und Praxistauglichkeit, was durch Nutzung eines ausgeklügelten Regelsystems unter Integration von organisatorischen Maßnahmen gut gelungen ist. Beispielsweise ist die Vorgabe möglich, zur Reidentifizierung von Datensätzen den Datenschutzbeauftragten mit heranziehen zu müssen. Das Tool lässt sich auf verschiedene Logformate in Unix-Systemen anwenden und anonymisiert sowohl Daten in Echtzeit als auch bereits bestehende Dateien. Insgesamt ist Pseudo/Core aus Datenschutzsicht durchaus zu empfehlen. Obwohl es bereits 2003 vorgestellt wurde, befindet sich das Tool aber noch immer in der Prototypphase.

Um eine datenschutzgerechte sowie praktikable Lösung des anonymen Loggings vorstellen zu können, hat die Universität Regensburg zusammen mit dem ULD eine Diplomarbeit mit dem Thema „Konzeption und Implementierung eines **universellen Logfile-Anonymisierers** mit intuitiver Bedienoberfläche“ betreut. Das Ergebnis ist ein plattformunabhängiges und auf verschiedene Logformate anwendbares Tool, das sowohl nachträglich als auch „on the fly“ Logdaten anonymisieren kann.

Bei ersten Tests erwies sich der universelle Logfile-Anonymisierer durchaus als **praxistauglich**. Die leicht zu bedienenden Funktionen des Tools sowie seine universellen Einsatzmöglichkeiten heben es in eine Favoritenrolle. Allerdings haben noch keine ausführlichen Langzeittests stattgefunden, um endgültige Aussagen über die Leistungsfähigkeit des Tools treffen zu können. Der Anonymisierer ist als Open Source entwickelt worden, sodass eine Verbesserung oder Erweiterung des Tools problemlos möglich ist.

Was ist zu tun?
Die Anonymisierung von Logfiles ist angesichts der Automation von immer mehr gesellschaftlichen Lebensbereichen eine der größten technischen Datenschutzherausforderungen. Es besteht Erprobungs- und Umsetzungsbedarf.

10.4 Festplattenverschlüsselung bei tragbaren Rechnern

Es ist eine Binsenweisheit der Informationsgesellschaft, dass die Daten und nicht die Menschen laufen sollen. Ob Bewegungsarmut für die Menschen gesund ist, steht auf einem anderen Blatt. Fest steht, dass die Daten der Menschen nicht nackt und ungeschützt durch die Gegend wandern sollten. Die Folgen können für Betroffene und Verantwortliche fatal sein.

Nach Presseberichten sind zwischen 1996 bis 2002 in britischen Ministerien über 1300 Laptops verloren gegangen. Spitzenreiter war das britische Verteidigungsministerium mit 594 nicht wieder zu findenden tragbaren Rechnern. Vergleichbare Zahlen aus Schleswig-Holstein über den **Verlust an Laptops** sind uns nicht bekannt. Sicher ist aber, dass die Verbreitung mobiler Endgeräte insbesondere bei Führungskräften und Projektleitern in der öffentlichen Verwaltung zunimmt. Insofern folgt die öffentliche Verwaltung der Entwicklung in der Wirtschaft.

> ***Im Wortlaut: § 6 Abs. 3 LDSG***
>
> *Werden personenbezogene Daten mithilfe informationstechnischer Geräte von der Daten verarbeitenden Stelle außerhalb ihrer Räumlichkeiten verarbeitet, sind die Datenbestände zu verschlüsseln. Die Daten verarbeitende Stelle hat sicherzustellen, dass sie die Daten entschlüsseln kann.*

Über den Schutzbedarf personenbezogener Daten auf mobilen Geräten sollte kein Zweifel bestehen. Im Unterschied zu fest stehenden Rechnern, die in abschließbaren Räumen eingesetzt werden, sind mobile Rechner besonderen Risiken ausgesetzt, gegen die angemessene Schutzmaßnahmen zu ergreifen sind. Eine unberechtigte Einsichtnahme von auf tragbaren Rechnern befindlichen personenbezogenen Daten ist durch eine **Verschlüsselung** der gespeicherten Datenbestände zu verhindern. Das Landesdatenschutzgesetz schreibt dies für den öffentlichen Sektor ausdrücklich vor. Für den Privatbereich gilt Entsprechendes nach dem Bundesdatenschutzgesetz als Regel zur Zugriffskontrolle.

In den Konzepten auf kommunaler (KITS) und Landesebene (IKOTECH III) sind Programme zur kompletten Verschlüsselung von Festplatten standardmäßig vorgesehen bzw. vorgeschrieben. Wir haben in unserem IT-Labor eine Vielzahl von **Programmen zur Festplattenverschlüsselung getestet**. Einige Programme erlauben nur das Einrichten so genannter „Container“ oder Partitionen, in denen Daten sicher verschlüsselt gespeichert werden können. Diese Container oder Laufwerke werden durch ein Programm oder einen im Hintergrund laufenden Dienst ver- und entschlüsselt. Im Labortest zeigten diese Programme jedoch einige Schwächen. So können z. B. außerhalb der explizit verschlüsselten Bereiche in temporären Dateien schützenswerte Daten abgelegt sein.

Wir empfehlen daher die Nutzung von Programmen, die die **komplette Festplatte verschlüsseln**. Nur so wird wirklich gewährleistet, dass niemand, der unberechtigten Zugriff auf den tragbaren Rechner erhält, auf sensible Daten zugreifen kann. Beim Starten muss dann in der Regel ein Passwort eingegeben werden, um die Festplatte freizuschalten („Sicherheit durch Wissen“). Bei einem erhöhten Sicherheitsbedarf sollte die Autorisierung zudem über eine Smartcard erfolgen („Sicherheit durch Besitz und Wissen“).

Was ist zu tun?
Werden Laptops zur Verarbeitung personenbezogener Daten eingesetzt, so müssen diese verschlüsselt werden. Unter Sicherheitsgesichtspunkten sollte ein Verfahren zur Verschlüsselung der gesamten Festplatte eingesetzt werden. Gerade Führungskräfte sollten sich in Anbetracht möglicher Schäden durch den Verlust von personenbezogenen Daten ihrer Vorbildfunktion bewusst sein.

10.5 Patchmanagement

Sicherheitslecks in Betriebssystemen und Programmen werden fast täglich entdeckt. Um diese zu beheben, müssen Updates eingespielt werden. Während dies bei kleinen Netzwerken noch von Hand erledigt werden kann, müssen bei größeren Netzwerken zentrale Lösungen für ein effizientes Patchmanagement gefunden werden.

Ob Anwendungssoftware oder Betriebssystem, das Prinzip der „**Bananensoftware**“ ist kaum noch aufzuhalten: „Die Software reift beim Kunden.“ Der Kunde ist auf eine funktionstüchtige und sichere Software angewiesen, aber wirklich verlassen kann er sich nur darauf, dass die nächsten Patches vor der Tür stehen. So kritisch diese Entwicklung auch ist, eine Trendwende hin zu einer qualitätsorientierten Softwareentwicklung ist nicht in Sicht. Die Folge ist, dass die IT-Verantwortlichen sehr viel Zeit auf die Beseitigung von Fehlern investieren müssen, was neudeutsch „Patchmanagement“ genannt wird.

In unserem IT-Labor haben wir für Betriebssysteme der Windows-Familie einige **Softwarelösungen getestet**, die (halb-)automatisiert die Inventur, Installation und Kontrolle von Fehlerbehebungen auf Rechnern durchführen. So bietet z. B. Microsoft kostenfrei verschiedene Lösungen an. Wir haben u. a. das **Produkt WSUS** – Windows Server Update Services – intensiv geprüft. Mithilfe dieser serverbasierten Lösung kann der Installationsstatus der Patches für eine große Anzahl von Rechnern mit Microsoft-Produkten einfach und übersichtlich eingerichtet werden. Eine zeitgesteuerte, in Gruppen aufteilbare Installation explizit ausgewählter Patches ist nach Freigabe des Administrators möglich. Verschiedene weitere Komfortfunktionen (wie z. B. ein umfangreiches Berichtswesen) ermöglichen es, mit geringem personellem Aufwand eine große Anzahl an Rechnern zu verwalten.

In **gemischten Netzwerken**, in denen auch Software und Betriebssysteme anderer Hersteller eingesetzt werden, sollten jedoch andere Lösungen in Betracht gezogen werden, um ein einheitliches und zentrales Patchmanagement zu gewährleisten.

Was ist zu tun?
IT-Verantwortliche sollten zumindest für die Betriebssysteme ein weitgehend automatisiertes Patchmanagement einführen. Mit WSUS bietet Microsoft für die aktuelle Generation seiner Betriebssysteme eine leistungsfähige und kostenfreie Lösung an.

10.6 WLAN: Sicher per „default“?

Drahtlose Netzwerke lassen sich ohne viel Aufwand installieren. Computer und Laptops sind innerhalb von Minuten an das Netzwerk angebunden. Doch eine Sicherheit bietende Verschlüsselung ist bei den meisten Geräten standardmäßig ausgeschaltet, oder der gewählte Standard ist bereits veraltet.

Drahtlose Netzwerke (Wireless Local Area Networks, kurz WLAN) haben gegenüber kabelgebundenen Netzen einen gravierenden Nachteil: Die Zugriffsmöglichkeiten auf diese Netze enden nicht am Kupferdraht der Leitung und an den Wänden des Gebäudes. Auf die Wellen eines örtlichen Funknetzes kann auch außerhalb der Gebäude zugegriffen werden. Um diesen Nachteil auszugleichen, bieten die Hersteller ihre WLAN-Systeme mit kryptografischen Algorithmen zur **Verschlüsselung** an, die eine aus Sicht der Hersteller mit herkömmlichen drahtgebundenen Netzen „vergleichbare“ Sicherheit gewährleisten sollen. Aus diesem Grund haben die Hersteller das derzeit noch weit verbreitete Verschlüsselungsverfahren auch WEP – wired equivalent privacy – getauft.

WEP gilt jedoch nach dem aktuellen Stand der Sicherheitstechnik als unsicher (27. TB, Tz. 10.5): Wir haben in verschiedenen, im IT-Labor nachgestellten Szenarien innerhalb von Minuten die unterschiedlichen **WEP-Verschlüsselungsalgorithmen** mit im Internet frei erhältlichen und kostenlosen Programmen brechen können. So genannte Sicherheitsmechanismen, die auch in der Fachpresse immer wieder genannt werden, wie das Filtern auf bekannte, erlaubte Geräte (MAC-Filterung), das „Verstecken“ des Accesspoint (SSID-Hiding) oder die Reduzierung der Sendeleistung, liefern lediglich minimale Sicherheitsgewinne. Sie verlängern die Gesamtzeit bis zum erfolgreichen Eindringen in ein WLAN nur um wenige Minuten.

Die Unsicherheit von WEP hat viele namhafte Hersteller dazu bewogen, eine Weiterentwicklung von WEP als neuen Standard zu deklarieren, den so genannten **WiFi Protected Access (WPA) Standard**. WPA ist sicherheitstechnisch ein Schritt in die richtige Richtung und gilt bei ausreichender Schlüssellänge als Mindeststandard für den Heimbereich.

Ein deutlich höheres Sicherheitsniveau bieten die Nachfolgestandards **WPA2 und IEEE802.11i** (27. TB, Tz. 10.5). Diese liefern nach dem derzeitigen Kenntnisstand ausreichende Schutzmechanismen für WLAN zur Verarbeitung von personenbezogenen Daten mit niedrigem bis mittlerem Schutzbedarf. Weiterhin gilt jedoch: Daten mit hohem Schutzbedarf dürfen in einem WLAN nicht ohne zusätzliche Sicherheitsmaßnahmen wie einer Verschlüsselung in einem Virtuellen Privaten Netzwerk (VPN) verarbeitet werden.

Was ist zu tun?
Der Betrieb eines WLAN sollte durch Verschlüsselungsstandards wie WPA2 oder IEEE802.11i abgesichert werden. Altgeräte, die nur WEP-Verschlüsselung unterstützen, sollten ausgetauscht oder die Software durch neue Treiber und Firmware aktualisiert werden. Bei einem hohen Schutzbedarf der Daten sind Funknetze als verschlüsselte Virtuelle Private Netzwerke (VPN) zu betreiben.

10.7 Sperren von Schnittstellen und Laufwerken

Über externe Schnittstellen und offene Laufwerke können Daten in IT-Netzwerke eingeschleust oder ausgelesen werden. Die Nutzung solcher Schwachstellen muss nicht auf böser Absicht beruhen. Den eingeschleusten Viren und Trojanern ist es aber egal, warum die Türen zu den Rechnern offen stehen. Entscheidend ist, dass der durch Viren oder Trojaner ausgelöste Schaden erheblich sein kann.

Die meisten IT-Verantwortlichen sichern ihre Netzwerke mit einem hohen Sach- und Personalaufwand gegen Angriffe von außen ab. Viele IT-Infrastrukturen sehen sich weiterhin einer großen Gefahr von innen ausgesetzt: **Offene Schnittstellen** wie USB und Firewire bieten einfach zu nutzende Anschlussmöglichkeiten für jede Art von Peripheriegeräten wie Tastaturen, Mäuse und Drucker, aber auch Massenspeicher wie USB-Sticks und externe Festplatten. Benutzern eröffnet sich damit die Möglichkeit, in großem Stil personenbezogene Daten, aber auch Betriebs- und Geschäftsgeheimnisse auf portable Geräte zu kopieren.

Man muss hierbei nicht immer gleich **Datendiebstahl** unterstellen. Die Daten mögen in der guten Absicht vom Dienstrechner kopiert werden, „um zu Hause an dem Dokument weiterzuarbeiten“. Gleich ob in der Verwaltung oder in der Wirtschaft: Bei der Datensicherheit genügen gute Absichten nicht. Personenbezogene Daten vom Arbeitsplatz gehören ebenso wie Betriebs- und Geschäftsgeheimnisse nicht in private Datenspeicher, Rechner oder Netzwerke.

Auch der umgekehrte Weg, dass Daten von einem externen Gerät in das interne Netz eingespielt werden, ist für die internen Netzwerke eine erhebliche Gefahr: **Eingeschleppte schadhafte Dateien** können bei einer schwachen Sicherung des internen Netzes gewaltigen Schaden anrichten.

Abhilfe ist auf vielen Wegen möglich. Der einfachste ist das Abschalten der externen Schnittstellen. Häufig steht dieser Lösung jedoch entgegen, dass die Schnittstellen in definierten Fällen für den Datenaustausch benötigt werden. Spezielle Software kann zwischen autorisierten und nicht autorisierten Geräten genau unterscheiden. Wir haben kommerzielle Softwareprodukte verglichen und Möglichkeiten getestet, wie die **Schnittstellen** kostengünstig **unter Kontrolle** zu bringen sind.

Unser Fazit ist, dass die Administratoren mit geringem finanziellem Aufwand und **einfachen Methoden** die Nutzung externer Schnittstellen wie USB und Firewire so ausgestalten können, dass eine nicht zugelassene Nutzung ausgeschlossen wird. Viele Verwaltungen und Unternehmen in Schleswig-Holstein setzen bereits solche Lösungen ein. Zwar können wir – auch wegen der Einsatzrahmenbedingungen – keine Produktempfehlungen aussprechen, doch beraten wir gerne. In Prüfungen werden wir verstärkt darauf achten und drängen, dass keine solchen Sicherheitslecks bestehen.

Was ist zu tun?
Um die Sicherheit im Netzwerk vor unerwünschter Software wie Viren und Trojanern deutlich zu erhöhen, müssen IT-Verantwortliche die externen Schnittstellen ihrer IT-Systeme kontrollieren. Derartige Sicherheitsmaßnahmen können durch zentrale Softwarelösungen unterstützt werden.

11 Europa und Internationales

Die Einbindung des Datenschutzes aus Schleswig-Holstein nicht nur in nationale, sondern auch in internationale Zusammenhänge geht weiter voran. Datenverarbeitung ist oft ein grenzüberschreitendes Geschäft. Daher muss dies auch für den Datenschutz gelten.

Die Zusammenarbeit des ULD mit internationalen Partnern erfolgt inzwischen auf sehr vielen Ebenen. Im Rahmen der **Projektarbeit** des ULD-i ist ein internationaler Austausch schon seit Jahren Standard (Tz. 8). Die Unterstützung des ULD bei dem Aufbau von rechtlichen Grundlagen und organisatorischen Strukturen zum Datenschutz in **neuen oder künftigen EU-Mitgliedstaaten** ist nicht nur eine Einbahnstraße. Die ULD-Mitarbeiterinnen und -Mitarbeiter knüpfen internationale Kontakte und sammeln Erfahrungen, die der praktischen Arbeit im eigenen Land zugute kommt. Nachdem ein Mitarbeiter des ULD über 15 Monate zu einem Twinning-Projekt nach Vilnius in Litauen abgeordnet war, betätigt sich das ULD nun als Projektpartner bei der Implementierung des Datenschutzes auf Malta.

Positiv ist die internationale, vor allem aber die europäische Resonanz auf die vom ULD als erster Datenschutzbehörde eingeführten Instrumente des **Datenschutz-Gütesiegels** und des **Audits**. Auf der 27. Internationalen Konferenz der Datenschutzbeauftragten in Montreux/Schweiz im September 2005, auf der das ULD mit einem eigenen Vortrag vertreten war, bestand Konsens, dass diese Instrumente weiterentwickelt werden müssen. Positive Resonanz kann das ULD diesbezüglich auch bei internationalen Konzernen verzeichnen, deren Interesse selbstverständlich vor allem darin liegt, ein europaweit einheitliches Gütesiegel erwerben zu können. Dieses Interesse verfolgt auch die nationale französische Datenschutzbehörde, die im Januar 2006 mit einer vierköpfigen Delegation in Kiel zu Besuch war, um für die Einführung eines französischen Gütesiegels von den Erfahrungen in Schleswig-Holstein zu profitieren (Tz. 9.2.6).

Eine wichtige Weiche wurde in der Europäischen Union (EU) gestellt, als die **Zuständigkeit für den Datenschutz** in der Kommission von der Generaldirektion „Binnenmarkt“ zur Generaldirektion „Freiheit, Justiz und Sicherheit“ wechselte. Damit wurde einerseits die bisherige Orientierung auf den grenzüberschreitenden Datenaustausch insbesondere in der Privatwirtschaft aufgegeben und zugleich der Datenschutz innerhalb der EU sowie in der staatlichen Verwaltung der EU-Mitgliedsländer in den Fokus genommen. Die Verortung des Datenschutzes unter dem Stichwort „Freiheit“ ist zweifellos zu begrüßen. Doch ist ein großes Risiko darin zu sehen, dass nunmehr Sicherheit und Datenschutz bei der EU unter einem Dach vereint sind, was die Gefahr birgt, dass Konflikte zwischen diesen Zielen nicht mehr öffentlich, sondern nur noch innerhalb der Generaldirektion ausgetragen werden und hierbei der Datenschutz unter die Räder gerät. Ob sich diese Befürchtung bewahrheitet, muss die Zukunft zeigen.

11.1 Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten

Nachdem Bestrebungen auf nationaler Ebene, Telekommunikationsverbindungsdaten für Sicherheitszwecke auf Vorrat speichern zu lassen, erfolglos geblieben sind, soll nun über die Europäische Union dieses Überwachungsinstrument rechtlich durchgesetzt werden.

Seit Jahren gibt es in Deutschland wie auch in anderen europäischen Ländern den Versuch, Telekommunikationsunternehmen zu verpflichten, die Verbindungsdaten der Nutzer nach Beendigung der Verbindung zu speichern, um hierauf im polizeilichen oder sonstigen sicherheitsbehördlichen Bedarfsfall zugreifen zu können (24. TB, Tz. 8.2; 25. TB, Tz. 8.5; 27. TB, Tz. 2.2). Bisher wurden diese Versuche vom Bundestag mit der richtigen Erwägung zurückgewiesen, dass es sich hierbei um eine **verfassungsrechtlich nicht zulässige** Vorratsdatenspeicherung handele. Die zum Verbindungsaufbau erhobenen Daten dürfen nicht allein wegen der völlig vagen Möglichkeit, sie könnten im Rahmen strafrechtlicher Ermittlungen benötigt werden, zweckentfremdet und langfristig vorgehalten werden. Damit würde die gesamte Bevölkerung unter einen Generalverdacht gestellt.

Die Diskussion wird nicht nur in Deutschland geführt, sondern in allen Mitgliedstaaten der EU. Einige von diesen haben nationale Regelungen erlassen, die Telekommunikationsunternehmen zur Vorratsdatenspeicherung verpflichten. Angesichts aktueller terroristischer Anschläge wurde der öffentliche Druck erhöht, eine entsprechende europaweite Verpflichtung einzuführen. Hiergegen hatte das Europäische Parlament lange erfolgreich Widerstand geleistet. Im Berichtsjahr wurde es nun **politisch in die Zange** genommen: Es wurde einerseits mit dem Entwurf eines sehr weit gehenden Rahmenbeschlusses des Europäischen Rates konfrontiert, zu dem das Parlament praktisch kein Mitspracherecht gehabt hätte, sowie mit einem weniger weit gehenden Richtlinienvorschlag der Kommission. Dies veranlasste das Europäische Parlament, Ende 2005 mit einer großen Mehrheit dem Kommissionsvorschlag zuzustimmen, der die obligatorische Speicherung von Telekommunikationsverkehrsdaten zwischen 6 und 24 Monaten auf Vorrat vorsieht.

Von dieser Art der elektronischen Überwachung sollen **sämtliche Formen der Telekommunikation** erfasst werden – nicht nur die Nutzung des Telefons, sondern auch von Fax, Mobilfunk, SMS, E-Mail sowie selbst jede Form der Internetnutzung. Der Zugriff auf diese Daten soll den Sicherheitsbehörden eingeräumt werden.

Näheres muss der **nationale Gesetzgeber** regeln. Durch die Wahl der kürzesten Speicherungsfrist von sechs Monaten und eine Eingrenzung der Speicheranlässe kann er versuchen, den Eingriff für Verbraucher wie auch für die TK-Unternehmen so gering wie möglich zu halten. Weitere Begrenzungen lassen sich durch inhaltliche Präzisierungen sowie durch technische und verfahrensrechtliche Vorschriften erreichen. Doch sämtliche Versuche der Schadensbegrenzung können nichts an dem Umstand ändern, dass langfristig das Telekommunikationsverhalten der gesamten Bevölkerung, und damit vor allem von völlig unverdächtigen und

unschuldigen Menschen, registriert wird. Wir sind weiterhin davon überzeugt, dass dies verfassungsrechtlich unzulässig ist. Spätestens nach Umsetzung der EU-Vorgaben in nationales Recht wird es zu einer Überprüfung durch das Bundesverfassungsgericht kommen. Entsprechende Klagen wurden schon angekündigt.

Wünschenswert wäre jedoch, dass die Vorratsdatenspeicherung schon **auf europäischer Ebene gestoppt** werden könnte. Der Europäische Gerichtshof kann feststellen, dass der Richtlinienbeschluss mit den Grundrechten auf Telekommunikationsfreiheit und Datenschutz, die auch auf EU-Ebene gelten, nicht vereinbar ist. Eine noch wirtschaftlichere Lösung bestünde darin, dass aufgrund der öffentlichen Debatte das EU-Parlament veranlasst würde, sich der Tragweite seiner Entscheidung bewusst zu werden und seine Entscheidung zurückzunehmen. Der Landtag Schleswig-Holstein hat diese Debatte schon aufgenommen.

Was ist zu tun?
Die Entscheidung zur Vorratsdatenspeicherung stellt eine Richtungsentscheidung für eine überwachte europäische Informationsgesellschaft dar. Auf allen Ebenen sollte versucht werden, diese aus Freiheitssicht folgenreiche Entscheidung rückgängig zu machen.

11.2 Grundsatz der Verfügbarkeit contra Zweckbindung

In einem Rahmenbeschluss will der Europäische Rat erreichen, dass im Grundsatz sämtliche Informationen aus der Strafverfolgung den Ermittlungsbehörden der anderen EU-Mitgliedstaaten zur Verfügung stehen. Dies steht im Widerspruch zu den Datenschutzgrundsätzen der Zweckbindung und der Verhältnismäßigkeit.

Es geht nicht nur um die Bekämpfung des Terrorismus. In jüngster Zeit sind auch schreckliche Sexualstraftaten und schwer wiegende Wirtschaftsdelikte bekannt geworden, wo Straftäter unbehelligt in einem EU-Mitgliedstaat weiter ihr Unwesen treiben konnten, obwohl über diese in einem anderen EU-Mitgliedstaat schon beachtliche Polizeierkenntnisse vorhanden waren, die aber den nun ermittelnden Strafverfolgern nicht verfügbar waren. Es ist aus polizeilicher Sicht daher sehr wohl verständlich, dass diese umfassend über die Erkenntnisse aus anderen Mitgliedstaaten informiert sein wollen. Diesem Bedürfnis versucht nun der Vorschlag für einen Rahmenbeschluss des Europäischen Rates gerecht zu werden. Darin werden die Mitgliedstaaten verpflichtet, gleichwertigen Strafverfolgungsbehörden und Europol die Daten zur Verfügung zu stellen, „die diese zur Erfüllung ihrer gesetzlichen Aufgaben im Hinblick auf die Verhütung, Aufdeckung und Untersuchung von Straftaten benötigen“. Hierfür soll der gegenseitige **Online-Zugang zu Strafverfolgungsdateien** eröffnet werden. Zugegriffen werden soll zunächst auf folgende Daten: DNA-Profile, Fingerabdrücke, Kfz-Halterdaten, Telefonbestands- und Verbindungsdaten sowie Identifizierungs- und Personenstandsdaten. Soweit die online angebundenen Verfahren Indexdateien sind, sollen auch die Dokumente beschafft werden können, auf die hingewiesen wird.

Gegen eine intensivierte polizeiliche Zusammenarbeit wäre nichts einzuwenden, wenn zugleich auch die nötigen **rechtsstaatlichen Sicherungen** vorgesehen wären. Da es sich bei Strafverfolgungsdaten oft um Verdachtsdaten und um ungesicherte Erkenntnisse handelt und selbst Zeugen, Hinweisgeber oder Kontaktpersonen betroffen sein können, muss gewährleistet werden, dass über die Datenübermittlungen den betroffenen Menschen keine unangemessenen Nachteile entstehen. Derartige Sicherungen finden sich aber in dem vorliegenden Entwurf nicht. Für den Bereich der Strafverfolgung gibt es in der EU bisher keinerlei verbindliche Festlegungen zum Datenschutz. Zurückgegriffen wird bisher auf eine unverbindliche Empfehlung des Europarates aus dem Jahr 1987 zum Datenschutz bei der Polizei.

Um dieses Manko zu beheben, hat die EU-Kommission den Entwurf eines weiteren Ratsrahmenbeschlusses vorgelegt, der den **Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit** in Strafsachen gewährleisten soll. Der vorliegende Text ist aber nicht geeignet, die Betroffenenbelange zu schützen. Er ergeht sich wortreich in allgemeinen Grundsätzen, um schließlich jede Datenverarbeitung zu erlauben, die nach nationalem Recht zugelassen wird und die „zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten oder zur Abwehr einer Bedrohung der öffentlichen Sicherheit oder einer Person erforderlich“ ist, wenn keine „Interessen oder Grundrechte der betroffenen Person“ überwiegen. Durch diese Abwägungsklausel ist letztendlich immer den beteiligten Strafverfolgungsbehörden die Bestimmung überlassen, unter welchen Voraussetzungen sich die Betroffeneninteressen den eigenen Interessen unterordnen müssen. Diese Festlegung ist aber Aufgabe des Gesetzgebers.

Der Entwurf des Rahmenbeschlusses nimmt keine Unterscheidung zwischen Strafverfolgung und Gefahrenabwehr vor. Jedes Bagatelldelikt kann den Austausch und die Nutzung von Daten legitimieren, selbst wenn dieses Delikt in einem der beteiligten Staaten nicht strafbar ist. Zwar wird zwischen verschiedenen Rollen der Betroffenen differenziert (z. B. Täter, Verdächtiger, Opfer, Hinweisgeber, Sonstiger), doch werden hieraus keinerlei materiellrechtliche Konsequenzen gezogen. Die Anwendbarkeit für Daten aus Akten wird ausgeschlossen. **So** lässt sich der Datenschutz im Bereich Justiz und Inneres der EU **nicht** gewährleisten!

Was ist zu tun?
Bevor umfassende Datenzugriffe zwischen den Strafverfolgern in der EU erlaubt werden, muss ein angemessener Datenschutzstandard bei allen Beteiligten festgeschrieben werden. Der geplante Rahmenbeschluss ist hierfür bisher nicht geeignet und muss grundlegend überarbeitet werden.

11.3 Das zweite Schengen: Der Vertrag von Prüm

Die Strafverfolger wollen nicht so lange warten, bis der Grundsatz der Verfügbarkeit EU-weit durchgesetzt ist. Deshalb preschen sie im Vertrag von Prüm außerhalb des institutionellen Rahmens der EU nach vorne.

Das **Europa der verschiedenen Geschwindigkeiten** ist im Bereich Inneres und Justiz der EU eine lang geübte Praxis. Schon der Vertrag von Schengen wurde zuerst als völkerrechtlicher Vertrag einiger EU-Staaten abgeschlossen, bevor er zum „Acquis" – also zum Rechtsbestand der EU – erklärt wurde. Deutschland, Spanien, Frankreich, Luxemburg, Holland, Österreich und Belgien exerzieren dieses Verfahren – an sämtlichen EU-Institutionen formell vorbei – erneut beim im Mai 2005 unterzeichneten Vertrag von Prüm.

In diesem Vertrag verpflichten sich die Staaten, **gegenseitigen Zugriff** auf die nationalen DNA-Datenbanken, die Fingerabdrucksammlungen sowie die Kfz-Halter- und Fahrzeugregister zu ermöglichen. Weitere Kooperationen mit Personenbezug werden vereinbart, z. B. bei Großereignissen der Informationsaustausch einschließlich der Übermittlung von schwarzen Listen.

Hinsichtlich des **Datenschutzes** werden keine zeitgemäßen Standards und keine präzisen Vorgaben festgelegt. Vielmehr versichern sich die Vertragsstaaten per Unterschrift, dass die Voraussetzungen für die Wahrung des Schutzes personenbezogener Daten bestünden oder zumindest hergestellt würden. Dieses gegenseitige Vertrauen wird leider weder durch Kontrollen noch durch sonstige institutionelle Vorkehrungen abgesichert.

Was ist zu tun?
Der Vertrag von Prüm verfolgt ein berechtigtes Informationsanliegen der Strafverfolgungsbehörden. Die legitimen Datenschutzinteressen der Betroffenen kommen dabei aber zu kurz. Eine Unterzeichnung durch den deutschen Gesetzgeber darf erst erfolgen, nachdem diesbezüglich nachgebessert wurde.

11.4 Der Energieendverbraucher im Visier der Kommission

Energieversorgungsunternehmen wurden europaweit aufgefordert, die Daten von sämtlichen Dauerkunden an die Europäische Kommission zu melden. Sinn und Zweck dieser Aktion sind nicht erkennbar.

Die Europäische Union (EU) ist darauf erpicht, das Image des bürokratischen Molochs abzulegen und den Eindruck zu vermitteln, im Interesse der Bürgerinnen und Bürger zu handeln. Dieses Bestreben wird aber immer wieder durch EU-Institutionen selbst konterkariert. Ein kommunales Energieversorgungsunternehmen wandte sich Hilfe suchend an uns: Mit der Erklärung, es solle eine „Untersuchung des Elektrizitätssektors" erfolgen, wurde es von der Europäischen Kommission aufgefordert, innerhalb von einem Monat in einer elektronischen Datei sämtliche „langfristigen Lieferverträge" aufzulisten, die zum Stichtag 1. April 2005 bestan-

den. Dass es sich nicht um einen Aprilscherz handelte, war daran zu erkennen, dass im Fall der Weigerung Geldbußen in Höhe von 1 % des im vorausgegangenen Geschäftsjahres erzielten Gesamtumsatzes bzw. Zwangsgelder bis zu 5 % des Tagesumsatzes pro Tag Verzug angedroht wurden. Mitgeteilt werden sollten nicht nur die Angaben über Großverbraucher, sondern über **sämtliche Endverbraucher** bis hin zum Einpersonenhaushalt unter genauer Benennung von Namen, Adresse und Vertragsbedingungen. Die Kommission behielt sich ausdrücklich vor, „Dritten Einsicht in die Kommissionsakten einschließlich ihrer Unterlagen zu gewähren".

Die Kommission berief sich auf eine Verordnung, die tatsächlich derartige Berichtspflichten vorsieht. Dieser Verordnung ist aber nicht zu entnehmen, was der Zweck dieser personenbezogenen Mammuterhebung ist. Die Kommission scheint sich keine Gedanken zum **Schutz personenbezogener Daten** der Endverbraucher gemacht zu haben. Mit der Zusammenstellung sämtlicher Auskünfte der Energieunternehmen erhält die Kommission eine umfassende Datenbank über sämtliche Elektrizität abnehmenden Haushalte in der EU.

Umgehend baten wir den Europäischen Datenschutzbeauftragten, in dieser Angelegenheit tätig zu werden. Die Datenerhebung – egal für welchen Zweck – bewerteten wir als unverhältnismäßig, was wir auch dem Energieunternehmen mitteilten. Das Recht auf Datenschutz ist in der EU im Grundsatz ebenso gewährleistet wie in Deutschland. Angesichts der immensen Strafandrohung sahen wir uns aber daran gehindert, dem Energieunternehmen zu empfehlen, die geforderten **Daten zu verweigern**. Der Europäische Datenschutzbeauftragte teilte zwar im Grunde unsere Bedenken, doch auch nach mehr als einem halben Jahr konnte er weder uns noch dem Unternehmen eine abschließende rechtliche Bewertung zur Verfügung stellen.

Was ist zu tun?
So wichtig Markttransparenz für die Kommission sein mag: Hierbei dürfen die datenschutzrechtlichen Belange der EU-Bürgerinnen und -Bürger nicht unter den Tisch gewischt werden.

12 Informationsfreiheitsgesetz

12.1 Die geplante Novelle des IFG-SH

Auf Landesebene soll wegen der Notwendigkeit der Umsetzung der Europäischen Umweltinformationsrichtlinie eine Ausweitung des Informationsfreiheitsgesetzes auf Umweltinformationen erfolgen. Statt einer transparenzfreundlichen Novellierung droht zugleich in anderen Bereichen eine Beschneidung der Informationsansprüche der Bürgerinnen und Bürger.

Ende 2004 hatte die SSW-Landtagsgruppe einen Entwurf zur Novellierung des Informationsfreiheitsgesetzes (IFG-SH) vorgelegt, um Unklarheiten aus der Gesetzesanwendung zu beheben und den Anwendungsbereich des Gesetzes auszuweiten. Zugleich sollte das **europarechtlich geforderte Umweltinformationsrecht** in das IFG-SH integriert werden. Vonseiten der Landesregierung war zunächst für Umweltinformationen ein eigenes Gesetz geplant. Das Ende der Legislaturperiode im Februar 2005 stand jedoch einer Einigung über konkrete Formulierungen des Gesetzentwurfes entgegen.

Im Mai 2005 legte die SSW-Landtagsgruppe erneut ihren Vorschlag vor. Neben der Einbeziehung des Umweltinformationsrechts stellt dieser Entwurf klar, dass **privatrechtliches Handeln** von Behörden unter den Anwendungsbereich des IFG-SH fällt. Zugleich sieht der Entwurf eine gewisse Ausweitung des Anwendungsbereiches auf natürliche oder juristische Personen des Privatrechts vor. Diese Änderungen verstehen sich als Antwort auf die Privatisierung bisheriger öffentlicher Aufgaben und werden vom ULD unterstützt.

Auch die **Landesregierung** will eine Novellierung des gesamten Rechtsbereiches – Umweltinformationsgesetz und Informationsfreiheitsgesetz – vornehmen. Der von ihr im Januar 2006 präsentierte Gesetzentwurf sieht aber **keine inhaltliche Integration** der Umweltinformationen in das IFG-SH, sondern eine strikte Trennung der beiden Rechtsgebiete vor. Gleichzeitig wird der Zugang zu den allgemeinen Informationen der Verwaltung **erheblich eingeschränkt**. Diese Änderungsvorschläge sind vor dem Hintergrund der positiven Erfahrungen mit dem geltenden IFG-SH und der bundesweiten Tendenz zu mehr Transparenz nicht nachvollziehbar.

Viele Punkte des Entwurfes der Landesregierung sind für uns unverständlich bzw. stark kritikwürdig:

Der Gesetzentwurf **unterscheidet** durchgehend zwischen Umweltinformationen und allgemeinen Informationen der Verwaltung. Das angekündigte Ziel der Vereinheitlichung des Rechtsbereichs „Informationsfreiheit“ wird aufgegeben. Es stellt sich die Frage, warum das IFG-SH und das UIG (Umweltinformationsgesetz) überhaupt zusammengefasst werden sollen. Die Umsetzung der Umweltinformationsrichtlinie auf Landesebene darf nicht zum Anlass genommen werden, Grundprinzipien des IFG-SH, die sich in der Praxis bewährt haben, grundlos zu streichen. Der Zugang zu allgemeinen Informationen der Verwaltung soll stark eingeschränkt werden:

- Das **privatrechtliche Handeln** der Behörden soll nicht mehr vom Anwendungsbereich des Gesetzes umfasst sein. Damit würde ein großer Bereich herausfallen, der von besonderem Interesse für die Bürger ist. Soll ein Informationsfreiheitsgesetz ernsthaft die Transparenz und Akzeptanz der Verwaltung erhöhen und die Mitgestaltungsmöglichkeiten der Bürger verbessern, darf nicht nur das klassische Verwaltungshandeln dem Informationszugang unterliegen. Gerade im Bereich der Mittelverwendung der öffentlichen Hand besteht ein gesteigertes Bedürfnis nach Transparenz. Eine Herausnahme des privatrechtlichen Handelns aus dem Anwendungsbereich stünde im Widerspruch zu der Rechtslage sämtlicher sonstiger Informationsfreiheitsgesetze und allen aktuellen Bestrebungen bei der Korruptionsbekämpfung.
- Natürliche und juristische Personen, denen öffentliche Aufgaben übertragen sind, sollen aus dem Anwendungsbereich herausgenommen werden. Angesichts der verstärkten Übertragung von öffentlichen Aufgaben auf Private würde ein bedeutender Bereich „informationsfrei“ gestellt werden. Dies ist nicht sachgerecht, da eine Behörde die Wahl hat, ihre Aufgaben in öffentlicher oder privatrechtlicher Handlungsform zu erledigen. Wählt sie letztere Möglichkeit und betraut eine nicht beliehene Person des Privatrechts mit der Erfüllung einer öffentlichen Aufgabe, sollten auch die an den Dritten übergebenen Informationen zugangspflichtig sein. Eine solche „Flucht ins Private“ steht im Widerspruch zu den Grundsätzen des Verwaltungsprivatrechts.
- Geschäfts- und Betriebsgeheimnisse sollen per se geheimhaltungspflichtig sein. Die geltende Klausel, die eine Abwägung zwischen dem Geheimhaltungsinteresse des Unternehmens und dem Offenbarungsinteresse der Allgemeinheit vorsieht, soll gestrichen werden. Vor dem Hintergrund der Debatte um eine effektivere Korruptionsbekämpfung, der die Informationsfreiheitsgesetze auch dienen sollen, ist eine pauschale Ablehnung bei Vorliegen eines Geschäftsgeheimnisses nicht haltbar. Ein überwiegendes Interesse der Allgemeinheit an der Offenbarung solcher Informationen ist in der Vergangenheit mehrfach – auch gerichtlich – festgestellt worden (z. B. Tz. 12.2.1). Gründe für eine Änderung der geltenden Regelung gibt es nicht.

Statt wegen der insgesamt guten Erfahrungen mit dem IFG-SH dieses umsichtig weiterzuentwickeln, versteckt sich hinter den bürokratisch daherkommenden Vorschlägen der Landesregierung ein massiver Rückbau der Informationsansprüche.

Wir haben den Verantwortlichen signalisiert, dass eine solche Initiative aus unserer Sicht nicht sachdienlich ist. Unsere vollständige Stellungnahme zu dem Gesetzentwurf der Landesregierung finden Sie unter

www.datenschutzzentrum.de/informationsfreiheit/stellungnahme-060216.htm

Was ist zu tun?
Die geplante Novellierung des IFG-SH sollte zu einem vernünftigen weiteren Ausbau der Informationsansprüche der Menschen führen und darf nicht zu deren Abbau genutzt werden.

12.2 Einzelfragen zum Informationszugang

12.2.1 Einsichtnahme in Protokolle von Aufsichtsratssitzungen einer GmbH

Gemeinden übertragen zunehmend ihre Aufgaben auf private Unternehmen. An den zumeist neu gegründeten Unternehmen sind die Kommunen beteiligt und üben durch die Entsendung des Bürgermeisters oder von Gemeindevertretern in das Kontrollorgan den gesetzlich vorgeschriebenen Einfluss aus. Die Informationen, die die Kommune im Rahmen ihrer Beteiligung erhält, sind für viele von großem Interesse.

Stadtverordnete hatten erfahren, dass bei einem in ihrer Stadt als GmbH betriebenen Freizeitbad hohe Defizite zu erwarten wären. Dies sollte die Erhöhung der städtischen Zuschüsse im Haushaltsplan zur Folge haben. Die Stadtverordneten wollten daher Einblick in die Protokolle und Niederschriften der Sitzungen des Aufsichtsrates des Freizeitbades nehmen. Dem Aufsichtsrat gehören der Bürgermeister sowie zwei weitere Stadtverordnete an. Der Bürgermeister lehnte diesen Antrag ab, weil in den Protokollen **Betriebs- und Geschäftsgeheimnisse** enthalten seien. Das Interesse der Allgemeinheit an der Offenbarung müsse zurückstehen. Eine Schwärzung der Betriebsinterna sei ausgeschlossen, da die Sitzungen pauschal geheimhaltungsbedürftig seien.

Eine solche **pauschale Ablehnung** erlaubt das IFG-SH nicht. Nicht alle Geschäftsgeheimnisse sind geheim zu halten. Es gibt keinen Grundsatz, wonach das Interesse des Unternehmens an der Geheimhaltung im Regelfall höher zu bewerten ist als das Offenbarungsinteresse der Allgemeinheit. Es ist vielmehr eine **Abwägung** vorzunehmen. Für die Geheimhaltung sprechen die Sicherung von Vermögenswerten und Wettbewerbsvorteilen. Relevant ist das Ausmaß des wirtschaftlichen Schadens, der entstünde, wenn ein Geheimnis preisgegeben würde. Dem steht das Informationsinteresse der Allgemeinheit entgegen, wie öffentliche Mittel verwendet werden. Die Stadt ist verpflichtet, möglichst sparsam zu wirtschaften.

Bei einer Durchsicht der Protokolle stellten wir fest, dass diese nur zum Teil Betriebs- und Geschäftsgeheimnisse enthalten und eine Abtrennung möglich ist. Die Stadt hat daraufhin den Stadtverordneten die Protokolle zur Verfügung gestellt. Passagen mit Betriebsgeheimnissen wurden geschwärzt.

Was ist zu tun?
Eine pauschale Ablehnung des Informationsersuchens aufgrund des Vorliegens von Geschäfts- und Betriebsgeheimnissen ist nicht zulässig. Erforderlich ist immer eine auf den Einzelfall bezogene Abwägung zwischen dem Geheimhaltungs- und dem Offenbarungsinteresse.

12.2.2 Informationszugang im Besteuerungsverfahren

Im Besteuerungsverfahren gelten die Vorschriften der Abgabenordnung. Die Finanzämter haben danach das Steuergeheimnis zu wahren. Die Finanzverwaltung meint, dass das IFG-SH im Besteuerungsverfahren nicht anwendbar sei.

Ein Petent hatte eine Zulage nach dem Eigenheimzulagengesetz beantragt und erhalten. Jetzt wollte er von seiner Finanzbehörde Auskunft über weitere Einzelfälle aus dem gleichen Zeitraum erhalten. Das Finanzamt verweigerte dies mit der Begründung, das IFG-SH sei im Besteuerungsverfahren nicht anwendbar. Die bundesrechtlichen Vorschriften der Abgabenordnung (AO) würden den landesrechtlichen Vorschriften des IFG-SH vorgehen: „**Bundesrecht bricht Landesrecht**“. Das Steuergeheimnis verbiete die Offenbarung personenbezogener Daten und Geschäftsgeheimnisse, die das Finanzamt von den Steuerpflichtigen zur Festsetzung der Steuer erhält.

Die AO enthält unbestreitbar besondere Vorschriften zum Schutz des Steuergeheimnisses und zur Anhörung des betroffenen Steuerpflichtigen. Dies schließt aber die Anwendung des IFG-SH nicht vollständig aus. Die Kollisionsnorm des Grundgesetzes kommt nur zur Anwendung, wenn die Vorschriften identische Sachverhalte mit unterschiedlichen Rechtsfolgen belegen. Die AO und das IFG-SH haben jedoch unterschiedliche Zielrichtungen und Adressaten. Die AO regelt ausschließlich die Beteiligung des betroffenen Steuerpflichtigen und garantiert dessen rechtliches Gehör. Das IFG-SH hingegen gewährt den Bürgerinnen und Bürgern generell einen individuellen Informationszugang und dient der Erhöhung der Transparenz in der Verwaltung. Daher kommen die Vorschriften des IFG-SH und der AO **nebeneinander zur Anwendung**. Eine Kollision der Vorschriften ist schon dadurch ausgeschlossen, dass das IFG-SH Akteneinsicht grundsätzlich nur unter Wahrung der Belange Dritter gewährt. Personenbezogene Daten Dritter dürfen auch nach dem IFG-SH nicht herausgegeben werden, sodass das Steuergeheimnis Dritter nicht gefährdet ist.

Das Finanzamt weigerte sich dennoch, dem Petenten Auskunft zu erteilen. Dies haben wir schon wegen der Begründung der Ablehnung **beanstandet**. Das Innenministerium Schleswig-Holstein als Kommunalaufsichtsbehörde hat sich allerdings der Argumentation des Finanzamtes angeschlossen. Der Betroffene kann daher seinen Anspruch nur noch im Wege eines Klageverfahrens geltend machen.

Was ist zu tun?
Die Finanzverwaltung muss akzeptieren, dass für sie in Sachen Informationsfreiheit kein Sonderrecht gilt.

12.2.3 Bauakte des Nachbarn

Informationsersuchen betreffen oft die nachbarrechtlichen Verhältnisse von Bürgern, insbesondere Streitigkeiten aus dem Bereich des Baurechts. Es ist dann zu klären, ob der Anfragende das Recht hat, personenbezogene Daten seines Nachbarn einzusehen.

Ein Petent wollte die Baugenehmigungsakte eines Hafens einsehen, der sich in unmittelbarer Nähe seines Grundstückes befand. Er befürchtete nach der geplanten Erweiterung des Hafens eine erhöhte **Lärmbelästigung und stärkeres Verkehrsaufkommen**. Die Baugenehmigungsakte enthält personenbezogene Daten des Adressaten, die nach dem IFG-SH nur im Ausnahmefall offenbart werden dürfen.

Ein solcher Sonderfall liegt vor, wenn der Antragsteller ein überwiegendes **rechtliches Interesse** an der Kenntnis der Daten hat. Dies ist der Fall, wenn der Antragsteller einen Anspruch verfolgt, der sich aus einer konkreten Rechtsbeziehung zu dem Betroffenen ergibt. Dabei kann es sich auch um Ansprüche handeln, die sich gegen eine öffentliche Stelle richten. Wendet sich ein Bürger gegen eine dem Nachbarn erteilte Baugenehmigung, liegen diese Voraussetzungen zweifelsfrei vor. Eine rechtswidrig erteilte Baugenehmigung und eine nicht der Baugenehmigung entsprechende Bauweise kann den Nachbarn in seinen Rechten verletzen. Bei einem Rechtsverstoß hätte er einen Anspruch gegen die Behörde auf Überprüfung und gegebenenfalls Aufhebung der Baugenehmigung. Ein solches rechtliches Interesse bestand hier, weil durch die Erweiterung des Hafenbetriebes mit unter Umständen unzumutbaren Belästigungen zu rechnen war. Der Petent hat letztlich Einsicht in die Bauakten des Hafens nehmen können.

12.2.4 Mitglieder von Bürgerinitiativen sind auch Privatpersonen

Menschen organisieren sich in Bürgerinitiativen, um gemeinsam auf die öffentliche Meinungsbildung Einfluss zu nehmen. Hierfür benötigen die Initiativen oft Verwaltungsinformationen. In diesem Fall können sich die Mitglieder auf das Informationsfreiheitsgesetz berufen.

Eine Gemeinde plante aufgrund verschiedener Bauprojekte Änderungen im Bebauungsplan. Ein Planungsbüro stellte hierzu seine Vorschläge in einer öffentlichen Sitzung des Planungsausschusses vor. Ein Rechtsgutachten zu dem Bebau-

ungsplan wurde erstellt. Da die Bauvorhaben in der Gemeinde auf Widerstand stießen, wurde eine Bürgerinitiative gebildet. Diese Initiative bat um Einsicht in die vom Planungsbüro vorgelegten Folien. Der Antrag wurde mit dem Argument abgelehnt, Bürgerinitiativen seien keine **juristischen Personen des Privatrechts** und nicht anspruchsberechtigt im Sinne des IFG-SH.

Diese Auslegung ist mit den **Zielen des Gesetzes** nicht vereinbar. Jede natürliche oder juristische Person des Privatrechts hat Anspruch auf Zugang zu den Behördeninformationen. Auch Bürgerinitiativen gehören dazu, auch wenn sie nicht ausdrücklich aufgeführt sind. Die Formulierung des Gesetzes zielt nicht auf eine Begrenzung des Kreises der Informationsberechtigten ab. Sinn und Zweck ist es vielmehr, gerade solchen Personenvereinigungen die nötigen Informationen zu verschaffen. Jedes einzelne Verbandsmitglied selbst ist anspruchsberechtigt, egal ob es als Mitglied oder als Privatperson handelt. Der Empfänger kann die erhaltenen Informationen zudem an die Initiative weitergeben. Es hat also keinen Sinn, Bürgerinitiativen die Berufung auf das IFG-SH zu verwehren.

Der Antrag wurde nicht nur von der Bürgerinitiative gestellt, sondern zugleich auch vom **Sprecher der Initiative** als Privatperson. Auch dieses Auskunftsersuchen ist abgelehnt worden, u. a. mit der Begründung, ein Anspruch bestünde nicht, da der Antrag von einer Person gestellt worden sei, die erkennbar für eine nicht anspruchsberechtigte Vereinigung, also die Bürgerinitiative, handelt. Die Gemeinde musste darauf hingewiesen werden, dass die Mitgliedschaft eines Antragstellers wie auch jede Motivation bei der Anfrage unwesentlich ist. Die Behörde ist nicht berechtigt, nach Mitgliedschaften und Beweggründen zu fragen.

Was ist zu tun?
Bürgerinitiativen und sonstige nicht rechtsfähige Vereinigungen sind bei Anträgen auf Informationszugang ebenso zu behandeln wie natürliche oder juristische Personen.

12.2.5 Protokolle der Denkmalschutzbehörde

Sind die Namen der ehrenamtlichen Mitarbeiter des Denkmalschutzrates personenbezogene Daten, die nicht offenbart werden dürfen? Dies sollte eigentlich kein Anlass zum Streit sein!

Ein Petent bat um Mitteilung der Namen der ehrenamtlich tätigen Mitglieder des Denkmalschutzrates. Zugleich wollte er die Protokolle der Sitzungen des Denkmalschutzrates einsehen. Beide Anträge wurden abgelehnt mit dem Hinweis, die **Namen** der Mitglieder seien personenbezogene Daten, die nicht offenbart werden dürfen.

Das IFG-SH verbietet grundsätzlich die Offenbarung **personenbezogener Daten**. Auch die Daten von Funktionsträgern, Gremienangehörigen und Beschäftigten öffentlicher Stellen sind personenbezogene Daten. Dies verhindert aber nicht die Veröffentlichung der Namen. Eine öffentliche Stelle ist nur über die Mitarbeite-

rinnen und Mitarbeiter als natürliche Personen handlungsfähig. Deren Namensnennung ist im Rahmen der Erforderlichkeit für die Aufgabenerfüllung zulässig. Bei der **Mitwirkung von Amtsträgern** an Verwaltungsvorgängen dürfen Name, Funktionsnummer bzw. Laufzeichen und Daten zur dienstlichen Erreichbarkeit genannt werden (Tz. 4.1.6). Dies gilt auch, wenn Mitarbeiter ehrenamtlich in der Verwaltung arbeiten, weil sie dann als Amtsträger tätig sind. Wir haben daher die Offenlegung der Namen des Denkmalschutzrates gefordert. Das Gleiche gilt für die Mitarbeiterdaten in den Protokollen. Die Protokolle können verwehrt werden, wenn diese neben den oben genannten Mitarbeiterdaten andere personenbezogene Daten enthalten. Dann ist zu prüfen, ob diese ausgesondert bzw. geschwärzt werden können oder die Einwilligung des Betroffenen eingeholt werden kann.

Erst nach unserer **förmlichen Beanstandung** hat die Denkmalschutzbehörde die Namen der Mitglieder des Denkmalschutzrates offenbart. Sie muss nun prüfen, inwieweit in den Protokollen andere schützenswerte Daten enthalten sind und ob diese offen gelegt werden können.

12.2.6 Schutzbedarf bei Mitarbeiterdaten einer Behörde

Immer wieder wird Bürgerinnen und Bürgern bei der Ablehnung von Informationsgesuchen vorgetragen, die erbetenen Unterlagen enthielten Mitarbeiterdaten. Diese sind aber nicht in jedem Fall vor Offenbarung geschützt.

Bei der Offenlegung von Mitarbeiterdaten kommt es darauf an, welche Daten betroffen sind und in welchem Zusammenhang diese stehen. Nach dem Informationsfreiheitsgesetz ist die Offenbarung von personenbezogenen Daten grundsätzlich unzulässig. Auch die Daten von Mitarbeitern einer Behörde gehören hierzu. Schon nach dem Datenschutzrecht ist jedoch eine Offenbarung von Mitarbeiterdaten erlaubt, soweit dies im Rahmen der **Durchführung des allgemeinen Dienstbetriebes** erforderlich bzw. geboten ist. Da eine öffentliche Stelle als Teil einer juristischen Person nur über ihre Mitarbeiterinnen und Mitarbeiter als natürliche Person handlungsfähig ist, ist die Bekanntgabe bestimmter Daten eines Amtsträgers erlaubt. Dies gilt, soweit die Daten zur rechtmäßigen Erfüllung der durch Rechtsvorschrift zugewiesenen Aufgaben der öffentlichen Stelle erforderlich sind. Wird eine Behörde mit Außenwirkung tätig, ist es nötig, den Namen des Beschäftigten, die postalische Adresse der Dienststelle, die Telefonnummer und eventuell die E-Mail-Adresse, unter der der unterzeichnende Mitarbeiter zu erreichen ist, sowie die Faxnummer der Dienststelle an die Öffentlichkeit zu geben. Nur so kann die Ansprechbarkeit der Behörde für die Bürgerinnen und Bürger gesichert werden (Tz. 4.1.6).

12.2.7 Rechtsanwaltskammer

Der Wunsch nach Einsichtnahme in Unterlagen der Rechtsanwaltskammer wurde pauschal mit der Begründung abgelehnt, dem Informationszugang stünden spezielle Regelungen in der Rechtsanwaltsordnung entgegen. Dies trifft nicht zu.

Die Bundesrechtsanwaltsordnung sieht bestimmte Einsichtsrechte für die Beteiligten an einem Beschwerdeverfahren vor der Rechtsanwaltskammer vor. Dieses spezielle Informationszugangsrecht für Verfahrensbeteiligte schließt die Anwendung des IFG-SH nicht aus. Ob eine **Konkurrenz von Regelungen** besteht, hängt von Sinn und Zweck der Vorschriften ab. Das IFG-SH tritt nur dann hinter anderen spezialgesetzlich geregelten Informationsrechten zurück und wird verdrängt, wenn die konkurrierenden Vorschriften identische Regelungsmaterien, d. h. die gleichen Ziele und Adressaten, haben. Die spezielle Zugangsregelung für Verfahrensbeteiligte der Bundesrechtsanwaltsordnung regelt lediglich Einsichtsrechte für Personen, die an dem Beschwerdeverfahren vor der Rechtsanwaltskammer beteiligt sind. Diese Vorschrift richtet sich damit an andere Adressaten und hat eine andere Zielrichtung als das IFG-SH.

Die Tatsache, dass die Verbandsmitglieder der Rechtsanwaltskammer nach der Bundesrechtsanwaltsordnung zur **Verschwiegenheit** verpflichtet sind, steht einer Anwendung des IFG-SH nicht entgegen. Auch nach dem IFG-SH ist es untersagt, personenbezogene Daten und Amtsgeheimnisse unbefugt zu offenbaren.

Was ist zu tun?
Das IFG zwingt die Verwaltung zu mehr Transparenz, auch die öffentlich-rechtlich organisierten Kammern. Dies sollte nicht nur als lästige Pflicht, sondern als Chance zu mehr Offenheit und Serviceorientierung verstanden werden.

12.2.8 Informationszugang zu Unterlagen der ARGEn

Seit Anfang 2005 kümmern sich Kommunen und die Bundesagentur für Arbeit in so genannten Arbeitsgemeinschaften gemeinsam um das Arbeitslosengeld II. Das Informationsinteresse der Bürgerinnen und Bürger hierzu ist sehr groß. Anträge nach dem IFG-SH werden jedoch oft abgelehnt.

Die Arbeitsgemeinschaften (ARGEn) sind ein Zusammenschluss von den Kommunen und der Bundesagentur für Arbeit. Bei diesen **Mischbehörden** stellt sich die Frage, ob sie unter den Anwendungsbereich des IFG-SH fallen, das von Behörden nach dem Landesverwaltungsgesetz spricht. Für die Anwendbarkeit spricht die Gesetzesbegründung, wonach der Geltungsbereich möglichst umfassend sein soll und nur Bundesbehörden ausgenommen sein sollen. Die ARGEn sind fast ausschließlich regional tätig. Es wird bei der Aufgabenerfüllung nicht zwischen den Aufgaben der Kommune und der Bundesagentur unterschieden. Die Mitarbeiter erfüllen jeweils die Aufgaben aus den ursprünglich getrennten Bereichen Sozialhilfe und Arbeitsverwaltung. Auch nach außen tritt die ARGE als

eigenständige Rechtspersönlichkeit auf und erlässt Verwaltungsakte und Widerspruchsbescheide in eigenem Namen und eigener Kompetenz. Eine Beschränkung des Informationszugangsrechts widerspräche dem gesetzlichen Anliegen und jeder praktischen Vernunft. Dies gilt erst recht seit Anfang 2006 und der Geltung des Informationsfreiheitsgesetzes des Bundes für die Bundesagentur.

Was ist zu tun?
Den Bürgern ist Einsicht in die Unterlagen der ARGEn zu gewähren – natürlich unter Berücksichtigung der einschränkenden Voraussetzungen des Gesetzes.

12.3 Verabschiedung des Bundes-IFG

Endlich ist das Bundesinformationsfreiheitsgesetz verabschiedet worden. Nach langem und manchmal zähem Hin und Her gibt es auch bei Bundesbehörden seit Anfang 2006 Informationsfreiheit.

Das Bundesinformationsfreiheitsgesetz (Bundes-IFG) sieht deutlich mehr Einschränkungsmöglichkeiten beim Zugang zu Verwaltungsdaten vor als das IFG-SH. Das Gesetz ist dennoch ein richtiger Schritt hin zu mehr demokratischer Transparenz. Ihm kommt **Signalwirkung** für einige Bundesländer zu, die nun die Einführung eines Landes-IFG vorantreiben. Es bleibt zu hoffen, dass diese sich dabei inhaltlich nicht am Bund, sondern an den bestehenden Landesgesetzen orientieren.

Der Schutz der öffentlichen wie der privaten Belange als **Ablehnungsgrund** sind im Bundes-IFG eindeutig zu weit gefasst. Einzelne Aufgabenbereiche der Verwaltung sollten nicht undifferenziert dem Anwendungsbereich entzogen werden. Enscheidend darf nur sein, dass durch die Bekanntgabe einer Information ein konkreter Schaden verursacht würde.

Im privaten Bereich sieht das Bundes-IFG einen absoluten Schutz von **Betriebs- und Geschäftsgeheimnissen** vor. Dies wird wegen der Unschärfe dieses Rechtsbegriffes zu vielen Konflikten und unberechtigten Auskunftsverweigerungen führen. Dem einseitig definierten Unternehmensinteresse an Geheimhaltung wird nach dem Gesetzestext der Vorrang eingeräumt. Demgegenüber enthält das IFG-SH eine Abwägungsklausel, die dem Geheimhaltungsinteresse das Interesse der Allgemeinheit an einer Offenbarung entgegenstellt. Praktisch relevant wird diese Frage in den vielen Fällen, wenn Behörden privatrechtlich tätig werden und Verträge mit privaten Unternehmen abschließen. Diese Verträge sind fast durchgängig von besonderem öffentlichen Interesse, da hier öffentliche Gelder eingesetzt werden. Die Bedingungen und geschäftlichen Details dieser Verträge sollten nicht der Allgemeinheit vorenthalten werden können.

Mit der Verabschiedung des Bundes-IFG wird jetzt auch die Bundesverwaltung transparenter. Es bleibt mit Spannung abzuwarten, wie die **Umsetzung des Bundes-IFG** erfolgt. Das Gesetz ist dokumentiert unter

www.datenschutzzentrum.de/material/recht/infofrei/ifg-bund.htm

Was ist zu tun?
Die Länder, die die Einführung eines Informationsfreiheitsgesetzes planen, sollten vorrangig auf die Regelungen und Erfahrungen der Bundesländer bei der Erstellung ihres Gesetzes zurückgreifen.

13 DATENSCHUTZAKADEMIE: Nur der Wandel ist beständig

Im zwölften Jahr ihres Bestehens bot die DATENSCHUTZAKADEMIE Schleswig-Holstein auch 2005 an den Standorten Kiel, Leck und Bordesholm in zahlreichen ein- bis viertägigen Seminaren ein preisgünstiges und qualitativ hochwertiges Fortbildungsprogramm zu vielen relevanten Datenschutzthemen.

Interessierte Bürgerinnen und Bürger, Behörden, Wirtschaftsunternehmen, Schulen ... alle können sich unter fachkundiger Anleitung **fit machen** für die Erfordernisse der Informationsgesellschaft. Behördliche Datenschutzbeauftragte werden zur Wahrnehmung ihrer verantwortungsvollen Aufgabe in schleswig-holsteinischen Dienststellen in Datenschutzrecht und -technik geschult. Datenschutzbeauftragte in der Wirtschaft erfüllen gesetzliche Anforderungen, wenn sie sich die Grundlagen von effektivem Datenschutzmanagement in ihren Betrieben aneignen.

Schulungen zum **betrieblichen Datenschutz** erfuhren im vergangenen Jahr eine verstärkte Beachtung: Drei zusätzliche Kurse mussten angeboten werden. Betrieblicher Datenschutz war auch ein gefragtes Thema bei Sonderkursen, die als Inhouse-Veranstaltungen in Absprache mit den Interessenten stattfinden. Verbände, Firmen, Behörden nutzten die Möglichkeit individueller Schulungsinhalte, um ihre Mitarbeiterinnen und Mitarbeiter in Sachen Datenschutzmanagement, Datenschutz am PC-Arbeitsplatz und anderen Fragen des Datenschutzarbeitsalltags schulen zu lassen.

In Sachen **Datensicherheit** reichen die Angebote von „Safer Surfen im Internet“ bis Firewall, von Linux bis Windows. Der Bedeutung des neuen Betriebssystems entsprechend hat die DATENSCHUTZAKADEMIE ihr Angebot um einen zweiten Sicherheitskurs („Windows 2003 Sicherheit II“) erweitert, dem 2006 der viertägige Kurs „Windows Terminal Server mit Citrix Metaframe 4.0“ folgen wird.

Leider ist die Zusammenarbeit von der DATENSCHUTZAKADEMIE und dem **Institut für Qualitätssicherung an Schulen Schleswig-Holstein** (IQSH) nahezu zum Erliegen gekommen. Dem ausgesprochen großen Bedarf der Schulen an qualifizierter Datenschutzweiterbildung (für Lehrer, Schüler, Schulleiter und Verwaltung) stehen offensichtlich keine finanziellen Mittel mehr zur Verfügung. Dies ist umso bedauerlicher, als die selbstbewusste und datenschutzgerechte Nutzung von Internet und Informationstechnik für die junge Generation von größtem Interesse wäre.

Regen Zuspruch erfahren die Angebote der DATENSCHUTZAKADEMIE hingegen bei der schleswig-holsteinischen **Wirtschaft**. Unternehmen, Verbände und Dienstleister nutzen die Fortbildungsangebote, um mit qualifizierten Mitarbeiterinnen und Mitarbeitern das gesetzlich geforderte Datenschutzmanagement zu realisieren.

Langfristig arbeitet die DATENSCHUTZAKADEMIE an der Erarbeitung eines Curriculums für den betrieblichen Datenschutz, das sowohl die notwendigen rechtlichen als auch technischen Inhalte enthält und mit einem **Datenschutzzertifikat für betriebliche Datenschützer** abschließen soll. Damit kann perspektivisch für die Absolventen eine wichtige Zusatzqualifikation in ihrer beruflichen Fortbildung geschaffen werden. In der Wirtschaft setzt sich zudem die Einsicht durch, dass ein geeignetes Datenschutzmanagement sinnvoll für den eigenen Workflow, unabdingbar für Kundenvertrauen und damit unbedingt ein Wettbewerbsvorteil ist.

Haben Sie Interesse?

Die DATENSCHUTZAKADEMIE bietet vor Ort Kurse zu Datenschutzthemen an und führt zu Themen Ihrer Wahl auch Inhouse-Veranstaltungen in Ihrer Behörde oder in Ihrem Betrieb durch, z. B. zu aktuellen Fragestellungen wie

- betrieblicher Datenschutz,
- Datenschutz in Kommunalverwaltungen,
- Datenschutz am PC-Arbeitsplatz,
- E-Government,
- Arbeitnehmerdatenschutz,
- Safer Surfen usw.

Die organisatorische Abwicklung und inhaltliche Schwerpunkte werden mit Ihnen besprochen. Voraussetzung ist die Teilnahme von mindestens 15 Personen.

Nähere Informationen unter:

Tel.: 0431/988-1281
E-Mail: akademie@datenschutzzentrum.de

- **Schulungsbetrieb 2005**

Im Jahr 2005 fanden 28 **Kurse**, Seminare und Workshops statt, in denen 401 Personen Grundlagen- und Spezialwissen zu einem breit gefächerten Spektrum von Datenschutzfragen erlangen konnten.

In insgesamt 11 **Sonderkursen** vermittelten die Referentinnen und Referenten der DATENSCHUTZAKADEMIE landesweit 300 Interessierten ihr Fachwissen. In inhaltlicher Abstimmung mit den teilnehmenden Behörden, Firmen und Verbänden wurden folgende Themen vor Ort bearbeitet:

- Schutz von Personaldaten,
- Führung von Personalakten,
- Informationsfreiheitsgesetz Schleswig-Holstein,

- betrieblicher Datenschutz in Pflegeeinrichtungen,
- Einführung in den Datenschutz für Kreisverwaltungen,
- Einführung in den Datenschutz für stationäre Einrichtungen,
- Datenschutz in ambulanten Pflegeeinrichtungen,
- allgemeines Datenschutzrecht, Sozialdatenschutzrecht in der Diakonie,
- Einführung in das Datenschutzrecht für Landtagsmitarbeiter,
- Datenschutzrecht für Personalräte.

Insgesamt absolvierten 701 Teilnehmer die Kurse der DATENSCHUTZAKADEMIE 2005. Die **Kursunterlagen**, die derzeit noch in gebundener Form mit kompaktem, didaktisch aufbereitetem Wissen aufwarten, werden im kommenden Jahr aus Gründen der Praktikabilität und besseren Aktualisierungsmöglichkeit in ansprechenden Ringordnern vorliegen.

- **Datenschutzzertifikat für Systemadministratoren**

2005 konnten – nach gründlicher Vorbereitung durch den Besuch mehrerer Kurse – sieben erfolgreiche Absolventen ihr „**Datenschutzzertifikat für Systemadministratoren**“ in Empfang nehmen. In einer fünfstündigen Prüfung stellten sie theoretisch und praktisch ihr Know-how zur datenschutz- und gesetzeskonformen EDV-Wartung unter Beweis. Dieses Schulungs- und Prüfungsangebot zielt darauf ab, Datenschutz und Datensicherheit bei den öffentlichen Stellen wie bei privaten Firmen zu verbessern. Langfristiges Ziel ist es, die vermittelten Kenntnisse zu Standardanforderungen an Systemadministratoren zu machen. In der Gesamtkonzeption des ULD, in der Datenschutz durch Technik eine zentrale Rolle spielt, sind datenschutzrechtlich zertifizierte Administratoren ein wichtiger Meilenstein.

- **Jahresprogramm 2006 der DATENSCHUTZAKADEMIE**

Veranstaltungsübersicht 2006 für die Kurse der DATENSCHUTZAKADEMIE Schleswig-Holstein			
Februar:	Windows 2003 Sicherheit I	WIN-I	28.02. - 03.03.2006
März:	Grundkurs Bundesdatenschutzgesetz Datenschutz in Unternehmen, Vereinen und Verbänden	BDSG-I	20.03.2006
	Betriebliches Datenschutzmanagement nach dem BDSG	BDSG-II	21.03.2006
	IT-Revision	ITR	22.03.2006
	Technischer Datenschutz/ Systemdatenschutz nach dem BDSG	SIB	23.03.2006
	Safer Surfen im Internet	SURF	28.03.2006
April:	Workshop für betriebliche Datenschutzbeauftragte	DWBT	19.04.2006
	Datenschutzrecht für behördliche Datenschutzbeauftragte	DR	24. - 25.04.2006

	Datenschutz im Krankenhaus	DK	25.04.2006
	Datenschutz in der Arztpraxis	AR	26.04.2006
	Datensicherheitsrecht, Prüfung und Bewertung von Sicherheitsmaßnahmen durch behördliche Datenschutzbeauftragte	DT	26. - 28.04.2006
Mai:	Windows 2003 Sicherheit II	WIN-II	16. - 19.05.2006
Juni:	Führung von Personalakten	PA	07. - 08.06.2006
	Einführung Datenschutz im Schulsekretariat	ES	19.06.2006
	Informationsfreiheitsgesetz Schleswig-Holstein	IFG	21.06.2006
	Grundkurs Bundesdatenschutzgesetz Datenschutz in Unternehmen, Vereinen und Verbänden	BDSG-I	26.06.2006
	Betriebliches Datenschutzmanagement nach dem BDSG	BDSG-II	27.06.2006
	IT-Revision	ITR	28.06.2006
	Technischer Datenschutz/ Systemdatenschutz nach dem BDSG	SIB	29.06.2006
September:	Datensicherheit und Datenschutz für SystemadministratorInnen	DS	05. - 06.09.2006
	Windows 2003 Sicherheit I	WIN-I	12. - 15.09.2006
	Datenschutzrecht für behördliche Datenschutzbeauftragte	DR	18. - 19.09.2006
	Datensicherheitsrecht, Prüfung und Bewertung von Sicherheitsmaßnahmen durch behördliche Datenschutzbeauftragte	DT	20. - 22.09.2006
	Landesdatenschutzgesetz Schleswig-Holstein	LDSG-R	20.09.2006
Oktober:	Einführung in datenschutzgerechtes Linux	LIN-I	04. - 05.10.2006
	Datenschutzgerechter Server mit Linux und Open-Source-Programmen	LIN-II	09. - 12.10.2006
	Sozialdatenschutzrecht	S	09. - 11.10.2006
	Grundkurs Bundesdatenschutzgesetz Datenschutz in Unternehmen, Vereinen und Verbänden	BDSG-I	16.10.2006
	Betriebliches Datenschutzmanagement nach dem BDSG	BDSG-II	17.10.2006
	IT-Revision	ITR	18.10.2006
	Technischer Datenschutz/ Systemdatenschutz nach dem BDSG	SIB	19.10.2006
November:	Datenschutz bei der Internetnutzung durch Schulen	L-INT	07.11.2006
	Windows 2003 Sicherheit II	WIN-II	14. - 17.11.2006
	Windows 2003 Terminal Server mit Citrix Metaframe 4.0	WIN-TS	20. - 23.11.2006
	Prüfung zum Systemadministrator mit Datenschutzzertifikat	SDZ	27. - 28.11.2006

*Sommerakademie 2006 * Sommerakademie 2006 * Sommerakademie 2006*

„Mach's gut." „Mach's besser!"

Datenschutzmanagement in Betrieb und Verwaltung:

Workflow – Datensparsamkeit – Betroffenenrechte

Datenschutzmanagement ist mehr als Datenschutz: Es optimiert die Organisationsstruktur und die Planung der Arbeitsabläufe und strukturiert den IT-Einsatz, die Entwicklung des Produktangebots und die Außendarstellung des Unternehmens bzw. der Behörde. Damit wirkt es im Ergebnis als Wettbewerbsvorteil. Audit und Gütesiegel fördern mit der Zertifizierung von IT-Verfahren und Produkten Wirtschaftlichkeit, Rechtssicherheit und Akzeptanz. Intelligente Pseudonymisierungskonzepte und Instrumente des Identitätsmanagements verbessern die Datensparsamkeit, tragen zur Risikominimierung bei und erhöhen die Effizienz der Datenverarbeitung.

28. August 2006
Kieler Schloss

Weitere Informationen zur Sommerakademie werden kontinuierlich 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 Verteiler 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

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z