Tätigkeitsbericht 2007

des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

Berichtszeitraum: 2006, Redaktionsschluss: 15.02.2007
Landtagsdrucksache 16/1250

(29. 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 Der präventive Datenschutz startet durch

Es ist eine schöne Erfahrung, dass die Arbeit des Unabhängigen Landeszentrums für Datenschutz (ULD) von sehr vielen unterschiedlichen gesellschaftlichen Kräften wertgeschätzt wird. In jüngster Zeit können wir die Ernte einfahren von dem, was vor vielen Jahren vom ersten Leiter des ULD, Dr. Helmut Bäumler, gesät und über Jahre vom Team des ULD sorgsam gehegt und gepflegt wurde: Das Konzept des präventiven Datenschutzes zeigt Erfolg. Dieser präventive Datenschutz konzentriert sich nicht auf seine Rolle als Warner und Mahner, sondern versteht sich vor allem als **Ideengeber** und **Gestalter**. So begründet viele Befürchtungen vor dem Marsch in den Überwachungsstaat sein mögen, wir sind davon überzeugt, dass allein dauerndes Beklagen, die Welt wäre auf dem falschen Weg, diesen Marsch nicht aufhält.

Wir suchen einen anderen Weg, um den Datenschutz zur Geltung zu bringen. Mit konstruktiven Vorschlägen zeigen wir den beteiligten Personen und Stellen, dass wir deren Interessen an personenbezogener Datenverarbeitung ernst nehmen. Wir erwarten und erleben im Gegenzug, dass das Datenschutzanliegen auch ernst genommen wird. Daher versuchen wir, ein „Nein“ zu vermeiden; auch mit einem „Ja, aber“ geben wir uns nicht zufrieden. Vielmehr ist unsere liebste Antwort auf eine Datenschutzfrage: „**So geht's.**“ Die Kombination von juristischer und technischer Fachkompetenz, von Bündnispartnern in Politik und Wirtschaft, Öffentlichkeit und Wissenschaft und einem umfangreichen gesetzlichen Instrumentarium führt dazu, dass dem ULD viele Türen offen stehen.

Im **Instrumentenkasten** des präventiven Datenschutzes hat das ULD zu bieten: Forschungsprojekte im Bereich der Infrastrukturen und der Produktentwicklung, Transfer von Datenschutzwissen durch unser Innovationszentrum und Kompetenznetzwerke, wirtschaftliche Anreizsysteme mit Audit und Gütesiegel, umfangreiche Beratungsleistungen und Angebote für Fort- und Weiterbildung. Allerdings entbindet dieser Instrumentenkasten das ULD nicht von der gezielten Beanstandung oder Sanktionierung von Datenschutzverstößen. Diese Instrumente sind oft der Auftakt für eine präventive Datenschutzstrategie. Nur bei wenigen Unbelehrbaren und Böswilligen, von denen es weniger gibt, als man vermuten sollte, sind die Datenschutzstrafen unvermeidbar.

- **Grundlagenarbeit**

Datenschutz, also Schutz von Persönlichkeit und Privatsphäre in der Informationsgesellschaft, ist zwar Thema, aber nur selten Forschungsthema – sowohl an den juristischen oder technischen Fakultäten von Universitäten als auch in der Wirtschaft. Dieses Defizit kann das ULD nicht beheben. Doch kann es, mit öffentlichen Fördermitteln, z. B. der Europäischen Union oder des Bundes, aus der eigenen Erfahrung Impulse für die Entwicklung von datenschutzkonformen Produkten und Anwendungen geben, Beiträge leisten und einzelne Mosaiksteine zu einer grundrechtlich orientierten Weiterentwicklung der Informations- und

Wissensgesellschaft beisteuern. So kamen und kommen aus der ULD-Werkstatt wichtige Beiträge zu Themen wie z. B. Anonymität, Biometrie, Identitätsmanagement, Pseudonymität, Scoring, Ubiquitous Computing und Verkettbarkeit. Themen, die das ULD vor Jahren aufgriff, wie z. B. Identitätsmanagement, sind angesichts der Herausforderungen des Web 2.0 oder des E-Government zu zentralen Fragen unserer gesellschaftlichen Zukunft geworden (Tz. 8).

- **Produktentwicklung**

Für die Produktentwicklung fehlen dem ULD in jeder Form die Ressourcen; diese sind bei der Wirtschaft zu finden. Doch kann das ULD in Projekten mit seiner Datenschutzexpertise eine besondere Form von Public Private Partnership praktizieren: Es kann die praktische Erfahrung einer Datenschutzaufsichtsbehörde, wissenschaftliche Expertise und sein organisatorisch-rechtliches Know-how in die Entwicklung von informationstechnischen (IT-) Produkten einbringen – alles Kompetenzen, die es auf dem freien Markt derzeit noch viel zu wenig gibt (Tz. 8.4, 9.2).

- **Transfer von Datenschutzwissen**

Ohne die Vermittlung von Datenschutzknow-how in die Wirtschaft, die Verwaltung, die Wissenschaft, die Politik und die Öffentlichkeit wäre Datenschutz nicht möglich. Die Erfahrung des ULD ist, dass es gerade hieran fehlt, wenn überzogene Überwachungsmaßnahmen ergriffen werden oder wenn persönlichkeitsgefährdende Profile von Schülerinnen und Schülern, Konsumentinnen und Konsumenten, Bürgerinnen und Bürgern erstellt und genutzt werden. Die Beschaffung von Planungsdaten, die Wahrung unserer Sicherheit, die Informationsvermarktung oder die Verhinderung von Leistungsmissbrauch, all dies sind Ziele, die mit dem Ziel des Datenschutzes in Einklang gebracht werden können – und müssen. Das Bewusstsein für und das Wissen über eine datenschutzgerechte Gestaltung sind bisher nur wenig verbreitet. Hierin sehen wir eine unserer Aufgaben (Tz. 13).

- **Kompetenznetzwerke**

Auch bei optimaler Ressourcenausbeute ist das ULD nicht in der Lage, die Kompetenzen auf sich zu konzentrieren, die für die Wahrung des Datenschutzes in so unterschiedlichen Feldern wie Verwaltung und Privatwirtschaft, Internet- und Biotechnologie, Funktechnik und globalen Netzen nötig ist. Ohne Arbeitsteilung geht es nicht. Dies bedeutet, Kontakte zu Netzwerken zu knüpfen und zu pflegen, Informationen und Erfahrungen zu sammeln und auszutauschen. Das ULD ist in einigen Netzwerken Zentrum, etwa mit der Geschäftsführung des virtuellen Datenschutzbüros, mit der Leitung des Arbeitskreises Sicherheit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder oder der Arbeitsgruppe Versicherungswirtschaft der Datenschutzaufsichtsbehörden. Oft profitieren wir im ULD als ein Knoten unter vielen von solchen Netzwerken, etwa im Rahmen von großen oder kleineren europäischen Projekten. Häufig verstehen wir uns als Mediator und Multiplikator, etwa wenn wir für betriebliche oder behördliche Datenschutzbeauftragte oder für Systemadministratoren relevante Informationen

aufarbeiten und weitergeben, damit die rechtlichen Anforderungen an Datenschutz und Datensicherheit erfüllt werden können.

- **Audit**

Seit zehn Jahren wird über das Datenschutz-Audit diskutiert. Seit gut sechs Jahren wird es vom ULD praktiziert. Im Jahr 2006 war „gutes Datenschutzmanagement" Thema unserer Sommerakademie. Inzwischen ist die Diskussion über die Integration des Datenschutzes in das IT-Sicherheits- und das Informationsmanagement im vollen Gange. Öffentliche Verwaltungen in Schleswig-Holstein wie auch Unternehmen in ganz Deutschland lassen sich mit unseren speziellen Auditerfahrungen beraten. Beim Audit können wir nachweisen, dass sich Datenschutz bezahlt macht – durch effektive schlanke Abläufe mit geklärten Verantwortlichkeiten und transparenten Strukturen – und dabei auch noch Grundrechte und Bürgerinteressen gewahrt werden können. Für alle Beteiligten wird der Datenschutz so zu einer Win-Win-Situation (Tz. 9.1).

- **Gütesiegel**

Datenschutzkonforme IT-Angebote und -Produkte sind die Tools für eine bürgerrechtlich orientierte Informationsgesellschaft. Derartige Angebote und Produkte lassen sich nicht so leicht vergleichen wie die Qualität und die Preise von Äpfeln und Birnen. Daher bietet das ULD ein gesetzlich vorgesehenes Verfahren zur Überprüfung und Bestätigung der Datenschutzkonformität an. Dieses rechtlich nur auf Schleswig-Holstein beschränkte Angebot wird inzwischen bundesweit in Anspruch genommen und stößt auf Interesse und Nachahmung in anderen Staaten (Tz. 9.2).

- **Beratung**

Neben der Bereitstellung von Informationen ist individuelle Beratung oft unabdingbar – zu unterschiedlich sind häufig die Probleme und die Lösungsmöglichkeiten bei der personenbezogenen Datenverarbeitung. Das Beratungsangebot des ULD richtet sich an alle Beteiligten: an Datenverarbeiter wie an Betroffene, an Behörden wie an Unternehmen, an Personalvertretungen wie an Arbeitgeber, an ehrenamtliche Organisationen wie an profitorientierte Großunternehmen. Dabei versucht das ULD, ein ehrlicher Makler zu sein: Bei allem Engagement für die Wahrung des Rechts auf informationelle Selbstbestimmung erkennen wir auch das Recht und das Interesse an Informationen an – als Informationsfreiheitsbeauftragter im Interesse demokratischer Transparenz, aber auch im sonstigen öffentlichen oder privaten Interesse.

- **Ausbildungsinitiativen**

Vor zwölf Jahren wurde gemeinsam mit dem Deutschen Grenzverein e.V. die DATENSCHUTZAKADEMIE Schleswig-Holstein gegründet, die inzwischen ein etablierter Bildungsträger des Landes ist. Vorlesungsangebote an der Verwaltungsakademie und der Universität zu Kiel kamen hinzu. Jüngster Spross des

ULD-Ausbildungsangebotes sind ein Kooperationsvertrag mit der Fachhochschule Kiel und dortige Bildungsangebote in der Bachelor- und Master-Ausbildung. Für Systemadministratoren wurde vor wenigen Jahren ein Zertifikat mit sehr vielen geforderten Voraussetzungen eingeführt. Der nächste Schritt drängt sich geradezu auf: die Standardisierung und Qualifizierung der Ausbildung zum behördlichen bzw. betrieblichen Datenschutzbeauftragten und die Einführung entsprechender Leistungsnachweise (Tz. 13).

1.2 Wir nehmen den Datenschutz ernst

„Sie müssen den Datenschutz nicht lieben; ernst nehmen wäre genug." Diesen Satz hätten wir im vergangenen Jahr häufig sagen oder schreiben können. Adressaten dieser Aufforderung sind so unterschiedliche Personen und Stellen wie der Innenminister, die Leitung des Bildungsministeriums und immer wieder Vertreter der Privatwirtschaft. Hintergrund unserer Aufforderung ist nicht eine ablehnende Einstellung gegenüber dem Datenschutz, sondern dessen **Ausblendung**. Der Innenminister nimmt seine Aufgabe als Polizeiminister ernst, ist aber auch Verfassungs- und damit Datenschutzminister. Im Bildungsministerium erhofft man sich genauere Informationen über das Schulsystem, um mit den validen Planungsdaten die Erziehungsmisere in den Griff zu bekommen. Aber man kümmerte sich bisher kaum darum, dass bei der Beschaffung dieser Daten, z. B. für ein nationales Schülerregister, massive Eingriffe in das Recht auf informationelle Selbstbestimmung der Schülerinnen und Schüler erfolgen und wirksame Schutzvorkehrungen erforderlich sind. Und in der Wirtschaft nehmen es manche Unternehmen mit dem Geldverdienen derart ernst, dass ihnen die Konsequenzen für die Selbstbestimmung der Konsumentinnen und Konsumenten aus dem Blick geraten.

So wie es die Aufgabe des Innenministers ist, um ein wirksames Polizeirecht zu streiten, die Aufgabe des Bildungsministeriums, gute Planungsdaten für eine optimale Erziehung zu beschaffen, die Aufgabe der Wirtschaft, für sich und das Land Gewinn zu erwirtschaften und Arbeitsplätze zu schaffen, so ist es die Aufgabe des Unabhängigen Landeszentrums für Datenschutz, für die informationelle Selbstbestimmung zu sorgen. Als Mittel hierfür haben wir keine Kompetenzen der Regulierung und nur wenige zur Sanktionierung. Unsere zentralen Mittel sind die **Macht der Argumente** und die Diskussion. Um den Argumenten Gehör zu verschaffen, mussten wir das eine oder das andere Mal die Diskussion nachhaltig einfordern, indem wir unseres Erachtens wichtige Themen öffentlich ansprachen.

Der **Gang an die Öffentlichkeit** ist jedes Mal der letzte – manchmal verzweifelte – Schritt, wenn alle direkten Diskussionsangebote zurückgewiesen werden. So war dies etwa beim Polizeirecht, als wir das Innenministerium mit schriftlichen Stellungnahmen auf die Verfassungswidrigkeit seiner Planungen hinwiesen. Nachdem selbst der direkte Appell an die Spitze des Ministeriums erfolglos war, blieb zum Zeitpunkt der ohnehin schon öffentlichen Verbandsanhörung dem ULD kein anderer Weg als der an die Öffentlichkeit (Tz. 4.2.1). In der Bildungspolitik zeigten wir vielleicht zu lange Geduld. Die Spitze des Ministeriums ließ sich mit Briefen und vielfältigen Gesprächsangeboten über mehr als ein halbes Jahr lang nicht von der Verfassungswidrigkeit seiner Gesetzesvorschläge zur individuellen

Schülerstatistik überzeugen. Als wir dann kurz vor der entscheidenden Bildungsausschusssitzung des Landtages an die Öffentlichkeit gingen, war die öffentliche Empörung über die Pläne groß, doch die Regierungsfraktionen hatten sich schon politisch festgelegt (Tz. 4.7). Im Bereich der Privatwirtschaft ist das ULD äußerst zurückhaltend bei der Benennung von Ross und Reiter. Der Gang in die Öffentlichkeit war aber auch hier nicht vermeidbar, als etwa die Bankwirtschaft und deren Dienstleister dem amerikanischen Geheimdienst in Millionenumfang sensible Kundendaten zur Verfügung stellten und trotz offensichtlicher Rechtswidrigkeit für keine Abhilfe sorgten (Tz. 5.1). Die Förderung der öffentlichen Debatte über den Datenschutz – und die Informationsfreiheit – gehört zu den originären gesetzlichen Aufgaben des ULD.

Dem ULD wurde in der öffentlichen Debatte manchmal Besserwisserei und Arroganz vorgeworfen. Sollte dieser Eindruck angesichts unseres Engagements entstehen, so tut uns dies leid. Wenn ein wirklicher Diskurs über einen Datenschutzkonflikt stattfindet und wir **bessere Argumente** vorgetragen bekommen, lassen wir uns hiervon gerne überzeugen. Um den Datenschutz im Interesse der Bürgerinnen und Bürger zu verwirklichen, muss man ihn oder das ULD nicht „lieb haben“. Es genügt, ihn ernst zu nehmen, indem man ihn als einen Aspekt bei der Gestaltung informationstechnischer Vorgänge beachtet. Bloße Verweigerung nützt niemandem.

An dieser Einsicht hat es im letzten Jahr nach unserem Eindruck bei einzelnen Fachressorts das eine oder das andere Mal gefehlt. Generell ist aber der Landesregierung zu bescheinigen, dass sie es mit dem Datenschutz bei der Verwirklichung von IT-Verfahren sehr ernst nimmt. Dies ist daran zu erkennen, dass das ULD von den Fachressorts und dem zumeist federführenden Finanzministerium in einem frühen Verfahrensstadium einbezogen wird. Diese Praxis basiert auf den Festlegungen des **IT-Gesamtplanes 2007 der Landesregierung**, wonach das ULD frühzeitig in die Planungsprozesse der Informationstechnik (IT) einzubeziehen ist und dessen Beratungskompetenz genutzt wird zur Analyse, Bewertung und strukturierten Gestaltung datenschutzkonformer und -sicherer Verarbeitungsprozesse einschließlich der jeweiligen Auftragsdatenverarbeitung.

1.3 Gesetzgebung im Land

Ein Exempel für Nichternstnehmen (Tz. 1.2) statuierte das Innenministerium bei der Gesetzgebung zum **Polizeirecht**. Dieses wähnte nicht nur den Datenschutz, sondern auch den Leiter des ULD „allein zu Haus“ und sich in allerbester Gesellschaft der ernst zu nehmenden gesellschaftlichen Kräfte bis hin zum Bundesverfassungsgericht. So sehr wir Verständnis dafür haben, dass es in der Politik nicht immer nur auf die besseren Argumente ankommt, so befremdet waren wir darüber, dass das Innenministerium zunächst partout nicht bereit war, diese zur Kenntnis zu nehmen. In der Sache war festzustellen, dass sich zunächst die Opposition und eine kritische Öffentlichkeit auf die Seite des ULD schlugen, dass die Gesamtheit aller Sachverständigen der Anhörung im Innen- und Rechtsausschuss unsere Position weitgehend teilte und dass schließlich auf Anforderung des Parlamentes dessen Wissenschaftlicher Dienst diese bestätigte.

Das Innenministerium muss nun nicht die Befürchtung haben, allein zu sein bei seinem Bestreben, ein wirksames und verfassungskonformes Polizeirecht zu schaffen. Das ULD hat seine Bereitschaft zur Zusammenarbeit in jedem Stadium der Beratungen zum Ausdruck gebracht. Die manchmal hitzige Diskussion sollte nun in ein ruhigeres Fahrwasser gebracht werden und die Suche nach **konstruktiven Lösungsvorschlägen** im Vordergrund stehen. Dabei machen wir uns nichts vor: Die Positionen des Innenministeriums weichen immer noch von dem ab, was wir im ULD gerade noch als verfassungsrechtlich akzeptabel ansehen. Dies erweist sich nicht nur bei der Polizeigesetzgebung, sondern auch bei der Implementierung neuer Informationstechnik in der Polizei oder beim Umgang mit den Betroffenenrechten, etwa dem Auskunftsanspruch (Tz. 4.2.1 bis 4.2.4).

Im Vorfeld der Gesetzgebung zum Informationsfreiheitsgesetz (IFG) hatte das ULD geradezu inständig darum gebeten, bei der gesetzlichen Umsetzung der **Umweltinformationsrichtlinie** der Europäischen Union die positiven Errungenschaften des bisherigen Gesetzes nicht aufzugeben. Tatsächlich ist anerkannt, dass das IFG-SH nicht nur in der Bundesrepublik, sondern auch darüber hinaus im Hinblick auf Kürze, Klarheit und Praktikabilität mit der Zielsetzung größtmöglicher demokratischer Transparenz vorbildlich ist. Auf diesem Wege wäre das ULD gerne gemeinsam mit dem Innenministerium und dem Gesetzgeber weitergegangen; entsprechende Vorschläge lagen dem Parlament vor. Der nunmehr gewählte Kompromiss, ein eigenes Umweltinformationsgesetz zu schaffen und das bisherige IFG unangetastet zu lassen, ist zwar gesetzessystematisch nicht so schön wie eine integrierte Regelung mit der bundesweit größtmöglichen Transparenz. Sie ist aber eine gediegene Grundlage für die Sicherung der berechtigten Informationsbedürfnisse der Bürgerinnen und Bürger im demokratischen Rechtsstaat (Tz. 12.1).

Bei der Diskussion um das **Schulgesetz** ging es in der öffentlichen Debatte noch um viele andere Themen als das des Datenschutzes. Daher versuchte das ULD, durch direkten Austausch mit dem zuständigen Ministerium die Fragen der optimalen Regulierung der schulischen Datenverarbeitung zu klären. Dieser Weg erwies sich teilweise als erfolgreich. Die Spitze des Ministeriums wollte sich aber nicht davon abbringen lassen, eine landesweite Schulstatistik als Teil eines bundesweiten Systems vorzusehen, bei dem jede Schülerin und jeder Schüler eine Identifizierungsnummer erhält, zu der die Daten des gesamten schulischen Verlaufes gespeichert werden. Herauskommen würde bei der Umsetzung der gefassten Beschlüsse die gläserne Schülerin bzw. der gläserne Schüler.

2 Datenschutz in Deutschland

Das Ernstnehmen des Datenschutzes scheint so manchem Verantwortlichen in Schleswig-Holstein schwerzufallen. Die Verhältnisse auf Bundesebene sind jedoch noch beängstigender. Der Lobby des Grundrechts auf informationelle Selbstbestimmung wird von den politischen Entscheidungsträgern nur dann Beachtung beigemessen, wenn es um fremde Ressorts geht. So ist verblüffend, wie etwa Sicherheitsbehörden und -politiker immer wieder darauf verweisen, dass doch in der Privatwirtschaft viel mehr Daten gesammelt würden als durch sie und dass sich dies die Menschen freiwillig gefallen ließen. Umgekehrt zeigen private Unternehmen mit dem Finger auf den staatlichen Datenhunger, gegenüber dem man selbst eher die Rolle eines Waisenkindes einnähme.

Die jeweiligen Fremdwahrnehmungen haben einen wahren Kern: **Staat und Wirtschaft** haben zur Jagd auf die personenbezogenen Daten der Bürgerinnen und Bürger geblasen. Dabei gibt es keinen Grund, den Schwarzen Peter beim jeweils anderen zu suchen. Schwarze Peter sind mehr als nur einer im Umlauf. Schlimmer noch: Waren bisher private und öffentliche Überwachung relativ sauber voneinander getrennt, so fließen diese Bereiche immer mehr ineinander. So war die öffentliche Empörung groß, als im Januar 2007 zur Überführung von mehreren Hundert Internetnutzern, die Kinderpornografie aus dem Netz geladen hatten, die Datensätze von 22 Millionen Kreditkartennutzern herangezogen wurden. Die Staatsanwaltschaft hatte sich die Datenbestände von den Finanzdienstleistern umfassend nutzbar gemacht. Groß war auch die Verblüffung, dass das ULD im Grundsatz gegen diese Praxis keine durchgreifenden Einwände erhob, wurden doch hierbei zur Aufklärung von konkreten Straftatverdächtigen anhand von bestimmten Merkmalen die Tatverdächtigen ermittelt. Dennoch bleiben Zweifel: Nicht immer wird von staatlichen Organen die erforderliche verfahrensrechtliche Disziplin gewahrt. Außerdem sind sich die Menschen nicht bewusst, dass all die Daten, die bei einer Bank, einer Versicherung, einem Warenhaus, einem Versandhändler, einem Vermietungsunternehmen oder einem Sportverein über einen vorhanden sind, potenzielle Ermittlungsdaten sind – nicht nur für Strafverfolgungsbehörden, sondern auch für Finanzämter, Sozialbehörden und Geheimdienste.

2.1 Der feste Griff des Terrorismus

Das mangelnde Bewusstsein über die tatsächlich über jeden Menschen stattfindende Datenverarbeitung und die möglichen Auswertungen veranlassen immer

noch einen Großteil der Bevölkerung zu dem Trugschluss: „Ich habe doch nichts zu verbergen." Daher könnten die Sicherheitsbehörden auch alles über sie erfahren mit dem berechtigten Ziel, den Terrorismus zu bekämpfen. So traten jüngst ohne größere öffentliche Debatte zwei neue Gesetze in Kraft, deren erklärtes Ziel die Terrorismusbekämpfung ist: das **Antiterrordateigesetz** (ATDG) und das **Terrorismusbekämpfungsergänzungsgesetz** (TBEG).

Entgegen dem offiziell vermittelten Eindruck werden damit aber nicht nur Terrorismusverdächtige erfasst, sondern auch – im weitesten Sinne des Wortes – Kontaktpersonen. In der Antiterrordatei und weiteren sogenannten Projektdateien oder in den Dateien der Geheimdienste dürfen nach diesen Gesetzen Daten von Menschen gespeichert werden, die sich nie etwas haben zuschulden kommen lassen. Sie werden nur deshalb gespeichert, weil sie zum falschen Zeitpunkt am falschen Ort waren oder aus falschem Anlass das Falsche gemacht haben und hieraus falsche Schlüsse gezogen werden. Die **Jedermannerfassung**, die auch im Land Schleswig-Holstein derzeit zur Diskussion steht, ist auf Bundesebene schon weit fortgeschritten und wird immer wieder mit der Terrorismusbekämpfung legitimiert.

ATDG und TBEG sind nur Wegmarken auf dem **langen Marsch** in eine Überwachungsgesellschaft unter dem Vorzeichen der Terrorismusbekämpfung. Schon lange vor dem 11. September 2001 haben die Sicherheitsbehörden gesetzliche Befugnisse zur Rasterfahndung, Schleierfahndung, Videoüberwachung, Telekommunikationsüberwachung, zu Lauschangriffen usw. eingeräumt bekommen. Nach diesem Datum gab es geradezu ein Feuerwerk neuer Sicherheitsgesetze, das mit den sogenannten Otto-Katalogen eingeläutet wurde und bei dem es um Dinge geht, die für Normalverbraucher wahrscheinlich immer ein Geheimnis bleiben werden und für die geheimnisvolle Begriffe stehen wie IMSI-Catcher, Kontodatenabfrage oder Abkürzungen wie PNR und SWIFT. Mit den beiden neuen Gesetzen wurde noch nicht das Ende der Planungen erreicht. In der Büchse der Pandora sind z. B. schon klar erkennbar die Telekommunikationsvorratsdatenspeicherung oder das heimliche staatliche Eindringen in den privaten PC.

Nicht nur im Lande Schleswig-Holstein, auch in den anderen Ländern und im Bund zeigen sich die Sicherheitspolitiker von **Entscheidungen der Verfassungsgerichte** fast völlig unbeeindruckt, die ihnen Verfassungsverstöße attestierten. Die Verfassungsgerichte des Bundes und der Länder haben – vor allem seit dem 11. September 2001 – die Grundrechtswidrigkeit von Gesetzen und staatlichen Ermittlungsmaßnahmen festgestellt und hierbei klare Rahmenbedingungen für Gesetzgeber und staatliche Ermittler festgelegt. Lauschangriff, Rasterfahndung, Schleierfahndung, Telefonüberwachung, Kfz-Durchsuchung ... all das ist nur unter engen materiellrechtlichen Grenzen und unter Beachtung gesetzlich zu regelnder rechtsstaatlicher Verfahren zulässig. Einen Kernbereich unseres Lebens haben die Verfassungsgerichte gar als unantastbar erklärt.

Diese Entscheidungen erfolgten nicht trotz, sondern wegen der latenten terroristischen Bedrohung: Der Rechtsstaat darf sich nicht von terroristischen Straftätern Regeln aufzwängen lassen, die Rechtsstaatlichkeit, Demokratie und Freiheits-

rechte beeinträchtigen. Die Bekämpfung von Unrecht darf nicht dazu führen, dass der Rechtsstaat zum Unrechtsstaat wird. Nicht nur das: Bislang sind die Sicherheitsbehörden den Nachweis schuldig geblieben, dass und wie ihr Instrumentarium zur Terrorismusbekämpfung hierzu taugt und wirkt. Die von Datenschützern immer wieder aufgestellte Forderung nach einer **unabhängigen Evaluierung** der erlaubten und durchgeführten Grundrechtseingriffe stößt in der Praxis weiterhin auf taube Ohren. Es besteht der begründete Verdacht, dass viele Maßnahmen nicht mehr Sicherheit bringen, ja gar selbst ein Sicherheitsrisiko darstellen. Da hierüber öffentlich diskutiert werden muss, wird sich die Sommerakademie 2007 mit dem Thema „Offene Kommunikationsgesellschaft und Terrorbekämpfung – ein Widerspruch?“ befassen (Tz. 13).

2.2 Haben wir wirklich alle nichts zu verbergen?

Wenn viele Menschen meinen, sie hätten nichts zu verbergen, so mag dies ihre persönliche Überzeugung sein. Dass viele Menschen selbst aus den intimsten Details in ihrem Leben kein Geheimnis machen, indem sie sich tatsächlich oder im übertragenen Sinn z. B. im Internet oder in Fernsehtalkshows nackt ausziehen, ist deren persönliche Entscheidung. Niemand kann daran gehindert werden, sein Innerstes nach außen zu wenden. Aber niemandem darf erlaubt sein, das Innerste anderer Menschen vor der Welt oder gegenüber bestimmten Adressaten zu offenbaren. Wer meint, nichts zu verbergen zu haben, darf von anderen nicht erwarten, dass auch sie sich nackt ausziehen lassen. Genau dies ist – populär formuliert – der Hintergrund des verfassungsrechtlich gewährleisteten Grundrechtes auf informationelle Selbstbestimmung und des Anspruchs auf **Wahrung der Privatsphäre**.

Denjenigen, die meinen, sie hätten nichts zu verbergen, muss mitgeteilt werden, dass ihnen das Wesen der Terrorismusbekämpfung verborgen geblieben ist: Hierbei geht es nicht nur um Fakten, sondern um Mutmaßungen und Verdachte und oft um falsche Annahmen der Sicherheitsbehörden. Mag sein, dass ein Mensch nichts dagegen hat, dass bei der Polizei – gut abgeschottet gegen Missbrauch durch Dritte – alles über sie gespeichert ist. Es ist aber nicht vorstellbar, dass irgendjemand wirklich damit einverstanden ist, dass er unberechtigt als Terrorismusverdächtiger gespeichert und behandelt wird. Derartige Speicherungen sind aber bei der Polizei und den Geheimdiensten notwendig, weil jedem Terrorismusnachweis ein Verdacht vorausgehen muss, der durch weitere Ermittlungen erhärtet wird. Wir Datenschützer verstehen unsere Aufgabe darin, dass wirklich nur reale Verdachte zu einer Speicherung als „verdächtig“ führen und nicht schon vage **Mutmaßungen**, **Hypothesen** oder **Denunziationen**.

Es ist unsere Aufgabe, dafür zu sorgen, dass die **Verdachtsdaten vertraulich behandelt** werden. Dies ist bei der Aufhebung der engen Zweckbindung im geplanten Landesverwaltungsgesetz für Polizeivorgangssysteme ebenso wenig gewährleistet wie in der Antiterrordatei von Bund und Ländern. Deshalb sind wir Datenschützer gegen diese geplanten Ermittlungswerkzeuge, nicht weil wir den Sicherheitsbehörden ihre Arbeit erschweren wollen. Letztendlich vertreten wir damit sogar die Interessen der Sicherheitsbehörden: Denn ohne Wahrung der

Vertraulichkeit ihrer Daten kann diesen schwerlich Vertrauen entgegengebracht werden.

2.3 Ungenutzte Chancen

Jenseits aller Sicherheitspolitik müssen wir feststellen, dass die Bundesregierung bisher alle Chancen verpasst, sich für eine rechtsstaatliche und moderne menschengerechte Informationsgesellschaft fit zu machen. Im Dezember fand mit großem Medienaufwand und angeführt von der Bundeskanzlerin ein Informationstechnik-(IT-)Gipfel statt, bei dem es darum ging, IT zukunftsfähig zu machen. Datenschützer waren nicht eingeladen. Erschreckend und zugleich hochgradig unvernünftig war, dass auch inhaltlich **Datenschutz und Verbraucherschutz keine Rolle** spielten.

Die Bundesregierung erklärte, ihre Präsidentschaft beim G8-Gipfel und bei der Europäischen Union dazu nutzen zu wollen, IT im **internationalen Kontext** voranzubringen. Was für Deutschland gilt, gilt für Europa und die gesamte Welt: Wer langfristig IT zum Wohle der Menschen einsetzen möchte und wer IT als Wachstumsfaktor, Beschäftigungsmotor und Profitquelle nutzen möchte, der muss darauf achten, dass Datenschutz und Datensicherheit als wichtige Bestandteile des Verbraucherschutzes und damit der Akzeptanz für die Konsumentinnen und Konsumenten gewährleistet sind. Dies erkennen immer mehr Unternehmen im In- und im Ausland, z. B. Microsoft, die weltweite Nummer eins im Bereich der Softwarewirtschaft. Microsoft hat sich die Datenschutzkonformität eines seiner Produkte vom ULD mit einem schleswig-holsteinischen Gütesiegel bestätigen lassen (Tz. 9.2.2).

Marktwirtschaftliche Instrumente des Datenschutzes wie z. B. Gütesiegel und Audit drängen auf rechtliche Anerkennung und Umsetzung. Der Bedarf der Wirtschaft nach solchen Instrumenten wird immer offensichtlicher. Nicht, dass sich die Bundesregierung mit guten oder schlechten Gründen diesem Bedarf entgegenstemmen würde, viel schlimmer: Sie hat bisher diesen **Bedarf schlicht ignoriert** und erweist sich insofern nicht gerade als zukunftsfähig.

3 Datenschutz im Landtag

Die Kooperation des ULD mit dem **Datenschutzgremium** ist inzwischen zur Routine geworden. Der stetige Erfahrungs- und Meinungsaustausch gewährleistet, dass über aktuell in der Landtagsverwaltung auftretende Fragen alle Beteiligten umfassend informiert sind und zeitnah notwendige Schritte eingeleitet werden. Dass das Datenschutzgremium seine Aufgabe ernst nimmt, zeigen anlassbezogene wie auch systematische Kontrollen, die sich der Landtag im Rahmen von Audits selbst auferlegt hat.

3.1 Videoüberwachung plus Zutrittsberechtigungssystem auditiert

Das Zutrittsberechtigungssystem des Schleswig-Holsteinischen Landtages wurde 2004 mit einem Datenschutz-Audit ausgezeichnet. Die Erweiterung des Sicherheitskonzepts um eine Videoüberwachungsanlage wurde jetzt in das Datenschutz-Audit aufgenommen.

Das chipkartenbasierte Zutrittsberechtigungssystem im Landtag war 2004 Gegenstand eines Datenschutz-Audits. Dabei wurde festgestellt, dass das Sicherheitskonzept des Landtages den Anforderungen an Datenschutz und Datensicherheit genügt (27. TB, Tz. 3.1). Dieses wurde nun um eine Videoüberwachungsanlage ergänzt, die die **„Außenhaut" des Landtages** überwacht. Bei weitreichenden Ergänzungen oder Änderungen an dem Gegenstand eines Datenschutz-Audits – wie hier – muss eine erneute Prüfung der Auditberechtigung erfolgen. Die Videoanlage überwacht die Fassade des Landeshauses, des Bürogebäudes Karolinenweg sowie Bereiche der Tiefgarage und der Garage Reventlouallee im Rahmen des Hausrechts. Über einen Bewegungssensor werden bewegliche Kameras auf diejenigen Bereiche geschwenkt, in denen Ereignisse festgestellt werden. Die Aufnahmen der Videoüberwachung werden in der Pförtnerei angezeigt. Von hier aus ist auch eine manuelle Steuerung der beweglichen Kameras möglich.

Durch Ausrichtung der Kameras, Begrenzung der Schwenkwinkel und automatische Ausblendung bestimmter Bereiche der Bilder wird erreicht, dass nur das Landeshaus sowie die zugehörigen Freiflächen, nicht aber andere öffentliche Wege wie der Düsternbrooker Weg oder die Kiellinie, die nicht zum Landeshaus gehören, überwacht werden können. Alle Aufnahmen werden für einen Zeitraum von drei bis fünf Tagen aufgezeichnet. Der Zugriff auf diese Aufzeichnungen ist durch ein Vieraugenprinzip abgesichert und erfordert die Mitwirkung von Mitarbeitern, die ausdrücklich von der Dienststellenleitung dazu ermächtigt wurden. Die Landtagsverwaltung hat **organisatorische Regelungen** zur Weitergabe von Aufzeichnungen an Dritte, z. B. für Zwecke der straf- oder zivilrechtlichen Verfolgung von Tätern, getroffen.

Bei dieser Gelegenheit wurde die Reauditierung des Zutrittsberechtigungssystems, die turnusgemäß im Jahr 2007 fällig gewesen wäre, vorgezogen. Wegen der engen Verzahnung mit der Videoüberwachung durch ein gemeinsames Sicherheitskonzept und wegen gemeinsamer organisatorischer Regelungen und Aufgabenfestle-

gungen in der Landtagsverwaltung wäre eine Trennung in zwei Auditgegenstände künstlich und mit unnötigem Aufwand verbunden gewesen. Bei der **Reauditierung** des Zutrittsberechtigungssystems wurde festgestellt, dass alle Datenschutzziele, die sich die Landtagsverwaltung im ersten Audit gesteckt hatte, zwischenzeitlich umgesetzt wurden. Der Vorbildcharakter des Zutrittsberechtigungssystems wurde uns hierbei deutlich. Inzwischen erreichen uns Anfragen von Firmen, die sich an Aufbau und Organisation des Zutrittsberechtigungssystems orientieren möchten.

Was ist zu tun?
Beim Einsatz von Videoüberwachung lassen sich die Bedürfnisse von Datenschutz und Sicherheit durch intelligente technische und organisatorische Maßnahmen gut in Einklang bringen. Dies ist den Anbietern und Nutzern solcher Systeme zu vermitteln.

3.2 Immunität der Abgeordneten und Datenübermittlung

Veranlasst durch einen vom ULD geprüften Einzelfall wurde im Innen- und Rechtsausschuss des Landtages die Frage aufgeworfen, ob die Staatsanwaltschaft dem Präsidenten des Landtages die Einleitung eines Vorprüfungsverfahrens mitteilen darf oder ob hierfür erst eine Rechtsgrundlage geschaffen werden muss.

Der Landtag legt zu Beginn jeder Legislaturperiode Grundsätze über die Behandlung von Immunitätsangelegenheiten fest. Nach diesen Grundsätzen soll die Staatsanwaltschaft vor Beginn einer näheren Prüfung – also bevor festgestellt wurde, ob eine Strafanzeige überhaupt einen strafrechtlichen Anfangsverdacht begründet – den **Landtagspräsidenten informieren**. Landesjustizministerium und Generalstaatsanwalt stellten infrage, dass für diese Datenübermittlung eine Rechtsgrundlage vorliegt.

Wir teilten dem Innen- und Rechtsausschuss mit, dass eine solche Übermittlung von Informationen an den Präsidenten des Landtages unmittelbar auf das in der Landesverfassung verankerte Auskunftsrecht des Parlaments gestützt werden könne. Der Wissenschaftliche Dienst des Landtages legt einen strengeren Maßstab an und hält eine Rechtsgrundlage für die Datenübermittlung für erforderlich. Diese Auffassung stößt bei uns auf Sympathie. Jedenfalls wäre **eine eigenständige gesetzliche Regelung** zu dieser Datenübermittlung nicht von Nachteil. Wir würden uns freuen, wenn die Strafverfolgungsbehörden auch in anderen Bereichen des Strafverfahrens wie hier eine enge Auslegung von oftmals wenig bestimmten Vorschriften zur Datenerhebung und -übermittlung vornehmen würden. Die Kommunikation zu dem Thema mit dem Landtag ist dokumentiert in den Landtagsumdrucken 16/883, 974, 1078 und 1205.

Was ist zu tun?
Unseres Erachtens kann das Verfahren zur Information des Landtagspräsidenten fortgesetzt werden. Eine eigenständige gesetzliche Regelung wäre aber zu begrüßen.

4 Datenschutz in der Verwaltung

4.1 Allgemeine Verwaltung

Im Bereich der Datenverarbeitung in der allgemeinen Verwaltung hat sich der Schwerpunkt der Tätigkeit des ULD von der klassischen Prüftätigkeit über die Jahre hinweg zur **Beratung** und zum **Datenschutz-Audit** verlagert: Administratoren und Anwender von informationstechnischen Programmen sowie die Verantwortlichen von der sachbearbeitenden bis zur leitenden Ebene wenden sich bei schwierigen oder kontroversen Datenschutzfragen regelmäßig vorab an das ULD, um Fehler zu vermeiden. Die Einzelfallberatung wird zunehmend ergänzt durch Ratschläge und Tipps zum Datenschutzmanagement und zu den Datenverarbeitungsstrukturen. Dennoch: Prüfungen sind unverzichtbar, denn nicht alle nehmen das Angebot des ULD rechtzeitig und freiwillig in Anspruch.

4.1.1 Datenschutzrechtliche Anforderungen an die kommunale Zusammenarbeit

Kommunen und Kreise verstärken mehr oder weniger freiwillig ihre Zusammenarbeit. Zum Teil werden Aufgaben vollständig übertragen, zum Teil wird lediglich das Rechenzentrum, eine Einrichtung oder der Verwaltungsvollzug einer anderen Kommune bzw. eines anderen Kreises genutzt. In jedem Fall tauchen datenschutzrechtliche Fragen auf, die vorab geklärt werden müssen.

Das Gesetz über kommunale Zusammenarbeit (GkZ) sieht verschiedene Kooperationsmöglichkeiten vor. In jedem dieser Fallgestaltungen muss geklärt werden, wer rechtlich für die Einhaltung der Vorschriften des Datenschutzes **verantwortlich** ist bzw. wird. Dies hängt von dem gewählten Kooperationsmodell und der Ausgestaltung des Kooperationsvertrages ab.

Beauftragt eine Kommune eine andere mit der Durchführung einer Aufgabe, die weisungsgebunden durchgeführt werden soll, ohne dass die Aufgaben selbst und die Organisationshoheit auf den Dritten übergehen, handelt es sich um eine **Auftragsdatenverarbeitung**. Der Auftraggeber bleibt für die Datenverarbeitung verantwortlich. Er muss eine datenschutzgerechte Datenverarbeitung sowie die Datensicherheit gewährleisten. Der Auftragnehmer darf die personenbezogenen Daten nur nach Weisung des Auftraggebers verarbeiten.

Wird eine Aufgabe zur **selbstständigen und eigenverantwortlichen Erfüllung** übertragen, so wechselt die Verantwortung für die Aufgabe und die Datenverarbeitung. Das GkZ sieht im Wesentlichen vier Kooperationsformen vor: die Grün-

dung eines Zweckverbandes, der Abschluss einer öffentlichen Vereinbarung, die Gründung einer Verwaltungsgemeinschaft und die Errichtung gemeinsamer Kommunalunternehmen. Diese Kooperationsformen sind datenschutzrechtlich unterschiedlich einzuordnen:

- Gründen mehrere Gemeinden, Ämter oder Kreise einen **kommunalen Zweckverband**, der für seine Mitglieder bestimmte Aufgaben übernimmt, wird dieser die für die Datenverarbeitung verantwortliche Stelle. Denn dieser erfüllt die ihm übertragenen Aufgaben in eigener Verantwortung.
- Auch eine **öffentliche Vereinbarung** hat im Regelfall die Übertragung einer Aufgabe zur eigenständigen Erfüllung zum Inhalt und führt daher zum Übergang der datenschutzrechtlichen Verantwortlichkeit. Diese steht auch hier im Gleichklang mit der Trägerschaft der Aufgabe.
- Anders ist die datenschutzrechtliche Rechtslage, wenn eine **Verwaltungsgemeinschaft** gegründet wird. Hier bedient sich eine öffentliche Stelle bei der Erfüllung ihrer öffentlichen Aufgabe einer anderen öffentlichen Stelle, ohne dass ihr die Aufgabe selbst übertragen wird. Lediglich der Vollzug erfolgt durch die verwaltungsführende Körperschaft. Der Auftraggeber kann dabei Weisungen erteilen, ohne dazu gesetzlich verpflichtet zu sein. Er kann auch vorsehen, dass die ausführende Stelle selbstständig tätig wird. Datenschutzrechtlich bleibt aber weiterhin die beauftragende Stelle verantwortlich.
- Neu aufgenommen ist im GkZ als Möglichkeit der kommunalen Zusammenarbeit die Errichtung **gemeinsamer Kommunalunternehmen**. Mit der Errichtung eines gemeinsamen Kommunalunternehmens entsteht ein selbstständiges Unternehmen.

Der Einordnung der Datenverarbeitung als Auftragsdatenverarbeitung steht es nicht unbedingt entgegen, dass der Dritte die übertragene **Aufgabe größtenteils selbstständig erfüllt**. Entscheidend ist, dass der Auftraggeber Träger der Aufgaben bleibt. Er hat dem Auftragnehmer Weisungen zu erteilen, soweit personenbezogene Daten verarbeitet werden. Ist eine Weisungserteilung nicht möglich, weil es bei der Übertragung gerade auf das Know-how des Dritten ankommt und aufgrund dieser Überlegenheit des Auftragnehmers Weisungen dem Auftragsverhältnis zuwiderlaufen würden, so müssen die Anforderungen an die Datenverarbeitung zumindest in abstrakter Form festgelegt werden. Der Auftraggeber bleibt hierfür verantwortlich und hat die Pflicht, die im Einzelfall erforderlichen Maßnahmen zur Wahrung von Datenschutz und Datensicherheit zu treffen.

Was ist zu tun?
Kooperationen zwischen öffentlichen Stellen sind in vielen Variationen denkbar. Bei jeder Kooperation ist vorab zu klären, wer für die Einhaltung des Datenschutzes verantwortlich ist.

4.1.2 Privatisierung kommunaler Archive

Angesichts knapper Kassen ist die Privatisierung öffentlicher Aufgaben von andauernder Aktualität. Ein Thema ist das Outsourcing von Aufgaben oder Teilaufgaben der kommunalen Archive.

Die Archivierung von Unterlagen der öffentlichen Verwaltung ist eine hoheitliche Aufgabe, die den Kommunen für ihren Bereich im Landesarchivgesetz zugewiesen ist. Eine Übertragung hoheitlicher Aufgaben auf Private ist nur auf Grundlage einer Rechtsvorschrift erlaubt. Weder das Landesarchivgesetz noch die Gemeindeordnung sehen Derartiges vor. Dies bedeutet aber nicht, dass kommunale Archive überhaupt nicht mit Privaten zusammenarbeiten dürfen. Zwar ist eine vollständige Funktionsübertragung mangels gesetzlicher Grundlage ausgeschlossen, doch können einem privaten Dritten als **Verwaltungshelfer** Aufgaben zur Erfüllung nach Weisung übertragen werden. Entscheidend ist, dass dieser keine hoheitlichen Befugnisse erhält, sondern ausschließlich Hilfstätigkeiten für den Auftraggeber vornimmt, ohne dass ihm eigene Entscheidungsbefugnisse bei der Verarbeitung personenbezogener Daten zustehen. Die Übernahme von Unterlagen mit Personenbezug in das Archiv, das Nutzbarmachen der Unterlagen für die Allgemeinheit und die Entscheidung über die Herausgabe von personenbezogenem Archivgut müssen danach weiterhin in öffentlicher Hand bleiben. Dagegen ist denkbar, dass ein Privater als Auftragnehmer die Katalogisierung und die Pflege des Archivgutes nach Weisung der öffentlichen Stelle übernimmt. Das Archiv muss sicherstellen, dass der ausgewählte Dritte die datenschutzrechtlichen Anforderungen einhält.

Was ist zu tun?
Die Inanspruchnahme eines privaten Dritten als Dienstleister der Behörden ist im Regelfall im Wege der Auftragsdatenverarbeitung möglich. Der Dritte muss dann allerdings von der Behörde sorgfältig ausgewählt und überwacht werden.

4.1.3 Online-Meldedatenabruf lässt auf sich warten

Schleswig-Holstein wird langsam, aber sicher zum Schlusslicht bei der bundesweiten Umsetzung des Online-Meldedatenabrufes für öffentliche und private Stellen. Betroffen ist auch das von uns im letzten Jahr geprüfte Polizeiabrufverfahren, bei dem erhebliche Mängel festgestellt worden sind. Der Startschuss für die beabsichtigte Erneuerung der Software soll Anfang 2007 endlich fallen.

Der Gesetzgeber hat seine Hausaufgaben rechtzeitig gemacht. Bereits im Juni 2004 trat im Land ein neues Melderecht in Kraft, wonach alle öffentlichen Stellen bundesweit Meldedaten online abrufen dürfen, soweit dies zu ihrer rechtmäßigen Aufgabenerfüllung erforderlich ist. Das Gleiche gilt auch für private Stellen, wenn die anfragende Stelle den gesuchten Einwohner eindeutig identifizieren kann (27. TB, Tz. 4.1.1). Durch frühzeitige Prüfung eines bestehenden Polizeiabrufverfahrens einer Stadt (28. TB, Tz. 4.1.1) wollten wir eventuell vorhandenen **Mängeln rechtzeitig begegnen**.

Unser bisheriges Resümee ist ernüchternd. Obwohl sich der Online-Abruf von Meldedaten wie kein anderer Bereich zum Bürokratieabbau und zu **Kosteneinsparungen in der Verwaltung** eignet, ist bei der technischen Umsetzung – fast – nichts geschehen. Dabei sind die Vorteile eines automatisierten Abrufverfahrens offensichtlich. Die Meldebehörden können Personalressourcen bei der schriftlichen Auskunftserteilung einsparen; andere Behörden können ebenso wie Firmen und Bürger ihre Meldevorgänge einfacher, schneller und kostengünstiger erledigen. Allein bei der Stadt Kiel fallen jährlich etwa 75.000 Meldedatenübermittlungen an andere Behörden an.

Zugleich kann der Online-Abruf eine **erhebliche Qualitätsverbesserung** bei der Meldedatenverarbeitung bewirken. Die Richtigkeit der verarbeiteten Daten wird verbessert, weil Übertragungs-, Schreib- und Eingabefehler weitgehend ausgeschlossen werden. Die Auskunft an die Betroffenen sowie die Revisionsfähigkeit der Datenverarbeitung werden erleichtert, weil eine manipulationssichere umfassende Dokumentation und Auswertbarkeit der einzelnen Verarbeitungsschritte in automatisierten Abrufverfahren ohne bedeutsamen Mehraufwand möglich sind.

- **Polizeiabrufverfahren**

Die Beseitigung der vom ULD festgestellten Mängel im bisherigen Verfahren lohnt sich aus Sicht des Dienstleisters dataport als Betreiber nicht. Es soll deshalb ein neues Verfahren entwickelt werden, welches zugleich den Abruf von Meldedaten durch weitere öffentliche sowie private Stellen ermöglicht. Allerdings ist dataport über die Erstellung eines entsprechenden Angebotes an das Innenministerium noch nicht hinausgekommen. Für längere Zeit wird also offensichtlich das rechtswidrige alte Polizeiauskunftsverfahren im Einsatz bleiben.

- **Online-Meldedatenabruf für Behörden und private Stellen**

Eine technische Unterstützung des Abrufs von Meldedaten für Behörden und private Stellen durch dataport ist vorläufig noch nicht in Sicht. Alternativen bestehen etwa mit dem Softwareprodukt MESO, das vom ULD 2005 mit einem Gütesiegel zertifiziert worden ist. Es wird inzwischen in einem zentralen mandantenfähigen Auskunftsrechner für alle Meldebehörden in Mecklenburg-Vorpommern angeboten. Erster und einziger Anwender in Schleswig-Holstein ist seit Mitte 2006 die Stadt Neumünster.

Der technische und administrative Aufwand für ein solches Auskunftsverfahren ist nicht unerheblich. Kleinere Kommunen dürften allein damit überfordert sein. Der Kreis Nordfriesland überlegt deshalb, als Serviceleistung für seine Kommunen einen **zentralen mandantenfähigen Auskunftsrechner** zu betreiben. Ein Durchbruch für Schleswig-Holstein, wie er bereits in Hamburg (Hamburg Gateway) und Mecklenburg-Vorpommern gelungen ist, wäre dies allerdings noch nicht.

Was ist zu tun?
Das Innenministerium sollte im Rahmen seiner Koordinierungsfunktion mit Nachdruck die technische Unterstützung eines Abrufs von Meldedaten durch Behörden und private Stellen organisieren und damit gleichzeitig die noch immer bestehenden Mängel im Polizeiabrufverfahren beseitigen.

4.1.4 Was wird zur Feststellung der Zweitwohnungssteuerpflicht benötigt?

Die Angaben Betroffener zu ihrer Zweitwohnungssteuerpflicht werden von den Kommunen zunehmend auf ihre Richtigkeit überprüft. Daten über Gäste sind dafür in der Regel nicht erforderlich und müssen dem Steueramt nicht mitgeteilt werden.

Das Steueramt einer Stadt hatte den Eigentümer einer Ferienwohnung aufgefordert, zum Nachweis der Zweitwohnungssteuerpflicht eine **namentliche Einzelaufstellung** darüber vorzulegen, wer dessen Wohnung in welchem Zeitraum genutzt hat. Bei unserer Überprüfung stellten wir fest, dass die Höhe der vom Betroffenen zu zahlenden Zweitwohnungssteuer nach der Kurabgabesatzung tatsächlich davon abhängig war, für welche Dauer eine Vermietung der Wohnung erfolgt war. Die Forderung nach einer Einzelaufstellung der realen Vermietzeiträume war deshalb plausibel. Dies galt jedoch nicht für die Forderung einer namentlichen Aufstellung der Feriengäste.

Die Stadt erläuterte ihre Anforderung namentlicher Einzelaufstellungen damit, nur so Eigenvermietungen aufdecken zu können. Bei Steuerpflichtigen, die ihre Wohnung selbst vermieten, sei eine Kontrolle der **Eigenvermietung** über die Angaben aus der Kurabgabeerhebung möglich, da hier zulässigerweise ein entsprechender Abgleich erfolge. Bei Einschaltung eines Vermietungsbüros fehlen entsprechende Angaben, da diese Büros die Kurabgabe nur summarisch gegenüber der Kurverwaltung nachweisen. Für diese Fälle haben wir mit der Stadt vereinbart, dass ihr künftig eine **Bescheinigung** des Vermietungsbüros ausreicht, wenn darin bestätigt wird, ob und gegebenenfalls für welchen Zeitraum eine Vermietung an Personen stattgefunden hat, die den gleichen Nachnamen des Steuerpflichtigen bzw. seines Ehegatten tragen. Auf diese Weise kann auf eine Angabe von Gästedaten künftig verzichtet werden.

Was ist zu tun?
Kommunen sollten ihre Maßnahmen zur Kontrolle der Zweitwohnungssteuerpflicht sorgfältig auf ihre Erforderlichkeit hin überprüfen und die Grundsätze der Datensparsamkeit und Datenvermeidung beachten.

4.1.5 Welche Daten sollen auf eine Gästekarte?

Elektronische Kurkarten kommen immer mehr in Mode. Sie dienen der Kontrolle der Kurabgabeerhebung und der Aufzeichnung des Gästeverhaltens bei der Nutzung der Kureinrichtungen. Hierüber soll eine Optimierung des Angebots erreicht werden. Auf eine personenbezogene Speicherung von Gästedaten auf den Karten kann vollständig verzichtet werden.

Viele Eingaben erreichten uns zur neu eingeführten elektronischen Gästekarte der Insel Sylt. Den Betroffenen war zumeist nicht klar, welche Daten darauf gespeichert und in welchem Umfang erhobene Daten weiterverarbeitet wurden. Wir stellten fest, dass auf den Karten, die von der Kurverwaltung entsprechend der Bettenzahl an die Vermietbetriebe ausgegeben wurden, über einen Code **lediglich der jeweilige Vermietbetrieb** gespeichert war. Die Karten konnten von Gast zu Gast weitergegeben werden. Da die Kurabgabe über den Vermietbetrieb abgerechnet wurde, konnte die Kurverwaltung bei Nutzung der Gästekarten überprüfen, ob die anfallenden Kurabgaben vom Vermietbetrieb abgeführt worden sind.

Ähnlich war das Verfahren für die Inhaber von **Jahreskurkarten** bzw. für Einheimische gestaltet. Sämtliche Inhaber dieser Karten wurden einer einheitlichen fiktiven Anschrift zugeordnet. Es erfolgte nur eine Zuordnung zur jeweiligen Wohnsitzgemeinde. Da mit der Erfassung der Gästekarten bei der Nutzung der Kureinrichtungen keine personenbezogenen Daten erhoben wurden, konnten wir den Petenten mitteilen, dass gegen das geprüfte Verfahren keine datenschutzrechtlichen Bedenken bestehen.

Was ist zu tun?
Kurverwaltungen können beim Einsatz elektronischer Gästekarten auf die Verarbeitung personenbezogener Daten verzichten. Den Gästen sollte durch geeignete Maßnahmen transparent gemacht werden, welche Daten auf den Karten gespeichert werden und in welchem Umfang und zu welchem Zweck eine Weiterverarbeitung erhobener Daten erfolgt.

4.1.6 Erhebung von Lichtbilddaten durch die Passbehörden

Die Speicherung digitaler Lichtbilddaten in Reisepässen ist seit mehr als einem Jahr Realität. Die Technik der Datenerhebung entspricht noch nicht den Standards, die an ein modernes E-Government-Verfahren zu stellen sind. Für die Bürger bedeutet dies eine unnötige Belastung.

Die elektronische Speicherung von biometrischen Merkmalen auf Ausweisen und Pässen bringt grundsätzliche Gefahren im Hinblick auf die Sicherheit mit sich (Tz. 8.5) und verursacht praktische Probleme. Mit Aufnahme des Funkchips in den Reisepass wird die Maschinenlesbarkeit der darin enthaltenen **Bilddaten** massiv erhöht. Die neue Technik hat nicht nur einen bürgerrechtlichen, sondern auch einen finanziellen Preis; dies spüren die Bürger bei der Gebührenerhebung für den Pass und zuvor bei den Kosten für ein biometrietaugliches Lichtbild, das

wegen des notwendigen „ernsten Blickes“ der Betroffenen für Bewerbungsverfahren oder für andere Zwecke absolut nutzlos ist.

In der Praxis fertigt der Fotograf mit einer Digitalkamera ein elektronisches Lichtbild, welches für den Kunden in Papier ausgedruckt wird. Damit geht der Betroffene zur Passbehörde, wo es über einen Scanner wieder in eine **elektronische Form** zurückgewandelt und anschließend so weiterverarbeitet wird. Das Papierbild wird nach dem Scannen nicht mehr benötigt. Im ungünstigen Fall entspricht das Papierbild nicht den biometrischen Anforderungen, sodass sich Betroffene erneut auf den Weg zum Fotografen machen müssen.

Für das ULD stellt sich die Frage, weshalb die Passbehörden die erforderlichen Daten nicht in der geeigneten Form selbst erheben. **Digitalfotografie** ist heute für Behörden durchaus beherrschbar; selbst Fotokabinen ohne Personal sind dazu in der Lage. So wird niemand auf die Idee kommen, die künftig zu erhebenden Fingerabdrücke von privaten Dritten erfassen und ausdrucken zu lassen, um sie später für das Passverfahren wieder einzuscannen.

Die notwendigen Aufwendungen für Hard- und Software der Digitalfotografie sind überschaubar. Entsprechende Schnittstellen für digital erfasste Fotos sind in den gängigen automatisierten Passverfahren bereits vorhanden. Die Bürger würden die entstehenden aufwandbezogenen Gebühren der Passbehörden sicher gern übernehmen, zumal die deutlich höheren Kosten für das Papierbild und Laufereien zum Fotografen eingespart werden können. Für die Passbehörden würden Probleme mit der fehlenden **Biometrietauglichkeit** vieler Bilder der Vergangenheit angehören. Im Bedarfsfall könnte ohne großen Aufwand ein neues Digitalbild gefertigt werden. Die Bürger wären über einen solchen Service bestimmt hocherfreut. Dies gilt ebenso für unsere Dienststelle, denn eine effiziente und bürgerfreundliche Form der Datenerhebung ist ein Anliegen des Datenschutzes.

Was ist zu tun?
Passbehörden sollten die Möglichkeiten der Digitalfotografie selbst nutzen und damit die zurzeit mit viel Aufwand verbundenen Medienbrüche bei der Erhebung von Lichtbilddaten in Papierform beseitigen.

4.1.7 Keine vollständige Firmenliste aus dem Gewerberegister für den NDR

Auch der NDR darf nur für ihn erforderliche Daten erhalten. Die Übermittlung einer vollständigen Firmenliste aus dem Gewerberegister einer Kommune ist unzulässig.

Der NDR hatte eine Stadt „für seine Tätigkeit im Bereich der Erhebung von Rundfunkgebühren“ um Zusendung einer Gewerbe- bzw. Firmenadressenliste mit allen gemeldeten Unternehmen gebeten. Die Gewerbeordnung erlaubt neben Einzelauskünften auch solche **Listenauskünfte**, allerdings nur, wenn alle in der Liste enthaltenen Daten tatsächlich zur Aufgabenerfüllung des Empfängers erforderlich sind.

Der NDR hatte sein Auskunftsbegehren nicht näher begründet. Unsere gemeinsam mit der Stadt vorgenommene **Schlüssigkeitsprüfung** ergab, dass zumindest ein Teil der Betriebe bereits bei der Gebühreneinzugszentrale (GEZ) angemeldet sein, ein anderer Teil nicht die Rundfunkteilnehmereigenschaft erfüllen dürfte. In diesen Fällen wäre die Datenübermittlung nicht zur Erhebung von Rundfunkgebühren erforderlich gewesen. Die Stadt musste das Ersuchen deshalb ablehnen.

Was ist zu tun?
Kommunen sollten bei Listenauskünften aus dem Gewerberegister sorgfältig prüfen, ob die zu übermittelnden Daten zur Aufgabenerfüllung des Empfängers erforderlich sind. Dies gilt auch für entsprechende Anfragen des NDR oder der für den NDR bzw. die GEZ tätigen Rundfunkgebührenbeauftragten.

4.1.8 Datennutzung für Vollstreckungszwecke

Gemeinsam mit dem Polizeirecht soll das Vollstreckungsrecht novelliert werden. Danach werden die Befugnisse für die Vollstreckung öffentlich-rechtlicher Forderungen erheblich ausgeweitet. Das Steuergeheimnis sowie das datenschutzrechtliche Zweckbindungsgebot dürfen dabei nicht auf der Strecke bleiben.

- **Gesetzgebungskompetenz**

Öffentlich wurde nur über das Polizeirecht gestritten (Tz. 4.2.1). Brisant sind aber auch die geplanten Vollstreckungsregeln: Künftig sollen Daten, die unter das Steuergeheimnis fallen, auch für die Vollstreckung anderer öffentlich-rechtlicher Forderungen verarbeitet werden dürfen. Dabei wird offensichtlich übersehen, dass die Abgabenordnung diesbezüglich eine **abschließende Bundesregelung** enthält. Eine Gesetzgebungskompetenz zur Modifikation des Steuergeheimnisses im Landesverwaltungsgesetz fehlt dem Land. Die Regelung würde – jedenfalls bei Steuerarten, für die die Abgabenordnung unmittelbar gilt – gegen das Grundgesetz verstoßen. Die abschließende Regelungskompetenz des Bundes wird auch dadurch nicht durchbrochen, dass die Abgabenordnung die Offenbarung von Steuerdaten und damit gegebenenfalls auch eine zweckändernde Weiterverarbeitung der Daten auf der Grundlage einer ausdrücklichen Regelung erlaubt. Da es sich bei solchen Regelungen um eine „Offenbarungsregelung im Bereich der steuerlichen Verfahren“ handelt, können diese nur vom Bundesgesetzgeber getroffen werden.

- **Fehlende Zweckbindung**

Die vorgesehene Zweckfestlegung „Vollstreckung öffentlich-rechtlicher Forderungen“ ist rechtssystematisch nicht möglich. Durch das öffentliche Recht wird der Verwaltung die Erfüllung bestimmter Aufgaben zugewiesen. Diese sind nach sachlichen Gesichtspunkten durch den Anwendungsbereich der einzelnen Gesetze gegliedert. So dient das Melderecht der Registrierung und Identitätsfeststellung der Bürger, das Beamtenrecht der Ausgestaltung des Rechtsverhältnisses zwischen den Dienstherren und ihren Beamten und das Waffenrecht der Regelung des

zulässigen Umgangs mit Waffen und Munition. Werden die Aufgaben von Servicestellen – wie Poststelle, Schreibdienst, Kasse und Vollstreckung – wahrgenommen, so erhält die Datenverarbeitung dadurch keinen neuen eigenen Verarbeitungszweck. Die einzelnen genannten Querschnittsaufgaben sind vielmehr **Annex** (Unterzweck) zu den jeweiligen Kernaufgaben Melderecht, Beamtenrecht oder Waffenrecht.

Um über den Umweg der Vollstreckung eine vollständige **Aufhebung der Zweckbindung** zu verhindern, soll nach dem Entwurf eine Weiterverarbeitung der Daten aus den verschiedenen Verwaltungsbereichen nur für Vollstreckungszwecke zulässig sein. Ob das Problem durch die geplante neue Zweckbindungsregelung gelöst werden kann, muss bezweifelt werden, da aus fachlichen Gründen oft ein umfassender Austausch zwischen Kernaufgabe und Vollstreckung notwendig ist. Vor diesem Hintergrund fordern wir, auf zusätzliche Verarbeitungsbefugnisse bei den besonders sensiblen Steuerdaten zu verzichten.

- **Datenerhebungsbefugnis bei anderen öffentlichen und privaten Stellen**

Weiterhin sollen alle natürlichen und juristischen Personen verpflichtet werden, **zur Durchführung einer Vollstreckung** Auskünfte in erheblichem Umfang an die Vollstreckungsbehörden zu erteilen. Eine derart weitreichende Generalermächtigung besteht bisher nur für Finanzbehörden in Steuersachen. Dabei ist zu berücksichtigen, dass für diese Daten das Steuergeheimnis gilt. Wir bezweifeln, dass eine solche Norm unter Beachtung des Verhältnismäßigkeitsgrundsatzes auf die Vollstreckung aller öffentlich-rechtlichen Forderungen übertragen werden kann.

Die Besteuerung der Bürger stellt einen besonders intensiven Eingriff in deren Grundrechtspositionen dar, der ohne konkrete Gegenleistung des Staates erfolgt. Da die Leistungsfähigkeit der Bürger ein wesentliches Kriterium für die Höhe der zu zahlenden Steuer ist, müssen aus Gründen der Steuergerechtigkeit für die Ermittlung der Bemessungsgrundlagen beim Bürger und die **Durchsetzung der Steuerschuld** weitreichende Befugnisse des Staates akzeptiert werden. Der Steuerbereich wird deshalb zu Recht dem Kernbereich hoheitlicher Tätigkeit zugerechnet.

Mit der beabsichtigten Änderung soll nun **jede öffentlich-rechtliche Forderung** in ihrer rechtlichen Bedeutung einer Steuerforderung gleichgestellt werden. Etwaige Liegeplatzgebühren für die Nutzung eines Sportboothafens oder Nutzungsentgelte in der Bücherei dürfen aber mit Steuerforderungen nicht gleichgesetzt werden. Die einzige Gemeinsamkeit, die Finanzierung der öffentlichen Aufgabenträger, rechtfertigt nicht die Einräumung umfassender Privilegien, wie sie für das Steuerverfahren bestehen.

Zudem ist der praktische Sinn der Regelung fraglich. Anfragen bei Dritten setzen die Kenntnis der Vollstreckungsbehörde voraus, dass dort für die Vollstreckung erhebliche Daten vorliegen. Bloße Verdachtsanfragen wären wegen des Verstoßes gegen das Erforderlichkeitsprinzip unzulässig. Solche Erkenntnisse sollen aber

gerade erst ermittelt werden. Die **Ermittlung von Arbeitgebern** zum Zweck der Gehaltspfändung ist, wie in der Gesetzesbegründung angegeben, so jedenfalls kaum möglich. Auch die in der Gesetzesbegründung genannten Telekommunikationsunternehmen oder Stadtwerke verfügen in der Regel nicht über vollstreckungsrelevante Daten, insbesondere nicht über Angaben zu Arbeitgebern.

Heikel ist der Umstand, dass mit jeder Anfrage einer Vollstreckungsbehörde die **Tatsache der Vollstreckung** bei der angefragten Stelle bekannt wird. Wegen der Vollstreckung einer kleinen Gebührenforderung kann es so dazu kommen, dass die finanzielle Leistungsfähigkeit des Betroffenen von der angefragten Stelle insgesamt in Zweifel gezogen und die Stadtwerke, das Telekommunikationsunternehmen oder die Bank ihrerseits die Geschäftsbeziehungen zu dem Betroffenen vorsorglich reduzieren oder ganz beenden. Auch aus diesem Grund sollte auf die geplante Regelung verzichtet werden.

Was ist zu tun?
Die geplante Regelung sollte vom Gesetzgeber sorgfältig auf ihre Erforderlichkeit und Geeignetheit überprüft werden. Eine zweckändernde Weiterverarbeitung von Daten für Vollstreckungszwecke kann allenfalls für Daten zugelassen werden, die keinem besonderen Berufs- oder Amtsgeheimnis unterliegen.

4.1.9 Keine Personendaten auf der Tagesordnung der Gemeindevertretersitzung

Gemeindevertretersitzungen sind grundsätzlich öffentlich. Sollen in der Sitzung persönliche Verhältnisse von Privatpersonen behandelt werden, hat diese unter Ausschluss der Öffentlichkeit stattzufinden. Auch die Tagesordnung darf keinen Aufschluss über die Betroffenen geben.

Ein Gemeindevertreter bat uns um Beratung im Vorfeld einer Gemeindevertretersitzung. Ein Grundstückseigentümer hatte sich beschwert, dass er **namentlich auf der Tagesordnung** der kommenden Sitzung aufgeführt sei. In der Sitzung, die öffentlich stattfinden sollte, ginge es um den Abschluss eines städtebaulichen Vertrages zwischen ihm und der Gemeinde.

Nach der Gemeindeordnung sind die Sitzungen der Gemeindevertretung grundsätzlich öffentlich. Die Öffentlichkeit ist aber auszuschließen, wenn überwiegende Belange des öffentlichen Wohls oder berechtigte Interessen Einzelner es erfordern. Gründe des öffentlichen Wohls liegen vor, wenn das Interesse der Öffentlichkeit an einer vertraulichen internen Beratung im Einzelfall größer ist als das Informationsbedürfnis der Öffentlichkeit. Dies ist generell der Fall, wenn die Vertraulichkeit bzw. Geheimhaltung durch sondergesetzliche Vorschriften vorgeschrieben ist. Die Wahrung datenschutzrechtlicher Belange einzelner Personen ist ein berechtigtes Einzelinteresse. **Grundstücksveräußerungen** oder Grundstückserwerbe, Darlehensaufnahmen, Personalangelegenheiten, Auftragsvergaben, Bauanträge, Steuerstundungen, Steuererlasse usw. sind daher grundsätzlich in nicht öffentlicher Sitzung zu behandeln.

Die Gemeindeordnung sieht vor, dass Zeit, Ort und Tagesordnung einer jeden Gemeindevertretersitzung örtlich bekannt gemacht werden. In Ermangelung gesetzlicher Konkretisierungen finden ergänzend die allgemeinen Bestimmungen des LDSG Anwendung. Eine Veröffentlichung personenbezogener Daten Dritter ist danach nur zulässig, wenn eine rechtfertigende Norm vorliegt oder der Betroffene eingewilligt hat. Diese Voraussetzungen lagen nicht vor. Die Verpflichtung zur **Offenbarung der Tagesordnung** ist keine Ermächtigung zur Offenbarung persönlicher Daten. Zudem hatte der Eigentümer ausdrücklich der Bekanntgabe widersprochen.

Was ist zu tun?
Bei der Durchführung von Gemeindevertretersitzungen und beim Abfassen von Tagesordnungen sind die datenschutzrechtlichen Belange Betroffener zu wahren und gegebenenfalls die Öffentlichkeit auszuschließen.

4.1.10 Beteiligung Dritter in Bewerbungsverfahren

Für die Verarbeitung von Bewerberdaten ist die Zustimmung der Betroffenen unverzichtbar. Diese sind frühzeitig und umfassend über die einzelnen Bearbeitungsschritte des Dienstherrn zu informieren. Dies gilt insbesondere, wenn Dritte am Verfahren beteiligt werden. Sind Betroffene damit nicht einverstanden, können sie gegebenenfalls ihre Bewerbung zurückziehen.

Unter welchen Voraussetzungen darf eine Fachhochschule Kontakt mit dem bisherigen Dienstherrn der Betroffenen aufnehmen, um die mit einer möglichen Versetzung verbundenen Versorgungslasten zu klären? In einem Bewerbungsverfahren hatte sich die Einstellung bereits stark konkretisiert; die Fachhochschule hatte zum Zeitpunkt der **Kontaktaufnahme** bereits einen „Ruf“, also eine Zusage erteilt. Unbestritten war, dass man bei einer solchen Ruferteilung durch Fachhochschulen auch ohne erfolgte Annahme von einer Wechselbereitschaft des Bewerbers ausgehen kann.

Die Entscheidung über eine Bewerbung ist nicht von der Aufteilung der Versorgungslasten abhängig. Dennoch ist es in Zeiten der Budgetierung durchaus vertretbar, dass im Rahmen der **Finanzplanung** einer Hochschule so früh wie möglich die relevanten Faktoren einbezogen werden. Daher war es nicht zu beanstanden, dass die Verhandlungen über die Versorgungslasten nicht auf einen Zeitpunkt nach Rufannahme verschoben wurden.

Fraglich blieb, ob und inwieweit die Betroffene über die beabsichtigten Verhandlungen mit dem bisherigen Dienstherrn aufzuklären war, um ihr die Möglichkeit für Einwendungen, gegebenenfalls sogar für eine Rücknahme der Bewerbung zu eröffnen. Das Landesdatenschutzgesetz enthält eine entsprechende **Verpflichtung zur Aufklärung** bei beabsichtigten Datenübermittlungen, soweit es nach den Umständen des Einzelfalles angemessen erscheint. Konkret hätte es hier keinen unverhältnismäßigen Aufwand bedeutet, die Betroffene schriftlich über die beabsichtigte Kontaktaufnahme mit dem bisherigen Dienstherrn aufzuklären. Ein pau-

schaler Hinweis anlässlich einer Probevorlesung, dass hiermit die Vertraulichkeit der Bewerbung nicht mehr gewährleistet sei, reichte nicht aus. Die Fachhochschule sicherte inzwischen zu, bei künftigen Verfahren die Aufnahme der Verhandlungen mit dem bisherigen Dienstherrn schriftlich den Betroffenen anzuzeigen.

Was ist zu tun?
Beschäftigungsdienststellen sollten im Bewerbungsverfahren bereits mit der Eingangsbestätigung die Betroffenen darüber aufklären, wer zu welchem Zeitpunkt am Bewerbungsverfahren beteiligt wird. Ergeben sich später Änderungen oder Ergänzungen, sollten die Bewerber auch darüber unverzüglich in Kenntnis gesetzt werden.

4.1.11 Informationsansprüche des Gesamtpersonalrates

Gesamtpersonalräte verfügen nach dem Mitbestimmungsgesetz nur über eine eingeschränkte Zuständigkeit. Ihre Informationsansprüche gehen nicht so weit wie die örtlicher Personalräte und Stufenvertretungen.

Im letzten Tätigkeitsbericht (28. TB, Tz. 4.1.9) hatten wir darauf hingewiesen, dass nach dem Mitbestimmungsgesetz schriftliche Unterlagen und in Dateien gespeicherte Daten der Dienststelle dem Personalrat in geeigneter Weise zugänglich zu machen sind, allerdings nur, soweit dies für die Erfüllung der Aufgaben des Personalrates erforderlich ist. Für den **Sonderfall** des Gesamtpersonalrates geht dieser Anspruch aber nicht so weit wie für örtliche Personalräte und Stufenvertretungen. Personalräte vor Ort werden in der Regel einzelfallbezogen an Personalmaßnahmen beteiligt und haben insoweit ein Initiativrecht. Diese Voraussetzung ist beim Gesamtpersonalrat nicht gegeben. Er ist nach dem Mitbestimmungsgesetz nur **zuständig** für Angelegenheiten, die mehrere in ihm zusammengefasste Dienststellen betreffen und die nicht durch die einzelnen Personalräte und Stufenvertretungen innerhalb ihres Geschäftsbereiches geregelt werden können. Damit sind sämtliche Personalentscheidungen dem Gesamtpersonalrat entzogen, da an den Entscheidungen im Einzelfall nur der zuständige örtliche Personalrat zu beteiligen ist.

Aus den anders gelagerten Aufgaben des Gesamtpersonalrates ergibt sich ein entsprechend reduzierter **Unterrichtungsanspruch**. Eine generelle Bereitstellung von Personallisten mit Beurteilungsnoten, Eingruppierungsdetails oder Ähnlichem im Hinblick auf die Aufgabenstellung des Gesamtpersonalrates ist nicht erforderlich. Eine Übermittlung von Personalaktendaten kommt allenfalls dann in Betracht, wenn der Gesamtpersonalrat seinen Informationsbedarf im konkreten Fall gegenüber der Dienststelle schlüssig begründet hat.

4.1.12 Datenweitergabe im Rahmen einer Beihilfeablöseversicherung

Die Übermittlung von Personalaktendaten an eine private Versicherung zur Durchführung einer Beihilfeablöseversicherung durch den Dienstherrn bedarf der Einwilligung der Betroffenen. Eine Übermittlung von gesundheitsbezogenen Beihilfedaten bedürfte darüber hinaus jeweils einer Einzelfalleinwilligung.

Diese rechtlichen Anforderungen verfahrenstechnisch praktikabel umzusetzen, ist kaum möglich. Mit den kommunalen Spitzenverbänden und der Versorgungsausgleichskasse der Kommunalverbände wurde deshalb eine Lösung erarbeitet, die versicherungsrechtlichen Bedürfnissen entspricht und ohne die Übermittlung von Beihilfedaten auskommt. Gemäß einer an dem Schutzzweck der beamtenrechtlichen Normen ausgerichteten Auslegung des Begriffs **Beihilfedaten** handelt es sich dabei um Angaben, aus denen sich die Art der gewährten Leistung (z. B. Arztrechnungen oder Rezepte) oder die Art der Erkrankung ergibt. Würden solche Daten für die Durchführung einer Beihilfeablöseversicherung benötigt, müssten Betroffene jeweils nach Erteilung des Beihilfebescheides fallweise in die Datenübermittlung an die Versicherung einwilligen. Die Leistungspflicht der Versicherung wäre von einem aufwendigen Verfahren und einer umfassenden Mitwirkung der Betroffenen abhängig. Eine Übermittlung von Beihilfedaten für Versicherungszwecke musste deshalb von vornherein vermieden werden.

Anders stellte sich die Situation bei der „normalen“ Einwilligung für Personalaktendaten dar. Hier kann bzw. wird die Kommune die Versicherung erst abschließen, wenn der Betroffene seine **Einwilligung** zur Übermittlung der Daten erteilt hat und damit die Leistungspflicht der Versicherung **grundsätzlich** gewährleistet ist. Für den Fall des Widerrufs der Einwilligung durch den Betroffenen sollte sich die Kommune gegenüber der Versicherung ein Sonderkündigungsrecht vorbehalten.

Mit der Versicherung konnte einvernehmlich erzielt werden, dass für die Beitragskalkulation die Übermittlung von Personalnummer, anspruchsberechtigter Person (Berechtigter/Ehegatte/Kind), Geburtsjahr, Geschlecht und Krankenversicherungsstatus ausreicht. Für die Leistungsauszahlung wird die Versorgungsausgleichskasse der Kommunalverbände im Auftrag der Kommunen der Versicherung eine quartalsweise Auswertung der aufgelaufenen Beihilfeaufwendungen in Form eines **Abrechnungsnachweises**, aufgeschlüsselt nach Antragsteller, Ehegatte und beihilfeberechtigten Kindern, zur Verfügung stellen. Damit dürfte jetzt eine praktikable und datenschutzgerechte Lösung für die Durchführung einer Beihilfeablöseversicherung gefunden worden sein.

4.2 Polizei und Nachrichtendienste

4.2.1 Neues Polizeirecht – Verfassungsmäßigkeit weiter fraglich

Das neue Polizeirecht sieht eine Reihe von erweiterten Befugnissen zur Erhebung und Verarbeitung personenbezogener Daten vor. In der öffentlichen Diskussion des Entwurfes sahen wir uns in unserer Kritik weitgehend bestätigt, so bei der Anhörung im Innen- und Rechtsausschuss und durch ein Gutachten des Wissenschaftlichen Dienstes.

Das ULD hatte im letzten Tätigkeitsbericht seine Bedenken gegen die zunehmende Erweiterung polizeirechtlicher Befugnisse im **Gefahrenvorfeld** vorgestellt (28. TB, Tz. 4.2.1). Die Kritik an solchen Vorfeldbefugnissen hat sich durch die Entscheidung des Bundesverfassungsgerichts zur Rasterfahndung vom 4. April 2006 als begründet erwiesen. Dennoch wurden in dem Entwurf an den folgenden Eingriffsbefugnissen festgehalten:

- **Videoüberwachung** und -aufzeichnung im öffentlichen Raum,
- präventive **Telekommunikationsüberwachung**,
- **Kfz-Kennzeichenüberwachung**,
- **erweiterte Kontrollbefugnisse** bei Schleierfahndung und Identitätsfeststellung,
- Erweiterung der **Generalermächtigung** zur vorbeugenden Straftatenbekämpfung.

Lediglich die im ersten Referentenentwurf vorgesehene und vom ULD scharf kritisierte **verdachtsunabhängige Tonaufzeichnung** in öffentlich zugänglichen Räumen wurde gestrichen.

Mit dem **Vorgangsbearbeitungssystem** führt der Entwurf einen bislang im Polizeirecht unbekannten Begriff ein und gibt den Polizeibehörden extrem weit reichende Speicherungs- und Abrufbefugnisse. Wenn die Polizei Daten erhoben hat, erfolgt dies zur Erfüllung einer konkreten Aufgabe, also für einen **konkreten Zweck**. Speichert sie diese Daten, so darf sie das bislang, wenn es zur Erfüllung der Aufgabe notwendig ist. Nach der neu geplanten Regelung kann die Speicherung auch zu einem anderen als dem Erhebungszweck erfolgen. Darüber hinaus kann die Polizei die gespeicherten Daten für jeden anderen Zweck verwenden, wenn dieser – allgemein – im Rahmen ihrer Aufgaben

Im Wortlaut: Volkszählungsurteil

Ein Zwang zur Angabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind. … Auch werden sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken müssen.

(Bundesverfassungsgericht, NJW 1984, 422)

liegt. Damit würde die Speicherung in Zukunft weitgehend losgelöst von der ursprünglich zu erledigenden Aufgabe möglich sein. Die Grundsätze der **Zweckbindung** und der **Erforderlichkeit** der Datenverarbeitung würden in weiten Teilen ausgehebelt. Jede Bürgerin und jeder Bürger kann davon betroffen sein: Nicht nur Daten über für eine Gefahr verantwortliche Personen werden in Vorgangsbearbeitungssystemen gespeichert, sondern z. B. auch Zeugen, Opfer oder Hinweisgeber. Die Neuregelung würde zu einer Aushöhlung des Rechts auf informationelle Selbstbestimmung führen. Der Wissenschaftliche Dienst des Landtags spricht zutreffend von einer „Entwidmung" der Daten (siehe zum Vorgangsbearbeitungssystem @rtus Tz. 4.2.3).

Im Rahmen einer **Sachverständigenanhörung** haben wir nochmals zu dem Gesetzentwurf Stellung genommen. Praktisch alle weiteren hinzugezogenen Sachverständigen und Verbände haben die vom ULD dargestellten verfassungsrechtlichen Mängel des Entwurfs bestätigt. Die verfassungsrechtliche Bestandskraft verschiedener geplanter Vorschriften wurde bezweifelt, weil diese nicht verhältnismäßig sind und nicht dem verfassungsrechtlichen Bestimmtheitsgebot (siehe Kasten) entsprechen. Ein Beispiel ist die Generalklausel zur Datenerhebung im Rahmen der vorbeugenden Straftatenverhütung. Dort werden die Begriffe der „organisierten" oder „serienmäßig begangenen" Straftaten eingeführt. Ebenso wie das ULD hielten auch die Gewerkschaft der Polizei, mehrere Richterverbände und ein früherer Bundestagsvizepräsident diese Formulierungen für zu unpräzise. Bei der Kfz-Kennzeichenerfassung – um ein anderes Beispiel zu nennen – bleibt unklar, was unter „Fahndungsbestand" zu verstehen sein soll. **Klar gefasste verhältnismäßige Regelungen** sind nicht nur aus Sicht der betroffenen Bürgerinnen und Bürger ein absolutes Muss. Auch den handelnden Polizeibeamtinnen und Polizeibeamten muss im Einsatzgeschehen durch klare gesetzliche Handlungsrichtlinien der Rücken freigehalten werden.

? ***Verfassungsrechtliches Bestimmtheitsgebot***

*Das **verfassungsrechtliche Bestimmtheitsgebot** soll das Verwaltungshandeln für die Bürgerinnen und Bürger vorhersehbar und für die Gerichte überprüfbar machen. Dies ist nur möglich, wenn aus den Eingriffsnormen klar erkennbar ist, welche Handlungsmaßstäbe für die Verwaltungsbehörden gelten. Zu unbestimmt ist eine Norm, wenn sich z. B. die Polizei die Maßstäbe für ihr Eingreifen selbst zurechtlegen muss. Dies kann etwa der Fall sein, wenn der Gesetzgeber unscharfe Begriffe verwendet, die in der Rechtsprechung und Rechtswissenschaft bislang nicht vorkommen (z. B. „Verfestigung" von Gefahren).*

Uns wurde während des gesamten Gesetzgebungsverfahrens immer wieder vorgeworfen, wir nähmen uns selbst zu wichtig und wir hätten **keine verfassungsrechtliche Verwerfungskompetenz**. Eine solche Kompetenz hat das ULD in der Tat nicht. Es ist aber unsere gesetzliche Aufgabe, dem Gesetzgeber im Vorwege die aus unserer Sicht bestehenden datenschutzrechtlichen Risiken mitzuteilen. Unser einziges Ziel war es, eine fundierte fachliche Diskussion zu den einzelnen Vorschriften anzustoßen. Wir hätten gerne zur Kenntnis genommen, aus welchen – fachlichen oder verfassungsrechtlichen – Gründen das Innenministerium unsere

Kritikpunkte für unbeachtlich hielt bzw. hält. Dieses hat sich jedoch leider einer Fachdiskussion mit uns oder auch im Landtag verweigert.

Die Stellungnahme des ULD zum Regierungsentwurf ist zu finden unter

www.datenschutzzentrum.de/polizei/060418-lvwg.htm

Eine Übersicht zu den Stellungnahmen der Sachverständigen ist veröffentlicht unter

www.datenschutzzentrum.de/polizei/polizeirecht.htm

Kurz vor Redaktionsschluss erreichte uns ein an die Fraktionen des Landtags gerichtetes **Papier des Innenministeriums** mit aktuellen Änderungsvorschlägen zum Polizeirechtsentwurf. Das darin vom Innenminister geäußerte Ziel, verfassungsrechtliche Zweifel ausräumen zu wollen, unterstützen wir nachdrücklich. Die Vorschläge führen teilweise zu Verbesserungen. So werden einige Eingriffsschwellen für polizeiliche Datenerhebungsmaßnahmen angehoben, etwa bei der Telekommunikationsüberwachung zur Gefahrenabwehr.

Die Vorschläge räumen unsere **verfassungsrechtlichen Bedenken** aber nicht vollständig aus. So wird z. B. bei der geplanten Regelung zu Vorgangsbearbeitungssystemen – statt den Tatbestand klar und bestimmt zu fassen oder auf eine Änderung zu verzichten – ein Satz aufgenommen, wonach „zusätzliche Aufgaben und Eingriffsbefugnisse … nicht zugewiesen“ werden sollen. Sinn und Zweck von Gesetzen ist es, Aufgaben und Eingriffsbefugnisse zu regeln. Der neue Regelungsvorschlag bleibt uns daher in seiner Bedeutung verborgen. Das ULD nahm gegenüber den Fraktionen zu den neuen Vorschlägen Stellung.

Was ist zu tun?
Vor der Verabschiedung des Entwurfes muss dieser unter Berücksichtigung der verfassungsrechtlichen Bedenken überarbeitet werden. Das ULD steht zur Beratung zur Verfügung.

4.2.2 Auskunft an Betroffene durch die Polizei – ein datenschutzrechtlicher GAU

Die Menschen haben einen verfassungsrechtlich garantierten Anspruch auf Auskunft über die zu ihrer Person gespeicherten Daten. In der Vergangenheit kam es immer wieder zu unrichtigen oder unvollständigen Auskünften durch die Landespolizei. Dies hat der Innenminister im Landtag eingestanden und Besserung zugesagt.

Wer in Datenbanken oder Akten der Polizei gespeichert ist, hat einen im Landesverwaltungsgesetz konkretisierten **Anspruch** auf umfassende unentgeltliche Auskunft über die zu ihm gespeicherten Daten. Es handelt sich um eine klare, über lange Zeit bewährte Regelung. Unsere Erwartung, dass deren praktische Umsetzung keine größeren Probleme verursachen könnte, erwies sich als falsch. Anhand von Eingaben mussten wir feststellen, dass es Probleme bei der Ausgestaltung des Auskunftsverfahrens gab und die Befugnis zur Auskunftsverweigerung überdehnt wurde.

Die Probleme bei der Ausgestaltung des Verfahrens (28. TB, Tz. 4.2.5) haben den Innen- und Rechtsausschuss des Landtags veranlasst, über die Praxis der Auskunftserteilung der Landespolizei einen Bericht zu erbitten. Das ULD hat dem Landtag im September 2006 einen **Sonderbericht** mit einzelnen Fallbeispielen vorgelegt.

Die **teilweise unvollständige Auskunftserteilung** hatte einen Grund darin, dass nicht alle automatisierten Datenverarbeitungssysteme der Polizei des Landes Schleswig-Holstein und der Verbundanwendungen (INPOL) beim Bundeskriminalamt (BKA) abgefragt wurden. Die Einzelfälle konnten inzwischen nachgebessert werden. Es handelte sich dabei aber nicht um „Ausreißer“, vielmehr bestanden systembedingte Mängel im Verfahren. Bereits im Juli 2005 hatte das ULD gegenüber dem Landeskriminalamt (LKA) dreizehn Punkte aufgelistet, in denen Optimierungsbedarf bestand. Ein Punkt wurde umgesetzt:

Bei der **Beauskunftung von Verbunddateien** haben BKA und LKA eine Regelung getroffen, die sicherstellen soll, dass der Betroffene von den Datenspeicherungen in INPOL erfährt. Im Übrigen wurde dem ULD bis heute nicht konkret mitgeteilt, wie unsere Anregungen seitens der Polizei im Einzelnen umgesetzt wurden. Bei den Beratungen des Sonderberichts im Landtag wurden vom Innenministerium Fehler eingeräumt, die aber Einzelfälle darstellten und behoben seien. Wir haben weiterhin die Hoffnung, dass die vom ULD vorgeschlagenen Anregungen umgesetzt werden.

Anhand von zwei konkreten Fällen zeigten sich fundamentale Meinungsverschiedenheiten zwischen ULD und Innenministerium in Bezug auf **Auskunftsverweigerungen**. In dem einen Fall bedurfte es des Verweises auf die Rechtsprechung des Bundesverfassungsgerichts, um dem Ministerium klarzumachen, dass deren Teilauskunftsverweigerung so nicht mehr haltbar war.

Der andere Fall betraf die Eingabe einer älteren, um ihre Privatsphäre besorgten Dame. Diese wollte sich Klarheit darüber verschaffen, ob über sie aus **Telefonüberwachung** erlangte Daten gespeichert sind. Selbst die Einschaltung des Staatssekretärs im Innenministerium führte nicht dazu, dass die erbetene Auskunft erteilt werden konnte.

Alle unsere Bemühungen sind bislang trotz parlamentarischer Unterstützung erfolglos geblieben. Der Innen- und Rechtsausschuss des Landtags wartet darauf, dass sich – unter Einbeziehung des Generalstaatsanwalts bzw. des Justizministeriums – Innenministerium und ULD auf eine rechtskonforme Auskunftspraxis verständigen. Die Betroffenen haben einen verfassungsrechtlichen Anspruch auf Antwort, ob Daten über sie erhoben wurden oder nicht – unabhängig davon, ob aus einer Telefonüberwachung Daten vorliegen oder nicht und ob eine solche Maßnahme überhaupt durchgeführt wurde. Würden sie keine Antwort erhalten, wären sie verunsichert und dadurch in ihrer **Grundrechtsausübung beeinträchtigt**. Dies wäre im Ergebnis – wie die umfangreiche Rechtsprechung des Bundesverfassungsgerichts herausgearbeitet hat – rechtsstaatlich einfach nicht akzeptabel. Wir werden das Thema weiterverfolgen.

Was ist zu tun?
Das Innenministerium sollte die Anregungen des ULD zum Verfahren der Auskunftserteilung umsetzen und die Änderungen im Einzelnen darlegen. Bei Auskunftsverweigerungen sollte es sich auf das verfassungsrechtlich Zulässige beschränken.

4.2.3 @rtus

Viele Dienststellen der Landespolizei arbeiten bereits mit @rtus, bei anderen soll es sukzessiv eingesetzt werden. Mit @rtus stellen sich viele – teilweise weiterhin unbeantwortete – datenschutzrechtliche Fragen. Die Richtung der Antworten bestimmt das Polizeirecht. Die grundlegende Ausgestaltung des Systems muss die Polizei in der Errichtungsanordnung konkretisieren.

In den Tätigkeitsberichten der vergangenen Jahre hat das ULD über das neue Vorgangsbearbeitungssystem der schleswig-holsteinischen Polizei mit dem alt- und zugleich neudeutschen Namen „@rtus“ berichtet (28. TB, Tz. 4.2.3). Der Grundkonflikt zu @rtus basiert darauf, dass mit dem Verfahren zwei sehr unterschiedliche Zwecke in einem System vereint werden sollen: Das Verfahren will nämlich Vorgangsbearbeitung und Vorgangsverwaltung zugleich ermöglichen. Dies ist auf der Grundlage des **bestehenden Rechts** grundsätzlich möglich. Doch wird @rtus weder datenverarbeitungstechnisch noch in der Errichtungsanordnung den rechtlichen Vorgaben entsprechend abgebildet.

Das Gesetz verlangt für die Datenverarbeitung Differenzierungen. Zur **aktuellen Aufgabenerledigung** inklusive Auskunftserteilung dürfen vielfältige Einzelinformationen gespeichert und genutzt werden. Für die Zwecke der Vorgangsverwaltung und Dokumentation ist der Datenumfang – insbesondere für den Zeitraum

nach Abschluss der Bearbeitung eines Vorgangs – erheblich auf das Maß des dann noch Erforderlichen zu reduzieren.

Vorgangsverwaltung ist im Wesentlichen nichts anderes als Registratur. Benötigt werden hierfür lediglich die Daten zum Auffinden der jeweiligen Vorgänge. Wir haben bereits im Februar 2005 das Innenministerium Schleswig-Holstein hierauf hingewiesen und Lösungsmöglichkeiten aufgezeigt, ohne uns auf eine Verfahrensvariante festzulegen. Die Entscheidung, welche konkrete Verfahrensvariante gewählt wird, liegt natürlich bei der verantwortlichen Stelle.

Zur **Errichtungsanordnung** erfolgte zunächst mit dem Landespolizeiamt, dann mit dem Innenministerium ein umfangreicher Schriftwechsel, der jedoch keine wesentlichen Fortschritte brachte. Auf die fachlich-rechtlichen Fragestellungen haben sich Innenministerium bzw. Landespolizeiamt bislang leider gegenüber dem ULD nicht fundiert eingelassen.

Statt die bestehenden rechtlichen Vorgaben zu prüfen und systemtechnisch umzusetzen, legte die Landesregierung den Entwurf einer neuen Vorschrift im Landesverwaltungsgesetz vor. Die darin vorgesehenen Änderungen sind aber so üppig ausgefallen, dass nicht nur das Not leidende System @rtus rechtlich saniert würde. Vielmehr ließen sich hierüber alle noch nicht bekannten, aber vermutlich anstehenden Erweiterungen von @rtus mühelos legitimieren (Tz. 4.2.1). Es spricht alles dafür, dass @rtus realisiert wurde, ohne die rechtlichen Rahmenbedingungen vorab hinreichend zu klären nach dem Grundsatz: **Die Technik regiert das Recht**. In einer rechtsstaatlichen Demokratie sollte aber das Recht die Technik regieren. Nicht die Anpassung des Gesetzes darf die Konsequenz sein, sondern die Anpassung des Systems an das geltende Recht, vor allem auch an das Verfassungsrecht. Der Konflikt von @rtus mit dem Recht auf informationelle Selbstbestimmung wird nicht dadurch beseitigt, dass man ihn gesetzlich für nicht existent erklärt. Die haushaltsrechtlichen Auswirkungen bewertet das ULD nicht.

Was ist zu tun?
Innenministerium und Landespolizeiamt sollten die datenschutzrechtlich gebotenen Änderungen am System @rtus vornehmen.

4.2.4 INPOL-neu – Innenminister wünscht keine datenschutzrechtliche Begleitung

INPOL-neu ist das Verbunddateisystem der Polizeibehörden des Bundes und der Länder, das sukzessive weiterentwickelt wird. Kooperation mit den Datenschutzbeauftragten und deren effektive Datenschutzberatung sichern die rechtskonforme Fortentwicklung eines derart komplexen und länderübergreifenden Systems.

Das Bundeskriminalamt (BKA) und die Polizeien der Länder arbeiten gemeinsam an der Fortentwicklung und Erweiterung des Systems INPOL-neu in einer **gemeinsamen Projektgruppe**. Hierbei geht es um die wichtige Frage, wie die gemeinsame Informationsverarbeitung der deutschen Polizei in der Zukunft aus-

sehen soll und wird. Erörtert werden die gemeinsam betriebenen automatisierten Verfahren wie z. B. der Kriminalaktennachweis, die Falldateien oder die DNA-Analysedatei, um den Polizeien auch künftig leistungsfähige und für die Aufgabenerfüllung adäquate Datenverarbeitungstechniken zur Seite stellen zu können. Neben der Optimierung der bestehenden Verfahren geht es auch um die Einführung neuer Verfahren, um die aus ihrer Sicht notwendigen und wünschenswerten Ergänzungen.

Der Arbeitskreis Sicherheit der Datenschutzbeauftragten des Bundes und der Länder hatte bereits zu Zeiten der ersten Projektgruppe INPOL-neu eine eigene Arbeitsgruppe gebildet, die die Projektgruppe beim BKA beriet (22. bis 24. TB, jeweils Tz. 4.2.2 bzw. 4.2.3). Diese kleine Arbeitsgruppe von Datenschützern bestand aus drei bis fünf Mitgliedern der Datenschutzbeauftragten und konnte flexibel und angemessen reagieren. Durch die Teilnahme an den Sitzungen der Projektgruppen beim BKA und die **Übersendung der erforderlichen Unterlagen** waren die Voraussetzungen für eine konstruktive Kooperation gegeben. Nachdem das Bundesinnenministerium bzw. das Bundeskriminalamt aus verschiedenen Gründen die Arbeiten an INPOL-neu aussetzte, verlor auch die Arbeitsgruppe der Datenschutzbeauftragten vorübergehend ihren Wirkungskreis.

Nun hat eine **neue Projektgruppe** die Fortführung der Weiterentwicklung von INPOL übernommen. Die Datenschutzbeauftragten aus Bund und Ländern stehen zur datenschutzrechtlich beratenden Begleitung dieses Großprojekts der deutschen Polizei mit der **Arbeitsgruppe** weiter bereit. In einer ersten gemeinsamen Sitzung mit Vertretern des BKA wurde hierüber eine grundsätzliche Verständigung erzielt. Es gilt nun, die Intensität und die Modalitäten abzustimmen.

Das ULD hat den Innenminister des Landes Schleswig-Holstein um **sachgerechte Beteiligung**, insbesondere um frühzeitige Unterrichtung und Übersendung der einschlägigen Unterlagen, gebeten. Dem ULD geht es darum, Unterlagen über das neue Verfahren möglichst frühzeitig zu erhalten und gegebenenfalls auch bilaterale Gespräche mit dem Landeskriminalamt Schleswig-Holstein führen zu können, um gemeinsam auf sachgerechte Lösungen bei INPOL-neu hinzuwirken. Dieses gemeinsame Interesse hat das Innenministerium bisher nicht erkannt. Unabhängig davon: Die vom ULD eingeforderten Unterlagen betreffen die Verarbeitung personenbezogener Daten in Verbunddateien, an denen die Landespolizei als verantwortliche Stelle beteiligt ist. Das ULD hat nach dem Landesdatenschutzgesetz einen Anspruch, sämtliche Unterlagen hierzu einzusehen. Nur eine rechtzeitige Kooperation hilft Probleme zu erkennen und gemeinsam zu lösen. Dem hat das Innenministerium eine Absage erteilt: Sowohl die Kommission INPOL-Technik als auch die AG Kripo seien Untergremien der Innenministerkonferenz; deren Vorsitzender sei der richtige Ansprechpartner.

Was ist zu tun?
Das Innenministerium des Landes Schleswig-Holstein sollte endlich grünes Licht für eine gute Zusammenarbeit bei INPOL-neu geben.

4.2.5 Zuverlässigkeitsüberprüfungen bei Großveranstaltungen

Veranstalter von Großereignissen bedienen sich zunehmend der Sicherheitsbehörden, um im Vorfeld freiwillige Helfer und Mitarbeiter in Akkreditierungsverfahren durchleuchten zu lassen. Der Verfassungsschutz und das Landeskriminalamt Schleswig-Holstein wirkten zuletzt im Rahmen der Fußball-WM 2006 und der Veranstaltungen zum Tag der Deutschen Einheit an solchen Verfahren mit.

Das **Akkreditierungsverfahren zur Fußball-WM 2006** konnten wir im Rahmen unserer Zuständigkeit nur in Bezug auf die Datenverarbeitung beim Landeskriminalamt (LKA) und bei der Verfassungsschutzbehörde des Landes prüfen. Die Prüfung beim LKA zeigte zweierlei: Positiv zu bewerten ist die restriktive Handhabung von Ablehnungen bei der Akkreditierung durch das LKA. Dieses ändert jedoch nichts an unserer grundsätzlichen Bewertung des bundesweit praktizierten Akkreditierungsverfahrens, das wir als unzulässig betrachten (28. TB, Tz. 4.2.9).

In Schleswig-Holstein wurden 1814 Personen überprüft. Lediglich in drei Fällen sprach das LKA ein ablehnendes Votum aus. Wir haben uns im Rahmen der datenschutzrechtlichen Kontrolle nicht nur diese Ablehnungen angesehen, sondern auch weitere „**Trefferfälle**“, die am Ende nicht zu einer Ablehnung führten. Das LKA hat jeden Fall einer gründlichen Prüfung unterzogen. Dabei wurden nicht nur die zur Person vorliegenden Erkenntnisse bewertet, sondern auch die Frage, ob die betroffenen Personen aufgrund ihrer konkret geplanten Verwendung im Stadion ein Sicherheitsrisiko darstellen können. Die Art und Weise der Durchführung gab demnach keinen Grund für Beanstandungen.

Problematisch bleibt die Teilnahme der Sicherheitsbehörden an dieser Prozedur. Bereits die Durchführung einer Zuverlässigkeitsüberprüfung stellt für die Betroffenen ein persönliches Risiko dar. Im Ablehnungsfall hat dies in der Regel Konsequenzen für das Arbeitsverhältnis. Eine **gesetzliche Grundlage** wäre ein absolutes Muss, liegt aber nicht vor; das Sicherheitsüberprüfungsgesetz regelt völlig andere Sachverhalte und kommt daher unstreitig nicht zur Anwendung.

Das Innenministerium erachtet die **Einwilligung der betroffenen Personen** für ausreichend. Diese Einwilligungserklärungen lagen jedoch – was unsere Prüfung bestätigte – zu keinem Zeitpunkt bei den Landesbehörden vor. Diese hatten lediglich die Datensätze der betroffenen Personen in elektronischer Form vom BKA erhalten. Das BKA seinerseits hatte die elektronischen Datensätze vom FIFA-Organisationskomitee bekommen, das die Anmeldungen der Arbeitgeber verwaltete. Die Einwilligungserklärungen sollten bei diesen vorliegen, was jedoch für uns nicht mehr nachvollziehbar war. Eine Prüfung durch die ausführenden (Landes-)Behörden, ob die Betroffenen jemals tatsächlich eine Einwilligungserklärung unterschrieben haben, war in den Planungen nicht vorgesehen. Der Versuch des ULD, im Rahmen seiner datenschutzrechtlichen Kontrolle beim LKA diese Einwilligungserklärungen, die Grundlage für die Datenverarbeitung sein sollten, zu überprüfen, um die Authentizität zu überprüfen, blieb erfolglos. Weder das LKA noch der eigens bestellte betriebliche Datenschutzbeauftragte des Deut-

schen Fußball-Bundes konnten sie vorlegen. Die automatisiert gespeicherten Daten und die Originalerklärungen waren bereits vor Ablauf der Aufbewahrungsfrist gelöscht bzw. vernichtet worden.

Wegen dieses fundamentalen Mangels und der Entscheidung des Innenministeriums, das Verfahren trotz Fehlen einer Rechtsgrundlage durchzuführen, waren wir – trotz der anerkennenswert restriktiven Handhabung durch das LKA – gezwungen, **in 1814 Fällen eine Beanstandung** auszusprechen.

Was ist zu tun?
Akkreditierungsverfahren bei Großveranstaltungen sind in der praktizierten Form datenschutzrechtlich nicht akzeptabel. Es dürfen keine außergesetzlichen Praktiken entstehen. Eine Rechtsgrundlage für die Durchführung von Sicherheitsüberprüfungen bei Großveranstaltungen liegt nicht vor.

4.2.6 Antiterrordatei – Angriff auf das Trennungsgebot

Nach langer Vorlaufzeit hatte es der Bundesgesetzgeber plötzlich sehr eilig beim Gesetz über gemeinsame Dateien von Nachrichtendiensten und Polizeibehörden – zum Schaden des Datenschutzes: Der Kreis der betroffenen Personen ist unverhältnismäßig und zu weit; das Gesetz ist nicht normenklar und teilweise unverständlich; das verfassungsrechtliche Trennungsgebot wird bis zur Unkenntlichkeit aufgeweicht.

Die Bekämpfung des internationalen Terrorismus ist ein hochrangiges Ziel. Daher würden wir hierfür eine reine Hinweis- bzw. **Indexdatei** akzeptieren (27. TB, 4.2.2). Hierdurch hätten die beteiligten Behörden die Information erhalten, ob über eine bestimmte verdächtige Person bereits ein Vorgang bei einer anderen Behörde geführt wird. Die Zulässigkeit der weiteren Übermittlung von Daten hätte dann im Einzelfall geprüft werden müssen und können. Hierbei ist es aber nicht geblieben. Das nunmehr verabschiedete Gesetz stößt auf vielfältige verfassungsrechtliche Bedenken: Es grenzt den Kreis der betroffenen Personen und Daten nicht hinreichend ein, ist in weiten Teilen unklar und unverständlich gefasst und verletzt das verfassungsrechtliche Trennungsgebot.

Als „Terrorverdächtiger“ wird nicht nur derjenige erfasst, bei dem objektive Fakten für eine Verbindung zu Terroraktivitäten sprechen. Vielmehr soll es genügen, wenn „tatsächliche Anhaltspunkte“ dafürsprechen. Ausreichend sind also **Indizien**, aus denen nach der **behördlichen Erfahrung** auf das mögliche Vorliegen eines Sachverhalts geschlossen werden kann. Diese Anhaltspunkte müssen sich nach dem Gesetz nicht auf eine konkrete Verbindung zu bestimmten Aktivitäten beziehen. Es genügt, wenn diese nach der behördlichen Erfahrung dafürsprechen, dass eine Person Gewalt zur Durchsetzung politischer Ziele in internationalem Kontext „**befürwortet**“. Damit sind die Sicherheitsbehörden rechtlich verpflichtet, in der Terroristendatei z. B. jeden zu speichern, der einen völkerrechtswidrigen Militäreinsatz gutheißt. Als **Kontaktperson** wird eine Bürgerin oder ein Bürger auch dann gespeichert, wenn z. B. tatsächliche Anhaltspunkte dafür vorlie-

gen, dass sie – auch unwissentlich – zu einer anderen Person in Kontakt steht, die in diesem Sinne als Befürworter von Gewalt gespeichert ist. Es zeigt sich: In der Antiterrordatei landen längst nicht nur Terrorismusverdächtige. Gespeichert werden darin von den Polizei- und Nachrichtendienstbehörden nicht nur Name und Adresse der Betroffenen, sondern ein großer Katalog weiterer Daten.

Die weiten Zugriffsbefugnisse stellen wegen der Einschränkung des **Trennungsgebotes** eine Gefahr dar: Für die Beobachtung etwa des islamistischen Extremismus ist nach den bisherigen Regelungen ausschließlich der Verfassungsschutz zuständig, nicht die Polizei. Diese kann erst dann tätig werden, wenn eine konkrete Gefahrenlage oder ein konkreter Tatverdacht – z. B. wegen Mitgliedschaft in einer terroristischen Vereinigung – vorliegt. Umgekehrt haben die Nachrichtendienste keine polizeilichen Befugnisse. So kann es den Diensten im Einzelfall verwehrt sein, bestimmte Informationen zu erhalten, etwa wenn diese nur mit Zwangsmitteln (z. B. Beschlagnahme) zu erlangen sind. Diese beiderseitigen Befugnisbegrenzungen dürfen nicht durch eine gemeinsame Informationsbasis umgangen werden. Mit der Antiterrordatei erfolgt eine solche Umgehung.

Das Gesetz regelt nicht nur eine zentrale Antiterrordatei, sondern ermöglicht es den Nachrichtendiensten und Polizeibehörden, weitere gemeinsame **Projektdateien** einzurichten. Die schon erwähnten Probleme stellen sich insofern mit besonderer Dramatik, da die Regelungen praktisch keine Einschränkungen an die inhaltliche Ausgestaltung der Dateien enthalten. Zu befürchten ist, dass die Hemmungen gegen einen umfassenden Datenaustausch zwischen Nachrichtendiensten und Polizeibehörden vollends schwinden.

Angesichts des Umfangs der gespeicherten Daten ist es äußerst erstaunlich, dass sowohl die Regelungen zur zentralen Antiterrordatei als auch zu den Projektdateien **keine eigenständigen Löschfristen, Berichtigungs- und Änderungspflichten** enthalten.

In Anbetracht der erheblichen verfassungsrechtlichen Defizite des – nunmehr verabschiedeten – Gesetzes haben wir vor der Beratung im Bundesrat gegenüber dem Innenministerium Stellung genommen, zumal auch die Sicherheitsbehörden Schleswig-Holsteins zur Teilnahme verpflichtet werden. Allein zum Aufbau der Datei in Schleswig-Holstein sollen zehn neue Stellen geschaffen werden. Die **Stellungnahme des ULD** ist erhältlich unter

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

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit einer Entschließung geäußert:

www.sachsen-anhalt.de/LPSA/index.php?id=20561

Was ist zu tun?
Soweit Gesetzesformulierungen Spielraum geben, sollte die Datenverarbeitung in verfassungskonformer Auslegung so eng wie möglich erfolgen. Ob das Gesetz einer verfassungsgerichtlichen Prüfung standhält, wird die Zukunft zeigen.

4.2.7 Terrorismusbekämpfung – die Grundrechtseinschränkungen gehen weiter

„Terrorismusbekämpfungsergänzungsgesetz“ heißt das aktuelle Wortungetüm, welches die immer geringer werdende Wertschätzung des Rechts auf informationelle Selbstbestimmung um ein Weiteres dokumentiert. Es enthält zahlreiche neue Befugnisse der Nachrichtendienste, heimlich Auskünfte einzuholen.

Mit dem Terrorismusbekämpfungsgesetz (TBG) wurden bereits in der Ära Schily erweiterte Auskunftsbefugnisse der Geheimdienste eingeführt. Danach darf z. B. das Bundesamt für Verfassungsschutz in erweitertem Umfang auf die bei Telekommunikationsdienstleistern oder Fluggesellschaften vorhandenen Daten zugreifen. Diese mit diesem Gesetz ausgedehnten Auskunftsbefugnisse galten bislang nur für die Terrorismusbekämpfung, werden mit dem Terrorismusbekämpfungsergänzungsgesetz (TBEG) aber auf die Bekämpfung des **Extremismus** erweitert. Damit wird der von der Datenerhebung betroffene Personenkreis kaum überschaubar ausgeweitet. Auch neue Auskunftsbefugnisse sind vorgesehen, so etwa der Zugriff auf Bank- bzw. Finanzdaten.

Die Einschränkung von Bürgerrechten mit dem Hinweis auf Terrorismusbekämpfung hat zurzeit offenbar auch dann Konjunktur, wenn die Vorschriften nicht der Beobachtung von Terrorverdächtigen dienen. Der Gesetzgeber hielt es nicht für notwendig, vor der weiteren Verschärfung die bislang bestehenden Regelungen durch eine ernst zu nehmende **Evaluation** auf den Prüfstand zu stellen. Die präsentierte Evaluation des TBG kann nicht ernsthaft als solche bezeichnet werden – nicht nur wegen ihrer offenkundigen Oberflächlichkeit, sondern auch, weil eine seriöse Prüfung nach wissenschaftlichen Maßstäben nur durch eine unabhängige Stelle durchgeführt werden kann. Dies ist nicht geschehen.

Angesichts der Vielzahl neuer Gesetze dürfen die einzelnen Vorschriften **nicht isoliert betrachtet** werden. Sorge bereitet insbesondere die Gesamtheit der in den letzten Jahren durch zahlreiche Einzelgesetze neu geschaffenen Einschränkungen des Rechts auf informationelle Selbstbestimmung. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich zur aktuellen Gesetzgebung zur Terrorismusbekämpfung mit einer Entschließung geäußert:


www.sachsen-anhalt.de/LPSA/index.php?id=20560

Was ist zu tun?
Sollte der Gesetzgeber nicht bereit sein, die neuen Gesetze zurückzunehmen, so muss wenigstens eine ernsthafte unabhängige Evaluation der Anwendung dieser Normen erfolgen.

4.2.8 ED-Daten aus Schleswig-Holstein beim Bundeskriminalamt

Daten von erkennungsdienstlich behandelten Personen werden zentral beim Bundeskriminalamt gespeichert. Verantwortliche Stellen, auch im Hinblick auf die Datenlöschung, bleiben aber diejenigen Behörden, die die Daten erhoben und in die Datei eingestellt haben, also in der Regel die Landeskriminalämter.

Beim Bundeskriminalamt (BKA) sind die erkennungsdienstlichen (ED-) Daten nach festgelegten Fristen auf ihre Löschungsmöglichkeit hin zu überprüfen. Eine vorzeitige Löschung muss erfolgen, wenn das jeweilige Landeskriminalamt (LKA) eine vorzeitige Löschung der Daten verfügt, etwa aufgrund einer ergangenen gerichtlichen Entscheidung, z. B. der Einstellung des Verfahrens wegen fehlenden Tatverdachts. In der Praxis prüft das BKA in diesen Fällen aber zunächst, ob eine weitere Speicherung zu dieser Person in seinen Dateien besteht. Wenn dies der Fall ist, **übernimmt das BKA den Besitz** an den ED-Daten des Landes, obwohl die näheren Umstände der Datenerhebung dem BKA unbekannt sind und obwohl die bei der zuständigen Polizeidienststelle des Landes bestehende Kriminalakte gelöscht wurde.

Die sich aus der Kriminalakte ergebenden Gesamtumstände sind aber erforderlich, um die gesetzlich geforderte sogenannte **Negativprognose** erstellen zu können. Diese Negativprognose ist Voraussetzung für die weitere Speicherung und kann nur abgegeben werden, wenn etwa wegen der Art oder Ausführung der Tat, der Persönlichkeit des Betroffenen oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass künftig weitere Verfahren gegen ihn zu führen sind. Das BKA weiß über die ED-Behandlung in der Regel nur den Tag der Maßnahme, das Delikt und die zuständige Polizeidienststelle. Dies sind die Informationen, die auf dem verwendeten Formular – dem sogenannten „100a-Blatt“ – zusammen mit den Originalfingerabdrücken festgehalten sind. Diese Daten reichen nicht aus, um verwertbare Aussagen über die betroffene Person zu machen. Die Tatsache, dass das Verfahren zwischenzeitlich eingestellt worden ist, kann nicht hinzugespeichert werden, obwohl dies im Interesse von Objektivität und Wahrheit geboten wäre.

Die Datenschutzbeauftragten des Bundes und der Länder halten dieses Verfahren für nicht hinnehmbar. Wir haben bei unserer Prüfung bereits festgestellt, dass das BKA in einigen Fällen Datensätze aus Schleswig-Holstein nicht gelöscht hat, obwohl eine entsprechende **Bitte des LKA beim BKA** erfolgte. Das BKA hat in einer ersten Stellungnahme bestritten, unterrichtet worden zu sein. Das ULD ist um die weitere Aufklärung dieser Fälle und eine Änderung des Verfahrens bemüht.

Was ist zu tun?
Die Löschung der Daten durch die Landespolizei Schleswig-Holstein muss konsequent beim BKA umgesetzt werden. Das BKA muss zu einem gesetzeskonformen Umgang mit Länderdaten bewegt werden.

4.2.9 Beobachtung von Versammlungen im Visier des ULD – Teil II

Das Landeskriminalamt hat in Abstimmung mit der Polizeiabteilung des Innenministeriums zum Prüfbericht über die Beobachtung von grundrechtlich besonders geschützten Versammlungen Stellung genommen, ohne aber alle Mängel behoben zu haben.

Das ULD hatte im 28. Tätigkeitsbericht (Tz. 4.2.7) über die Kontrolle der Datenverarbeitung beim Landeskriminalamt (LKA) im Zusammenhang mit Versammlungen im Jahre 2005 berichtet.

- **Hinzuspeicherungen aus Anlass der erlaubten Teilnahme an Veranstaltungen**

Erlaubte Teilnahmen an Veranstaltungen werden vom LKA als Erkenntnis gespeichert, sofern bereits aus anderen Gründen über den Betroffenen eine Kriminalakte besteht. Diese Speicherungen haben zwar keine Auswirkungen auf die Dauer des Fortbestandes der Kriminalakte und auf die dazugehörige Dateispeicherung. Sie sind aber datenschutzrechtlich nicht akzeptabel, weil die Bürgerinnen und Bürger durch die Teilnahme an einer solchen Veranstaltung ihre **verfassungsrechtlichen Grundrechte aus Art. 8, 9 Grundgesetz (GG)** wahrnehmen. Die erlaubte Teilnahme – die selbst mit Straftaten nicht zusammenhängt – darf nicht zu rechtlichen Nachteilen für Betroffene führen. Die Hinzuspeicherung von Erkenntnissen wurde von uns beanstandet. Das Landesverwaltungsgesetz und eine Verwaltungsvorschrift (z. B. Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen – KpS-Richtlinien) können nichts Abweichendes bestimmen. Das LKA vertritt in Abstimmung mit dem Innenministerium die Auffassung, dass sich die Legitimation für die Datenverarbeitung insoweit aus den KpS-Richtlinien ergibt und hierüber in den Jahren 1996 und 1997 mit dem ULD gesprochen worden war.

- **Datei „COMPAS“**

Die Datei „COMPAS“ wird beim LKA und bei den Polizeidienststellen im Land Schleswig-Holstein als Vorgangsbearbeitungssystem geführt. Es wird nach Angaben des Innenministeriums schrittweise durch das Verfahren „@rtus“ binnen der nächsten fünf Jahre abgelöst. COMPAS wird von der Polizei auch als Posteingangs- und Postausgangsbuch sowie als Tagebuch geführt. Bei dieser Verwendung fällt eine Vielzahl von gespeicherten personenbezogenen Informationen an. Das Verfahren ist technisch so konzipiert, dass es einzelfallbezogene Löschung nicht zulässt. Die Speicherungsfristen für den Bereich „Tagebuch“ wurden, da es sich nach Angabe des LKA bei diesen Datensätzen jeweils um Urkunden handele, pauschal auf zehn Jahre festgesetzt. Nach Ablauf dieser Frist erfolge eine automatische Löschung. In keinem der Fälle ist bisher diese Löschfrist erreicht. Es stellt sich die Frage, wie diese Datensätze mit der Einführung von @rtus behandelt werden. Das ULD hatte das **Fehlen von Löschmöglichkeiten bei COMPAS** beanstandet und um Klärung gebeten, wie mit dem Datenbestand bei der Ablösung des Verfahrens COMPAS verfahren wird (28. TB, Tz. 4.2.7).

Das Landeskriminalamt bezieht sich auf eine eigene **Geschäftsanweisung**, die den Nachweis über Vorgangseingänge regelt. Danach ist der Nachweis für mindestens zehn Jahre zu führen; erst danach stünden die Datensätze zur Löschung an. Unter Beachtung dieser Vorgaben sind von der Abteilung 3 des LKA noch keine Datensätze gelöscht worden, da das Verfahren noch keine zehn Jahre eingesetzt ist. Einen Gesetzesverstoß bei der Vorgangsverwaltung und Dokumentation wollte man nicht erkennen.

Das Innenministerium hat nach unserer Intervention wegen der sich abzeichnenden schwierigen Situation für das auslaufende COMPAS im August 2006 die Aufbewahrungsfrist von Vorgängen und Durchschriften in COMPAS für die Abteilung 3 des LKA wie folgt **neu geregelt**:

- Im Falle der Vorgänge, bei denen die originäre **Sachbearbeitung beim LKA** (Abteilung 3) liegt, bleibt der Eintrag in COMPAS-AWS im Rahmen der Fristen des Durchschriftenerlasses zu Zwecken der Dokumentation des polizeilichen Handelns bestehen, auch wenn die dazugehörige Aktenunterlage bereits vernichtet ist.
- Die Speicherungen von Durchschriften aus Vorgängen über Straftaten und Ordnungswidrigkeiten, die im Rahmen des **Meldedienstes** (Zentralstellenfunktion vom LKA (Abteilung 3) im Bereich der politisch motivierten Kriminalität) ausgewertet, analysiert und bewertet werden und die noch zur Aufklärung ungeklärter Straftaten oder zur Aufklärung künftiger Straftaten dienen, bleiben in COMPAS-AWS so lange bestehen, wie es einen Aktenrückhalt dazu gibt. Wird der Aktenrückhalt vernichtet, ist auch die Speicherung in der Datei zu löschen, da diese ohne Aktenrückhalt keine Aussagekraft mehr besitzt und deshalb nicht mehr erforderlich ist.
- Dasselbe gilt für Durchschriften von **Berichten zur Gefahrenabwehr**, die im Rahmen des Meldedienstes übersandt, analysiert und bewertet werden.

Nach Auffassung des Innenministeriums Schleswig-Holstein bleibt nur noch die Frage offen, ob **einzelne Datensätze** gelöscht werden können oder sich nur anonymisieren lassen. Dies werde durch das LKA zu prüfen sein.

Bezüglich der Übertragbarkeit dieser Regelung auf das neue Verfahren **@rtus** hat sich das Innenministerium noch nicht abschließend geäußert. Das LKA verwies darauf, dass sich die Datenverarbeitung zukünftig an der @rtus-Errichtungsanordnung orientieren werde. Ein abgestimmtes Löschkonzept liege allerdings noch nicht vor. Es sei aber fraglich, ob es bei der bisher gültigen Speicherungsfrist von zehn Jahren bleiben müsse. Möglich seien differenzierte Prüffristen in Abhängigkeit von der Vorgangsart. Ungeklärt war bis vor Kurzem die Frage, ob es für die Übergangszeit einen Parallelbetrieb der beiden Verfahren geben oder ob eine Migration der Daten bevorzugt wird. Das ULD hatte bereits im Jahre 2005 darauf hingewiesen, dass vor einer Übernahme des Datenbestandes in @rtus eine Selektion der gesamten Daten unter Erforderlichkeitsgesichtspunkten im Einzelfall unerlässlich ist.

Um Datenschutzverletzungen durch die fortbestehende Speicherung in COMPAS zu minimieren, hatte das ULD empfohlen, den Datenbestand bis zur endgültigen Klärung einer einzelfallgerechten Löschung bzw. einer selektiven Übernahme in das System @rtus zu **sperren**. Leider nahm das LKA diese Anregung nicht an; es will die Daten zukünftig nutzen wie bisher. Diese Reaktion, die wir nicht nachvollziehen können, bedauern wir.

Wir erfuhren im Februar 2007, dass der COMPAS-Datenbestand des LKA, Abteilung 3, in das Verfahren @rtus importiert worden ist. Es handelt sich dabei um ca. 17.000 Vorgänge mit über 30.000 Personendaten. Sie sind als COMPAS-Daten in @rtus gekennzeichnet. Da vor der Migration der Daten in das neue Verfahren keine Erforderlichkeitsprüfung stattgefunden hat, will das LKA die Bestandsbereinigung nachholen und wöchentlich etwa 250 Vorgänge durch die Sachgebiete überprüfen. Nach etwa einem Jahr wird demzufolge der Datenbestand entsprechend der oben genannten Kriterien des Innenministeriums überprüft sein. Das LKA geht davon aus, dass ca. 11.000 Datensätze zu löschen sind. Die alten COMPAS-Arbeitsplätze werden abgebaut, sobald eine störungsfreie Verarbeitung der Daten in @rtus gewährleistet ist. Eine Löschung des COMPAS-Datenbestandes der Abteilung 3 des LKA wird dann ebenfalls vorgenommen.

- **Datei „ISSH“**

Die Notwendigkeit der Weiterführung oder Änderung der Datei „ISSH“ – Innere Sicherheit Schleswig-Holstein – (28. TB, Tz. 4.2.7) wollte das LKA kurzfristig prüfen. Sofern sie – neben @rtus – bestehen bleibe, will das LKA die **fehlende Errichtungsanordnung** fertigen. Das Gleiche gilt auch hinsichtlich der Datenverarbeitung in der „Warndatei Rechts“.

Wir konnten die rechtlichen Anforderungen gegenüber dem LKA und dem Innenministerium bei allem Verständnis nur bekräftigen. Die Aufbewahrungsfristen für COMPAS-AWS können wir nur mit Blick darauf akzeptieren, dass das System in Kürze ausläuft. Davon kann aber **keine Präzedenzfallwirkung** für andere Fallgestaltungen ausgehen.

Was ist zu tun?
Die Konzeptionierung und Implementierung von @rtus zeigen, dass eine rechtzeitige Koordination, etwa im Hinblick auf Auswirkungen auf andere Dateien, erforderlich gewesen wäre. Die lang genug bekannten Mängel sollten nun zügig beseitigt werden, sodass eine den verfassungsrechtlichen Anforderungen genügende Datenverarbeitung sichergestellt ist.

4.2.10 Eine unzulässige Datenübermittlung und ihre Folgen

Eine Petentin, die im Alter von 13 Jahren eines Ladendiebstahls verdächtigt worden war, hatte sich für den Polizeidienst eines anderen Bundeslandes beworben. Die Polizei in Schleswig-Holstein übermittelte den Kollegen des anderen Landes die „Erkenntnis". Die Bewerbung wurde abgelehnt.

Die Petentin wollte Polizistin in Niedersachsen werden. Kurz vor Abschluss des Auswahlverfahrens erhielt sie die Nachricht, dass sie ausgeschieden sei. Mit dreizehn Jahren war sie **eines Ladendiebstahls verdächtigt** worden. Ihr war damals gesagt worden, dass der Eintrag nach einer bestimmten Zeit gelöscht werde.

Die für das Auswahlverfahren zuständige Polizeibehörde hatte bei der Wohnsitzpolizeidienststelle in Schleswig-Holstein nachgefragt, ob über die Bewerberin Erkenntnisse hinsichtlich eines gegen sie geführten polizeilichen, staatsanwaltschaftlichen oder gerichtlichen Ermittlungsverfahrens vorliegen. In den Dateien der Polizei waren zum Zeitpunkt unserer Kontrolle keine Informationen mehr gespeichert. Der von uns mit eingeschaltete Landesbeauftragte für den Datenschutz Niedersachsen prüfte parallel bei der für das Auswahlverfahren zuständigen Polizeidirektion und erfuhr, dass die Dienststelle des Wohnortes der Bewerberin mitgeteilt hatte, dass ein Verfahren bei der Staatsanwaltschaft Itzehoe geführt wurde, das **mangels Tatverdachts eingestellt** worden ist. Diese Mitteilung war der Grund für den Ausschluss der Bewerberin aus dem Auswahlverfahren. Die Information hätte schon längst gelöscht sein müssen und nicht mehr mitgeteilt werden dürfen.

Da die Petentin nach dem bisherigen Stand des Auswahlverfahrens ein gutes Ergebnis erzielt hatte, entschloss sich die Polizei in Niedersachsen, die Bewerberin nach unserer Prüfung doch in den Polizeidienst einzustellen. Die Auskunft über das eingestellte Verfahren hatte die Polizei aus dem Verfahren MESTA erhalten. Die Übermittlung wurde von uns beanstandet. Die Polizei teilte uns mit, sie werde durch interne Regelungen sicherstellen, dass in vergleichbaren Fällen keine Auskunft mehr erteilt wird.

Was ist zu tun?
MESTA darf außerhalb der Zweckbestimmung nicht dazu verwendet werden, Daten zu übermitteln, die bei der Polizei selbst nicht mehr vorhanden sind.

4.2.11 Auskunftsverweigerungen durch Verfassungsschutzbehörde

Auskünfte an mögliche Betroffene können von der Verfassungsschutzbehörde verweigert werden, wenn das öffentliche Interesse an der Geheimhaltung überwiegt.

Der Verfassungsschutz ist wieder seit den jüngsten terroristischen Anschlägen und der Veröffentlichung von angeblichen behördlichen Unregelmäßigkeiten im Fokus der öffentlichen Auseinandersetzung. Dies gilt ebenso für die Verfassungsschutz-

behörde des Landes, was u. a. dazu führt, dass verstärkt Personen nachfragen, ob Daten über sie dort gespeichert sind. Ein solcher **gesetzlicher Anspruch** besteht und führt in vielen Fällen zur Auskunftserteilung.

Eine Auskunftsverweigerung ist aber im Einzelfall zulässig. Dies gilt, wenn über die Auskunft **geheime Erkenntnisse offengelegt** werden müssten oder Schlüsse auf nachrichtendienstliche Arbeitsmethoden oder Mittel gezogen werden können. Wird eine Auskunft verweigert, so muss dies dem Betroffenen nicht begründet werden, wenn dadurch das Geheimnis herauskäme. Doch müssen die Gründe für die Ablehnung aktenkundig gemacht werden. Die Antragsteller werden dann darauf hingewiesen, dass sie sich an das ULD wenden können. Einige solche Fälle hat es im Berichtszeitraum gegeben.

Dabei erfolgt im jeweiligen Einzelfall eine **aufwendige Prüfung des ULD** in der Verfassungsschutzbehörde und eine Erörterung der Gründe. Haben diese Gründe uns überzeugt, so wie dies bisher der Fall war, so teilt das ULD dem Betroffenen lediglich mit, dass eine Prüfung stattgefunden hat und hierbei keine Verstöße festgestellt werden konnten. In vielen Fällen liegt einer Auskunftsverweigerung der Umstand zugrunde, dass über die Person aus Sicht der Behörde sensible Daten vorhanden sind. Will eine Person es genauer wissen, so bleibt ihr nur die gerichtliche Prüfung der als Verwaltungsakt erlassenen Auskunftsverweigerung.

Was ist zu tun?
Die Auskunftserteilung ist wohl das wichtigste Instrument des Datenschutzes. Bei der Ablehnung einer Auskunft müssen immer gute Gründe vorliegen, die von einer unabhängigen Stelle überprüft werden können.

4.3 Justizverwaltung

4.3.1 Neuregelung der verdeckten Ermittlungsmaßnahmen im Strafverfahren

Die Bundesregierung will die verdeckten Ermittlungsmaßnahmen in der Strafprozessordnung neu regeln. Das proklamierte begrüßenswerte Ziel, ein „harmonisches Gesamtsystem“ zu schaffen, wird mit dem bisher vorliegenden Referentenentwurf nicht erreicht. Vielmehr werden das Telekommunikationsgeheimnis und das Recht auf informationelle Selbstbestimmung weiter ausgehöhlt.

Die Neuregelung der verdeckten Ermittlungsmaßnahmen in der Strafprozessordnung (StPO) soll parallel zur Einführung der Vorratsdatenspeicherung erfolgen (Tz. 7.1). Es geht hierbei schwerpunktmäßig um die Überarbeitung der Eingriffsschwellen und der sonstigen Eingriffsvoraussetzungen, nicht nur bei der Telekommunikationsüberwachung. Diese soll in Zukunft weiterhin möglich sein, wenn der Verdacht einer in einem **Anlasstatenkatalog** genannten „schweren Straftat“ besteht. Aus diesem Katalog wurden bei der Überarbeitung nur solche Straftaten gestrichen, die in der Praxis ohnehin gar nicht oder kaum vorkommen, so etwa die Fahnenflucht. Zugleich sind die Erweiterungen beträchtlich, wie etwa die Aufnahme bestimmter Urkunden- oder Betrugsdelikte.

Unverhältnismäßig ist auch die **Verbindungsdatenabfrage**, die bereits bei jedem Verdacht einer mittels Telekommunikation begangenen Straftat möglich werden soll. Nach der Begründung soll die Abfrage dynamischer IP-Adressen zur Strafverfolgung sogar praktisch voraussetzungslos über das Telekommunikationsgesetz möglich sein.

Erlaubt wird die Überwachung unverdächtiger (!) Kontakt- und Begleitpersonen – sogar mit **Wanzen** und **Richtmikrofonen**.

Der Schutz des **Kernbereichs privater Lebensgestaltung** soll in Zukunft nur bei der akustischen Wohnraumüberwachung und der Telekommunikationsüberwachung gelten. Dies genügt nicht. Kernbereichsschützende Regelungen sind auch für weitere heimliche Maßnahmen verfassungsrechtlich zwingend, so etwa für das Abhören von Gesprächen außerhalb von Wohnungen, z. B. im Auto.

Die Schutzansprüche der **Zeugnisverweigerungsberechtigten** drohen durch weiche Abwägungsklauseln verwässert zu werden. Eine Differenzierung nach verschiedenen Klassen ist nicht nachvollziehbar und untergräbt einen wirksamen Grundrechtsschutz. Aus welchem Grund wird ein Arzt oder Rechtsanwalt weniger geschützt als ein Strafverteidiger oder Geistlicher? Nach welchen Regeln soll entschieden werden, ob ein Gespräch schutzwürdig ist oder nicht? Die dafür vorgesehene wortreiche Abwägungsklausel lässt jeden objektiv messbaren Maßstab vermissen.

Begründungspflichten für – auch gerichtliche – Überwachungsanordnungen und hinreichende Verwertungsverbote sollten klar geregelt werden. Für eine notwendige **Evaluation** sind umfassende Berichtspflichten zu allen heimlichen Maßnahmen vorzusehen.

Was ist zu tun?
Das Land Schleswig-Holstein sollte dem Entwurf im Bundesrat wegen verfassungsrechtlicher Bedenken nicht zustimmen. Der Bedarf für eine Verschärfung der Vorschriften wurde bisher nicht nachgewiesen.

4.3.2 Nicht eingeleitete Strafverfahren – dennoch gespeichert

Wird mangels Tatverdachts die Einleitung eines Verfahrens abgelehnt, so stellt sich die Frage, wie solche Vorgänge in MESTA – im Automationssystem der Staatsanwaltschaft – zu speichern sind.

Ein Betroffener war offensichtlich ohne Grundlage und mit Schädigungsabsicht angezeigt worden. Die Staatsanwaltschaft kam zu dem Ergebnis, dass **kein Anfangsverdacht einer Straftat** vorlag und sah demgemäß von der Einleitung eines Strafverfahrens ab. Dennoch wurde der Vorgang in MESTA gespeichert.

In einigen Fällen waren die Vorgänge nur teilweise mit einer eigenen Löschfrist für die Verwendung in zukünftigen Verfahren versehen. Klärungsbedürftig war,

weshalb Daten aus Verfahren, bei denen nicht einmal ein Anfangsverdacht vorlag, für zukünftige Verfahren benötigt würden. Die Staatsanwaltschaft meinte, die Strafprozessordnung differenziere bei der Dokumentation nicht nach der Art der Verfahrensbeendigung. Dies ist für uns nicht einsichtig: Jede Datenspeicherung muss stets im Einzelfall erforderlich sein. Zudem mussten wir feststellen, dass Teillöschungen nicht durchgeführt worden waren. Dieser konkrete Mangel wurde nach Angaben der Generalstaatsanwaltschaft behoben. Generell bedarf die **Ausgestaltung des Systems MESTA** aber offensichtlich weiterer datenschutzrechtlicher Beobachtung, auch im Hinblick auf die Protokollierung der Verarbeitungsprozesse. Die Generalstaatsanwaltschaft signalisierte diesbezüglich Gesprächsbereitschaft.

Was ist zu tun?
Die Vergabe von Löschfristen, die technische Ausgestaltung der Löschungen und die Protokollierung in MESTA bedürfen einer vertieften Prüfung.

4.3.3 Kontrollbefugnis bei der Staatsanwaltschaft

Im Rahmen der unter Tz. 4.3.2 dargestellten Eingabe konnten wir unsere Kontrolle nicht vollständig durchführen. Es wurde uns keine vollständige Akteneinsicht gewährt. Dies haben wir formell beanstandet.

Die Prüfung bei der betreffenden Staatsanwaltschaft fand in freundlicher Gesprächsatmosphäre statt. Man war sehr bemüht, uns mündlich Auskünfte zu erteilen. Die Einsicht in die Datei MESTA wurde uns gewährt, nicht jedoch die vollständige Einsicht in die zugrunde liegenden Vorgänge: Die Akten, die wir prüfen wollten, lagen auf dem Tisch; uns wurde auszugsweise daraus vorgelesen; einzelne Schriftstücke wurden uns vorgezeigt. Die vollständige Akteneinsicht wurde uns jedoch – offenbar aufgrund einer Anweisung des Generalstaatsanwalts – verweigert. Die ULD-Prüfer konnten also nicht **uneingeschränkt die Akten durchsehen**. So war uns z. B. unmöglich zu klären, ob sich aus den Akten eine Weitergabe an andere Stellen ergab. Wir waren insofern auf die uns gemachten mündlichen Angaben der geprüften Stelle angewiesen. Nur durch ein Durchblättern der Akten ist es aber möglich, etwaige weitere – möglicher-

Im Wortlaut: § 39 Abs. 1 LDSG

Das Unabhängige Landeszentrum für Datenschutz überwacht die Einhaltung der Vorschriften über den Datenschutz bei den öffentlichen Stellen, auf die dieses Gesetz Anwendung findet. Die Gerichte und der Landesrechnungshof unterliegen seiner Kontrolle, soweit sie nicht in richterlicher Unabhängigkeit tätig werden.

Im Wortlaut: § 41 Abs. 1 LDSG

Die öffentlichen Stellen sind verpflichtet, das Unabhängige Landeszentrum für Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen. Ihm ist dabei insbesondere

1. Auskunft zu erteilen sowie Einsicht in Unterlagen und Dateien zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, besondere Amts- und Berufsgeheimnisse stehen dem nicht entgegen. …

weise übersehene – Eintragungen, Vermerke oder Ähnliches zu Datenübermittlungen oder -erhebungen zu finden.

Der Generalstaatsanwalt begründet seine Weisung damit, dass das ULD von vornherein keine datenschutzrechtliche Kontrolle der staatsanwaltschaftlichen Fachentscheidung über die Einleitung von Strafverfahren habe vornehmen wollen, sondern lediglich Einsicht in MESTA und die zugrunde liegenden Vorgänge erlangen wollte. Dann sei eine Akteneinsicht des ULD in Aktenteile untersagt, auf die es das Prüfrecht gerade nicht erstrecken wolle. Dies erforderten die berechtigten Datenschutzinteressen von Opfern und Geschädigten. Dem ULD sei nicht die Einsicht in die Bereiche, die Gegenstand der Kontrolle waren, verweigert worden. Soweit es um Datenübermittlungen gegangen sei, habe man dem ULD alle diesbezüglichen Eintragungen auf Nachfrage vorgelegt. Den ULD-Mitarbeitern war mitgeteilt worden, dass der **Inhalt von Strafanzeigen und die Sachentscheidung** selbst nicht zur Akteneinsicht freigegeben werde. Der Generalstaatsanwalt sieht also einen Teilbereich der Akten der Prüfkompetenz des ULD entzogen. Eine andere Sachlage hätte, so der Generalstaatsanwalt, vorgelegen, wenn das ULD erklärt hätte, es wolle sich anstelle einer vollständigen Akteneinsicht mit einem Durchblättern begnügen. Eine seriöse und unabhängige Datenschutzkontrolle setzt aber voraus, dass sich die Prüfer ein eigenes Bild machen und dazu sämtliche Unterlagen durchsehen können.

Selbstverständlich bewertet das ULD nicht die allein von der Staatsanwaltschaft zu beurteilende Entscheidung, ob ein strafrechtlicher Anfangsverdacht vorliegt oder nicht. Dies rechtfertigt aber nicht die Eingrenzung der Einsichtsbefugnisse des ULD in personenbezogene Daten. Das ULD kann vor der Kontrolle seinen Prüfauftrag mit Bindung gegen sich selbst auch nicht durch einen Verzicht auf die Einsicht in bestimmte Aktenteile begrenzen. Welche Akten im Einzelnen vom ULD gesichtet werden, steht im **Ermessen der Prüfer vor Ort**. Eine Vorabselbstbeschränkung wäre praktisch unsinnig. Die Entscheidung darüber, welcher Teil der Akten der Prüfkompetenz des ULD unterliegt, kann natürlich nicht bei der geprüften Stelle liegen. Das ULD hat die gesetzliche Pflicht, sich selbst ein Bild zu machen, ob ein datenschutzrechtlicher Bezug im Einzelfall vorliegt. Für die Staatsanwaltschaft sieht das Gesetz keine Sonderbehandlung vor. Daher haben wir die teilweise verweigerte Akteneinsicht formell beanstandet.

Was ist zu tun?
Die Staatsanwaltschaft muss dem ULD bei dessen Kontrollen vollständigen Einblick in Akten und Dateien gewähren. Dass dabei das ULD nur Fragestellungen mit datenschutzrechtlichem Bezug bewertet, ändert hieran nichts.

4.4 Verkehr

4.4.1 StVG-Übermittlungsnorm verunsichert Polizei und Fahrerlaubnisbehörden

Die Polizei ist nach einer Vorschrift im Straßenverkehrsgesetz verpflichtet, der Fahrerlaubnisbehörde Tatsachen mitzuteilen, die aus Sicht der Polizei dauernde Fahreignungsbedenken nach sich ziehen.

Kontrollen bei Fahrerlaubnisbehörden zeigen: Die im Straßenverkehrsgesetz (StVG) vorgesehene pauschale Übermittlungsverpflichtung sorgt für Irritationen bei der Polizei. Die Praxis der Polizeidienststellen im Lande Schleswig-Holstein dazu könnte nicht unterschiedlicher sein. Polizeidienststellen übermitteln oft einen bunten Strauß von Informationen. Vom Drogen- bzw. Alkoholdelikt über Körperverletzungen bis zum Fahren ohne Fahrerlaubnis ist alles dabei. Dabei handelt es sich oftmals um geringfügige Delikte, die zudem **keinen direkten Verkehrsbezug** haben. Auch spielt es oft keine Rolle, ob die betroffene Person überhaupt im Besitz einer Fahrerlaubnis ist.

Im Wortlaut:
§ 2 Abs. 12 Straßenverkehrsgesetz

Die Polizei hat Informationen über Tatsachen, die auf nicht nur vorübergehende Mängel hinsichtlich der Eignung oder auf Mängel hinsichtlich der Befähigung einer Person zum Führen von Kraftfahrzeugen schließen lassen, den Fahrerlaubnisbehörden zu übermitteln, soweit dies für die Überprüfung der Eignung oder Befähigung aus der Sicht der übermittelnden Stelle erforderlich ist.

Soweit die mitgeteilten Informationen für die Beurteilung der Eignung oder Befähigung nicht erforderlich sind, sind die Unterlagen unverzüglich zu vernichten.

Besonders heikel ist die Übermittlungspraxis in Bezug auf Jugendliche, da Übermittlungen im Widerspruch zu den Intentionen des Jugendgerichtsgesetzes stehen können. Der Gesetzgeber wollte zwar, dass **jugendliche Straftäter** tatsächlich die Folgen ihres Handelns spüren. Die von den Jugendgerichten gefällten Urteile sollen den Jugendlichen aber nicht in anderen Bereichen angelastet werden und deren Zukunft versperren.

Die Fahrerlaubnisbehörden speichern Hinweise über Jugenddelikte, die sie von der Polizei erhalten haben, oft über Jahre hinweg, weil – so die Argumentation – anzunehmen sei, dass der Jugendliche irgendwann eine Fahrerlaubnis beantragen wird. Die langfristige Speicherung diene dem Zweck der **Verkehrssicherheit**, da nur Personen am Straßenverkehr teilnehmen dürfen, die charakterlich und körperlich geeignet und befähigt seien. Die Informationen benachteiligen die Betroffenen aber zumeist unangemessen. Fahrerlaubnisbehörden werden z. B. aufgrund von Informationen tätig, die schon lange nicht mehr aktuell sind. Der Betroffene wird mit Vorkommnissen konfrontiert, die längst abgeschlossen sind und ihm auch nicht mehr vorgehalten werden dürfen.

So berechtigt das generelle Anliegen der Fahrerlaubnisbehörden sein mag, rechtfertigt es aber nicht pauschale und undifferenzierte Datenübermittlungen seitens

der Polizei und langfristige Speicherungen dieser Informationen auf Vorrat bei den Fahrerlaubnisbehörden. Daher haben wir einen **Dialog** mit dem Verkehrsministerium und der Polizei begonnen, um Leitlinien zu formulieren, an denen sich Polizei und Fahrerlaubnisbehörden orientieren können.

Was ist zu tun?
Die Polizei muss in jedem Einzelfall prüfen, ob sie wirklich Tatsachen übermittelt, die auf eine dauernde Nichteignung für den Straßenverkehr schließen lässt. Die Fahrerlaubnisbehörden müssen die erhaltenen Informationen zeitnah auf ihre Erforderlichkeit prüfen. Langfristige Speicherungen sind zu vermeiden.

4.4.2 Chaos bei Zentralisierung der Führerscheindaten beim Kraftfahrt-Bundesamt

Der Zeitdruck, die Daten der Führerscheininhaber nur noch zentral beim Kraftfahrt-Bundesamt zu speichern und die örtlichen Datenbestände bei den Fahrerlaubnisbehörden aufzulösen, führt offensichtlich zu Problemen. Nicht genügend durchdachte technische Konzeptionen erschweren diese Umstellung und bergen die Gefahr von Datenverlusten.

Unsere schlimmsten Bedenken bezüglich des Vorhabens, beim Kraftfahrt-Bundesamt (KBA) die Datenverarbeitung der Fahrerlaubnisbehörden (FEB) zu zentralisieren (28. TB, Tz. 4.4.3), scheinen sich zu bewahrheiten.

Vorgeschichte

Bei der Neuregelung des Straßenverkehrsgesetzes (StVG) im Jahre 1998 wurde festgelegt, dass die bei den örtlichen FEB gespeicherten Daten der Führerscheininhaber zukünftig nur noch zentral beim KBA gespeichert werden sollen. Alle FEB sollen zukünftig ihre Daten dort abspeichern und auch ändern oder löschen dürfen. Für die Umstellung sah der Gesetzgeber eine Übergangsfrist von fünf Jahren vor. Diese Frist wurde bis Ende 2006 verlängert. Nun sollten nur noch die Daten der Kartenführerscheininhaber gelöscht werden. Die anderen Daten sollen zunächst in den örtlichen Registern bleiben, bis hierfür auch Kartenführerscheine ausgestellt werden. Grund dafür war, dass die FEB bisher erst circa 60 % der Daten überhaupt an das KBA abgeben konnten. Es gibt nämlich keinen Zwangsumtausch der alten Papierführerscheine zu den neuen Kartenführerscheinen. In den vergangenen sechs Jahren wurden nur die Daten von Betroffenen übermittelt, die einen **neuen Führerschein** erhielten. Alle anderen Führerscheininhaber sind bisher nicht im Zentralen Fahrerlaubnisregister (ZFER) erfasst. Die Datenschutzbeauftragten des Bundes und der Länder hatten bereits anlässlich der Verabschiedung des Gesetzes vor den absehbaren technischen und organisatorischen Schwierigkeiten gewarnt und auf unzureichende Regelungen hingewiesen. Die Vorbehalte wurden jedoch nicht berücksichtigt.

Aktuelle Situation in Schleswig-Holstein

Nur ein Teil der FEB hat die Daten der Führerscheininhaber überhaupt vollständig in ihren örtlichen elektronischen Systemen gespeichert. Viele Daten von Altführerscheininhabern werden **noch auf Karteikarten** vorgehalten. Dies erschwert ein schnelles Überführen in das zentrale Register zusätzlich. Die Daten können dem Kraftfahrt-Bundesamt nicht übermittelt werden, weil sie elektronisch gar nicht verfügbar sind. Diese Situation scheint sich nunmehr – auch wegen des gesetzlichen Zeitdrucks – zu einem Debakel zu entwickeln:

- Bevor die Löschung der Daten über Kartenführerscheininhaber in den örtlichen FEB erfolgt, müssten die bereits beim KBA gespeicherten Informationen nochmals auf Richtigkeit überprüft werden. Es hat sich nämlich herausgestellt, dass eine nicht geringe Anzahl unrichtig ist.
- Die Daten der Altführerscheininhaber in den EDV-Systemen der örtlichen FEB verbleiben weiterhin dort. Für die Richtigkeit dieser Daten können die örtlichen FEB jedoch oftmals ohnehin nicht garantieren. Bei der Übernahme der Informationen von den Karteikarten gab es immer wieder Übertragungsfehler. Für einen zeitnahen Abgleich der einzelnen elektronisch gespeicherten Datensätze mit den alten Karteikarten fehlen den FEB die personellen Kapazitäten.
- In den Führerscheindatenbeständen der örtlichen FEB befinden sich zudem eine unbekannte Anzahl von Führerscheindaten, die schon hätten gelöscht werden können, weil der Fahrerlaubnisinhaber verstorben ist.

Die Einhaltung der gesetzlichen Verpflichtung, die Daten der Kartenführerscheininhaber aus den örtlichen Fahrerlaubnis-Registern bis Ende 2006 zu löschen, dürfte noch Jahre dauern. Die örtlichen Register gänzlich aufzulösen, liegt in ferner Zukunft.

Die Folgen

Zukünftig sind die FEB gezwungen, in zwei unterschiedlichen Verzeichnissen nachzuschauen, ob eine Person im Besitz einer Fahrerlaubnis ist. Dabei ist nicht sichergestellt, dass diese Informationen auch tatsächlich richtig sind. Obwohl dies alles bekannt ist, wird die Zentralisierung der Führerscheindaten ohne Berücksichtigung dieser Umstände weiter fortgeführt. Dies hat für die Betroffenen zur Folge, dass ihre Daten unter Umständen falsch gespeichert sind, ohne dass die Richtigkeit nachvollzogen werden könnte, oder dass die **Nachweise** über die Fahrerlaubnis vollständig **verloren gehen**.

Die Datenschutzbeauftragten des Bundes und der Länder haben eine **Arbeitsgruppe** gebildet, die in Zusammenarbeit mit dem KBA und dem Bundesamt für Sicherheit in der Informationstechnik nach Wegen sucht, die Richtigkeit, Authentizität und Rechtmäßigkeit der Daten der Betroffenen sicherzustellen.

Was ist zu tun?
Die aktuellen beschleunigten Zentralisierungsbemühungen, die übrigens auch im Bereich der Kfz-Zulassung verfolgt werden, müssen ausgesetzt werden. Nur über eine gemeinsame Planung und eine geordnete Datenüberführung kann der Anspruch der Betroffenen auf fehlerfreie Speicherung ihrer personenbezogenen Informationen gewährleistet werden.

4.4.3 Fahrerlaubnisbehörden sind überwiegend gut aufgestellt

Die Kontrolle von vier Fahrerlaubnisbehörden zeigte, dass diese mittlerweile die rechtlichen Vorgaben des Straßenverkehrsgesetzes und des Landesdatenschutzgesetzes gut umgesetzt haben.

Wir konnten feststellen, dass die Akten zu Betroffenen, denen die Fahrerlaubnis entzogen wurde, mittlerweile nur noch so lange aufbewahrt werden, wie es der Gesetzgeber fordert. Dies war in der Vergangenheit ein häufiger Kritikpunkt von unserer Seite gewesen. Aktenbestände, die auch höchst sensible medizinisch-psychologische Gutachten enthalten, werden inzwischen überall so **sicher aufbewahrt**, dass ein Zugang Unbefugter verhindert wird.

Die Speicherung von Daten, die die Fahrerlaubnisbehörden über **möglicherweise ungeeignete Fahrzeugführer** von den Polizeidienststellen erhalten, wird in den Fahrerlaubnisbehörden dagegen unterschiedlich gehandhabt. Hier zeigt sich, dass es unbedingt erforderlich ist, einheitliche Regelungen zu finden (Tz. 4.4.1).

4.5 Soziales

Hartz IV schafft Arbeit! Was sich die Arbeitsmarktreformer erträumten, ist zumindest beim ULD Wahrheit geworden. Die Anzahl der Eingaben und Anfragen erreichte einen traurigen Rekord.

2007 dürfte im Sozialbereich des ULD „**Vollbeschäftigung**“ garantiert sein. Zwar stellt die Bundesagentur für Arbeit (BA) seit Juni 2006 endlich die mit den Datenschutzbeauftragten überarbeiteten und nunmehr datenschutzgerecht gestalteten Vordrucke zur Verfügung. Gleichwohl fehlt es weiterhin an datenschutzgerechten Berechtigungs- und Löschungskonzepten für zentrale EDV-Verfahren wie A2LL (28. TB, Tz. 4.5.1). Durch Prüfungen vor Ort werden wir auf aktuelle Missstände reagieren (Tz. 4.5.3).

2006 war ein Jahr, in dem Fälle von **misshandelten Kindern** traurige Schlagzeilen machten. Am Datenschutz kann es nicht gelegen haben. Die bestehenden Vorschriften im Kinder- und Jugendhilferecht ermöglichen notwendige Mitteilungen und eröffnen dadurch Handlungsoptionen für alle beteiligten Stellen, doch Aufklärung tut not (Tz. 4.5.11).

4.5.1 Datenschutzkontrollzuständigkeit über die Arbeitsgemeinschaften (ARGEn)

Über das Gesetz zur Fortentwicklung in der Grundsicherung findet sich seit dem August 2006 im Sozialgesetzbuch II eine Regelung, wonach die Bundesanstalt für Arbeit die datenschutzrechtlich verantwortliche Stelle ist, wenn die ARGEn Aufgaben der BA wahrnehmen. Doch wie weit geht diese Verantwortung?

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat eine aus unserer Sicht zutreffende und praxistaugliche Auslegung dieser Regelung geliefert. Den einzelnen Leistungsträgern, also der Bundesagentur für Arbeit (BA) und den Kommunen, obliegt eine **Finanzierungs- und Gewährleistungsverantwortung**. Korrespondierend hierzu stellt die BA den ARGEn zentrale IT-Verfahren, verbindliche Handlungsempfehlungen und einheitliche Vordrucke zur Verfügung.

Aufgabe der ARGE ist es, mittels dieser zentralen Vorgaben vor Ort die Leistungsgewährung durchzuführen. Den ARGEn obliegt insoweit die **Aufgabenwahrnehmungs- bzw. Durchführungsverantwortung**. Der gesetzliche Auftrag des individuellen Förderns und Forderns von Hilfebedürftigen ist durch die ARGEn wahrzunehmen. Die Datenschutzbeauftragten des Bundes und der Länder haben in einem Beschluss die sich daraus ergebenden Konsequenzen aufgezeigt:

- Die Kontrollkompetenz der Landesbeauftragten für den Datenschutz bezieht sich auf alle Leistungen nach dem Sozialgesetzbuch (SGB) II.
- Die ARGEn sind unmittelbare Adressaten von eventuellen Beanstandungen der Landesbeauftragten. In Fällen grundsätzlicher Art soll der BfDI über Beanstandungen unterrichtet werden.
- Auch wenn der BfDI Kontrollstelle für die zentralen IT-Verfahren der BA ist, sind die ARGEn verpflichtet, den Landesbeauftragten Einblick in oder Auskunft über die technischen Verfahren zu geben, die zu bestimmten Beschwerden Anlass geben. Entsprechendes gilt auch für die Hinweise zu den Verfahren, Empfehlungen usw. der BA. Die Landesbeauftragten können diese Verfahren/Hinweise selbst nicht datenschutzrechtlich bewerten, aber sie müssen diese zur Kontrolle der datenschutzgerechten Aufgabenerfüllung der ARGEn direkt vor Ort zur Kenntnis nehmen können.

Das Bundesministerium für Arbeit und Soziales (BMAS) als Aufsichtsbehörde teilt diese rechtliche Bewertung. So sind – trotz mancher Unklarheit in der gesetzlichen Regelung – zumindest auf Vollzugsebene die **Irritationen** über die Zuständigkeit bei der Datenschutzkontrolle hoffentlich **beseitigt** (28. TB, Tz. 4.5.1).

Was ist zu tun?
Die Datenverarbeitung in den ARGEn ist kein kontrollfreier Raum. Die Landesbeauftragten überwachen in enger Abstimmung mit dem Bundesbeauftragten die Einhaltung datenschutzrechtlicher Vorschriften bei der Gewährung von Arbeitslosengeld II. Die Geschäftsführungen der ARGEn haben bei dieser Aufgabenwahrnehmung gegenüber den Landesbeauftragten eine Mitwirkungspflicht.

4.5.2 Viel Ärger um die ARGE Lübeck

Ende November 2005 erfolgte eine Prüfung der konventionellen Datenverarbeitung bei der ARGE Lübeck. Die Prüfung war geprägt von massiven Behinderungen der Prüftätigkeit des ULD. Trotz unserer beschränkten Erkenntnismöglichkeiten waren die Ergebnisse unserer Prüfung alarmierend.

Die Geschäftsführung der ARGE war vorab von unserer beabsichtigten Prüfung unterrichtet worden. Vom ersten Tag an weigerte sie sich, den Prüfern **Einblick in die elektronischen Datenverarbeitungssysteme** wie A2LL oder coArB zu gewähren und bestehende Dienstanweisungen bzw. Arbeitsrichtlinien auszuhändigen. In den Akten wurden die zahlreichen Ausdrucke aus den EDV-Verfahren unkenntlich gemacht. Der Geschäftsführer der ARGE behauptete, auf Weisung der Regionaldirektion Nord der BA zu handeln. Die Regionaldirektion erklärte später, eine derartige Weisung nie erteilt zu haben.

Aufgrund dieser Weigerung war es unmöglich, die geprüften Einzelfälle komplett nachzuvollziehen. Ausgehende Schreiben befanden sich meist nicht in der Papierakte, sondern ausschließlich im Computer, ebenso waren viele Vermerke der Sachbearbeiter im IT-System gespeichert, die allenfalls als Screenshot ausgedruckt in die Akte gelangten und den Prüfern verweigert wurden. Eine **reguläre datenschutzrechtliche Prüfung** war nicht möglich.

Die **Weigerung** der Geschäftsführung wurde als Verstoß gegen die gesetzliche Mitwirkungspflicht der öffentlichen Stellen, das ULD bei der Erfüllung seiner Aufgaben zu unterstützen und hierzu die erforderlichen Auskünfte zu erteilen sowie Einsicht in Unterlagen und Dateien zu gewähren, beanstandet.

Weiterhin mussten wir beanstanden, dass die Geschäftsführung zum Zeitpunkt der Prüfung die gesetzlich geforderten schriftlichen **Dienstanweisungen** nicht vorlegen konnte bzw. auf mündliche Anweisungen verwies, die bei den Mitarbeiterinnen und Mitarbeitern aber – wenn überhaupt – nur bedingt bekannt waren bzw. von diesen nicht beachtet wurden. Dieser Verstoß wiegt besonders schwer, zumal wir feststellen mussten, dass – wohl auch wegen des Fehlens entsprechender Dienstanweisungen – in verschiedenen Bereichen unzulässige Datenerhebungen, -speicherungen oder -übermittlungen erfolgten. Schriftliche Dienstanweisungen sind unabdingbare Voraussetzung für die Beachtung des Sozialgeheimnisses.

Es überraschte uns schon nicht mehr, dass bei der Prüfung der **Einzelakten** der Sachbearbeiter (der sogenannte persönliche Ansprechpartner) bzw. der Vorgänge des Ermittlungsdienstes weitere schwerwiegende Verstöße zu beanstanden waren. Alleine in acht von zehn nach einem Zufallsprinzip ausgesuchten Akten der persönlichen Ansprechpartner fanden sich zum Teil gleich mehrere Datenschutzverletzungen. Fast durchgängig waren nicht erforderliche Daten erhoben und gespeichert worden (Kontoauszüge, Mietverträge ...). Bei dem besonderen Problembereich Ermittlungsdienst mussten wir u. a. feststellen, dass in Abwesenheit der Eltern minderjährige Kinder befragt wurden und regelrechte Observationen erfolgt waren.

Es passte ins Bild, dass die Geschäftsführung der ARGE es nicht für notwendig hielt, einen Mitarbeiter zum **behördlichen Datenschutzbeauftragten** zu bestellen. Dieser hätte vielleicht einiges verhindern können.

Was ist zu tun?
Die Geschäftsführung einer ARGE darf sich ihrer datenschutzrechtlichen Verantwortung nicht entziehen. Die Mitarbeiterinnen und Mitarbeiter benötigen verbindliche schriftliche Vorgaben. Durch Schulungen ist auf die konsequente Beachtung des Sozialdatenschutzes hinzuwirken.

4.5.3 Hausbesuche? Wenn überhaupt, dann bitte datenschutzgerecht!

Hausbesuche sind als besondere Form der Datenerhebung nicht grundsätzlich unzulässig, oft aber nicht erforderlich. Wegen ihres für den Betroffenen besonders belastenden Charakters muss der Außendienst in jedem Fall besondere Regeln beachten.

Die **Liste der Eingaben** von ALG-II-Empfängern beim ULD ist erschreckend lang. Bei einer Prüfung mussten wir feststellen, dass eine Hilfesuchende verdeckt observiert wurde. In der Akte befand sich ein Überwachungsprotokoll. In einem anderen Fall wurde die minderjährige Tochter gefragt, ob die Mama nicht einen neuen Freund habe. Die Mutter selbst war gerade auf der Arbeit. Eine andere Betroffene schilderte uns, dass ohne ihr Wissen ihr Briefkasten durchsucht worden sei. Eine völlig verunsicherte Frau beschwerte sich, dass mit einer Videokamera Aufnahmen von ihrem Schlafzimmer und anderen Räumen gemacht wurden. Hilfesuchende, die nur zur Untermiete wohnten, schilderten uns, dass Außendienstmitarbeiter darauf bestanden, dass auch die vom Hauptmieter genutzten Räume besichtigt wurden, obwohl diese gar keine Leistungen bezogen.

Häufigster Grund für Hausbesuche scheint der Verdacht einer ARGE zu sein, dass der Hilfesuchende in einer Einstands- und Verantwortungsgemeinschaft lebt („eheähnliche Gemeinschaft“), dieses jedoch verschweigt (23. TB, Tz. 4.7.3). Beim Vorliegen einer solchen **Bedarfsgemeinschaft** ist das Einkommen und Vermögen des Lebenspartners zu berücksichtigen. Seit August 2006 können auch gleichgeschlechtliche Beziehungen als eheähnliche Gemeinschaft bewertet werden.

Nach unserer Kenntnis können in Schleswig-Holstein alle ARGEn auf einen **Außen- bzw. Ermittlungsdienst** zurückgreifen. Das Gesetz sieht dies neuerdings zur Bekämpfung von Leistungsmissbrauch ausdrücklich verpflichtend vor. Doch für die Wahrnehmung der Aufgabe versäumte es die BA, den ARGEn praktikable und datenschutzkonforme Vorgaben zu machen. Dieses Defizit ist vor Ort sofort erkennbar. Wann ist ein Hausbesuch als letztes Mittel der Sachverhaltsklärung zulässig? Welche Befugnisse hat der Außendienstmitarbeiter bzw. welche Rechte und Mitwirkungspflichten der Betroffene? Welche Daten dürfen wie erhoben werden? Wie muss die Tätigkeit des Außendienstes in der Leistungsakte beweiskräftig dokumentiert werden? Wie prüft man, ob zwei Hilfesuchende zusammen

leben? Dürfen Nachbarn befragt werden? Ohne Hilfestellung kommt es zwangsläufig zu den beschriebenen Fehlern beim Einsatz des Ermittlungsdienstes. Unter

www.datenschutzzentrum.de/sozialdatenschutz/hausbesuche.htm

haben wir „**Hinweise zur datenschutzgerechten Ausgestaltung** von Hausbesuchen im Bereich der Leistungsgewährung nach den Vorschriften des SGB II und SGB XII“ als Handreichung für die ARGEn zur rechtskonformen Durchführung von Ermittlungen veröffentlicht.

Diese Hinweise enthalten neben einer **Musterdienstanweisung** auch Mustervordrucke eines Prüfauftrages, eines Prüfprotokolls und eines Prüfberichtes. Die Unterlagen stehen als bearbeitbare RTF-Dateien zur Verfügung.

Was ist zu tun?
Leistungsträger, die einen Außen- bzw. Ermittlungsdienst einrichten, sollten durch innerorganisatorische Maßnahmen dafür sorgen, dass unsere Hinweise zur datenschutzgerechten Ausgestaltung von Hausbesuchen beachtet werden.

4.5.4 Informationsbroschüre zum Arbeitslosengeld II

Was ist der Unterschied zwischen einer Wohn-, einer Haushalts- und einer Bedarfsgemeinschaft? Muss ich meine Kontoauszüge vorlegen? Darf das Amt bei meiner Bank mein Konto einsehen? Wenn ein Mitarbeiter der Behörde an meiner Wohnungstür klingelt, muss ich ihn reinlassen?

Unsere aktuelle Informationsbroschüre „Arbeitslosengeld II – Die häufigsten Fragen zum Datenschutz beim Arbeitslosengeld II“ gibt **kurze und leicht verständliche Antworten** auf diese und weitere Fragen. Die Broschüre kann unter der Telefonnummer 0431/988-1210 angefordert oder unter

www.datenschutzzentrum.de/download/br_alg2.pdf

heruntergeladen werden.

4.5.5 Vermittlungsvorschlag – Einwilligung zwecks Übermittlung an potenziellen Arbeitgeber?

Es ist übliche Praxis der ARGEn, potenzielle Arbeitgeber zu informieren, welche Arbeitsuchenden aufgefordert wurden, sich bei ihnen zu bewerben. Gleichzeitig wird der Arbeitgeber gebeten, über das Ergebnis der Bewerbung zu berichten. Der Arbeitsuchende selbst erfährt von diesem „Datenaustausch“ oft nichts.

Diese Praxis geht auf eine Vorgabe der BA zurück. Wird der Kandidat nicht eingestellt, so wird **vom Arbeitgeber Auskunft** verlangt, weshalb der Bewerber nicht für geeignet gehalten wurde, welche gesundheitlichen Einschränkungen

dieser geltend machte oder ob diesem Arbeitsweg, Arbeitszeit oder Gehalt nicht zusagten.

Die BA begründete diesen Datenaustausch damit, Arbeitsuchende und Arbeitgeber müssten zusammengebracht werden. Arbeitsvermittler bestätigen aber immer wieder, dass es oft gerade nicht hilfreich ist, wenn beim Arbeitgeber der Eindruck entsteht, der Arbeitsuchende bewerbe sich nur, weil das Amt ihn hierzu aufgefordert hat. Letztlich räumte die BA ein, dass das eigentliche Ziel der automatischen Einschaltung der Arbeitgeber in der **Kontrolle der Arbeitsuchenden** liegt. Es sei erforderlich, bei einem Nicht-zustande-Kommen eines Arbeitsverhältnisses die Gründe zu analysieren und gegebenenfalls zu beseitigen, um die Chancen für künftige Bewerbungsversuche zu verbessern. Wir fragten die BA, ob dieses Ziel denn nur dadurch erreicht werden könne, dass Arbeitgeber hinter dem Rücken der Bewerber ausgefragt werden. Die Antwort der BA erstaunte uns. Die Arbeitsvermittlung sei eben Aufgabe der BA. Den Betroffenen einzubeziehen, ihn zu informieren oder sogar um Einwilligung zu bitten, würde angeblich die Anbahnung eines Beschäftigungsverhältnisses be- oder gar verhindern.

Bei dem „Vermittlungsvorschlag“ handelt es sich um einen zentralen Vordruck der BA. Die datenschutzrechtliche Bewertung dieses Vordruckes bzw. das Verfahren an sich und die sich hieraus ergebende Speicherung der Daten im EDV-Verfahren VerBIS liegt formell in der Zuständigkeit des Bundesbeauftragten für den Datenschutz. Wir haben dem Bundesbeauftragten unsere kritische Sicht mitgeteilt und gebeten, sich für ein Verfahren einzusetzen, das für den Betroffenen datenschutzfreundlicher ist.

Was ist zu tun?
Die BA ist aufgefordert, die Datenschutzrechte der Betroffenen stärker zu berücksichtigen. Die Verarbeitung seiner Daten muss für den Hilfesuchenden transparent gestaltet werden. Arbeitsuchende sind vorab zu unterrichten und um Einwilligung zu bitten, bevor Arbeitgeber durch die Übersendung eines Vermittlungsvorschlages hinter dem Rücken der Betroffenen informiert oder ausgefragt werden.

4.5.6 Die Ortsabwesenheitsklausel

Eingliederungsvereinbarungen enthalten für den Arbeitsuchenden u. a. die Verpflichtung, sich nur nach Absprache und mit Zustimmung des persönlichen Ansprechpartners außerhalb des zeit- und ortsnahen Bereiches aufzuhalten und persönlich an jedem Werktag am Wohnsitz oder gewöhnlichen Aufenthaltsort erreichbar zu sein.

Muss sich der Betroffene bei seinem persönlichen Ansprechpartner (pAp) – also dem Sachbearbeiter – abmelden, wenn er zum Einkaufen in die Stadt fährt? Wird eine Liste über die Ortsabwesenheiten geführt? Auf Nachfrage erfuhren wir, dass die in den Eingliederungsvereinbarungen verwendeten Formulierungen zentral von der Bundesagentur für Arbeit (BA) vorgegeben sind. Erstaunt hat uns die Unkenntnis in den ARGEn hierzu. Kaum eine ARGE konnte uns konkret darlegen, welche Abwesenheiten der Betroffene anzugeben hat. Dabei hilft ein Blick ins Gesetz. Das Sozialgesetzbuch II verweist auf eine **Erreichbarkeitsanordnung** der BA. Die BA stellt den ARGEn zudem ausführliche fachliche Hinweise zur Verfügung. Aus diesen Unterlagen, die spätestens auf Nachfrage jedem Betroffenen auszuhändigen sind, ergibt sich u. a. Folgendes:

Erreichbar zu sein bedeutet zunächst sicherzustellen, dass der Hilfebedürftige persönlich an jedem Werktag an seinem Wohnsitz oder gewöhnlichen Aufenthaltsort unter der von ihm genannten Anschrift **durch Briefpost** erreicht werden kann. Dadurch soll sichergestellt werden, dass die Leistungsträger den Betroffenen über aktuelle Arbeitsangebote oder Eingliederungsmaßnahmen informieren können und dass der Hilfebedürftige hierauf zeitnah reagieren kann. Es ist nicht erforderlich, den ganzen Tag in seiner Wohnung vor dem Telefon zu sitzen. Der Betroffene kann sich also grundsätzlich frei bewegen, ohne sich bei seinem persönlichen Ansprechpartner abmelden zu müssen.

Verlässt der Hilfeempfänger seinen Wohnort, bleibt aber im **Nahbereich** erreichbar, so muss er dem Amt seine Anschrift für die Dauer der Abwesenheit mitteilen. Zum Nahbereich gehören die Orte in der Umgebung der ARGE, von denen aus der erwerbsfähige Hilfebedürftige in der Lage wäre, den Leistungsträger oder unter Umständen mögliche Arbeitgeber täglich und ohne unzumutbaren Aufwand zu erreichen. Entscheidend ist, dass der Hilfebedürftige für die Vorsprache im Amt eine Pendelzeit von weniger als insgesamt 2,5 Stunden benötigt.

Verlässt der Hilfebedürftige diesen Nahbereich bzw. ist er nicht mehr werktags erreichbar, so bedarf es der vorherigen **Zustimmung der ARGE**. Aber auch Arbeitslose haben einen Anspruch auf Urlaub. Dieser muss jedoch beantragt und genehmigt werden.

Was ist zu tun?
Wird eine konkrete Forderung für den Hilfeempfänger in die Eingliederungsvereinbarung aufgenommen, z. B. zur Erreichbarkeit, so muss diese verständlich sein. Dem Betroffenen sind ausreichend Informationen, z. B. durch die Aushändigung der Handlungshilfen, zu geben.

4.5.7 Datenaustausch zwischen ARGE und Maßnahmeträgern

Ein-Euro-Jobs, Bewerbungstraining, Umschulungs- oder Qualifizierungsmaßnahmen – die ARGEn haben ein umfangreiches Angebot, zu dem sie häufig private Unternehmen, die sogenannten Maßnahmeträger, beauftragen. Vieles wird vom Land oder aus Mitteln des Europäischen Sozialfonds (ESF) gefördert. Damit alles reibungslos funktioniert, werden Unmengen von Daten zwischen den beteiligten Stellen ausgetauscht.

Auf welcher Rechtsgrundlage geschieht dies eigentlich? Der Arbeitsuchende ist vor Beginn über die Inhalte und Zielsetzung der Maßnahme und den Umfang der zu erwartenden Datenverarbeitung zu unterrichten. Dieses **Wissen ist Grundlage** für die Rechtmäßigkeit der Datenverarbeitung und zwingend erforderlich, damit der Betroffene frei entscheiden kann, ob er an einer konkreten Maßnahme teilnehmen möchte. Die Teilnahme an einer Maßnahme kann Gegenstand der Eingliederungsvereinbarung sein.

- **Darf die ARGE Daten an den Maßnahmeträger übermitteln?**

Wird der Maßnahmeträger von der ARGE bzw. der BA mit der Durchführung der Maßnahme beauftragt, so darf die ARGE dem Maßnahmeträger Sozialdaten des Betroffenen übermitteln, soweit dies zur Erfüllung der übertragenen Aufgabe erforderlich ist (§ 50 SGB II). Hat der Betroffene zuvor seine Bereitschaft an der Teilnahme der Maßnahme erklärt, so bedarf es nun für die Übermittlung der erforderlichen Daten keiner weiteren Einwilligung des Betroffenen. In vielen Fällen mag es aber durchaus möglich und auch sinnvoll sein, dass der Betroffene selbst dem Maßnahmeträger die erforderlichen Daten liefert.

- **Darf der Maßnahmeträger an die ARGE Daten übermitteln?**

Er ist durch das SGB II dazu sogar verpflichtet. Er muss Auskunft darüber erteilen, ob und inwieweit zu Recht Leistungen erbracht werden. Wird die Maßnahme nicht ordnungsgemäß durchgeführt, so sind auf Nachfrage die Gründe hierfür mitzuteilen. Dies können z. B. Fehlzeiten, die unzureichende Mitwirkung, die Unterbrechung oder der Abbruch der Maßnahme sein. Das Gesetz ermöglicht die aktuelle Unterrichtung der ARGEn, ob der Betroffene die Maßnahme begonnen hat und durchgehend teilnimmt.

Ein Maßnahmeträger ist zudem verpflichtet, eine **Beurteilung von Leistung und Verhalten** des Teilnehmers vorzunehmen und dieses Ergebnis unverzüglich der ARGE mitzuteilen. Hat der Betroffene zuvor seine Bereitschaft zur Teilnahme an der Maßnahme erklärt und wurde er über die bevorstehende Datenverarbeitung unterrichtet, so ist keine zusätzliche Einwilligungserklärung nötig. Die Regionaldirektion Nord der BA erläuterte uns, dass es bislang keine verbindlichen Vorgaben gebe, wie eine derartige Beurteilung durchzuführen bzw. in welcher Form sie der ARGE mitzuteilen ist. Üblich sei ein Arbeitszeugnis am Ende einer Maßnahme. Dieses könne der Betroffene auch bei Arbeitgebern vorlegen. Aus unserer Sicht ist ein solches Arbeitszeugnis eindeutig einer ungeregelten Rückmeldung vorzuziehen.

- **Darf der Maßnahmeträger Daten von Teilnehmern an andere Dritte wie Arbeitgeber oder Förderer übermitteln?**

In Ermangelung einer gesetzlichen Befugnis ist dies nur zulässig, wenn der Betroffene zuvor über die beabsichtigte Übermittlung unterrichtet wurde und – grundsätzlich schriftlich – seine Einwilligung erklärt hat. Entsprechende Erklärungen sollten zu Beginn der Maßnahme eingeholt werden und können Bestandteil eines Betreuungs- oder Maßnahmevertrages zwischen dem Maßnahmeträger und dem Betroffenen sein.

Was ist zu tun?
Die ARGEn, aber auch die Maßnahmeträger, müssen die Betroffenen umfassend über Art und Inhalt einer Maßnahme und die beabsichtigte Datenverarbeitung unterrichten. Die ARGEn haben weitgehende Möglichkeiten zum transparenten Informationsaustausch mit den Maßnahmeträgern. Übermittlungen an andere dritte Stellen, wie z. B. Arbeitgeber, bedürfen grundsätzlich einer schriftlichen Einwilligungserklärung des Betroffenen.

4.5.8 Beschäftigungsorientiertes Fallmanagement im SGB II

Erfolgreiche Arbeitsvermittlung setzt zielgerichtetes Fallmanagement voraus. Im Rahmen eines sogenannten Profiling erfolgt eine umfangreiche Datenerhebung über die berufliche, familiäre und soziale Situation des Betroffenen. Die Verwendung und Nutzung dieser Daten bedürfen dringender denn je einer datenschutzrechtlichen Bestandsaufnahme.

Es gibt in Deutschland keine Behörde, die **so viele so sensible Informationen** von so vielen Menschen sammelt wie die ARGEn und die BA. Bereits die Antragsvordrucke enthalten auf aktuell 31 Seiten (!) Unmengen an Datenfeldern. Zusätzlich erfolgt ein intensives Profiling mithilfe eines Profilingbogens. Schon 2005 präsentierte die BA ihr Fachkonzept „Beschäftigungsorientiertes Fallmanagement im SGB II“. Dieses Konzept sieht u. a. die Erfassung aller erwerbsfähigen Leistungsempfänger vor. Fragen zum schulischen und beruflichen Werdegang, zur familiären und gesundheitlichen Situation, zu Drogen, Vorstrafen, Schulden, Eheproblemen, ja selbst zum Freundeskreis sind zu beantworten. Dies soll eine Chancen- und Risikoeinschätzung ermöglichen und Vermittlungshemmnisse feststellen.

Sind wirklich alle Daten erforderlich? Bringen die Daten den Arbeitsuchenden wirklich einem Arbeitsplatz näher? Wie wird mit diesen riesigen Datenmengen gearbeitet? Nur wenn sich diese Fragen zufriedenstellend beantworten ließen, wäre die Datenerhebung erforderlich und damit zulässig. Nötig ist ein Blick hinter die Kulissen: Beim Profiling werden „harte“ und „weiche“ Daten erhoben. So gehören z. B. Daten über den beruflichen Werdegang zu den harten Daten; diese sind objektiv und bedürfen keiner **Einschätzung durch den Sachbearbeiter**. Anders hingegen die weichen Daten. Bei Angaben zur Motivation oder zum Erscheinungsbild muss der Sachbearbeiter eine Bewertung vornehmen. Diese

Bewertung erfolgt vergleichbar mit einem Schulnotensystem. Alle diese Daten werden in zentralen Verfahren wie A2LL oder VerBIS verwaltet. Aus Datenschutzsicht bestehen u. a. folgende Anforderungen:

- **Prüfung der Erforderlichkeit im konkreten Einzelfall**

Daten können in einem Fall erforderlich, im nächsten Fall aber völlig unwichtig sein. Jeder Vordruck, jedes standardisierte Verfahren bedingt die Gefahr einer unreflektierten schematischen Datenerhebung. So muss z. B. nicht in jedem Fall nach der Konfession gefragt werden; nur bei wenigen Berufen spielt diese wirklich eine Rolle. Entsprechend variabel sind die Verarbeitungssysteme und die Befragungspraxis zu gestalten. Hilfesuchende müssen besser unterrichtet, die Mitarbeiterinnen und Mitarbeiter stärker sensibilisiert werden. Das neue Allgemeine Gleichbehandlungsgesetz führt zu weiteren Restriktionen bei der Datenerhebung.

- **Transparenz der Datenerhebung**

Jede Datenerhebung muss für den Betroffenen transparent sein. Der Betroffene muss wissen oder zumindest erkennen können, welche Daten zu welchem Zweck bei ihm oder anderen Stellen erhoben werden. Daher sind Verfahren zu begrüßen, die systemseitig eine laufende Unterrichtung des Hilfesuchenden, z. B. durch Ausdruck und Aushändigung des vorhandenen Datenprofils, vorsehen.

- **Handlungsbedarf statt Schulnoten**

Wem nützt es, wenn ein Sachbearbeiter in dem Datenfeld „Erscheinungsbild“ eine Schulnote von 1 bis 6 eingibt und diese Eingabe keine weitere praktische Konsequenz hat? Ein zielgerichtetes System sollte statt subjektiver Schulnoten Handlungsbedarf aufzeigen und umsetzen. Ist ein Sachbearbeiter der Meinung, dass ein Vermittlungshemmnis vorliegt, so muss diese Einschätzung zu einer Handlung führen, unter Umständen umgesetzt über Vorgaben für die abzuschließende Eingliederungsvereinbarung.

Was ist zu tun?
BA und ARGEn sind aufgefordert, ihre Datenerhebung vor allem im Bereich des Profiling kritisch auf die fachliche Erforderlichkeit zu hinterfragen. In Schleswig-Holstein bieten Audit- oder Gütesiegelverfahren eine Basis zur formellen Feststellung der datenschutzgerechten Gestaltung der Datenverarbeitung.

4.5.9 ARGE will gemeinnützigen Verein abschöpfen

Wer einem Arbeitslosengeld-II-Empfänger Leistungen erbringt, die geeignet sind, die Leistung des ALG II auszuschließen oder zu mindern, hat der ARGE auf Verlangen hierüber Auskunft zu erteilen. So will es das Gesetz. Dies berechtigt aber nicht zur Nachfrage bei einem gemeinnützigen Verein, welche Personen wie unterstützt wurden.

Stolz hielt die Vorsitzende eines gemeinnützigen Vereins einen Zeitungsartikel in ihrer Hand, der ausführlich darüber berichtete, wie ehrenamtlich gesammelte Spenden an Not leidende Bürgerinnen und Bürger ihrer Gemeinde verteilt wurden. Einer Familie wurde eine Kaffeemaschine geschenkt. In einem anderen Fall wurde dem Sohn ein Malkurs ermöglicht. Der Zeitungsartikel versprach Publicity und neue Spenden. Umso größer war der Schreck, als nur wenige Tage später Post von der örtlichen ARGE kam. Diese forderte die Vereinsvorsitzende unter Androhung eines Bußgeldes auf, Namen und Anschriften der **Spendenempfänger mitzuteilen**, die ALG II erhalten. Es müsse geprüft werden, ob die Spendenmittel auf das ALG II angerechnet werden könnten. Hilfe suchend bat uns die Vorsitzende um Rat.

Wir teilten der ARGE und dem Verein mit, dass derartige Anfragen nur zulässig sind, wenn sich die ARGE auf einen **konkreten Fall** beziehen kann. Die ARGE hat kein Recht, Daten nicht näher bezeichneter Personen von Dritten, hier vom Verein, zu erfragen, um diese dann abzugleichen. Unzulässig wäre auch die Weitergabe einer Liste mit Verdachtsfällen an den Verein mit der Aufforderung, die Fälle zu bestätigen. Dadurch käme es zu einer unzulässigen Übermittlung von Daten an den Dritten. Nur wenn es um klar zu benennende Hilfesuchende geht, kommt eine Einholung der Auskunft bei einer dritten Stelle in Betracht. Für die Zulässigkeit ist weiterhin erforderlich, dass ausreichende Anhaltspunkte dafür bestehen, dass die weitergeleiteten Spenden wirklich auf das ALG II anzurechnen sind. Eine geschenkte Kaffeemaschine führt ebenso wenig zu einer Leistungskürzung wie ein unentgeltlicher Malkurs. Nötig wären schon die Unterstützung des ALG-II-Empfängers mit **regelmäßigen bzw. größeren Geldbeträgen**. Zudem muss einer Datenerhebung bei einer dritten Stelle immer der Versuch vorausgehen, die Daten beim Betroffenen zu erheben. Erst wenn sich das als erfolglos erweist, kommt die Befragung Dritter in Betracht.

Was ist zu tun?
Auskunftsersuchen bei dritten Stellen sind nur unter engen Voraussetzungen zulässig. Die dritten Stellen sind auf die in Anspruch genommenen gesetzlichen Befugnisse hinzuweisen.

4.5.10 Datenerhebung im Jugendamt – Welche Rechte hat ein Amtspfleger?

Amtspfleger haben die Aufgabe, Unterhaltsansprüche eines Kindes gegenüber dem unterhaltspflichtigen Elternteil geltend zu machen. Dafür sind Angaben über die Einkommens- und Vermögensverhältnisse des Unterhaltsschuldners nötig. Was ist zu tun, wenn der Unterhaltsschuldner seine Mitwirkung – zu der er an sich verpflichtet ist – verweigert?

Im vom ULD zu beurteilenden Fall ging es um bestimmte Subventionen einer Behörde im Bereich der Landwirtschaft an den Unterhaltspflichtigen. Der Amtspfleger begehrte hierüber Auskunft. Der nach dem Bürgerlichen Gesetzbuch bestehende **Auskunftsanspruch** richtet sich primär gegen den Unterhaltspflichtigen. Das Kind bzw. die Kindesmutter kann diesen Auskunftsanspruch nur zivilgerichtlich durchsetzen. Der Amtspfleger hat jedoch aufgrund seiner Stellung als Mitarbeiter des Jugendamtes weitergehende Möglichkeiten.

Der Amtspfleger darf direkt Daten bei **Arbeitgebern und öffentlichen Stellen** erheben, wenn

- der Unterhaltsschuldner über seine Auskunftspflicht gegenüber dem unterhaltsberechtigten Kind bzw. dem Amtspfleger/Unterhaltsbeistand unterrichtet worden ist,
- der Betroffene unter Hinweis darauf, dass vom Amtspfleger/ Unterhaltsbeistand bei fehlender oder bei nicht ausreichender Auskunft eine direkte Datenerhebung beim Arbeitgeber oder öffentlichen Stellen erfolgt, gemahnt wurde und
- der Unterhaltsschuldner dennoch seiner Auskunftspflicht nicht oder nicht ausreichend nachgekommen ist.

Der Auskunftsanspruch erstreckt sich auch auf die Personen, mit denen der Unterhaltsschuldner in einer neuen Ehe bzw. in einer Lebensgemeinschaft lebt, soweit die **Einkünfte des neuen Ehepartners** bzw. des neuen Lebensgefährten dem Unterhaltsschuldner zuzurechnen sind. Öffentliche Stellen sind nach dem allgemeinen Datenschutzrecht zur Auskunftserteilung gegenüber dem Amtspfleger/ Unterhaltsbeistand berechtigt und grundsätzlich auch verpflichtet.

Was ist zu beachten?
Ein Amtspfleger bzw. Unterhaltsbeistand hat unter Beachtung der datenschutzrechtlichen Vorschriften das Recht, erforderliche Daten über das Einkommen und Vermögen des Unterhaltsschuldners direkt bei Arbeitgebern und öffentlichen Stellen zu erheben, wenn der Unterhaltsschuldner entgegen seiner Verpflichtung die erforderlichen Auskünfte nicht erteilt.

4.5.11 Informationen zum Schutz des Kindeswohls

Das Gesetz zur Weiterentwicklung der Kinder- und Jugendhilfe (KICK) macht Jugendämtern sowie freien Trägern der Jugendhilfe Vorgaben, wie sie sich bei einem Verdacht auf Kindeswohlgefährdung verhalten müssen. Diese Vorgaben gilt es in die Praxis umzusetzen.

Man stelle sich folgenden Fall vor: Eine Erzieherin bemerkt in ihrem Kindergarten, wie sich ein vormals fröhliches und aufgeschlossenes Kind immer mehr zurückzieht. Wiederholt wird das Kind von der Mutter nicht pünktlich abgeholt. Anstelle eines gesunden Frühstücks hat das Kind neuerdings nur unregelmäßig einen Schokoriegel im Gepäck. Die Kleidung ist nicht mehr so gepflegt wie noch vor wenigen Monaten. Sind dies erste Anzeichen einer Vernachlässigung? Wie soll die Erzieherin reagieren – die Mutter ansprechen oder gleich das **Jugendamt informieren**? Das Gesetz sieht für die Erzieherin ein Vorgehen in Stufen vor.

Stufe 1 – Einschätzung des Gefährdungsrisikos

Zunächst muss die Erzieherin aus fachlicher Sicht eine Einschätzung des Gefährdungsrisikos vornehmen. Diese Einschätzung sollte die Erzieherin gemeinsam mit (eventuell externen) Fachkräften vornehmen. Der Gesetzgeber verlangt, dass dabei den Fachkräften nicht der Name des Kindes bzw. der Sorgeberechtigten mitgeteilt wird („Pseudonymisierung“). Nur wenn es aus fachlicher Sicht nicht vermeidbar ist, darf die Identität des Kindes preisgegeben werden. Soweit möglich und angebracht, sollen bei der Einschätzung des Gefährdungsrisikos die Personensorgeberechtigten und das Kind einbezogen werden.

Stufe 2 – Angebot einer Hilfestellung

Wenn nach Einschätzung des Gefährdungsrisikos zur Abwendung der Gefahr die Gewährung von Hilfen für geeignet und notwendig gehalten wird, sind diese den Personen- bzw. Sorgeberechtigten anzubieten. Die (externen) Fachkräfte sollen darauf hinwirken, dass die Personen- bzw. Sorgeberechtigten die Hilfen annehmen.

Stufe 3 – Unterrichtung des Jugendamtes

Werden die angebotenen Hilfestellungen nicht angenommen oder sind diese nicht ausreichend, um die Gefährdung des Kindeswohls abzuwenden, so ist mit Einwilligung des Personen- bzw. Sorgeberechtigten das Jugendamt zu informieren. Wird die Einwilligung nicht erteilt, kann eine Unterrichtung dennoch erfolgen, wenn die Kindeswohlgefährdung nicht anderweitig abgewendet werden kann.

Stufe 4 – Unterrichtung des Familiengerichtes durch das Jugendamt

Sind die Personen- oder Sorgeberechtigten nicht bereit, an der Gefährdungseinschätzung mitzuwirken, oder hält das Jugendamt es aus anderen Gründen für erforderlich, kann es das Familiengericht anrufen.

Stufe 5 – Inobhutnahme des Kindes durch das Jugendamt

Besteht eine dringende Gefahr und kann die Entscheidung des Familiengerichtes nicht abgewartet werden, so ist das Jugendamt verpflichtet, das Kind in Obhut zu nehmen.

Stufe 6 – Einschaltung der Polizei

Soweit es zur Abwendung der Gefährdung erforderlich ist, hat das Jugendamt bzw. der freie Träger der Jugendhilfe den Personen- bzw. Sorgeberechtigten aufzufordern, die Polizei, andere Leistungsträger oder Einrichtungen der Gesundheitshilfe in Anspruch zu nehmen. Ist ein sofortiges Tätigwerden erforderlich oder wirken die Personensorgeberechtigten nicht mit, so muss das Jugendamt diese Stellen selbstständig einschalten.

Zur Umsetzung dieses Verfahrens sollen die Jugendämter mit den freien Trägern der Jugendhilfe **Vereinbarungen** treffen. Darin sind insbesondere Regelungen zur Einschaltung und zum Tätigwerden der (externen) Fachkräfte vorzusehen.

An dieser Stelle muss das Amt für Jugend und Sport des **Kreises Plön lobend erwähnt** werden. Es organisierte für die Leitungskräfte aller Kindertageseinrichtungen die Veranstaltungsreihe „Kinderschutz in Kooperation von Kindertageseinrichtungen und dem Allgemeinen Sozialen Dienst“. Die Teilnehmerinnen und Teilnehmer wurden über die aktuelle Rechtslage unterrichtet und konnten ihre Erfahrungen austauschen. Das ULD war eingeladen, über die Vorschriften zu referieren und mit zu diskutieren. Dabei zeigte sich: Nicht Datenschutz, sondern mangelnde Kenntnis der Vorschriften behindert die Arbeit.

Was ist zu tun?
Die datenschutzrechtlichen Vorschriften im Bereich der Kinder- und Jugendhilfe geben den Jugendämtern und den freien Trägern der Jugendhilfe hilfreiche Vorgaben, wie bei einem Verdacht von Kindeswohlgefährdung zu verfahren ist. Die Mitarbeiterinnen und Mitarbeiter sind aufgefordert, sich die erforderlichen Kenntnisse anzueignen.

4.5.12 Neue Instrumente bei der Eingliederungshilfe

Neue Methoden wie z. B. eine konsequente Hilfeplanung und das sogenannte Case-Management sollen behinderten Menschen effektivere Hilfen ermöglichen. Die Datenschutzrechte der Betroffenen dürfen dabei nicht ausgehebelt werden.

Menschen, die durch eine Behinderung wesentlich in ihrer Fähigkeit zur Teilhabe am gesellschaftlichen Leben eingeschränkt sind oder denen eine solche Behinderung droht, erhalten häufig Eingliederungshilfe nach den Vorschriften des Zwölften Buches des Sozialgesetzbuches (SGB XII). Viele der Hilfeempfänger sind von psychischen Problemen oder Sucht betroffen. Vor allem freie Träger halten in

unterschiedlich spezialisierten Einrichtungen passgenaue Angebote für die Eingliederungshilfe bereit. Die Bandbreite reicht von ambulanter Hilfe im Sinne von Hausbesuchen über betreutes Wohnen bis hin zu stationären Einrichtungen. Für die erbrachten Leistungen gewähren die Träger der Sozialhilfe eine Vergütung. Eine gewisse Zäsur brachte der Jahreswechsel 2006/2007: Bisher war das Land als überörtlicher Träger der Sozialhilfe für die Eingliederungshilfe in stationären und teilstationären Einrichtungen zuständig, hatte die Durchführung der Aufgaben aber auf die Kreise und kreisfreien Städte übertragen. Seit Anfang 2007 sind diese nun selbst zuständig und führen die **Aufgabe im Rahmen der kommunalen Selbstverwaltung** durch.

Schon bisher war die Erfüllung dieser Aufgabe mit erheblichen Kosten für die Sozialhilfeträger verbunden. Dennoch gab es kein ausgeprägtes **System zur Rückmeldung von Fortschritten** bei der Eingliederung der einzelnen Leistungsempfänger. Die freien Träger rechneten regelmäßig pauschal für die in den Einrichtungen untergebrachten oder von diesen betreuten Personen ab. Den Kostenträgern war somit häufig nicht erkennbar, welche Erfolge oder Konsequenzen ihr finanzieller Einsatz hatte.

Vor diesem Hintergrund begannen die Kreise und kreisfreien Städte im Rahmen des Sozialhilferechts nach dem SGB XII eine verstärkte Steuerung einzelner Hilfefälle vorzunehmen. Dazu gehört die frühzeitige Aufstellung eines **Gesamtplans zur Durchführung der Leistungen** für den jeweiligen Leistungsempfänger durch den Träger der Sozialhilfe. Die Einzelfälle sollen künftig im Wege eines sogenannten Case-Managements behandelt werden. Dies bedeutet, dass eine organisierte, bedarfsgerechte Hilfeleistung gemäß eines Ablaufschemas erbracht wird, wobei der Versorgungsbedarf eines Klienten über einen definierten Zeitraum und unter Einbeziehung aller relevanten Dienstleistungen und Ämter geplant, koordiniert und evaluiert wird.

Ein Instrument hierfür ist der sogenannte **Entwicklungsbericht**. Mit diesem soll zunächst der Status quo bei neuen Fällen erfasst werden. Weiterhin dient er der kontinuierlichen Überwachung der Hilfefälle durch Nacherhebung in bestimmten Zeitabständen. Jeder individuelle Hilfefall weist seine besonderen Eigenschaften auf, auch wenn sich bestimmte Fallgruppen identifizieren lassen. Gleichwohl haben viele Sozialleistungsträger einen einheitlichen Befragungsbogen zur Erstellung des Entwicklungsberichts entwickelt. Dieser soll bei allen Hilfefällen eingesetzt werden. Um für alle Eventualitäten und Fallgestaltungen Platz vorzuhalten, versammeln solche Erhebungsbögen ein maximales Maß möglicher Fragen, frei nach Goethe: „Wer vieles bringt, wird manchem etwas bringen." Natürlich sind nicht alle Fragen in allen Fällen einschlägig. Zumeist wird die Beantwortung nur eines Teils erforderlich sein. Andererseits lässt sich im Hinblick auf die große Zahl möglicher Fallgestaltungen nicht im Voraus sagen, welche Fragen jeweils nicht hilferelevant sind.

Aus Datenschutzsicht ist bei der Datenerhebung streng der Grundsatz der Erforderlichkeit zu beachten. Wegen der Vielzahl der möglichen Fallgestaltungen machen unterschiedliche Fragebögen wenig Sinn. Doch müssen die Betroffenen

beim Ausfüllen, das in der Regel mithilfe der Mitarbeiter der Einrichtungen erfolgt, darauf **hingewiesen** werden, dass sie nicht sämtliche, sondern nur für ihren Fall relevante Angaben machen. Diese Daten werden benötigt und dürfen erhoben werden. In absehbarer Zukunft werden sich Standards für die Arbeit mit Entwicklungsberichten herauskristallisieren. Das ULD wird durch Nachschauen dafür sorgen, dass der Grundsatz der Erforderlichkeit gewahrt wird.

In Workshops und unter Beteiligung des ULD wurden Standards für Verfahren der Eingliederungshilfe und die Lösung einzelner Probleme erörtert. Aus unserer Sicht waren dabei die Diskussion von Konzepten für zwei **landesweite Datenbanken** von Interesse, die jeweils zum Management der Zielgruppe und der Anbieter erarbeitet werden sollen. Unter Beteiligung der künftig allein zuständigen Kreise und kreisfreien Städte und des noch zuständigen Landessozialministeriums wurden dabei Gestaltungsanforderungen definiert, die für mehr Transparenz und Effektivität bei der Eingliederungshilfe sorgen sollen. Durch die frühzeitige Beteiligung des ULD wird eine datenschutzkonforme Gestaltung der Datenbanken möglich. Es ist vorgesehen, dass die einzelnen Kostenträger in ihrem Zuständigkeitsbereich Zugriff auf die Daten haben. Die neue Datenbank zur Zielgruppe soll es den Kostenträgern ermöglichen, auf statistische Angaben aus den bei anderen Kostenträgern geführten Verfahren zuzugreifen. Ein Zugriff auf personenbezogene Daten in Verfahren außerhalb der eigenen Zuständigkeit wird jedoch ausgeschlossen.

Was ist zu tun?
Die Sozialleistungsträger müssen beim Einsatz von neuen Hilfsmethoden und Instrumenten den Sozialdatenschutz im Auge behalten, insbesondere die Beschränkung der Datenerhebung auf das erforderliche Maß. Bei der Weiterentwicklung von zentralen Datenbanken zu Zielgruppen- und Anbietermanagement sollte das ULD wie bisher einbezogen werden.

4.6 Schutz des Patientengeheimnisses

4.6.1 Elektronische Gesundheitskarte in der Entwicklung

Wesentliche Voraussetzung für einen datenschutzkonformen Einsatz der elektronischen Gesundheitskarte ist, dass die Patienten in die Lage versetzt werden, die ihnen zustehenden Datenschutzrechte wahrzunehmen. Diesem Ziel hat man sich ein Stück weiter genähert.

Die Einführung der elektronischen Gesundheitskarte (eGK) wird **vom ULD laufend begleitet** (28. TB, Tz. 4.6.1). Im Berichtszeitraum wurden weitere wesentliche Schritte unternommen, wenn auch der Voll- und Echtbetrieb in einiger Ferne liegt. Von der Firma „gematik“ wurden die Arbeiten an den technischen Spezifikationen fortgesetzt und in einer vorläufigen Endversion veröffentlicht. Diese umfasst noch nicht sämtliche zum Betrieb erforderlichen Komponenten.

Der **Test der eGK** kommt voran. Noch im Jahr 2005 hatten sich acht Regionen für die Testung der Gesundheitskarte beworben und den Zuschlag erteilt bekommen. Eine Testregion ist inzwischen wieder ausgeschieden. Zu den Testregionen

gehört auch die Region Flensburg mit einer sehr weit entwickelten technischen und organisatorischen Infrastruktur – dank dem Vorprojekt „Elektronische Gesundheitskarte Schleswig-Holstein“. Der Test soll in vier Stufen durchgeführt werden. Zunächst erfolgt die Ausgabe von Testkarten an zunächst bis zu 10.000 freiwilligen Teilnehmern. Mit dieser sogenannten 10.000er-Testung wurde in Schleswig-Holstein – als bundesweit erster Region – im Dezember 2006 begonnen. Von da an werben die Krankenkassen als Projektbeteiligte ihre Mitglieder für die Teilnahme an dem Projekt. Das ULD nahm auf die Gestaltung der Einwilligungserklärungen und Informationsmaterialien für die Anwerbung von Testkandidaten wesentlichen Einfluss. Leider konnten sich die in der Region vertretenen Krankenkassen nicht auf einheitliche Materialien einigen; nur einige wenige Kassen gehen insofern gemeinsam vor. Gleichwohl haben die meisten Beteiligten ihre Materialien mit dem ULD abgestimmt.

Ein wesentliches Element der Telematikinfrastruktur, in die der Einsatz der Karte eingebettet sein soll, sind Lösungen, die es den Karteninhabern ermöglichen, ihre Rechte zur **Steuerung des Zugriffs** auf die gespeicherten Informationen selbst wahrzunehmen. Nach den vorliegenden technischen Konzepten soll es möglich sein, dass ein Patient bestimmte Informationen auf der Karte verbirgt und sie gezielt nur für bestimmte Leistungserbringer freigibt. So kann ein Patient ein Rezept in einer bestimmten Apotheke einlösen und dabei vor dem Apotheker verbergen, dass noch weitere Verschreibungen vorliegen. Diese könnten dann an anderer Stelle, z. B. auch in einer Versandapotheke, eingelöst werden.

Zur Umsetzung dieses Konzepts ist es erforderlich, dass der Patient auf eine technische Infrastruktur mit entsprechenden Auswahlmöglichkeiten zugreifen kann. Im Gespräch sind dafür sogenannte E-Kioske oder **Patiententerminals**, die z. B. in Apotheken aufgestellt werden, so wie dies schon im Vorprojekt in Flensburg der Fall war. Ebenso ist es in der Planung, den Versicherten zu Hause über das Internet die Möglichkeit zu geben, die Inhalte ihrer Karte zu lesen und Sperrungen darauf vorzunehmen. Es liegt auf der Hand, dass diese Variante erhebliche Anforderungen an die Sicherheit der Systeme stellt. Es muss ausgeschlossen werden, dass nicht berechtigte dritte Personen auf die gesundheitlichen Daten der Betroffenen zugreifen.

Diese Instrumente zur Wahrung der Versichertenrechte waren im Grundsatz in die technischen Spezifikationen aufgenommen worden (28. TB, Tz. 4.6.1). Im Zusammenhang mit der vorgesehenen Testung ergaben sich jedoch Schwierigkeiten. In der zunächst verabschiedeten Version der als Rechtsgrundlage hierfür nötigen Verordnung fehlten **Regelungen zur Erprobung der Wahrnehmung der Patientenrechte** vollständig, auch eine Regelung zur Kostenübernahme war nicht vorhanden. Damit war unklar, wie eine Testung der Einrichtungen durchgeführt

werden sollte. Nach deutlichen Hinweisen auf diese Versäumnisse aus dem Kreis der Datenschutzbeauftragten wurden diese durch eine Verordnungsänderung im Oktober 2006 behoben. Die Erprobung von Einrichtungen zur Wahrnehmung der Versichertenrechte ist nunmehr eindeutig Bestandteil des Gesamttests. Noch nicht abzusehen ist, wann diese Tests Realität werden, da diesbezüglich noch konkrete technische Vorgaben fehlen.

Was ist zu tun?
Alle Beteiligten müssen auch bei den künftigen Schritten zur Einführung der eGK streng darauf achten, dass Datenschutzvorgaben und Selbstbestimmungsrechte der Patienten nicht zu kurz kommen. Das ULD sieht sich dafür in der Testregion Flensburg wie bundesweit in der Pflicht.

4.6.2 Dokumentenmanagementeinführung im Gesundheitsamt

Der Schritt von papiergebundener Vorgangsbearbeitung zum ausschließlich elektronischen Dokumentenmanagementsystem will wohlgeplant sein. Dies gilt besonders bei der Verarbeitung sensibler Daten, wie sie im Gesundheitsamt anfallen. Eine Kommune brachte das Verfahren bei seinem Gesundheitsamt mit ULD-Hilfe datenschutzkonform zum Laufen.

Die Gesundheitsämter bei den Kreisen und kreisfreien Städten haben eine Vielzahl unterschiedlicher Aufgaben zu erfüllen. Dazu gehören die Durchführung der Schuleingangsuntersuchungen von Kindern, die Ausstellung von amtlichen Zeugnissen im Hinblick auf bestimmte gesundheitliche Vorkommnisse sowie die Begutachtung von Personen bei deren Aufnahme ins Beamtenverhältnis. Der Sozialpsychiatrische Dienst des Gesundheitsamtes kümmert sich um Personen mit psychischen Auffälligkeiten, die teilweise eine immer wiederkehrende Betreuung benötigen und die Erstellung umfangreicher Unterlagen veranlassen. Eine weitere Aufgabe ist die Durchführung der Schwangerschaftskonfliktberatung, die einem Schwangerschaftsabbruch vorausgehen muss. Bereits aus der Zusammenstellung dieser Tätigkeitsfelder wird deutlich, dass bei den Gesundheitsämtern eine **Vielzahl äußerst sensibler Daten** anfällt. Diese sind nicht nur durch die Vorschriften des Landesdatenschutzgesetzes besonders geschützt, sondern unterliegen in der Regel dem Patientengeheimnis. Eine Offenbarung gegenüber dritten Personen, die nicht fachlich mit der jeweiligen Problematik befasst sind, muss unbedingt verhindert werden.

Stellt eine Verwaltungsbehörde, die derart sensible Daten vorhält, ihre papiergebundenen Vorgänge komplett auf elektronische Aktenbearbeitung um, so bringt dies Risiken, aber auch Chancen mit sich. Elektronische Aktenführung ermöglicht ein **differenziertes System von Rechtevergaben**; Einsichtsrechte und damit faktische Zugriffsmöglichkeiten einzelner Mitarbeiter lassen sich genau steuern. Allerdings steckt der Teufel häufig im Detail: Die verwendeten Systeme müssen diese Möglichkeiten technisch detailliert abbilden. Außerdem müssen die bisher mehr oder weniger unreflektiert durchgeführten Prozesse der Fallbearbeitung bei der Einführung der neuen elektronischen Systeme genau definiert werden, um

festzustellen, welche Personen zu welchen Zwecken auf welche Daten zugreifen müssen und dürfen.

Ein Sonderproblem besteht bei Gesundheitsämtern, die nicht von einer Person mit ärztlicher Qualifikation geleitet werden. Bei Untersuchungen im Gesundheitsamt können mehrere Ärzte, die eine gleichartige Aufgabe ausüben, als Behandlungsteam angesehen werden. Sie dürfen sich dann gegenseitig die den Patienten betreffenden Informationen mitteilen bzw. diese im Dokumentenmanagementsystem (DMS) einsehen, soweit der Patient nicht ausdrücklich etwas anderes verfügt hat. Dies gilt jedoch nicht für die nicht ärztliche Leitung des Gesundheitsamtes. Denn die Amtsärzte sind in der Ausübung ihrer ärztlichen Fachkompetenz selbstständig und nicht an Weisungen gebunden. Dies gilt umso mehr, wenn die **Leitung des Gesundheitsamtes** durch eine nicht ärztliche Person wahrgenommen wird. In diesem Fall scheidet aus fachlichen wie aus rechtlichen Gründen eine Weisungsmöglichkeit aus. Andererseits muss die Leitung die Möglichkeit haben, organisatorische Informationen zur Kenntnis zu bekommen, um beispielsweise Arbeitsvolumen und planerische oder disziplinarische Fragen bewerten zu können.

Diese Vorgaben lassen sich umsetzen, wenn eine Rechtevergabe in einem Dokumentenmanagementsystem nicht nur an bestimmte Rollen gebunden ist, sondern die gespeicherten **Dokumente mit bestimmten Eigenschaften** versehen werden. So können solche Dokumente identifiziert werden, die von Ärzten erzeugt wurden oder nur diesen zugänglich sein sollen. Diese lassen sich unterscheiden von anderen, welche dem organisatorischen Bereich zugehören und damit in den Zugriffsbereich der Leitung fallen. Als das Gesundheitsamt das ULD um Beratung ersuchte, war eine solche Zuweisung von Eigenschaften an Dokumente nicht umgesetzt. Dennoch konnte eine zweckmäßige Lösung gefunden werden, die den rechtlichen Vorgaben genügt.

Die Beratung bestätigte einmal mehr, dass **bereits bei der Beschaffung und Grundkonfiguration** von Dokumentenmanagementsystemen darauf zu achten ist, dass eine detaillierte und differenzierte Vergabe von Rechten im Hinblick auf Rollen und die entsprechende Zuordnung von Eigenschaften zu Dokumenten möglich ist. Solche anspruchsvollen Systeme sollten in der Verwaltung zunächst dort eingeführt werden, wo weniger sensible Daten anfallen. Die dabei gewonnenen Erfahrungen können der Einführung in schwierigeren Bereichen wie einem Gesundheitsamt zugutekommen. Werden sensible Daten mit dem System verarbeitet, so ist eine Vorabkontrolle vor dem Start mit dem Dokumentenmanagementsystem unabdingbar.

Was ist zu tun?
Planung, Beschaffung und Einführung von Dokumentenmanagementsystemen müssen von Anfang an über Rechtevergaben das jeweils bereichsspezifisch geltende Datenschutzrecht berücksichtigen.

4.6.3 Mammografie-Screening am Start

Viele Krebserkrankungen können erfolgreich bekämpft werden, wenn sie frühzeitig erkannt werden. Im Kampf gegen den Brustkrebs wird Frauen einer bestimmten Altersgruppe künftig ein Screening angeboten. Nach jetzigem Stand ist der Datenschutz dabei zufriedenstellend umgesetzt.

Bundesweit ist eine flächendeckende Röntgenreihenuntersuchung (Mammografie-Screening) für Frauen zwischen 50 und 69 Jahren geplant. Diese sollen alle zwei Jahre schriftlich zu einer freiwilligen Brustkrebsuntersuchung eingeladen werden (28. TB, Tz. 4.6.4). In Schleswig-Holstein wurde hierfür eine allgemeine gesetzliche Grundlage zur Durchführung von Reihenuntersuchungen (Reihenuntersuchungsgesetz – RUG) sowie eine auf die konkrete Maßnahme bezogene spezifische Verordnung erlassen. Diese Verordnung bestimmt die Kassenärztliche Vereinigung Schleswig-Holstein (KV SH) zur **zentralen Stelle** im Sinne der Regelungen zum Mammografie-Screening. Diese übernimmt das Management der Daten – die Sammlung der Daten der einzuladenden Frauen von den Einwohnermeldeämtern und die Aussendung der Einladungen. Die Befugnisse und Pflichten der zentralen Stelle sind in der Verordnung geregelt.

Da die Teilnahme am Screening freiwillig ist, müssen die Daten der eingeladenen Personen nicht dauerhaft gespeichert werden. Die Daten für die Einladungen stammen aus den kommunalen Melderegistern. Die angeschriebenen Frauen **können unterschiedlich reagieren**, was unterschiedliche Folgeverarbeitungen ihrer Daten nach sich zieht. Für diejenigen, die an der Untersuchung teilnehmen wollen, muss diese vorbereitet werden, insbesondere Ort (es wird vier Screening-Einheiten in Schleswig-Holstein geben) und Zeitpunkt. Melden Frauen zurück, derzeit nicht teilnehmen zu wollen, so muss sichergestellt werden, dass ihre Daten zunächst nicht weiterverarbeitet werden, dass sie aber zum nächsten möglichen Screening-Termin zwei Jahre später wieder eingeladen werden. Verweigert eine Frau die Teilnahme auch für die Zukunft, so wird eine generelle Sperre in das System eingetragen. Bei alledem ist zu vermeiden, dass die Daten der Frauen länger im System gespeichert werden als erforderlich für die jeweilige Umsetzung des geäußerten Verfahrenswunsches. Hierzu sind bestimmte Mechanismen, etwa der Einsatz kryptografischer Verfahren, geplant, womit die Speicherung der Klardaten solcher Frauen vermieden wird, die nicht zum angefragten Termin oder gar nicht teilnehmen wollen.

Die zentrale Stelle befindet sich noch im Aufbau. Details ihrer Arbeit wurden bereits mit dem ULD abgeklärt. Der datenschutzkonforme **Einsatz der verwendeten Programme** ist ein zentraler Aspekt. Die Machbarkeit hat sich in anderen Bundesländern schon erwiesen. Die KV SH hat langjährige Erfahrungen im Umgang mit sensiblen medizinischen Informationen und hat datenschutzrechtliche Belange bisher sehr ernst genommen.

Was ist zu tun?
Ein datenschutzkonformer Echtbetrieb ist unabdingbare Voraussetzung für die öffentliche Akzeptanz des Screening-Verfahrens.

4.6.4 Der private Praxisgebühreneintreiber

Die Einschaltung von privaten Dienstleistern für das Inkasso von Forderungen aus dem Sozialbereich ist nicht unproblematisch und an hohe Voraussetzungen gebunden.

Gesetzlich Versicherte müssen beim Besuch einer Arztpraxis in jedem Quartal eine Praxisgebühr von 10 Euro entrichten. Die Durchsetzung dieses Anspruchs obliegt zunächst der jeweilig zuständigen Kassenärztlichen Vereinigung. Die Kassenärztliche Vereinigung Schleswig-Holstein (KV SH) hat zur Aufgabenerledigung einen **Vertrag mit einem Rechtsanwaltsbüro** abgeschlossen, das sich auf sogenanntes Forderungsmanagement spezialisiert hat. Das ULD erfuhr hiervon erst durch eine Eingabe eines Kassenmitgliedes.

Die Einschaltung von Auftragsdatenverarbeitern im Sozialbereich ist unter bestimmten Voraussetzungen zulässig. Dazu gehören enge Bindungen und Vorgaben des Auftraggebers. Eine Auftragsvergabe an eine nicht öffentliche, d. h. private Stelle ist nur dann zulässig, wenn ohne diese Fremderledigung beim Auftraggeber Störungen im Betriebsablauf auftreten würden oder wenn die übertragenen Arbeiten beim Auftragnehmer **erheblich kostengünstiger** besorgt werden können. Im zweiten Fall ist zudem Bedingung, dass nicht sämtliche beim Auftraggeber gespeicherten Daten an den Auftragnehmer weitergegeben werden dürfen (27. TB, Tz. 6.1).

Bei der Vergabe des Forderungsmanagements an einen privaten Dienstleister ist bereits fraglich, ob es sich begrifflich überhaupt um Auftragsdatenverarbeitung handelt. Dies wäre nicht der Fall, wenn die auftragnehmende Stelle eine **eigene Entscheidungskompetenz** im Hinblick auf die Durchführung des Forderungsmanagements hätte. Im konkreten Vertrag wurde daher genau festgelegt, in welcher Weise der Auftragnehmer für die KV SH das Inkassoverfahren durchführen soll. Weiterhin wurde uns dargelegt, dass auch der vom Gesetz geforderte erhebliche Vorteil im Hinblick auf die Kosten vorliegt.

Erfahrungen begründen Zweifel an der **Zuverlässigkeit mancher Inkassounternehmen**. Da hier konkret eine Rechtsanwaltskanzlei beauftragt wurde, ließen sich diese Zweifel nicht einfach übertragen. Die gesetzlich festgelegte Rechtsstellung von Anwälten sieht besondere Pflichten vor, mit denen eine besondere öffentliche Vertrauensstellung als unabhängiges Organ der Rechtspflege korrespondiert. Da im vorgelegten Vertrag jedoch nicht alle Details der Auftragsdatenverarbeitung wie gesetzlich gefordert geregelt waren, musste auf der Basis von Hinweisen des ULD eine Nachbesserung vorgenommen werden.

Was ist zu tun?
Um bei der Beauftragung von privaten Stellen mit der Verarbeitung von Sozialdaten zu verhindern, dass diese Daten außer Kontrolle geraten, sind die engen gesetzlichen Voraussetzungen streng zu prüfen und vertraglich umzusetzen.

4.6.5 Betrugsbekämpfung im Gesundheitswesen

Bei Krankenkassen und Pflegekassen sind Stellen zur Bekämpfung von Fehlverhalten im Gesundheitswesen zu bilden, die Anhaltspunkten für Unregelmäßigkeiten oder rechtswidriger Nutzung von Finanzmitteln nachgehen sollen. Ein Austausch von Sozialdaten zwischen diesen Stellen ist jedoch gesetzlich nicht vorgesehen.

Die Regelungen zur Betrugsbekämpfung wurden mit dem **Gesundheitsmodernisierungsgesetz** in das Sozialgesetzbuch V und IX eingeführt. Die Krankenkassen hatten die Stellen zur Bekämpfung von Fehlverhalten Anfang 2004 einzurichten. Im Abstand von zwei Jahren soll über die Arbeit dieser Stellen und die erzielten Ergebnisse an den Verwaltungsrat der jeweiligen Krankenkasse sowie an die zuständige Aufsichtsbehörde ein Bericht geschickt werden; dieser stand somit erstmals Ende 2005 an.

Dabei kam die Frage auf, ob die bei den einzelnen Kassen gebildeten Stellen auch dazu berechtigt seien, personenbezogene Daten einer Stelle an die **Stelle einer anderen Krankenkasse** weiterzugeben. Denkbar sind Angaben zu den Versicherten und deren Inanspruchnahme von Gesundheitsleistungen als auch Informationen über das Abrechnungsverhalten einzelner Leistungserbringer wie Ärzte oder Physiotherapeuten. Unsere Antwort war klar: Eine Weitergabe von personenbezogenen Daten ist nicht zulässig. Zwar ergibt sich aus den Vorschriften klar, dass die Stellen zur Bekämpfung von Fehlverhalten auf die Sozialdaten zurückgreifen dürfen, die bei der eigenen Kasse angefallen sind. Der Datenpool der Krankenkasse darf genutzt werden, um Anhaltspunkte für ein entsprechendes Fehlverhalten aufzuspüren. Die Weitergabe an andere Stellen ist dagegen aber nicht zugelassen, was aus der Gesetzesbegründung eindeutig hervorgeht. Sollte der Bundesgesetzgeber es für erforderlich halten, im Einzelfall Daten zum Zweck der Bekämpfung des Fehlverhaltens im Gesundheitswesen auszutauschen, so müsste er eine entsprechende Rechtsgrundlage schaffen.

Was ist zu tun?
Die Krankenkassen müssen die Grenzen der Vorschriften zur Errichtung der Stellen zur Bekämpfung von Fehlverhalten im Gesundheitswesen beachten. Ein Datenaustausch von einer Kasse zu einer anderen kommt zu diesem Zweck nicht in Betracht.

4.6.6 Fortbildungspunkte für Ärzte – elektronisch erfasst und verteilt

Die Ärztekammer Schleswig-Holstein setzt im Verbund mit den Kammern der anderen Länder zunehmend auf elektronische Formen der Aufgabenerfüllung. Dazu gehört die elektronische Erfassung von Fortbildungspunkten für die ärztlichen Mitglieder.

Als den Ärzten im Land im September 2005 ein Bogen mit **Barcode-Aufklebern** zugesandt wurde, staunten einige nicht schlecht. Die Ärztekammer teilte ihnen

mit, diese Aufkleber enthielten eine einheitliche Fortbildungsnummer (EFN), mit der die Kammer künftig die Fortbildungspunkte der Ärzte sammelt und verwaltet. Bei Erreichen der vorgeschriebenen Punktzahl werde das gesetzlich vorgesehene Fortbildungszertifikat ausgestellt.

Das Verfahren hatte schon Datenschutzbeauftragte anderer Länder beschäftigt. Die Barcode-Aufkleber sollen beim Besuch von Fortbildungsveranstaltungen in einer Teilnehmerliste eingeklebt werden. Der Veranstalter übermittelt die mittels des Barcodes gespeicherten Fortbildungsnummern an einen **zentralen Server bei der Bundesärztekammer** in Berlin. Die Nummern werden durch die Ärztekammern der Länder vergeben; eine Weitergabe der Zuordnungsfunktion nach Berlin erfolgt nicht. Daher sind die EFN für die Bundesärztekammer pseudonymisierte Daten, die sie nicht selbst einer Person zuordnen kann. Die Nummern, die eine Länderziffer enthalten, werden zurück an die Ärztekammer übermittelt, bei denen der an der Fortbildung teilnehmende Arzt Mitglied ist.

Es war schon bisher die Aufgabe der Landesärztekammern, auf Antrag der Ärzte einen Fortbildungsnachweis auszustellen. Der Unterschied zum früheren Verfahren besteht darin, dass die Landesärztekammern die Fortbildungspunkte bereits im Vorfeld über einen Zeitraum von fünf Jahren hinweg vor Ausstellung der Fortbildungsnachweise sammeln. Bisher mussten die Ärzte die **Punkte selbst sammeln** und für die Ausstellung des Nachweises bei der Ärztekammer einreichen, sodass die Angaben nur für einen kürzeren Zeitraum vorlagen.

Auch die neue Verfahrensweise ist vom einschlägigen Heilberufsgesetz des Landes gedeckt. Es ist Aufgabe der Kammer, die Erfüllung der Berufspflichten der Mitglieder – dazu gehört die Teilnahme an Fortbildungsveranstaltungen – zu überwachen. Die Erhebung und Verarbeitung der Teilnehmerdaten ist gesetzlich ausdrücklich vorgesehen. Die gefundene Verfahrensweise stellt sicher, dass die Identitätsdaten ausschließlich bei der Landesärztekammer vorliegen. Anders als bisher müssen die Ärzte ihre Identität nicht einmal bei der Teilnahme an den einzelnen Veranstaltungen offenbaren, was eine Verbesserung in Sachen **Datensparsamkeit** darstellt.

Die Übersendung der Barcode-Aufkleber hatte bei einigen Adressaten für – im Ergebnis unbegründete – Irritationen gesorgt. Inzwischen steht eine Informationsseite im Internet zur Verfügung, die das Verfahren sehr **transparent** darstellt:

www.eiv-fobi.de

Zudem hat die Ärztekammer klargestellt, dass die Ärzte nicht zur Teilnahme an dem neuen Verfahren verpflichtet sind. Wer seine Fortbildungspunkte selbst verwalten will, kann dies weiterhin tun und so verhindern, dass die Kammer im Vorfeld der Ausstellung der Zertifikate Kenntnis von den besuchten Veranstaltungen erhält.

Was ist zu tun?
Neue elektronische Verfahren stoßen oft, vor allem bei unzureichender Transparenz für die Betroffenen, auf Skepsis und Ablehnung, auch wenn sie datenschutzkonform sind. Ein Datenschutz-Audit kann dazu beitragen, Befürchtungen auszuräumen.

4.7 Wissenschaft und Bildung

4.7.1 Ist der „gläserne Schüler“ geplant?

Das Bildungsministerium will sich an einer zentralen Schülerdatenbank der Bundesländer beteiligen. Der Bildungsverlauf jeder Schülerin und jedes Schülers soll dort mithilfe einer persönlichen Identifikationsnummer von der Einschulung bis zur Schulentlassung verfolgt werden können.

Lange Zeit ohne öffentliche Aufmerksamkeit verfolgten die Bildungsverwaltungen der Länder und die Kultusministerkonferenz (KMK) das Ziel der Einführung einer **bundesweiten Schuldatenbank**. Darin sollen die Bildungsverläufe von Schülerinnen und Schülern von der Einschulung bis zur Schulentlassung pseudonymisiert und damit personenbeziehbar verfolgt werden können. Einer einheitlichen Schüler-Identifikationsnummer (ID) sollen viele Daten zur Person und zum Schulverlauf zugeordnet werden, z. B. Nationalität, Muttersprache, Elternhaus, zu sämtlichen Schuljahren Art der Schule, Wiederholungen, Schwerpunkte und Ziele der Ausbildung. Darüber könnte die gesamte Schulkarriere nachvollzogen und bewertet werden. Leider zeigten das Bildungsministerium und die Kultusministerkonferenz – trotz unseres Hinweises – lange Zeit kein Problembewusstsein. Es wird bis heute versichert, dass an den personenbezogenen Daten kein Interesse bestehe. Über die Schüler-ID, zu der die aktuellen Identifizierungsangaben aufbewahrt werden, wäre jederzeit eine Reidentifizierung und Zuordnung der Daten möglich. Sicherungen zur Verhinderung des „gläsernen Schülers“ wurden nicht angeboten. Ein Schelm, der Böses dabei denkt? Im Sommer 2006 machte sich jedenfalls über die Pläne bundesweit Empörung breit.

Um die geplante Datenverarbeitung zu legitimieren, ist eine **Ergänzung des Schulgesetzes** erfolgt. Die darin genannten Zwecke sind jedoch so unpräzise, dass sie den verfassungsrechtlichen Ansprüchen nicht genügen. Wir haben dem zuständigen Ministerium mitgeteilt, dass mit der verabschiedeten Regelung keine Grundrechtseingriffe legitimiert werden können. Auf besondere Schutzregelungen für das Persönlichkeitsrecht der Betroffenen verzichtete man. Die Regelung stellt auf eine IT-Infrastruktur ab, die in Schleswig-Holstein überhaupt noch nicht existiert und deren Kosten nicht beziffert wurden.

Die Konferenz der Datenschutzbeauftragten hat sich für einen Verzicht der Schüler-ID ausgesprochen. Sie ist einmütig der Auffassung, dass die verfolgten Ziele mit weniger einschneidenden Mitteln als einer Totalerhebung angestrebt werden müssen. Welche Informationsbedürfnisse die Bildungspolitiker für welche Zwecke haben, hatten sie selbst fünf Jahre nach Beginn der Planungen immer noch nicht klar definiert. Von Planungsgrundlagen und PISA ist immer wieder die

Rede. Die Teilnahme an den durchgeführten wissenschaftlichen Untersuchungen wie PISA, IGLU oder TIMMS war bisher freiwillig. Wir haben den Eindruck, dass solche Tests ausreichende Erkenntnisse über Schülerlaufbahnen geben können. Das geplante zentrale Register wäre ein nicht erforderlicher und damit **unverhältnismäßiger Eingriff** in das informationelle Selbstbestimmungsrecht der betroffenen Schülerinnen und Schüler.

Was ist zu tun?
Die Planungen zur Einrichtung einer zentralen Schülerdatenbank und zur Vergabe von Schüler-Identifikationsnummern sollten aufgegeben werden.

4.7.2 Informationstechnologie an Schulen

Die Einführung moderner Informationstechnologie in den Schulverwaltungen gestaltet sich schwierig: Unklare Verantwortlichkeiten, eine angespannte Finanzlage und ein fehlendes zentrales Konzept führen zu datenschutzwidrigen Zuständen. Das ULD unterstützt Initiativen zur Standardisierung innovativer, datenschutzfreundlicher Lösungen.

Viele Schulen befinden sich beim IT-Einsatz in einer konzeptionellen Notlage, die durch den Einsatz einfach anzuwendender **Standardsystemkonzepte** zu beheben versucht wird. Das ULD unterstützt die beiden Modellprojekte „sh21 Basis“ des Bundesministeriums für Bildung und Forschung sowie das Standardisierungsprojekt „Landesnetz Bildung“ des Ministeriums für Bildung und Frauen des Landes Schleswig-Holstein. Durch standardisierte Systemkonzepte besteht die Hoffnung, das Datenschutzniveau an Schulen zu heben, indem die lokale Systemadministration von konzeptionellen Tätigkeiten entlastet wird.

Diese Konzepte müssen sicherstellen, dass die Schulen selbst als für den Datenschutz verantwortliche Stellen ihren **Kontrollpflichten** nachkommen können. Die Entwürfe müssen die lokale Verantwortung berücksichtigen und durch Dokumentation und Technikunterstützung die Ordnungsmäßigkeit der Datenverarbeitung prüfbar machen. Zudem muss durch flankierende Schulungen der Schulverwaltungen sowie der Lehrer das Datenschutzwissen beim IT-Einsatz verbessert werden.

Zu den Aufgaben der Projektverantwortlichen für „sh21 Basis“ und „Landesnetz Bildung“ gehört eine sorgfältige **Evaluation** nach Abschluss des Projektes. Da im „Landesnetz Bildung“ mit realen personenbezogenen Daten gearbeitet wird, gehört hierzu auch die konkrete Beachtung der Anforderungen von Datenschutz und Datensicherheit.

Was ist zu tun?
Bevor die Ergebnisse der Modellprojekte flächendeckend verfügbar gemacht werden, müssen sie auf Herz und Nieren bezüglich Datenschutz und Datensicherheit geprüft werden.

4.8 Steuerverwaltung

4.8.1 Einsicht in die Unterlagen der Steuerfahndung

Betroffene haben einen Anspruch auf Einsicht in die Unterlagen der Steuerfahndung. Die Steuerverwaltung lehnt weiterhin Auskunftsersuchen von Betroffenen ohne triftigen Grund ab.

Ergeben sich für die Finanzbehörden Anhaltspunkte einer Steuerstraftat, so übergibt sie den Fall der Steuerfahndung. Diese ermittelt, ob der Verdacht begründet ist, und leitet bei dessen Bestätigung ein Strafverfahren ein. Die Betroffenen erhalten im weiteren Verfahren Akteneinsicht nach den Vorschriften der Strafprozessordnung. Erweist sich der Verdacht als unbegründet, erfolgt ein entsprechender Vermerk im **Fallheft der Steuerfahndung**, und der Fall ist abgeschlossen.

Durch Einsicht in andere Unterlagen der Finanzverwaltung hatte ein Petent erfahren, dass in seiner Sache die Steuerfahndung eingeschaltet worden ist. Er beantragte daher die Einsichtnahme in die Unterlagen der Steuerfahndung. Diese **verweigerte die Auskunft** mit der Begründung, er habe kein Einsichtsrecht, da die Abgabenordnung (AO) eine solche nicht vorsehe. Dieser Schluss ist falsch.

Die Betroffenen haben einen grundrechtlich gesicherten Anspruch gegenüber öffentlichen Stellen zu wissen, wer was wann wo und zu welcher Gelegenheit über sie gespeichert hat. Dies gilt auch für den Bereich des Steuerwesens (28. TB, Tz. 4.8.2). Die Finanzverwaltung einschließlich der Steuerfahndung muss über solche Anträge **nach pflichtgemäßem Ermessen** entscheiden. Würde die Akteneinsicht dazu führen, dass weitere Ermittlungsbemühungen der Fahndungsstelle wesentlich erschwert bzw. das laufende Ermittlungsverfahren gefährdet würde, kann das Interesse an der Geheimhaltung der Informationen überwiegen. Eine Auskunftsverweigerung kann auch mit dem Schutz personenbezogener Daten Dritter gerechtfertigt sein. So müssen z. B. die Namen von Informanten nicht mitgeteilt werden, es sei denn, der Informant hat die Behörde wider besseren Wissens oder leichtfertig falsch informiert.

Unter diesen „Informantenschutz“ fallen selbstverständlich nur natürliche Personen. Die **Information von Behörden** untereinander basiert ausschließlich auf gesetzlicher Grundlage; es besteht kein berechtigter Schutzzweck der Geheimhaltung. Nach einigen Erörterungen hat die Steuerverwaltung die Unterlagen dem Petenten unter Schwärzung der personenbezogenen Daten Dritter zugänglich gemacht.

Was ist zu tun?
Das Recht auf Akteneinsicht ist ein verfassungsrechtlicher Anspruch, der nur in begründeten Ausnahmefällen nach erfolgter Interessenabwägung abgelehnt werden darf. Die Finanzverwaltung muss Anträge sorgfältig prüfen und gegebenenfalls Teilauskunft gewähren.

4.8.2 Data Center Steuern

„Data Center Steuern“ ist das gemeinsame Rechenzentrum der Steuerverwaltungen von Hamburg, Mecklenburg-Vorpommern, Bremen und Schleswig-Holstein. Dienstleister ist dataport, das einen neuen Standort in Rostock eröffnet hat.

Das Steuergeheimnis verpflichtet die Beteiligten, besondere Vorkehrungen zu treffen, um einen unbefugten Zugriff auf die besonders schützenswerten Daten zu verhindern. Im Data Center Steuern in Rostock sollen zukünftig zentral alle Steuern der vier Bundesländer berechnet werden. Gedruckt und versandt werden diese zentral im dataport Druckzentrum am Standort Altenholz in Kiel. Die Steuerverwaltungen, die dataport als Dienstleister beauftragen, und dataport selbst müssen durch vertragliche Regelungen und angemessene technische und organisatorische Maßnahmen den **Schutz des Steuergeheimnisses** gewährleisten.

Zur Sicherung einer effektiven und effizienten **datenschutzrechtlichen Beratung und Kontrolle** des Data Center Steuern haben die Datenschutzbeauftragten der beteiligten Länder eine Kooperationsvereinbarung getroffen. Diese

- sieht eine Abstimmung in allen wesentlichen Fragen vor,
- vereinbart eine wechselseitige Beauftragung zur Durchführung von effektiven Datenschutzkontrollen vor Ort und
- hat ein einheitliches Auftreten gegenüber dataport zum Ziel.

Wir haben unter der Federführung des Landesdatenschutzbeauftragten Mecklenburg-Vorpommerns zu den erforderlichen vertraglichen Regelungen zwischen den Steuerverwaltungen und dataport Hinweise gegeben. Außerdem haben wir ein **Sicherheitskonzept des Auftragnehmers** eingefordert, das auch den Anforderungen des LDSG und der DSVO gerecht wird. In dem Vertrag sind den Auftraggebern Weisungs- und Kontrollrechte einzuräumen.

Was ist zu tun?
Steuerverwaltungen und dataport haben die gemeinsame Aufgabe und Pflicht, das Steuergeheimnis technisch und organisatorisch zu schützen. Die Steuerverwaltungen müssen dataport vertraglich zu entsprechenden Vorkehrungen verpflichten.

4.8.3 Einführung einer einheitlichen Steuernummer

Von Juli 2007 an soll eine für jede Bürgerin und jeden Bürger zu vergebende einheitliche Steuernummer zur Optimierung des Besteuerungsverfahrens beitragen. Deren Speicherung ist auch in den Melderegistern vorgesehen. Zur Bereinigung der Meldedaten will das Bundeszentralamt für Steuern einen bundesweiten Abgleich vornehmen. Vieles ist bisher noch völlig unklar.

Mit der Vergabe einer einheitlichen steuerlichen Identifizierungsnummer (**Steuer-ID**) an alle Bürger soll die Qualität der Steuererhebung erhöht und damit eine größere Steuergerechtigkeit erreicht werden. Hiergegen bestehen grundsätzlich Datenschutzbedenken (26. TB, Tz. 4.9.1).

Konkrete Bedenken haben wir gegen den vorgesehenen bundesweiten Abgleich der **zu übermittelnden Meldedaten**. Die entsprechende Rechtsverordnung des Bundes erlaubt pauschal „die Zusammenführung und Bereinigung sämtlicher von den Meldebehörden zu übermittelnden Daten“, ohne weitere Einzelheiten für das Verfahren festzulegen. Das Bundeszentralamt für Steuern wird ermächtigt, im Vorfeld des Vergabeverfahrens weitere Meldedaten zu Erprobungszwecken zu erheben und weiterzuverarbeiten. Offensichtlich bestanden bei Verordnungserlass noch keine konkreten Vorstellungen darüber, wie überhaupt ein Abgleich realisiert werden kann. Weitere handwerkliche Mängel sind angesichts der kurzen Entwicklungs- und Probezeit vorprogrammiert.

Ergeben sich bei dem geplanten Abgleich **Konfliktfälle**, müssen die beteiligten Meldebehörden unterrichtet werden, um diese unter Einbeziehung der Betroffenen aufzuklären. Der Verwaltungsaufwand dafür wird erheblich sein. Es ist absehbar, dass zusätzlich Außendienstmitarbeiter für Ermittlungen vor Ort eingesetzt werden müssen. Entscheidend ist die Frage, welche und damit auch wie viele Fälle unter welchen Voraussetzungen als Konfliktfälle ausgewiesen werden. Ein elektronischer Abgleich kann allenfalls Anhaltspunkte für die Unrichtigkeit der Melderegisterdaten geben. Seriöse Aussagen darüber, ob und in welchem Umfang die Meldedaten tatsächlich unrichtig sind, lassen sich bisher nicht einmal ansatzweise machen. Folgende Fragen sind noch unbeantwortet:

- Ist das Abgleichverfahren überhaupt geeignet, um jedenfalls das Gros der Fehler in den Meldedaten aufzudecken?
- Welche Daten werden wie abgeglichen?
- In welchen Fällen liegen Anhaltspunkte für die Unrichtigkeit von Meldedaten vor?
- Wann sind diese Anhaltspunkte so konkret, dass ein Konfliktfall ausgewiesen wird?

Trotz fehlender Antworten hat der Verordnungsgeber den Startschuss für den Abgleich gegeben. Es kann nur gehofft werden, dass das Bundeszentralamt für Steuern – wie auch immer – die notwendigen Lösungen in der verfügbaren Zeit

finden wird. Von einer **ordnungsgemäßen Datenverarbeitung** kann derzeit jedenfalls keine Rede sein. Es kann dazu kommen, dass die Meldebehörden mit viel Aufwand die berühmten Stecknadeln im Heuhaufen suchen müssen und viele Bürgerinnen und Bürger mit „Meldeverstößen“ konfrontiert werden, die sie nie begangen haben. Ohne ein klares, Erfolg versprechendes Verfahren ist weder der Verwaltungsaufwand für die Meldebehörden noch die Inanspruchnahme der Bürgerinnen und Bürger zu Kontrollzwecken zu rechtfertigen.

Was ist zu tun?
Der Melderegisterabgleich muss verschoben werden, bis gesicherte Erkenntnisse über das Verfahren und die Qualität der zu erzielenden Ergebnisse vorliegen.

5 Datenschutz in der Wirtschaft

5.1 Auslandsüberweisungen aus Schleswig-Holstein über Brüssel an die CIA

Haben Sie schon einmal eine Kiste trockenen toskanischen Rotwein beim Winzer vor Ort geordert und zur Bezahlung eine Auslandsüberweisung getätigt? Wussten Sie, dass die Überweisungsdaten direkt bei US-Geheimdiensten und sonstigen US-Behörden landen können? Grund hierfür ist SWIFT.

Die Society for Worldwide Interbank Telecommunications – kurz SWIFT – ist weltweit Quasimonopolist für **internationale Geldüberweisungen** durch Banken und Betreiber einer hierfür geeigneten Telekommunikationsinfrastruktur. Seit 2001 übermittelt das bei Brüssel in Belgien ansässige Unternehmen die ihm von Banken weltweit überlassenen Kundendaten regelmäßig millionenfach eigenmächtig an US-Behörden. Grundlage dafür sind ein Geheimabkommen zwischen dem Unternehmen und dem US-Finanzministerium und Anordnungen des US-Präsidenten. In den USA fehlt es bislang an mit europäischen Grundrechtsstandards vergleichbaren Schutzvorkehrungen für den Datenschutz.

Nachdem im Juni 2006 erstmals die Öffentlichkeit über einen Zeitungsbericht von dem Vorgang erfuhr, nahm das ULD als für die Finanzinstitutionen des Landes zuständige Aufsichtsbehörde bei den wichtigsten Banken und Sparkassen **Ermittlungen** auf. So wurden die Kollegen der Bundesländer über den Vorgang informiert und bei einer gemeinsamen Sitzung mit dem Zentralen Kreditausschuss (ZKA) auf sofortige Aufklärung gedrungen. Leider konnte der ZKA als Dachverband der bundesdeutschen Banken nichts mitteilen, was nicht auch schon in der Zeitung gestanden hatte.


www.datenschutzzentrum.de/wirtschaft/swift/060710_swift.htm

SWIFT ist aus datenschutzrechtlicher Sicht schlicht **Auftragnehmer** der sie beauftragenden Banken. SWIFT hatte offenbar ohne Kenntnis seiner Auftraggeber deren Kundendaten an die US-Behörden weitergegeben und hierüber lediglich die Bundesbank informiert.


www.datenschutzzentrum.de/wirtschaft/swift/060825_swift.htm

Zwischenzeitlich hat auch der Düsseldorfer Kreis, das oberste Abstimmungsgremium der **Aufsichtsbehörden der Bundesländer**, und die sogenannte Artikel-29-Gruppe der europäischen Datenschutzbeauftragten die Datenweitergabe einhellig als rechtswidrig kritisiert und die das Unternehmen beauftragenden Banken aufgefordert, diesen Zustand umgehend zu beenden.


www.datenschutz.de/aufsicht_privat/
www.datenschutz.de/news/detail/?nid=1997

Das ULD hatte aufgrund der datenschutzrechtlich eindeutigen Rechtslage als bundesweit einzige Behörde sofort ein **Verfahren eingeleitet**, um weiteren Schaden

für die Rechte der Betroffenen abwenden zu können. Die als Girozentrale für zahlreiche Einzelbanken arbeitende HSH-Nordbank erklärte sich schnell bereit, ihre Kunden umgehend über die drohende Möglichkeit der unrechtmäßigen Datenweitergabe bei Auslandsüberweisungen zu informieren. Weitere Institute und Verbände prüfen zurzeit, auf welche Weise sie zukünftig ihre Kunden über das Risiko des Datenverlustes bei Auslandsüberweisungen aufklären werden. Die Banken wie auch der ZKA verweisen stets darauf, man sei auf SWIFT angewiesen und stehe deren unbefugten Datenweitergaben ohnmächtig gegenüber.

Nach derzeitigem Kenntnisstand dauert die Datenweitergabe an die USA unvermindert an. Es ist davon auszugehen, dass millionenfach Datensätze von unbescholtenen Bürgern weitergegeben werden und dass diese von den US-Geheimdiensten rasterfahndungsähnlich ausgewertet werden. Der Zugriff von US-Behörden auf die Datensätze von SWIFT ließe sich relativ leicht unterbinden, indem die zurzeit aus Sicherheitsgründen bestehende **Datenvorhaltung auf einem Spiegelserver** in den USA abgebrochen wird. Offenbar bedarf es dazu weiteren internationalen Drucks auf das Unternehmen. Sollte die fehlende Bereitschaft zur Beachtung des Datenschutzes durch SWIFT andauern, so müssen alternative Infrastrukturen für Auslandsüberweisungen geschaffen und genutzt werden. Eine Nutzung des Dienstleisters SWIFT durch bundesdeutsche Banken ist schon heute eine schwere Missachtung des Bankgeheimnisses der Kunden.

Was ist zu tun?
Die verantwortlichen bundesdeutschen Banken müssen den Nachweis erbringen, alles in ihrer Macht Stehende zu tun, um die unzulässige Datenweitergabe über SWIFT an US-Behörden so schnell wie möglich zu beenden.

5.2 Bürokratieabbau durch Datenschutzverkürzung?

Seit Jahren wird in der Fachwelt eine längst überfällige Reform zur Modernisierung des Bundesdatenschutzgesetzes gefordert. Stattdessen wurden unter dem Vorwand des Bürokratieabbaus teilweise Verschlechterungen realisiert.

Seit einem Gutachten im Auftrag des Bundesinnenministeriums aus dem Jahr 2000 ist unbestritten, dass das Bundesdatenschutzgesetz (BDSG) im Interesse von Verbrauchern wie Unternehmen gleichermaßen **effektiver gestaltet und modernisiert** werden muss. Die wesentlichen Punkte dieses Gutachtens zielen auf eine Vereinfachung und Straffung der gesetzlichen Regelungen ab; eine Umsetzung ist bisher nicht erfolgt. Statt der erhofften Reform kam es zu einer BDSG-Änderung im Rahmen eines Gesetzes zum Abbau bürokratischer Hemmnisse.

Es enthält vor allem zwei Änderungen. Zum einen wird der Schwellenwert für die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten von fünf auf zehn mit der automatisierten Verarbeitung personenbezogener Daten beschäftigte Mitarbeiter heraufgesetzt. Zum anderen unterfallen externe betriebliche Datenschutzbeauftragte zukünftig den **Geheimnisschutzbestimmungen des § 203 Straf-**

gesetzbuch, werden vom Beschlagnahmeschutz mit umfasst und können somit auch bei Berufsgeheimnisträgern tätig werden. Die zweitgenannte Änderung wird von uns begrüßt, weil sie eine lang andauernde Unsicherheit bei der Bestellung externer Datenschutzbeauftragter zugunsten des Schutzes der Daten der betroffenen Verbraucher löst.

Die Heraufsetzung des **Schwellenwertes für die Bestellpflicht** hingegen ist schädlich. Das bundesdeutsche Modell interner betrieblicher Kontrolle des Datenschutzes ist weltweit anerkannt und ein „Exportschlager". Erst kürzlich hat Frankreich den betrieblichen Datenschutzbeauftragten für Unternehmen eingeführt. Zielsetzung ist die Vermeidung von Bürokratie: In den Unternehmen sollen vor Ort sachkompetente Mitarbeiter, nicht eine weit entfernte Aufsichtsbehörde beurteilen, wo es in Sachen Datenschutz noch hakt. Mit der Heraufsetzung des Schwellenwertes durch ein Bürokratieabbaugesetz fallen bei der mittelständisch geprägten bundesdeutschen Wirtschaft zahlreiche Unternehmen aus der internen Kontrolle durch einen betrieblichen Datenschutzbeauftragten heraus.

Die Bestimmungen des BDSG bleiben aber für diese Stellen anwendbar. Die Kontrolle übernimmt nun die staatliche Aufsichtsbehörde, wenn die Unternehmen nicht **freiwillig einen Beauftragten bestellen**. Diesen ist dies dringend anzuraten, auch zur Vermeidung von Datenschutzpannen und den möglichen Fehlern beim Umgang mit sensiblen personenbezogenen Daten. Die vom Gesetzgeber behauptete Entlastung der mittelständischen Wirtschaft wird, so ist zu befürchten, zu mehr Belastung der ohnehin überforderten Aufsichtsbehörden durch vermehrte Direktanfragen aufgrund des Wegfalls interner Kontrollstrukturen führen sowie zu mehr staatlicher Bürokratie durch das europarechtlich begründete Wiederaufleben von Meldepflichten. Angesichts der teilweise hohen Technisierung von Kleinunternehmen ist die Anzahl der Mitarbeiter ein wenig tauglicher Anknüpfungspunkt für die Bestellungspflicht; sinnvoller wäre z. B. die Einstufung eines Unternehmens nach Art der Tätigkeit und der dabei konkret entstehenden Risiken für die Daten der Verbraucherinnen und Verbraucher.

Was ist zu tun?
Die längst überfällige Reform des Bundesdatenschutzgesetzes ist auf den Weg zu bringen. Dabei sollte ein neuer, sachgerechterer Anknüpfungspunkt für die Auslösung der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten gefunden werden.

5.3 Wo wohnt der Richter, der mir Unrecht antat?

Der Betreiber einer privaten Homepage veröffentlichte Namen und Anschriften von Richterinnen und Richtern sowie Staatsanwältinnen und Staatsanwälten eines örtlichen Amts- und Landgerichtes im Internet.

Der Betreiber der Homepage nutzte als Datenquelle die von den Gerichten herausgegebenen Geschäftsverteilungspläne mit den sogenannten Funktionsträgerdaten, d. h. den dienstlichen Daten der Richter und Staatsanwälte (Name, Vor-

name, Amtsbezeichnung, Zuständigkeit), und das im Buchhandel zu erwerbende Handbuch der Justiz, welches sich bei Richtern und Staatsanwälten ebenfalls auf die Nennung von dienstlichen Angaben (Name, Vorname, Dienststellung, Dienstalter und Geburtsdatum) beschränkt. Privatanschriften der Richter und Staatsanwälte sind in diesen **Veröffentlichungen** nicht enthalten.

Im von der Kommune herausgegebenen Adressbuch sowie dem offiziellen örtlichen Telefonbuch fand er – wenn auch lückenhaft – die Privatanschriften der betroffenen Juristen. Das Adressbuch basiert auf den Daten des Einwohnermeldeamtes. Aus gutem Grund besteht nach dem Melderecht die Möglichkeit einer Weitergabesperre hinsichtlich der Veröffentlichung in Adressbüchern. Auch die Kunden von Telefonanbietern haben seit langer Zeit das Recht, per **Widerspruch** die Veröffentlichung ihrer Daten in Kundenverzeichnissen ganz oder teilweise zu verhindern.

Der Homepagebetreiber hatte die Veröffentlichungen von **dienstlichen und privaten Daten verknüpft** und ins Internet gestellt. Dadurch entstand eine Datensammlung mit neuer Qualität. Die Information, „Richter Müller wohnt privat da und da“, war bisher nicht einfach verfügbar. Für einschlägig Interessierte, wie z. B. verurteilte und zwischenzeitlich aus der Haft entlassene Straftäter, ließ sich nunmehr mit einem Klick erfahren, wo die Richter privat anzutreffen waren. Diese Datensammlung steigerte für die betroffenen Richter und Staatsanwälte die Gefahr, von enttäuschten oder wütenden Prozessverlierern belästigt oder bedroht zu werden.

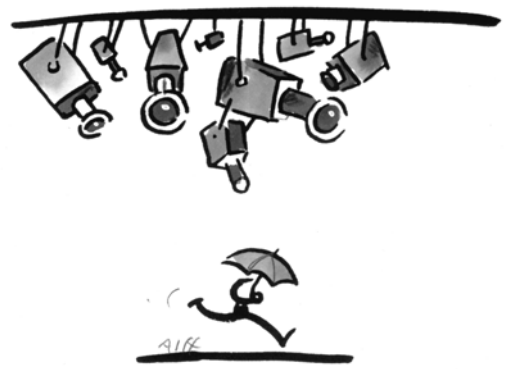
Das Bundesdatenschutzgesetz (BDSG) erlaubt grundsätzlich die Verarbeitung und Nutzung personenbezogener **allgemein zugänglicher Daten**. Der Erlaubnistatbestand gilt aber nur, wenn das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich nicht überwiegt. Hiervon mussten wir in diesem Fall in Anbetracht des Gefährdungspotenzials aber ausgehen. Die somit unzulässige Datensammlung wurde vom ULD beanstandet. Inzwischen ist der Homepagebetreiber – wenn auch zögerlich – der Aufforderung des ULD nachgekommen, die Privatadressen zu löschen.

Was ist zu tun?
Die Zusammenführung mehrerer Daten aus verschiedenen öffentlich zugänglichen Quellen kann für die Betroffenen im Einzelfall sehr problematisch sein. Daher ist bei der Veröffentlichung Vorsicht geboten.

5.4 Neues von der Videofront

Persönlichkeitsrechtsverletzungen durch unzulässige Videobeobachtung sind ein Dauerbrenner. Im Folgenden werden einige exemplarische Fälle vorgestellt:

- **Videoüberwachung von öffentlichen Straßen und Gehwegen**



Hausbesitzer und Mieter beobachteten nicht selten **ihre am Straßenrand abgestellten Kraftfahrzeuge** mit einer Videokamera, um Diebstahl oder Sachbeschädigungen zu verhindern. Während Hausbesitzer ihre Kameras in der Regel sichtbar an der Gebäudeaußenwand anbrachten, installierten Mieter die Geräte meist versteckt auf Balkonen oder hinter Fensterscheiben. Bei diesen Videobeobachtungen werden zwangsläufig Teile der Straße und des Bürgersteiges mit erfasst. Dies ist unzulässig: Die Sicherung des öffentlichen Straßenraums ist allein Aufgabe der Polizei. Die Betreiber der Videoanlagen zeigten sich zumeist – oft erst nach umfangreichem Schriftwechsel und der Drohung mit Bußgeldverfahren – einsichtig und bauten die Kameras wieder ab.

- **Videoüberwachung in Gaststätten**

Immer mehr Gaststätten gehen dazu über, neben Kassen und Eingangstüren auch reine Aufenthaltsbereiche der Gäste mit Kameras zu beobachten. Bei Letzteren handelt es sich um **Freizeitbereiche**, die nicht gefilmt werden dürfen. Das Persönlichkeitsrecht begründet den Anspruch, dass Menschen sich in ihrer Freizeit unbefangen verhalten können und unbeobachtet bleiben.

- **Videoüberwachung in einem Hotel**

Die Videobeobachtung eines Hotels in Kiel muss noch mit den Bestimmungen des BDSG in Einklang gebracht werden. Hoteleigene Parkplätze, die Außenfassade, Zugangstüren und der Tresen mit der Kasse wurden gefilmt und die Bilder für eine gewisse Zeit aufbewahrt. Durch Veränderung des Erfassungsbereichs einer Außenkamera sowie auffälligere Hinweisschilder konnten Verbesserungen erreicht werden. Doch es war noch ein Monitor installiert – gut einsehbar für alle Hotelgäste. Die Begründung des Geschäftsführers: „Das ist doch ein deutlich sichtbarer Hinweis auf unsere Videoüberwachung!“ Dass Hotelgäste sich hierüber gegenseitig beobachten konnten, war für ihn kein Problem. Der Aufforderung des ULD, den Monitor der **Neugierde der Hotelgäste** zu entziehen, wollte das Hotel zunächst nicht nachkommen.

- **Webcam in der Fußgängerzone**

Ein Kaufhaus installierte an der Außenfassade eine Kamera und übertrug die Bilder aus der **Fußgängerzone** in Kiel ins Internet. Gezeigt wurde ein Bereich, der sich unmittelbar vor der Dienststelle des ULD befand. Zwar bedurfte es für das Erkennen der gezeigten Personen im Internet eines gewissen Zusatzwissens: „Der Kollege Meier ist aber heute mal wieder sehr spät dran!“ oder: „Meine von Hartz IV lebende Nachbarin geht schon wieder zu Douglas!“ Eine Personenbeziehbarkeit ließ sich aber unseres Erachtens nicht leugnen. Wir schlugen dem Kaufhaus vor, das Problem durch Veränderung des Erfassungswinkels der Kamera oder der Bildschärfe zu lösen. Das Kaufhaus griff den zweiten Vorschlag des ULD auf und stellte den sensiblen Nahbereich zur Kamera unscharf.

Weitere Themen waren die Videoüberwachung in Umkleideräumen, von Nachbargrundstücken, von Arbeitnehmern usw. Erschreckend weit verbreitet sind technischer Spieltrieb gepaart mit Unvernunft und fehlender Sensibilität für das Persönlichkeitsrecht anderer Menschen. Die Beschwerdezahlen steigen. Die personellen Kapazitäten des ULD für die mit Steuermitteln finanzierte Streitschlichtung sind ausgeschöpft. Angesichts der Erlöse der Unternehmen der Videowirtschaft und deren teilweise dummdreister Werbung, die zur Persönlichkeitsverletzung einlädt, liegt der Schluss nahe, von dieser Branche nach dem Verursacherprinzip eine **Datenschutzabgabe** einzuführen. Auch eine bußgeldbewehrte Meldepflicht der im öffentlichen Raum installierten Kameras hätte vielleicht eine erzieherische Wirkung (27. TB, Tz. 5.10).

Was ist zu tun?
Der Gesetzgeber bleibt aufgerufen, die immer weiter um sich greifende Videoüberwachung im Privatbereich einzugrenzen.

5.5 König Fußball und der Datenschutz

Ein Bezirksgericht des Schleswig-Holsteinischen Fußballverbandes (SHFV) veröffentlichte Zusammenfassungen seiner Entscheidungen sowie teilweise vollständige Urteile bzw. Beschlüsse im Internet.

Unter der Rubrik „Aktuelle Urteile“ und „Berufungsurteile“ fand die Öffentlichkeit auf der **Internetseite eines Bezirksgerichts** des Schleswig-Holsteinischen Fußballverbandes Informationen zu verhängten Spielersperren und Geldstrafen mit Namen der verurteilten Spieler, deren Vereinszugehörigkeiten und Kurzbeschreibungen der Vergehen (z. B. grobes Foulspiel) sowie Beschlüsse der Berufungsinstanz im Volltext.

Für den ordnungsgemäßen Ablauf des Spielbetriebes ist es nicht erforderlich, dass Spielersperren bzw. Geldstrafen inklusive zugrunde liegender Fouls öffentlich gemacht werden. **Spielersperren** werden anders durchgesetzt: Die Spieler müssen vor einem Fußballspiel ihre Spielerpässe beim Schiedsrichter vorlegen. Dieser vermerkt die Teilnehmenden namentlich im Spielbericht und reicht den Bericht an

den Verband weiter. Der Verband verfügt über die Informationen zu Sperren und Sportgerichtsentscheidungen und kann eine unberechtigte Spielteilnahme feststellen. Die besondere (Un-)Annehmlichkeit für die Vereine rechtfertigt die Veröffentlichung im Internet nicht.

Die **Rechtsordnung des Fußballverbandes** sieht die Veröffentlichung von Sportgerichtsentscheidungen vor. Danach werden bestimmte Urteile (Verbandsurteile und Entscheidungen über Vereinssperren) im amtlichen Mitteilungsblatt des SHFV veröffentlicht. Die Veröffentlichung im Internet verletzt hingegen schutzwürdige Interessen der Betroffenen, da sie leicht und weltweit verfügbar ist – anders als das von einem begrenzten Personenkreis genutzte Mitteilungsblatt. So geht etwa den Kollegenkreis oder den Arbeitgeber möglicherweise unsportliches Verhalten im Freizeitbereich nichts an. Einmal im Internet Veröffentlichtes lässt sich nicht mehr sicher und rückstandsfrei löschen, da nie sicher ist, ob die Daten irgendwo gespiegelt oder weiter reproduziert wurden. Das Sportgericht hat nach unserer Beanstandung die veröffentlichten Urteile und Berufungsurteile von den Webseiten entfernt und die bisherige Veröffentlichungspraxis eingestellt.

Was ist zu tun?
Die Veröffentlichung von personenbezogenen Daten im Internet stellt eine Datenübermittlung an einen unbegrenzten Personenkreis dar, die einer gesetzlichen Grundlage oder Einwilligung bedarf. In Printmedien veröffentlichte Informationen dürfen nicht automatisch auch ins Internet gestellt werden.

5.6 Unzulässige Halterabfrage mit Folgen

Der Mitarbeiter einer Versicherung missbrauchte seine Stellung und holte Auskünfte über den Halter eines Fahrzeuges zu privaten Zwecken ein.

Der Mitarbeiter einer Versicherung nutzte den Briefkopf seines Arbeitgebers und führte eine Halterabfrage zu einem Fahrzeug bei der zuständigen Kfz-Zulassungsstelle durch, obwohl für dieses Fahrzeug kein Haftpflichtschaden gemeldet war. Er verwies dabei auf einen tatsächlich bei der Versicherung anhängigen Schadenshergang, um ein **berechtigtes Interesse vorzutäuschen**. So gelangte er an die gewünschten Auskünfte über den Halter des abgefragten Fahrzeuges, die er in Wahrheit zu rein privaten Zwecken nutzen wollte.

Das ULD verhängte ein **Bußgeld**. Der Versicherungsmitarbeiter handelte ordnungswidrig, indem er vorsätzlich nicht allgemein zugängliche Informationen über den Halter durch unrichtige Angaben bei der Kfz-Zulassungsstelle erschlich.

Was ist zu tun?
Mitarbeiter, die über ihre Funktion im Unternehmen an geschützte Personendaten gelangen können, z. B. Kfz-Halterinformationen oder Bonitätsauskünfte, sind vom Arbeitgeber besonders auf ihre Geheimnisverpflichtung hinzuweisen. Die Zugriffe auf solche Informationen müssen dokumentiert und sollten zumindest stichprobenartig kontrolliert werden.

5.7 Videotheken und Datenschutz

Prüfungen von Videotheken zeigten, dass es gängige Praxis ist, bei der Ausstellung eines Videothekenausweises die Personalausweisnummer der Kundinnen und Kunden zu speichern. Die Angaben zu Leihvorgängen wurden oft zu lange gespeichert.

Das Personalausweisgesetz will die Nutzung der Personalausweisnummer als eindeutige **Personenkennziffer verhindern**. Diese Nummern dienen dem Zweck, die Ausstellung von Dubletten zu vermeiden. Sie dürfen nicht als Ordnungsmerkmale in anderen Zusammenhängen verwendet werden. Daher ist hierüber der Abruf personenbezogener Daten sowie die Verknüpfung von verschiedenen Datenquellen verboten. Um dieses Verbot effektiv umzusetzen, ist bereits die Erhebung und Speicherung der Personalausweisnummer in der Regel unzulässig.

Bei den geprüften Videotheken erfolgte die Speicherung der Ausweisnummer, ohne dass sie für die **Durchführung des Mietvertrags** erforderlich war. Sie war schon aus diesem Grunde unzulässig.

> **?** ***Warndatei***
>
> *Im Vermietungsgewerbe besteht regelmäßig ein großes Interesse, unternehmensübergreifende „schwarze Listen" oder sonstige **Warndateien** aufzubauen, in denen über bestimmte Suchmerkmale vermeintlich schwarze Schafe ohne Aufwand gefunden und verknüpft werden können. Als Suchmerkmal eignet sich die Personalausweisnummer, da sie eindeutig und über die Ausweisvorlage leicht zu erheben ist. Warndateien tangieren in der Regel die schutzwürdigen Interessen der Betroffenen, weil nicht transparent wird, aufgrund welcher Verhaltensweisen eine Einmeldung in die Liste erfolgt, und weil eine Klassifizierung als schwarzes Schaf im Einzelfall nicht gerechtfertigt sein kann.*

Die Prüfungen ergaben, dass die Videotheken Ausleihdaten, also z. B. Datum und Dauer der Vermietung sowie Produktbezeichnung, über den Zeitpunkt der Rückgabe hinaus speicherten. Sobald der ausgeliehene Spielfilm ordnungsgemäß zurückgegeben ist und die Ansprüche aus dem Mietverhältnis abgewickelt sind, besteht für eine weitere Speicherung der Ausleihdaten keine weitere Notwendigkeit. Bei den Ausleihdaten kann es sich um höchst sensitive Informationen handeln, wenn z. B. im Erotikbereich Angaben zum Namen eines Films, die Einordnung als pornografisch und Angaben über die Ausleihdauer Rückschlüsse auf das Sexualleben bzw. sexuelle Präferenzen der betroffenen Kunden zulassen. Die Betroffenen haben einen Anspruch auf eine freie, unbeobachtete und vor allem **nicht dokumentierte Entfaltung ihrer Persönlichkeit**. Dieser Anspruch besteht auch gegenüber der Videothek.

Das ULD **beanstandete** die Speicherung der Personalausweisnummern bei den geprüften Unternehmen und forderte deren Löschung. Die Unternehmen wurden darauf hingewiesen, dass die Ausleihdaten zu löschen sind, sobald deren Speicherung zur Abwicklung des Mietverhältnisses nicht mehr erforderlich ist. Die allgemeinen Geschäftsbedingungen der geprüften Unternehmen waren in puncto Datenschutzhinweis zum Teil nachbesserungswürdig. Wir machten deutlich, dass

die Nutzung von Telefonnummern zu Werbezwecken, auch zur Versendung von Werbe-SMS, ohne ausdrückliche Einwilligung der Kunden unzulässig ist. Um über die konkreten Prüfungen hinaus sowohl Kundinnen und Kunden als auch Betreibern von Videotheken einen Überblick über die Datenschutzrechte und -pflichten zu geben, haben wir hierzu Informationen zusammengestellt und veröffentlicht.

www.datenschutzzentrum.de/wirtschaft/videothek.htm

Was ist zu tun?
Der Personalausweis darf als Sichtvorlage zur Identifikation der Kunden bei der Ausstellung des Videothekenausweises verwendet werden. Eine Speicherung der Personalausweisnummer und die Erstellung und Aufbewahrung von Kopien des Ausweises sind dagegen unzulässig. Nutzungsdaten müssen im Regelfall gelöscht werden, wenn der Mietvertrag abgewickelt ist, es sei denn, der betroffene Kunde hat in die Aufbewahrung ausdrücklich schriftlich eingewilligt.

5.8 Scoring bei Girokonten ohne Dispositionskredit

Ein Bürger ärgerte sich: Sein Antrag auf ein Girokonto ohne Dispositionskredit wurde abgelehnt, nachdem er Angaben zu Beruf, Branche, Voranschrift und Anstellungsdauer verweigerte.

Der Einsatz von Scoring-Verfahren zur Entscheidung über einen Kreditantrag **kann datenschutzrechtlich zulässig sein**, wenn der Kreditantragsteller in die Ermittlung eines Scorewertes eingewilligt hat oder die Durchführung des Scorings dem Vertragszweck dient und zum Bestandteil des Kreditantrages gemacht wird. Im letzteren Fall dürfen allerdings nur solche Angaben in das Verfahren einfließen, die einen unmittelbaren, plausibel nachvollziehbaren Einfluss auf die Einkommens- und Vermögensverhältnisse des Betroffenen haben. In beiden Fällen ist es unabdingbar, dass der Betroffene vorab hinreichend informiert wird, insbesondere über den Zweck und die Durchführung des Scorings, die einbezogenen Kategorien von Daten und deren Bedeutung.

Die kritisierte Bank hatte es dem Betroffenen gegenüber nicht für nötig befunden, ihre Kunden über den Einsatz eines internen Scoring-Verfahrens überhaupt zu informieren. Das Unternehmen verwies darauf, dass den Kunden aus der allgemeinen Lebenserfahrung, der Berichterstattung in den Medien oder aufgrund anderer Kontobeziehungen bewusst sein sollte, dass sich eine Bank solcher Verfahren bediene. Damit befand die Bank sich auf dem Holzweg: Die **mangelnde Transparenz** für die Kunden beanstandete das ULD nicht zuletzt mit dem Hinweis, dass weder die allgemeine Lebenserfahrung noch die Medien die datenschutzrechtlich verantwortliche Stelle von ihren gesetzlichen Informations- und Unterrichtungsverpflichtungen befreien kann.

Zwar kann ein Scoring-Verfahren zulässig im Rahmen von Kreditanträgen durchgeführt werden. Vorliegend ging es allerdings um einen Antrag auf ein **Girokonto ohne Dispositionskredit**. Die Bank meinte, für ein Girokonto werde automatisch auch eine EC-Karte ausgehändigt und die Ausgabe der Karte käme faktisch einer Kreditgewährung gleich. Mit der EC-Karte könnten Kunden nämlich auch bei fremden Kreditinstituten am Geldautomaten Geld abheben. Dabei erfolge kein sofortiger Abgleich mit dem Konto des Kunden. Vielmehr werde den Kunden ein standardisierter Verfügungsrahmen von 1000 Euro pro Tag und 2000 Euro pro Woche eingeräumt. Die tatsächliche Deckung durch das Konto werde erst zu einem späteren Zeitpunkt festgestellt.

? *Scoring*

Scoring-Verfahren sollen zukünftiges Verhalten vorhersagen. Häufig geht es darum, das Notleiden eines Kredits zu prognostizieren, d. h. festzustellen, mit welcher Wahrscheinlichkeit der Betroffene künftig zahlungsfähig und zahlungswillig sein wird, z. B. einen Kredit zurückzahlen wird. Beim Kredit-Scoring werden bestimmte Merkmale wie Wohnort, Familienstand, Beruf, Kfz-Besitz usw. einer Vielzahl von Personen statistisch danach ausgewertet, ob zwischen den Merkmalen und dem Zahlungsverhalten der Personen statistische Zusammenhänge bestehen. Die einzelnen Ausprägungen der Merkmale werden aufgrund eines Punktesystems danach bewertet, ob sie sich statistisch gesehen eher positiv oder eher negativ auf das Zahlungsverhalten der Personen auswirken. Anhand der individuellen Merkmale des Kunden wird dann ein Punktewert errechnet, der eine Wahrscheinlichkeit für bestimmtes zukünftiges Zahlungsverhalten zum Ausdruck bringen soll.

Für den Betroffenen war dies nicht ohne Weiteres erkennbar. Der Antragsteller musste davon ausgehen, dass kein kreditorisches Risiko seitens der Bank besteht. Er wollte auch kein Kreditverhältnis, sonst hätte er einen Antrag auf Dispositionskredit gestellt. Im Falle eines Antrages auf ein Girokonto ohne Dispositionskredit ist daher grundsätzlich eine **Einwilligung des Betroffenen** zur Ermittlung eines Scorewertes erforderlich. In jedem Fall muss der Antragsteller darüber aufgeklärt werden, dass das Bankinstitut mit der Aushändigung einer EC-Karte von einem kreditorischen Risiko ausgeht.

Die konkreten Anforderungen an ein **datenschutzkonformes Kredit-Scoring** hat das ULD in einem Gutachten dargelegt, das im Internet zum kostenlosen Download zur Verfügung steht (28. TB, Tz. 8.8).

www.datenschutzzentrum.de/scoring/index.htm

Was ist zu tun?
Die gängige Praxis der Scoring-Verfahren in Banken und Kreditinstituten verstößt weiterhin in vieler Hinsicht gegen das Datenschutzrecht. Die gesamte Branche und jedes einzelne Institut sind aufgefordert, endlich rechtmäßige Zustände herzustellen. Dazu gehört hinreichende Transparenz für die Betroffenen über alle relevanten Umstände.

5.9 Übermittlung von Mieterdaten bei Mieterhöhungen

Immer wieder wird das ULD mit der Frage konfrontiert, welche Angaben über andere Mieter zur Begründung von Mieterhöhungsverlangen offenbart werden dürfen.

Will ein Vermieter die Miete erhöhen, so kann er sein Mieterhöhungsverlangen nach dem Bürgerlichen Gesetzbuch durch die Angabe von **drei Vergleichswohnungen** begründen. Um die Vergleichbarkeit der Wohnungen mit der eigenen im Zweifel überprüfen zu können, muss der Mieter diese einwandfrei identifizieren können. Damit sein Mieterhöhungsverlangen eventuell auch vor Gericht Bestand hat, hat der Vermieter ein Interesse an möglichst genauer Benennung der Vergleichswohnungen. Damit muss er allerdings sensitive Informationen der Bewohner der Vergleichswohnungen offenbaren. Deren Namen lassen sich einfach aufgrund der Angaben zu den Wohnungen feststellen. Die Angaben über Art, Größe, Preis und Lage einer Wohnung lassen Rückschlüsse auf die Lebensverhältnisse der Mieter zu. Details über den intimen Lebensbereich „Wohnung“ geheim zu halten, gehört zu deren schutzwürdigen Interessen. Es besteht also ein Konflikt zwischen dem Interesse eines Vermieters an begründeten Mieterhöhungsverlangen und dem Interesse von Mietern, die Vertraulichkeit ihrer Lebensumstände zu wahren.

Dieser Konflikt lässt sich nur über größtmögliche **Transparenz und Beachtung von Zweckbindung und Datensparsamkeit** auflösen: Mieter sind in jedem Fall vom Vermieter darüber zu informieren, welche Angaben zu ihrer Wohnung an andere Mieter weitergegeben werden. Der Empfänger eines Mieterhöhungsschreibens ist darauf hinzuweisen, dass die erhaltenen Angaben über andere Mieter ausschließlich zum Zweck der Überprüfung des Mieterhöhungsverlangens genutzt werden dürfen. Die Weitergabe von Namen zusätzlich zu den Angaben zu einer Wohnung bedarf der vorherigen schriftlichen Einwilligung.

Was ist zu tun?
Vermieter müssen sich bei Mieterhöhungsverlangen streng daran orientieren, was an Offenlegung über die Vergleichswohnungen und deren Bewohner nötig ist. Diese sind vorher zu informieren.

5.10 Inkasso – Pfändungsbeschlüsse beim Arbeitgeber

Dürfen Inkassounternehmen bei Arbeitgebern Auskünfte über Schuldner einholen? Derartige Anfragen sind aus Datenschutzsicht grundsätzlich möglich. Einer Auskunftserteilung durch den Arbeitgeber können aber schutzwürdige Interessen des Arbeitnehmers entgegenstehen.

Personenbezogene Daten sind grundsätzlich **beim Betroffenen zu erheben**. Von diesem Direkterhebungsgrundsatz gibt es allerdings Ausnahmen, z. B. wenn der Geschäftszweck eine Erhebung bei Dritten erforderlich macht. Bei Inkassounternehmen entspricht es regelmäßig dem Geschäftszweck, ergänzende Auskünfte

Dritter einzuholen, um die Ansprüche ihrer Auftraggeber bzw. der von ihnen gekauften Forderungen z. B. im Vollstreckungsverfahren zu realisieren. Es besteht regelmäßig ein berechtigtes Interesse an Auskünften von Dritten, wenn das Inkassounternehmen beabsichtigt, den Geschäftsbesorgungsvertrag mit dem Auftraggeber zu erfüllen und die zur Einziehung übertragenen Forderungen zu realisieren.

Schutzwürdige Interessen der betroffenen Schuldner, keinen Ausforschungen hinter ihrem Rücken ausgesetzt zu sein, müssen zumeist zurücktreten, soweit ein **rechtskräftiger Vollstreckungstitel** besteht. Der Gesetzgeber hat eine Vollstreckung bei Dritten in einem sogenannten Drittschuldnerverfahren, also z. B. beim Arbeitgeber, ausdrücklich in der Zivilprozessordnung vorgesehen.

Gleichwohl ist der **Arbeitgeber** nicht verpflichtet und in vielen Fällen aus Datenschutzsicht ohne die ausdrückliche Einwilligung des Schuldners bzw. Arbeitnehmers auch nicht legitimiert, Auskünfte an anfragende Inkassounternehmen zu erteilen. Der Arbeitgeber hat eine Fürsorgepflicht beim Umgang mit den Daten seiner Arbeitnehmer. Nach der Wertung des BDSG unterliegen die Arbeitnehmerdaten, auch die Information, dass der Schuldner Arbeitnehmer beim angefragten Arbeitgeber ist, einem besonderen Schutz. Dieser kann nicht allein unter Hinweis auf ein berechtigtes Interesse des Inkassounternehmens aufgegeben werden. Wenn der Arbeitgeber bereits als potenzieller Drittschuldner bekannt ist und bei diesem angefragt wird, kann allerdings aufgrund eines eigenen berechtigten Interesses zur Vermeidung drohender hoher Kosten unter Unterrichtung der betroffenen Mitarbeiter die Erteilung von Auskünften – je nach den konkreten Umständen – rechtmäßig sein.

Was ist zu tun?
Der Arbeitgeber muss in Anbetracht des besonderen Schutzes von Arbeitnehmerdaten und seiner Fürsorgepflicht aus dem Arbeitsverhältnis davon ausgehen, dass das schutzwürdige Interesse des Arbeitnehmers gegenüber einem berechtigten Interesse eines Dritten auf Erteilung von Auskünften überwiegt. Jeder Fall ist – unter Einbeziehung des Betroffenen – sorgfältig zu prüfen.

5.11 Sparkassen – Papierkörbe, Aktenvernichtung und Schlüsselverwaltung

Das ULD wurde darauf aufmerksam gemacht, dass es in einer schleswig-holsteinischen Sparkasse offensichtlich Unregelmäßigkeiten bei der Einhaltung von technischen und organisatorischen Sicherheitsmaßnahmen gab.

Eine kurzfristig angesetzte Prüfung eines Kreditinstitutes ergab Folgendes: Abfallpapier mit personenbezogenen Daten sollte gemäß Weisung in Papierkörben gesammelt und abends von den Reinigungskräften in den verschließbaren Containern einer Aktenvernichtungsfirma zwischengelagert werden. Leider standen diese **Papierkörbe** aber in für Kunden zugänglichen Bereichen. Ein Mitarbeiter des ULD fand beim ersten Griff in einen solchen Papierkorb den Auszug aus einer notariellen Beurkundung mit Namen und Anschrift des Notars sowie der Mandanten.

Der **Container der Aktenvernichtungsfirma** stand im verschlossenen Heizungsraum der Filiale, war aber selbst nicht verschlossen. Reinigungskräfte oder Heizungsmonteure hatten so vor der regulären Vernichtung der Akten unbeschränkt auf das im Container lagernde Altpapier mit den personenbezogenen Daten Zugriff.

Sämtliche Räume mit sensitiven Daten waren zwar mit **Sicherheitsschlössern** oder elektronischen Codes gesichert. Die Verantwortlichen der Filiale konnten uns jedoch keine genauen Auskünfte darüber machen, wer über welchen Schlüssel bzw. Code verfügt und durch welches Prozedere die Zutrittscodes geändert werden.

In einer anderen Filiale derselben Sparkasse fand der Prüfer des ULD in einem für die öffentliche Müllabfuhr vorgesehenen **gelben Müllsack** personenbezogene Unterlagen, z. B. Kontoblatt mit Name und Anschrift der Kontoinhaberin sowie Angaben zum Umsatz und zu Kontoständen. Eine Reinigungskraft hatte offensichtlich personenbezogenes Altpapier anstatt in den Container des Aktenvernichters, der auch unverschlossen war, in den normalen Hausmüll gegeben.

Die Sparkasse teilte dem ULD inzwischen mit, dass in den Kundenbereichen Aktenschredder oder kleine verschlossene Aktencontainer aufgestellt werden sollen. Es wurden nachträglich Arbeitsanweisungen zur Datensicherheit und umfangreiche Auszüge aus einem Sicherheitshandbuch zur Verfügung gestellt. All das wäre schon vor der Prüfung nötig gewesen. Die aufmerksamen Augen von Kundinnen und Kunden und ein kurzer Hinweis beim ULD können sicher auch in anderen Fällen zur nötigen **Abhilfe von Mängeln** beitragen.

Was ist zu tun?
Jedes Finanzinstitut benötigt interne Arbeitsanweisungen zum Datenschutz und zur Datensicherheit. Diese müssen aber auch mit Leben gefüllt werden, z. B. indem periodisch auf sie hingewiesen und ihre Einhaltung durch den betrieblichen Datenschutzbeauftragten oder andere Verantwortliche tatsächlich kontrolliert wird.

5.12 Füllstand bei Flüssiggasbehältern

Ein kurioser Vorgang: Die Speicherung und Übermittlung des Füllstandes bei Flüssiggasbehältern führte zu datenschutzrechtlichen Verwicklungen.

Bei der Flüssiggasbelieferung mietet der Endkunde in der Regel einen Flüssiggasbehälter bei einem Versorgungsunternehmen bzw. Gaslieferanten. Die Anschaffung, Wartung und Pflege des Tanks wird dann über den Versorgungsvertrag subventioniert. Bedingung für die Subvention ist, dass sich der Endkunde nicht von anderen Gaslieferanten beliefern lässt. Die Versorgungsunternehmen beauftragen zur **Wartung der Behälter** externe Prüfgesellschaften, die eine gesetzlich vorgeschriebene äußere Prüfung an den Flüssiggasbehältern vornehmen. Bei dieser Gelegenheit wird regelmäßig auch der Füllstand des jeweiligen Gasbehälters

erhoben und im Prüfbericht vermerkt. Der Prüfbericht wird an den Gaslieferanten übermittelt.

Ein Bürger machte das ULD darauf aufmerksam, dass die Gaslieferanten die auf diesem Wege erlangten Informationen über den Füllstand dazu nutzen, den Befüllungsgrad mit den eigenen Daten über das Verbrauchsverhalten der Kunden abzugleichen. Ergeben sich dabei Unstimmigkeiten, werden die Kunden unter Umständen mit dem **Vorwurf der Fremdbefüllung** konfrontiert. Allein aus einem geringeren Gasverbrauch kann allerdings noch nicht auf eine Fremdbefüllung geschlossen werden. Vielmehr können für einen niedrigeren Verbrauch vielfältige Umstände eine Rolle spielen, z. B. eine Wärmedämmung, neue Fenster, sparsamer Verbrauch.

Den Endkunden wurde nicht mitgeteilt, dass der Füllgrad ihres Flüssiggasbehälters bei der äußeren Prüfung erhoben, gespeichert und an das Versorgungsunternehmen zur Dokumentation der ordnungsgemäß durchgeführten Prüfung übermittelt wird. Der von der Prüfgesellschaft er- und übermittelte Befüllungsgrad des Flüssiggasbehälters unterliegt einer klaren Zweckbindung. Er dient allein dazu, die ordnungsgemäß durchgeführte Prüfung gegenüber dem Versorger zu dokumentieren und darf beim Versorgungsunternehmen nicht zu Verbrauchsverhaltenskontrollen verwendet werden. Das ULD regte gegenüber dem Deutschen Verband Flüssiggas e.V. an, die angeschlossenen Versorgungsunternehmen von Verbandsseite darüber zu informieren, dass eine Nutzung der Füllstandsinformation zur Kontrolle einer etwaigen Fremdbefüllung nicht zulässig ist. Der Prüfgesellschaft wurde von uns aufgetragen, die **Endkunden** über die Speicherung und Übermittlung des Füllstandes zu **informieren**. Zu diesem Zweck wurde vorgeschlagen, im Prüfbericht, von dem der Endkunde eine Kopie erhält, auf die Übermittlung des Füllstandes hinzuweisen. Dies wurde umgehend aufgegriffen und umgesetzt.

Was ist zu tun?
Beabsichtigen Versorgungsunternehmen Kontrollen zur Verhinderung von Fremdbefüllungen, so muss dies vertraglich mit dem Endkunden geregelt werden. Die Endkunden sind von den Prüfgesellschaften über die Speicherung und Übermittlung des Befüllungsgrades anlässlich der äußeren Prüfung zu unterrichten.

5.13 Taxifahrerdaten für die Krankenkassen

Zur Durchführung von Patientenfahrten schloss ein Landesverband für Taxifahrer in Schleswig-Holstein einen Vertrag mit den Krankenkassen und verpflichtete sich, in regelmäßigen Abständen Mitgliederlisten an die Krankenkassen zu übermitteln.

In dem Vertrag wurde die Durchführung und Vergütung von Patientenfahrten in Schleswig-Holstein, die als solche im Sozialgesetzbuch ausdrücklich vorgesehen sind, vereinbart. Die Übermittlung der Mitgliederlisten sollte den Krankenkassen

dazu dienen zu überprüfen, ob die Taxifahrer, die nach dem mit dem Landesverband vereinbarten Tarif für die Patientenfahrten abrechnen, auch tatsächlich Mitglied des Vertragspartners sind. Wir beanstandeten, dass die Übermittlung der Daten über die Köpfe der Mitglieder hinweg durch den Verband erfolgen sollte. In der **Verbandssatzung** bzw. in den **Mitgliedsverträgen** fehlte es an Regelungen und Hinweisen hierzu. Auch gehörte es nach der Verbandssatzung grundsätzlich nicht zu den Aufgaben des Landesverbandes, Vereinbarungen mit den Krankenkassen nach dem Sozialgesetzbuch über die Durchführung von Patientenfahrten zu schließen.

Zwar kann die Vertretung der wirtschaftlichen Interessen der Mitglieder im Bereich der Vergütung von Krankenfahrten ein Betätigungsfeld des Verbandes sein. Es lag im Rahmen des Verhandlungsmandates und des Verbandsinteresses, mit den Krankenkassen eine Überprüfung eingehender Abrechnungen der Taxifahrer auf deren Anspruchsberechtigung für den vereinbarten Tarif hin vorzusehen. Dies gilt insbesondere vor dem Hintergrund, dass die Verhandlungen für die Mitglieder durch die stete Information über den Fortgang in den Mitgliederrundschreiben und durch das Angebot der Übersendung des Vertrages auf Anfrage nach Abschluss des Verfahrens auch transparent waren. Doch handelt es sich bei der getroffenen Vereinbarung aus datenschutzrechtlicher Sicht um einen **Vertrag zulasten Dritter**, solange aus Mitgliedersicht keine eindeutig an den Verband delegierte Verfügungsbefugnis über die Daten bestand. Das schutzwürdige Interesse der Mitglieder hätte es erforderlich gemacht, mit Rücksicht auf die Verfügungsbefugnis jedes einzelnen Mitglieds über seine Daten eine gesonderte und ausdrückliche Information hinsichtlich der Datenübermittlung durchzuführen und den Mitgliedern ein individuelles Widerspruchsrecht gegen die Übermittlung ihrer Daten einzuräumen.

Zudem wäre eine **datensparsamere Lösung** möglich gewesen: Die Taxifahrer hätten bei der Abrechnung selbst ihre Mitgliedschaft gegenüber der Krankenkasse nachweisen können. Die automatische monatliche Übermittlung der Mitgliederlisten wäre so nicht erforderlich gewesen; die Krankenkassen hätten trotzdem überprüfen können, ob eine Abrechnung zum vereinbarten Tarif berechtigt ist.

Dem Landesverband wurde aufgegeben, die Altmitglieder in verständlicher Form zu informieren mit dem **Hinweis auf die Möglichkeit eines Widerspruches** gegen die Datenübermittlung innerhalb einer angemessenen Frist. Die Neumitglieder sollen im Aufnahmevertrag über die listenmäßige Übermittlung aller Mitgliedsdaten an die Krankenkassen aufgeklärt werden. Dem Verband wurde zudem empfohlen, eine Satzungsänderung vorzunehmen, um von vornherein Transparenz hinsichtlich der vorgenommenen Datenverarbeitungen herzustellen.

Was ist zu tun?
Vereine und Verbände dürfen nur solche Datenverarbeitungen vornehmen, die vom Zweck bzw. ausdrücklichen Regelungen der Satzung erfasst werden. Darüber hinausgehende Datenverarbeitungen, vor allem solche, die schutzwürdige Interessen der Mitglieder betreffen, bedürfen eines expliziten Einverständnisses.

6 Systemdatenschutz

6.1 Transparenz und Revisionssicherheit: Basis jedes Datenschutzmanagements

Die automatisierte Verarbeitung personenbezogener Daten muss jederzeit auf ihre Gesetzeskonformität hin überprüft werden können. Dem dient ein Datenschutzmanagementsystem, dessen primäre Funktion darin besteht, nachweisbar für Transparenz und Revisionsfähigkeit zu sorgen.

Ein **Datenschutzmanagementsystem** (DSMS) integriert sämtliche datenschutz- und datensicherheitsrelevanten Prozesse einer Organisation. Durch ein funktionierendes DSMS wird dafür gesorgt, dass schon in der Planungsphase beim Neu- oder Redesign von Informationstechnologie die künftige Einhaltung gesetzlicher Regelungen berücksichtigt wird. Beim Betrieb der Verfahren müssen anlassbezogen und regelmäßig Kontrollen der Verarbeitung auf ihre Ordnungsmäßigkeit hin durchgeführt werden können. Dies funktioniert nur dann effektiv und wirtschaftlich, wenn bei der Auswahl von Systemen und Programmen und bei den technischen und organisatorischen Vorgaben für den Einsatz eines Verfahrens auf zwei Aspekte besonders geachtet wird: Transparenz und Revisionsfähigkeit.

Ein DSMS umfasst diejenigen **Kontroll- und Konzepttätigkeiten**, die Datenschutzbeauftragte zusammen mit den fachlich und technisch Verantwortlichen regelmäßig oder anlassbezogen durchführen. Ein DSMS kann Bestandteil eines bereits bestehenden Gesamtprozessmanagements – beispielsweise eines Ministeriums – sein. Oder es dient als zentrale Steuerungs- und Kontrollinstanz für alle Aspekte des Einsatzes von Informations- und Kommunikationstechnologie in kleineren Verwaltungseinheiten, etwa auf kommunaler Ebene, und wird so als Kern des Prozessmanagements genutzt.

Zu einem Datenschutzmanagementsystem gehört ein Datenschutzbeauftragter, der alle in einer Organisation auftauchenden Datenschutzfragen betreut, sowie ein Regelwerk, aus dem hervorgeht, welche Prüfkriterien gelten, wie diese zu kontrollieren sind, welche Abweichungen vom Sollwert inakzeptabel sind und was bei inakzeptablen Abweichungen zu tun ist. Der Datenschutzbeauftragte beteiligt sich an der Erstellung datenschutzgerechter Regelwerke und stellt den Grad der Konformität von Verfahren zu diesen Regelwerken fest. Als Regelwerke gelten neben den Gesetzen auch interne Dienstvereinbarungen, Dienstvorschriften oder Verträge mit externen Dienstleistern. Das ULD empfiehlt gerade öffentlichen Stellen mit großer Regelungsverantwortung – allen voran Finanzministerium, Innenministerium und dataport, aber auch den Kreisverwaltungen –, sich an internationalen Standards zum **Prozessmanagement** zur Organisation des IT-Bereichs (z. B. ITIL, COBIT) zu orientieren. Hier sind viele bereits in der Praxis erprobte Prozesse und deren Management prototypisch beschrieben. Sie können als Grundlage für ein übergreifendes, integriertes Datenschutzmanagement dienen.

Ziel der Orientierung am Prozessmanagement ist eine **Abkehr von der „freien Improvisation“**, wie sie heute immer noch in vielen IT-Bereichen anzutreffen ist. Eine Datenverarbeitung „auf Zuruf“ ist bei öffentlichen Stellen schlicht unzulässig.

Transparenz bei der Verarbeitung personenbezogener Daten besteht, wenn sämtliche Tätigkeiten bei der Planung, der Einführung und dem Betrieb von IT-Verfahren vordefiniert und dokumentiert sind. Außerdem muss geklärt sein, wie der Betrieb kontrolliert wird bzw. werden kann.

Die Datenschutzverordnung des Landes (DSVO) fördert Transparenz vor allem durch ihre Anforderung an die Verfahrensdokumentation. In einem informationstechnischen Konzept, kurz **IT-Konzept**, müssen die technischen und organisatorischen Vorgaben sowie die erzielbaren Ergebnisse beschrieben werden. Datenschutzbeauftragte können über dieses Mittel Transparenz in der Planung und im Betrieb herstellen. Es ist jederzeit klar, wozu das Verfahren dient und, nicht minder wichtig, wie es eingesetzt werden wird. Eine öffentliche Stelle kann mit einem IT-Konzept den korrekten Ablauf der Verarbeitung personenbezogener Daten bereits frühzeitig festlegen.

Aufbauend auf dem IT-Konzept fordert die DSVO, dass diejenigen technischen und organisatorischen Maßnahmen in einem **Sicherheitskonzept** dokumentiert werden, mit denen die Vertraulichkeit, Integrität und Verfügbarkeit der Verarbeitung personenbezogener Daten sichergestellt sind. Während also im IT-Konzept dargestellt wird, was gemacht werden soll, wird im Sicherheitskonzept festgelegt, wie es möglichst sicher gemacht werden soll. Über das Sicherheitskonzept werden Fragen des Datenschutzes und der Sicherheit gestellt und beantwortet. Die Güte der Sicherheitsmaßnahmen wird durch eine kritische Betrachtung in einer **Risikoanalyse** geprüft.

IT-Konzept, Sicherheitskonzept und Risikoanalyse sind die zentralen Dokumente für ein funktionierendes Datenschutzmanagementsystem. Datenschutzbeauftragte müssen dafür sorgen, dass die Prozesse, mit denen Informationstechnik geplant, beschafft und in Betrieb genommen wird, sauber dokumentiert sind. Sie müssen darauf achten, dass die **Integration von Datenschutz und Datensicherheit** durch eine Beteiligung des Datenschutzbeauftragten in all diesen Prozessen gewährleistet ist. Dabei müssen sie vor allem dafür sorgen, dass der alltägliche Betrieb tatsächlich so funktioniert wie geplant. Hier setzt die Revisionsfähigkeit an.

Revisionsfähigkeit bezeichnet die Möglichkeit, dass prüfbar ist, ob bei einem konkreten Vorgang die gesetzlichen Vorgaben auch tatsächlich so eingehalten werden bzw. wurden, wie es vorher im IT- und Sicherheitskonzept festgelegt und dokumentiert wurde. Vielfach lassen sich Verfahren nicht so planen, dass eine Fehlfunktion oder ein Missbrauch vollkommen ausgeschlossen ist. Daher müssen in öffentlichen Verwaltungen Vorkehrungen getroffen werden, um Missbrauch oder Fehlfunktionen zumindest im Nachhinein zu erkennen und gegebenenfalls zu beheben. Im Rahmen von regelmäßigen oder anlassbezogenen Kontrollen müssen Datenschutzbeauftragte die ordnungsgemäße Funktion von Verfahren und die rechtmäßige Verwendung personenbezogener Daten kontrollieren können. Deshalb sind bereits bei der Planung eines Systems **Prüfpunkte** zu definieren, an denen die Korrektheit der Datenverarbeitung kontrolliert werden kann.

Die Datenschutzverordnung (DSVO) unterstützt hier IT-Verantwortliche und Datenschutzbeauftragte mit konkreten Anforderungen zur Protokollierung (28. TB, Tz. 6.5). Datenschutzbeauftragte müssen darauf achten, dass eine angemessene, aussagekräftige und zugleich gegenüber den Mitarbeitern **datenschutzkonforme Protokollierung** von Zugriffen auf personenbezogene Daten oder von administrativen Änderungen an Fachverfahren geplant und implementiert wird.

Erst durch eine derart transparente und revisionsfähige Datenverarbeitung ist ein effektives Management von Datenschutz und Datensicherheit möglich. Datenschutzbeauftragte müssen dafür sorgen, dass Datenschutz und Datensicherheit in **sämtliche relevanten Prozesse** einer Organisation eingebunden werden. Dies kann sowohl informell durch die Teilnahme an Planungsrunden oder der weitverbreiteten wöchentlichen Kaffeerunde mit den IT-Verantwortlichen geschehen als auch formal über schriftlich fixierte Prozessbeschreibungen. Ebenso lassen sich in Teilen Synergien mit anderen Abteilungen, die mit Controlling etwa aus betriebswirtschaftlicher Sicht befasst sind, erzielen.

Was ist zu tun?
Datenschutzbeauftragte müssen zusammen mit den Fachverantwortlichen für eine transparente und revisionssichere Datenverarbeitung sorgen. Die Leiterinnen und Leiter öffentlicher Stellen müssen diese Qualitätskriterien als wichtige Leitlinien für ihre Organisation begreifen und mit Nachdruck für deren Umsetzung sorgen.

6.2 ISO 27001 – der neue Grundschutz

Das Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik wurde Anfang dieses Jahres grundlegend überarbeitet. Die Überarbeitung erweist sich in der Praxis als hilfreich. Die BSI-Sicherheitskonzeption und die Anforderungen der Datenschutzverordnung wurden einander angenähert.

Das ULD hat das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) vorgeschlagene Vorgehen zur Erstellung von Sicherheitskonzepten bereits mehrfach betrachtet und entsprechende Hinweise zur Nutzung und Weiterentwicklung gegeben (28. TB, Tz. 6.4). Unsere Kritik richtete sich vor allem auf die unbedarfte Anwendung der Maßnahmenkataloge unter Nutzung des Grundschutztools (GS-Tool). Die derart erstellten Sicherheitskonzepte folgen meist nicht dem vom BSI angedachten Konzept, sondern werden methodisch unreflektiert automatisiert erstellt. Fehlt zudem die qualitative Dokumentation der Sicherheitsmaßnahmen, so sinkt die Aussagekraft derartig erstellter Dokumente weiter ab. **Sicherheitskonzepte auf Knopfdruck** kann es weiterhin nicht geben.

Geht man dagegen methodisch korrekt vor und hält sich an die vom BSI entwickelte Vorgehensweise, so kann IT-Grundschutz eine zuverlässige Methode sein, dem Stand der Technik entsprechende IT-Sicherheitsanforderungen zu identifizieren und Sicherheitsmaßnahmen umzusetzen. IT-Sicherheit bedeutet mehr als

das Umsetzen von Katalogen von Sicherheitsmaßnahmen. Das ULD empfiehlt öffentlichen Stellen bei der Umsetzung der Datenschutzverordnung (DSVO), stets den Prozesscharakter von Datensicherheit und Datenschutz zu beachten. Das heißt konkret: Verantwortlichkeiten müssen geklärt und regelmäßige und anlassbezogene Kontrollen durchgeführt werden. Ferner sind Sicherheitskonzepte zu planen, umzusetzen und fortzuschreiben. Datenschutz und Datensicherheit müssen bereits in der Planungsphase neuer oder bei der Innovation laufender Verfahren berücksichtigt werden. Die Handlungsanweisung zur Durchführung des Datenschutz-Behördenaudits fasst diese Prozesse unter dem Begriff des **Datenschutzmanagementsystems** (DSMS) zusammen (Tz. 6.1).

Das BSI hat Ende 2005 eine **Überarbeitung des Grundschutzhandbuchs** vorgenommen. Als Implementierung des international ausgerichteten Standards ISO 27001 bietet es neben begrifflichen Veränderungen und einer Überarbeitung und Erweiterung der Maßnahmenkataloge als größte Neuerung eine verstärkte Prozesssicht auf IT-Sicherheit. Damit bewegt sich das Modell des IT-Grundschutzes auf die vom ULD im Sinne der DSVO geforderte qualitative Betrachtung von IT-Sicherheit zu. Durch die Einführung eines Managementsystems für IT-Sicherheit (ISMS) werden erstmalig auch qualitative Aspekte der Durchsetzung von Datensicherheit betrachtet.

Die Einführung von Managementsystemen speziell für Datensicherheit und speziell für Datenschutz kann theoretisch unabhängig voneinander erfolgen. In der Praxis führt dies jedoch zu doppeltem Aufwand. Datenschutz ist und bleibt ein großer Treiber für Maßnahmen aus dem Bereich der Datensicherheit. Somit bietet es sich an, neben den vorhandenen Prozessen zum Datenschutz den eigenen **Datenschutzbeauftragten** auch mit dem Management der Datensicherheit gemäß dem IT-Grundschutz zu beauftragen. Hinderlich ist hierfür der bisherige Zustand des Kapitels „Datenschutz“ im Grundschutzhandbuch, weil es kein integraler Bestandteil und zudem rechtlich als auch technisch veraltet ist.

Das ULD arbeitet deshalb aktiv in einer Unterarbeitsgruppe des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder mit. Im Frühjahr 2007 will diese Arbeitsgruppe eine **Erweiterung der BSI-Methodik um Datenschutzaspekte** veröffentlichen. Darüber hinaus erarbeitet das ULD ein Vorgehensmuster, wie die Datenschutzverordnung in Verbindung mit ISO 27001 umgesetzt werden kann.

Was ist zu tun?
IT-Verantwortliche oder Datenschutzbeauftragte, die die Datenschutzverordnung in Verbindung mit ISO 27001 umsetzen möchten, können sich vom ULD beraten lassen.

6.3 Verzeichnisdienste I: Active Directory

Zentrale Verzeichnisdienste wie das von Microsoft angebotene „Active Directory“ bilden das Herz zur Verwaltung vieler Netzwerke. Hier werden Berechtigungen und Einstellungen für Benutzer, Benutzergruppen bzw. Abteilungen, Computer und Programme vorgenommen. Die Umsetzung der rechtlich geforderten Protokollierung, die über das Active Directory erfolgen kann, ist jedoch unzulänglich.

Die Einführung von Verzeichnisdiensten ermöglicht es, zentral Berechtigungen für die Ressourcen einer Organisation – also vor allem für Benutzer und Programme – zu vergeben. Dem Administrator bleibt erspart, jeden PC-Arbeitsplatz einzeln aufzusuchen, um dort die Benutzer und Passwörter einzurichten. Mit dem Active Directory von Microsoft (AD) ist der klassische Verzeichnisdienst um viele weitere Funktionen gewachsen. So können neben Benutzern auch Clients, Server und Drucker sowie die Anwendungsprogramme der Verfahren verwaltet und administriert werden. Die sogenannten **Gruppenrichtlinien** ermöglichen diese Steuerung von Berechtigungen. Diese komfortable Funktionalität erlaubt es wenigen Administratoren, eine vergleichsweise große Anzahl an Computern gleichzeitig und relativ übersichtlich zu verwalten.

Diese Zentralisierung der Macht hat aber zwei Seiten: Einerseits ist eine effiziente Steuerung möglich, andererseits entscheidet ein Administrator mit zwei Klicks zwischen so unterschiedlichen Berechtigungen wie „Gast“ oder „Domänenadministrator“. Wenn eine Organisation hierbei einem Administrator schlicht vertraut, ihn also nicht zu kontrollieren imstande ist, handelt sie fachlich fahrlässig und zugleich rechtswidrig. Eine **Protokollierung von administrativen Tätigkeiten**, die die Organisation der IT und der Verfahren betrifft, ist unabdingbar, um ein Fehlverhalten von Software sowie den Missbrauch von administrativen Rechten nachweisen und aufklären zu können.

Unsere Versuche und Tests im IT-Labor des ULD haben gezeigt, dass eine **revisionssichere und manipulationssichere Protokollierung** im AD zurzeit nicht möglich ist. Dieser Aussage wird von Microsoft nicht widersprochen. Die Funktionalitäten der kommenden Betriebssystemgenerationen lassen erkennen, dass sich daran erst einmal auch nichts wesentlich ändern wird. Es kommt hinzu, dass einige Protokolleinträge **nur schwer lesbar** sind, weil sie unverständliche Detailangaben und scheinbar unnütze, damit ermüdende Quasi-Informationen enthalten. Das ULD empfiehlt, trotz dieser Einschränkungen die Protokollierungsfunktionen unter den Windows-Betriebssystemen so weit wie möglich zu nutzen. Inzwischen gibt es Programme von Drittherstellern, die zumindest in Teilbereichen eine deutlich bessere Protokollierung von Änderungen im Active Directory ermöglichen. Dabei werden spezielle Protokoll- bzw. Logserver eingesetzt, deren Datenbestände auf Einwegmedien geschrieben sind, die dem Einzugsbereich der AD-Administration entzogen sind. Zu beachten bleibt, dass die Protokollierung von Mitarbeitertätigkeiten als ein eigenständiges Verfahren aufzufassen und zu behandeln ist (28. TB, Tz. 6.5).

Was ist zu tun?
Active-Directory-Umgebungen protokollieren nur unzureichend entsprechend den gesetzlichen Anforderungen. In größeren und kritischen Umgebungen sollten spezielle Protokoll- bzw. Logserver eingesetzt werden.

6.4 Verzeichnisdienste II: Virtuelle Verzeichnisdienste

Das Kommunale Forum für Informationstechnik der Kommunalen Landesverbände in Schleswig-Holstein (KomFIT) hat mit dem Aufbau eines virtuellen Verzeichnisdienstes begonnen. Informationen aus unabhängigen Verzeichnisdiensten des kommunalen Bereichs sollen an einer zentralen Stelle abgerufen werden können.

Kreise und Kommunen in Schleswig-Holstein setzen Verzeichnisdienste ein, um **Informationen über ihre Nutzer und IT-Infrastruktur** an zentraler Stelle vorzuhalten. Im Rahmen eines landesweiten E-Governments besteht zudem Bedarf, diese Informationen auch anderen Interessierten sicher und datenschutzkonform bereitzustellen.

Durch Standardsystemkonzepte wie KITS („Kommunale IT-Standards“) nehmen bereits viele öffentliche Kommunen an einem zentralen Verzeichnisdienst (Tz. 9.1.9) teil. Dennoch werden Kommunen und Kreise weiterhin eigene Infrastrukturen planen und betreiben. Im Sinne eines datenschutzfreundlichen E-Governments müssen diese über offene, standardisierte Schnittstellen die für die Zusammenarbeit notwendigen Daten austauschen. Der Zugriff auf in Verzeichnisdiensten verfügbaren Daten ist eine wesentliche Komponente eines **kooperativen E-Government-Ansatzes**.

In einem Modellprojekt hat sich das KomFIT nach ausführlicher Evaluation verschiedener Lösungsansätze für den Aufbau eines **virtuellen Verzeichnisdienstes** entschieden. Dieser integriert die Informationen aus verschiedenen Verzeichnissen dynamisch zur Laufzeit und stellt sich nach außen als ein einziges Verzeichnis dar. Das ist für eine dezentrale kommunale Struktur eine naheliegende Konstruktion. Dies bietet den Vorteil, dass die Speicherung und Pflege der Verzeichnisdaten vor Ort geschieht, also qualitätsorientiert nahe an den Datenquellen ist, der Abruf jedoch von zentraler Stelle aus geschehen kann.

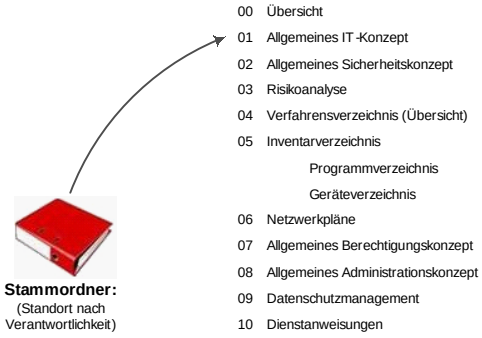
Das ULD unterstützt KomFIT in der Projektarbeit. Wir haben die **Rahmenkriterien** für die Suche in den Datenbeständen definiert, um zu verhindern, dass beispielsweise über eine Suchanfrage der komplette Datenbestand ausgelesen werden kann. Weiterhin hat das ULD die Protokollierung begutachtet. Am Beispiel virtueller Verzeichnisdienste lässt sich erkennen, dass die Arbeit mit dezentralen Datenbeständen durchaus praktikabel und aus Datenschutzsicht sogar ein Gewinn sein kann.

Was ist zu tun?
Das KomFIT sollte das vielversprechende Projekt zu einer einsatzfertigen Lösung fortentwickeln – im Interesse des Aufbaus innovativer Lösungen beim kommunalen E-Government.

6.5 Systematische Dokumentation nach LDSG und DSVO – ein Strukturierungsvorschlag

Im Rahmen von Prüfungen, Beratungen und Audits stellten wir fest, dass vielen Verantwortlichen und Datenschutzbeauftragten die praktische Umsetzung einer datenschutzrechtlich konformen Dokumentation entsprechend dem Landesdatenschutzgesetz (LDSG) und der Datenschutzverordnung (DSVO) Schwierigkeiten bereitet.

Der Grund dafür ist nicht fehlende Sensibilisierung oder Unkenntnis gesetzlicher Vorschriften. Vielmehr ist es schwierig, die Zusammenhänge zwischen konzeptioneller Vorarbeit und laufender Systemdokumentation, organisatorischen und technischen Regelungen, Differenzierung einzelner automatisierter Verfahren und den Revisionsinstrumenten zu berücksichtigen und zugleich die Übersicht zu behalten. Deshalb haben wir dieses Thema aufgegriffen und einen Strukturierungsvorschlag als vorbildhaftes Beispiel einer ordnungsgemäßen Dokumentation erarbeitet. Dieser Vorschlag soll den Verantwortlichen exemplarisch eine Empfehlung an die Hand geben, wie eine datenschutzkonforme Dokumentation strukturiert, übersichtlich erstellt und bequem gepflegt werden kann.



Die Grundlage einer modularen, übersichtlichen und leicht zu erweiternden Dokumentation bildet ein übergeordneter Ordner, der die allgemeinen Konzepte, Verzeichnisse und Anweisungen enthält. Dieser **Stammordner** verweist in einzelnen Gliederungspunkten auf speziellere Dokumentationen. Das Verfahrensverzeichnis verweist beispielsweise auf die entsprechenden Verfahrensakten, das Inventarverzeichnis auf die entsprechenden Systemakten.

Das **Verfahrensverzeichnis** soll den Überblick und die öffentliche Kenntnis über alle automatisierten Verfahren einer Organisation sicherstellen. Wie in der Abbildung oben im Gliederungspunkt 04 dargestellt, kann im Stammordner ein Verfahrensverzeichnis in Form einer Auflistung der gesetzlich vorgeschriebenen Angaben erstellt werden. Diese Auflistung schafft aufgrund ihrer Kürze einen hohen

Grad an Übersichtlichkeit und dient als eine Art „Deckblatt“, das den Verweis (Aktenzeichen) auf die ausführliche Dokumentation in einer Verfahrensakte liefert.

Gliederung

00 Übersicht
01 IT-Konzept (auf Verfahren bezogen)
02 Verfahrensbeschreibung
03 Sicherheitskonzept (auf Verfahren bezogen)
04 Risikoanalyse (auf Verfahren bezogen)
05 Test und Freigabe
06 Berechtigungskonzept
07 Administrationskonzept (auf Verfahren bezogen)
08 Verträge
09 Benutzer- und Administrationshandbücher/Herstellerdaten
10 Protokolle/Kontrollen

In die **Verfahrensakte** werden systematisch alle notwendigen Konzepte und Dokumentationen aufgenommen. Dabei kann die nebenstehende Gliederung bei jedem Verfahren unterschiedlich umfangreich ausfallen. Grundsätzlich werden in den Verfahrensakten immer dann Konzepte, Verträge oder Ähnliches aufgenommen, wenn sie sich speziell auf das Verfahren beziehen und nicht durch die allgemeine Dokumentation im Stammordner abgedeckt werden. So gehören z. B. Test und Freigabe, die spezifisch für jedes automatisierte Verfahren durchgeführt bzw. erteilt werden müssen, in die Verfahrensakte.

Gliederung

00 Übersicht
01 Systembeschreibung
02 Benutzer- bzw. Administrationshandbücher
03 Berechtigungskonzept
04 Administrationskonzept
05 Datensicherungskonzept (bei Servern/dedizierten Rechnern)
06 Verträge
07 Laufende Systemdokumentation (z. B. Patches, Programme usw.)
08 Protokolle/Kontrollen

Das **Inventarverzeichnis** im Stammordner stellt in unserem Strukturierungsvorschlag die Verknüpfung zu den einzelnen Systemakten dar, in denen die einzelnen IT-Komponenten dokumentiert werden. In eine Systemakte gehören alle Konzepte, Verträge oder Ähnliches, die sich speziell auf die entsprechende IT-Komponente beziehen und nicht durch die allgemeine Dokumentation im Stammordner abgedeckt werden. So können z. B. die speziellen Berechtigungen, die für einen Systemadministrator an einem Datenbankserver vergeben wurden, in der **Systemakte** des Datenbankservers dokumentiert werden. Die laufende Dokumentation nimmt einen hohen Stellenwert beim Führen der Systemakte ein, z. B. das regelmäßige Protokoll zur Durchführung der Datensicherung.

Was wird mit der vorgestellten Struktur erreicht? Unser Gliederungsvorschlag orientiert sich an einem **hierarchischen modularen System**, das sowohl für einen Prüfer oder Auditor als auch für den Systemverantwortlichen und alle an der Dokumentation beteiligten Personen einen hohen Grad an Übersichtlichkeit, Strukturierung und Flexibilität liefert. So ist im Stammordner auf einen Blick sowohl der strukturelle und technisch-organisatorische Aufbau einer IT-Organisation ersichtlich als auch ein Überblick über die datenschutzkonforme Dokumentation entsprechend dem LDSG und der DSVO gegeben. Für nähere Informationen zu einem bestimmten Verfahren oder System kann dann entsprechend der vermerkten Verweise (Aktenzeichen) auf die spezielleren Dokumentationen in den Verfahrens- bzw. Systemakten zurückgegriffen werden. Die vorgeschlagene Struktur dient als Grundlage und muss an die technischen und organisatorischen Gegebenheiten der Daten verarbeitenden Stelle angepasst werden.

Was ist zu tun?
Die Strukturierung ist ein Gliederungsvorschlag zur datenschutzkonformen Dokumentation entsprechend dem LDSG und der DSVO. Jede öffentliche Stelle kann die beratende Unterstützung des ULD in Bezug auf die Konzeption und Umsetzung einer datenschutzkonformen Dokumentation in Anspruch nehmen.

6.6 Fehlermanagement über die Clearingstelle

Das melderechtliche Rückmeldeverfahren wird in Schleswig-Holstein und Hamburg über die Clearingstelle bei dataport vermittelt. Diese Clearingstelle hat eine grundlegende konzeptionelle Schwäche, weil dataport Zugriff auf Inhaltsdaten der Meldebehörden bekommt. Als positiv erweist sich dagegen das Fehlermanagement.

Seit Anfang 2007 erfolgt die Übermittlung der **elektronischen Rückmeldung zwischen Meldeämtern** nach bundeseinheitlichen Vorgaben. Im Grundsatz darf eine Meldung nicht mehr auf Papier, sondern nur noch digital erfolgen. Die Kommunikation zwischen den rund 200 Meldeämtern des Landes und der Hamburger Meldebehörde sowie den restlichen ca. 5200 Meldebehörden in Deutschland erfolgt in Schleswig-Holstein über eine zentrale Vermittlungsstelle, die sogenannte Clearingstelle.

Die Landesmeldeverordnung legt fest, dass die schleswig-holsteinischen Meldebehörden die Clearingstelle benutzen müssen. Sie kann aber nur eine **Übergangslösung** sein, weil die zentrale Übersetzung von Daten aus Sicherheitsgründen eine konzeptionelle Schwachstelle darstellt (28. TB, Tz. 6.7). Zudem sind die Meldebehörden in Schleswig-Holstein mittlerweile technisch in der Lage, deutschlandweit verschlüsselt direkt miteinander Daten auszutauschen. Ungeachtet dieser grundsätzlichen Einwände fällt nach Prüfung des mittlerweile vorliegenden Sicherheitskonzepts und der Erfahrungen aus dem ersten Betriebsmonat das Urteil über die Clearingstelle positiv aus.

Die Clearingstelle wird von Schleswig-Holstein und Hamburg gemeinsam betrieben; die operative Durchführung ist dataport übertragen worden. Die Übermittlung der Daten zwischen der Meldebehörde und dataport erfolgt verschlüsselt über das auditierte Landesnetz (Tz. 9.1.1). Der konzeptionell kritische Punkt beim Betrieb besteht darin, dass die Meldedaten bei einem Transfer über die Landesgrenzen von Hamburg und Schleswig-Holstein hinaus nicht schon in der absendenden Meldebehörde vor Ort, sondern erst in der Clearingstelle in das verschlüsselte Übermittlungsformat OSCI-Transport übersetzt werden. Im Prinzip wäre es nicht nötig, dass dataport überhaupt **Zugriff auf die Inhaltsdaten** bekommt.

Zusammen mit den Kollegen vom Hamburgischen Datenschutzbeauftragten konnte das ULD die Konzeptionierung der Clearingstelle begleiten. Zentrale rechtliche Fragen wurden geklärt und technische Sicherheitsanforderungen eingearbeitet. Die Clearingstelle konnte den Betrieb pünktlich und spezifikationsgemäß aufnehmen. Die ersten Erfahrungen Ende Januar 2007 belegen eine signifikante Zahl an **Fehlermeldungen** an der Clearingstelle, die durch Meldebehörden außerhalb von Schleswig-Holstein verursacht wurden. Fehlermeldungen mag man als Hinweis auf konzeptionelle Schwächen bedauern. Aus Datenschutzsicht sind sie hier aber ein positiver Indikator für ein umsichtiges Fehler- und Sicherheitsmanagement, denn eine Rückmeldenachricht darf selbstverständlich nicht zugestellt werden, wenn ein Zertifikat nicht gültig oder abgelaufen ist oder sich der Empfänger nicht korrekt identifizieren lässt. Aufgrund der Fehlermeldungen kann dataport systematisch feststellen und nachvollziehen, dass einige Meldebehörden bzw. Clearingstellen in anderen Ländern ihre Technik nicht korrekt betreiben, und bei diesen entsprechende Fehlerkorrekturen anmahnen bzw. veranlassen.

Trotz der positiven Erfahrung mit der Clearingstelle im Rückmeldeverfahren gilt nach wie vor, dass sie nicht die Anforderung einer Ende-zu-Ende-Sicherheit erfüllt. Voraussetzung für einen etwaigen Einsatz der Clearingstelle für andere Daten und Nachrichten im Sinne eines „**universellen Nachrichtenbrokers**“ ist die Prüfung, ob der damit verbundene Zugriff in der Clearingstelle auf die Inhaltsdaten erforderlich ist.

Was ist zu tun?
Der Betrieb der Clearingstelle muss durch ein Datenschutzmanagement flankiert werden, in dem systematisch Fehlermeldungen ausgewertet und bearbeitet werden. Der Nachrichtenbroker muss nachweisen, dass er die hohen Anforderungen an die Mandantenfähigkeit zur Erfüllung der Anforderungen aus Datenschutz und Datensicherheit sowohl konzeptionell als auch im Betrieb erfüllt.

7 Neue Medien

7.1 Vorratsdatenspeicherung

Ein Gesetzentwurf aus dem Bundesjustizministerium zur Umsetzung der Europäischen Richtlinie zur Vorratsdatenspeicherung kann die gravierenden verfassungsrechtlichen Bedenken gegen die flächendeckende und anlasslose Speicherung der Verkehrsdaten der Telekommunikation einschließlich IP-Adressen und Standortdaten nicht ausräumen.

Nach den Plänen der Bundesregierung sollen alle Anbieter von Dienstleistungen der Telekommunikation (TK) wie Festnetztelefon, Handy und Internet verpflichtet werden, die Verkehrsdaten über Teilnehmer, Ort und Zeit der Verbindungen **ohne Anlass sechs Monate** zu speichern, obwohl diese Speicherung für das Angebot, den Betrieb oder die Abrechnung der Dienste nicht erforderlich ist. Mit dieser Änderung des Telekommunikationsgesetzes soll die EG-Richtlinie zur Vorratsdatenspeicherung 2006/24/EG umgesetzt werden (28. TB, Tz. 11.1).

Die Änderung ist gravierend. Bisher werden in der Praxis bei Diensten mit einer Kostenabrechnung Verkehrsdaten in der Regel nicht länger als 80 Tage gespeichert. Bei Diensten mit einer Flatrate wie dem Zugang zum Internet hat der Bundesgerichtshof jüngst bestätigt, dass die Verkehrsdaten **nach der Verbindung unmittelbar gelöscht** werden müssen, es sei denn, sie sind für Zwecke der Abrechnung erforderlich. In dem Einzelfall eines Gerichtsverfahrens wurde die Speicherfrist zu Abrechnungszwecken sogar auf nur acht Wochen beschränkt.

Die Vorratsspeicherung ist **völlig unverhältnismäßig**. Das Bundesverfassungsgericht hat Anfang 2006 in seiner Entscheidung zur Rasterfahndung das Verbot einer Speicherung auf Vorrat unterstrichen. Zur Verdeutlichung: Es handelt sich um mehrere Milliarden Datensätze pro Jahr, wer wann mit wem von wo wie lange und mit welchem Datenvolumen telekommuniziert hat, die ohne jeden konkreten Grund verdachtslos gespeichert werden sollen. Nach einer Zusammenstellung des Branchenverbandes BITKOM wären dies allein bei einem größeren Internetprovider eine Datenmenge von bis zu 40.000 Terabyte pro Jahr.

Die Verpflichtung zur Speicherung auf Vorrat wird mit den **Informationsbedürfnissen der Sicherheitsbehörden** begründet. Allerdings zeigen Erfahrungen aus anderen europäischen Staaten, dass sich die weit überwiegende Anzahl derartiger Auskunftsersuchen auf einen Zeitraum von nur drei Monaten beschränkt. Auch eine Zusammenstellung des Bundeskriminalamtes macht deutlich, dass die Kassandrarufe der Innenpolitiker übertrieben sind: Über einen Zeitraum von neun Monaten konnten von den TK-Anbietern nur zwei Auskunftsersuchen mit dem Hintergrund Terrorismus bzw. organisierte Kriminalität wegen der Löschung dieser Daten nicht beantwortet werden. Ermittlungsbehörden verfügen in der Regel über mehrere Ermittlungsansätze und sind nicht nur auf die Daten aus der Telekommunikation angewiesen.

Es steht außerdem zu befürchten, dass die Vorratsdaten massenhaft von den Inhabern digitaler Verwertungsrechte genutzt werden, um ihre **zivilrechtlichen Auskunftsansprüche** über möglicherweise bestehende Urheberrechtsverletzungen mithilfe der TK-Wirtschaft zu verfolgen. Dies wäre eine völlig andere Qualität, weil dann alle Teilnehmer an der Telekommunikation ohne einen konkreten Anlass eine staatliche Zwangsspeicherung hinnehmen müssten, die ausschließlich privatnützig ist. Auch dies wäre eindeutig verfassungswidrig.

Gravierende Bedenken gegen die Vorratsdatenspeicherung bestehen zudem mit Blick auf den **Schutz besonderer Vertrauensverhältnisse**. Dazu zählt der Schutz des Patientengeheimnisses, des Beichtgeheimnisses, des Mandantengeheimnisses oder die Kommunikation zwischen Journalisten und Informanten. Bedroht ist weiterhin die **Unabhängigkeit des Abgeordnetenmandates** und dessen Kontrollfunktion gegenüber der Regierung, weil die Vorratsdatenspeicherung auch die Kommunikation mit den Bürgerinnen und Bürgern erfasst. Der Wissenschaftliche Dienst des Landtags teilt die Einschätzung des ULD und hat seine verfassungsrechtlichen Bedenken in einem gesonderten Gutachten dem Landtag näher dargelegt (Landtagsumdruck 16/620). Der Gesetzentwurf aus der Bundesregierung berücksichtigt diese Einwände nicht.

Das ULD hat seine verfassungsrechtlichen Bedenken gegenüber dem Landtag in einer Stellungnahme im Oktober 2006 dargelegt (Landtagsumdruck 16/1267):

www.lvn.ltsh.de/infothek/wahl16/umdrucke/1200/umdruck-16-1267.pdf
www.datenschutzzentrum.de/rotekarte/initiativen.htm

Was ist zu tun?
Die Vorratsdatenspeicherung darf nicht realisiert werden.

7.2 Telemediengesetz: Notwendige Vereinheitlichung bringt Verschlechterungen

Der Bundestag hat ein Telemediengesetz verabschiedet, das die Datenschutzregelungen des Teledienstedatenschutzgesetzes und des Mediendienste-Staatsvertrages ablöst. Die im Grunde zu begrüßende Neuregelung enthält aus Datenschutzsicht jedoch substanzielle Verschlechterungen.

Die Wirksamkeit des Datenschutzes erhöht sich, wenn seine Regelungen einfach und verständlich sind. Je komplizierter die Regelungen, desto geringer ist die Wahrscheinlichkeit, dass sie von den Adressaten umgesetzt werden. Das **Datenschutzrecht** soll **möglichst einfach** sein. Daher ist der Gesetzgeber mit dem Telemediengesetz (TMG), in dem das bisherige Teledienstedatenschutzgesetz (TDDSG) sowie der Mediendienste-Staatsvertrag (MDStV) zusammengeführt werden, grundsätzlich auf dem richtigen Weg. Dessen Regelungen sollen zudem für Rundfunkdienste gelten; der Rundfunkstaatsvertrag in der Fassung des 9. Rundfunkänderungsstaatsvertrages wird für den Datenschutz auf die Regelungen im Telemediengesetz verweisen.

Allerdings halten sich die Gewinne dieser Vereinheitlichung in Grenzen; die Datenschutzregelungen waren schon immer weitgehend gleichlautend. Einen wirklichen Schritt zur Vereinheitlichung hätte der Gesetzgeber erreicht, wenn er die längst fällige Integration der Datenschutzregelungen für die Diensteanbieter von **Telemedien und Telekommunikation** in Angriff genommen hätte (26. TB, Tz. 7.1). Die Abgrenzung zwischen Telemedien und Telekommunikation wirft alte und neue schwierige Auslegungsfragen auf.

? Telemedien

Telemedien *sind alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes (TKG), die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 TKG oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind (§ 1 Abs. 1 TMG).*

Zu kritisieren ist die Einschränkung des datenschutzrechtlichen Auskunftsanspruchs der Betroffenen sowie die Ausweitung der Auskunftspflichten der Anbieter von Telemediendiensten gegenüber den **Sicherheitsbehörden**. Verfassungsrechtlich unzulässig ist die Ausweitung der Auskünfte über Bestands- und Abrechnungsdaten „zur **Durchsetzung der Rechte am geistigen Eigentum**“. Damit hebt der Gesetzgeber das Interesse einzelner Wirtschaftsunternehmen auf eine Stufe mit den im Gemeinwohlinteresse erfolgenden Eingriffen durch die Sicherheitsbehörden. Diese Regelung macht die Anbieter von Telemedien – auch nach deren eigener Einschätzung – zu „Hilfssheriffs für jedermann“. Zum Entwurf des Telemediengesetzes hat das ULD im Rahmen einer Anhörung des Wirtschaftsausschusses des Deutschen Bundestags Ende 2006 Stellung genommen.

www.datenschutzzentrum.de/allgemein/061211-tmg.htm

Was ist zu tun?
Der Gesetzgeber sollte die Auskunftspflichten der Diensteanbieter gegenüber den Sicherheitsbehörden begrenzen und gegenüber den Inhabern von Verwertungsrechten zurücknehmen.

7.3 Private Nutzung dienstlicher E-Mail-Accounts

Betriebs- oder Dienstvereinbarungen zur Nutzung von Internet und E-Mail sind im Interesse der betroffenen Beschäftigten und des Arbeitgebers dringend notwendig. Die private Nutzung dienstlicher E-Mail-Accounts sollte zur Vermeidung von Rechtsverstößen ausgeschlossen sein.

Unsere Empfehlung ist eindeutig: Alle Beteiligten haben ein Interesse daran, dass eine private Nutzung dienstlicher E-Mail-Accounts ausgeschlossen wird (27. TB, Tz. 7.1). Greift ein Arbeitgeber auf den dienstlichen E-Mail-Account aus betrieblichen oder dienstlichen Gründen zu, weil der Arbeitnehmer seine E-Mails z. B. wegen Krankheit oder aus Vergesslichkeit nicht an seinen Vertreter umgeleitet

hat, dann verletzt er mit der Kenntnisnahme der privaten E-Mails das **Fernmeldegeheimnis der externen Kommunikationspartner** des Beschäftigten. Häufig wird übersehen, dass das Fernmeldegeheimnis die private Kommunikation von beiden Kommunikationspartnern schützt. Das Fernmeldegeheimnis der externen Kommunikationspartner steht nicht zur Disposition des Beschäftigten und schon gar nicht des Arbeitgebers. Es kann also nicht über eine Dienst- oder Betriebsvereinbarung aufgehoben werden. Übrigens: Die Verletzung des Fernmeldegeheimnisses ist ein Straftatbestand, den nicht nur die Verantwortlichen des Unternehmens, sondern auch die Beschäftigten – wie z. B. die Administratoren – im Fall eines rechtswidrigen Zugriffes begehen würden.

Welche praktischen Probleme die Zulassung der privaten Kommunikation über den dienstlichen E-Mail-Account aufwerfen kann, zeigt der Fall der **sofortigen Beurlaubung eines Mitarbeiters**. Wegen der ausdrücklichen Zulassung privater E-Mail-Kommunikation hätte ein vom Arbeitgeber veranlasster Zugriff auf den dienstlichen E-Mail-Account dazu geführt, dass das Fernmeldegeheimnis der Kommunikationspartner des Beschäftigten verletzt wird. Eine Lösung war möglich, aber aufwendig: Zunächst wurde eingestellt, dass alle Absender neuer E-Mails automatisch darauf hingewiesen wurden, dass der Empfänger-Account deaktiviert ist, die Organisation aber über eine bestimmte E-Mail-Adresse erreichbar ist. Um die bereits eingegangene dienstliche E-Mail-Kommunikation lesen und bearbeiten zu können, haben wir empfohlen, den beurlaubten Mitarbeiter im Rahmen seiner arbeitsrechtlichen Pflichten anzuweisen, sich zu einer bestimmten Zeit im Betrieb einzufinden und seine privaten E-Mails zu löschen.

Einfacher wäre es gewesen, derartige kritische Sachverhalte von Anfang an im Sinne unserer Empfehlung datenschutzkonform in einer Betriebs- oder Dienstvereinbarung zu regeln. Vergessen wird häufig, dass für leitende Angestellte – wie z. B. Geschäftsführer – die betrieblichen Regelungen nicht unmittelbar gelten. Ihre analoge Anwendung sollte im Arbeitsvertrag ausdrücklich aufgenommen werden.

Wenn private Kommunikation über E-Mail während der Arbeitszeit zulässig sein soll, empfehlen wir, den lesenden und schreibenden Zugriff auf einen ausschließlich **privaten E-Mail-Account**

Im Wortlaut:
Auszug aus der 59er-Dienstvereinbarung Internet und E-Mail

3.3. Die Nutzung von E-Mail ist ausschließlich für dienstliche Zwecke zulässig.

3.4 Für private Zwecke ist den Beschäftigten die unentgeltliche Nutzung des dienstlichen Internetzugangs ausschließlich zum Nutzen von Webseiten (Dienste http/https) gestattet, soweit dienstliche Interessen nicht entgegenstehen.

(Amtsblatt Schl.-H. 2005, S. 27)

über Webmail zu erlauben. Aus Sicherheitsgründen sollte der Down- oder Upload von Dateien über Webmail aber ausgeschlossen sein. Eine geeignete Regelung enthält die 59er-Vereinbarung über die Nutzung von Internet und E-Mail, die zwischen Land und Gewerkschaften unter unserer beratenden Mitwirkung abgeschlossen worden ist (Amtsblatt Schl.-H. 2005, S. 27; 27. TB, Tz. 7.1). Die dort vereinbarte Evaluierung der Regelung soll im Jahr 2007 durchgeführt werden.

Was ist zu tun?
Die private Nutzung von E-Mail über den dienstlichen Account sollte ausgeschlossen werden. Private E-Mail am Arbeitsplatz kann über die Nutzung privater E-Mail-Accounts über Webmail zugelassen werden.

7.4 Gebührenbefreiung durch Bescheinigung statt Bescheid

Nach geltendem Recht muss der Antragsteller zur Befreiung von der Rundfunkgebühr die Voraussetzungen seiner Befreiung durch Vorlage des Originalbescheides oder in beglaubigter Kopie nachweisen. Nach Gesprächen zwischen den Rundfunkreferenten der Länder soll auch eine datensparsamere Bescheinigung ausreichen.

Der Zustand ist zum Glück nur vorübergehend: Um von der Rundfunkgebühr befreit zu werden, müssen die Antragsteller die Kosten für die Beglaubigung ihrer Leistungsbescheide tragen; bei der Gebühreneinzugszentrale (GEZ) in Köln sammeln sich ohne Not Millionen Befreiungsbescheide. Einfacher und billiger ist die Vorlage einer schlichten **Bescheinigung** über die Erfüllung der Befreiungsvoraussetzung (28. TB, Tz. 7.3). Auf die Rückkehr zu dieser früheren Praxis haben sich die Rundfunkreferenten und die Datenschützer geeinigt. Dies soll durch eine Änderung des Runfunkgebührenstaatsvertrags umgesetzt werden, leider erst im Rahmen des 10. Rundfunkänderungsstaatsvertrags, der noch in Vorbereitung ist.

Eine Besserung ist schon heute in Sicht, wenn die Bescheinigungslösung in die Software implementiert ist, die von den Behörden zur Unterstützung ihrer Arbeit eingesetzt wird. Werden die Bescheinigungen zur Vorlage bei der GEZ erst einmal standardmäßig mit dem jeweiligen Leistungsbescheid ausgedruckt, dann hält sich der Verwaltungsaufwand in engen Grenzen: Die Hersteller von derartigen Softwareprogrammen haben standardmäßige Implementierungen entweder schon umgesetzt oder diese zumindest in der Planung. Die GEZ akzeptiert im Vorgriff auf die kommende Regelung schon heute als Nachweis der Voraussetzungen zur Gebührenbefreiung die sogenannte „Bescheinigung zur Vorlage bei der Behörde“.


www.gez.de/door/gebuehren/gebuehrenbefreiung/

Was ist zu tun?
Der 10. Rundfunkänderungsstaatsvertrag ist zügig zu verabschieden. Die Bescheinigungslösung durch Implementierung entsprechender Software sollte umgehend umgesetzt werden.

7.5 Adresshandel der GEZ: Ein unbefriedigender Kompromiss

Der Gesetzgeber hat zugelassen, dass sich die Rundfunkanstalten bzw. die von ihr beauftragte Gebühreneinzugszentrale (GEZ) Adressdaten zur Gebührenerhebung über den Adresshandel beschaffen. Eine Neuregelung soll den Betroffenen ein Widerspruchsrecht einräumen.

Die Beschaffung von Adressdaten auf dem freien Markt durch die GEZ stieß auf den Widerstand der Datenschützer: Wie kann es sein, dass die Rundfunkanstalten als Körperschaften des öffentlichen Rechts, die einen privilegierten Zugriff auf Adressdaten aus dem Melderegister haben, gleichzeitig wie ein privater **Nachfrager** auf dem Marktplatz der Adressdaten agieren (27. TB, Tz. 7.6)?

Wie berechtigt unsere Kritik ist, zeigt der Fall betagter Großeltern, deren engagierter Enkel sich schließlich der Sache annahm: Obwohl die Großeltern seit Jahrzehnten **rechtstreu und pünktlich** ihre Rundfunkgebühren bezahlen, erhielten sie immer wieder Post von der GEZ, die sie nachdrücklich bis zur Androhung von Zwangsmaßnahmen an ihre Verpflichtung zur Zahlung der fälligen Rundfunkgebühr erinnerte. Wiederholte Hinweise auf die pünktliche Begleichung der Gebührenschuld fruchteten nicht. Eine Intervention des Datenschutzbeauftragten des NDR klärte schließlich, dass die GEZ die Anschrift der Großeltern aus einem gekauften Adressdatenbestand bekommen hatte, in dem eine Betriebsstätte geführt wurde, die der Großvater vor Jahrzehnten innehatte.

Die wiederholten Anschreiben kamen zustande, weil die GEZ erstens einen **„schmutzigen" Adressdatenbestand** angemietet hatte, der um die längst geschlossene Betriebsstätte nicht bereinigt war, und zweitens diesen Adressdatenbestand nicht mit ihrem eigenen Bestand abgeglichen hatte. Wir empfahlen den Betroffenen, bei dem Adresshändler Widerspruch gegen die Verwendung der Adressdaten einzulegen. Man sieht, wozu die Regelung führt: Die Rundfunkanstalt kauft mit Gebührengeldern „schmutzige" Adressen, und die Betroffenen müssen dafür sorgen, dass sie bereinigt werden. Dass die GEZ im Übrigen auf die Hinweise der Betroffenen nicht umgehend selbst reagiert hatte, gehört zu den Merkwürdigkeiten des Gebühreneinzugsverfahrens.

Die Verhandlungen zwischen Rundfunkreferenten und Datenschützern zur Frage des Adresshandels haben diese Grundsatzfrage nicht wirklich befriedigend lösen können. Mit dem **10. Rundfunkänderungsstaatsvertrag** soll eine Regelung verabschiedet werden, die den Betroffenen ein Widerspruchsrecht einräumt und die Dauer der Datenspeicherung begrenzt.

Was ist zu tun?
Die Regelung über den Adressenkauf der Rundfunkanstalten sollte so bald wie möglich außer Kraft gesetzt werden. Die Finanzierung des öffentlich-rechtlichen Rundfunks ist auf ein datensparsames Verfahren umzustellen.

8 Modellprojekte und Studien

Seit Jahren nutzt das ULD die über Modellprojekte und Studien zusätzlich eingeworbenen Ressourcen, um seine Präventionskonzeption mit Leben zu füllen (Tz. 1.1). Damit können neue technische Herausforderungen frühzeitig erkannt und mit der Brille und den Werkzeugen des Datenschützers analysiert und gestaltet werden. Das Ergebnis sind datenschutzgerechte Standards, Vorgehensweisen, Verfahren und Produkte. Das daraus erlangte Wissen kann weitergegeben und praktisch erprobt werden. Es ist die Grundlage unserer Öffentlichkeitsarbeit und unserer Tätigkeit in den Bereichen Ausbildung, Beratung und Prüfung. Bei jedem der vom ULD durchgeführten Projekte finden nationale, oft auch internationale Kooperationen statt. Einbezogen sind nicht nur Technik und Recht, sondern die Gesellschaft im weitesten Sinn: Partner sind Universitäten, auch aus dem sozialwissenschaftlichen Bereich, ebenso wie Unternehmen, Behörden, Verbraucher- und Bürgerrechtsorganisationen. Letztendlich zielen die Projekte und Studien darauf ab, für die Idee des **Datenschutzes als Grundrechtsschutz** zu werben und für dessen gesellschaftliche Realisierung die Basis zu schaffen.

8.1 Mit bdc\Audit ohne Umwege zur datenschutzgerechten Biobankforschung

Die Entwicklung von Methoden und Kriterien für die Erstellung und Überprüfung – Auditierung – von Datenschutzmanagementsystemen in der Biobankforschung ist das Ziel des Projekts bdc\Audit. Es wird durch einen Forschungsverbund durchgeführt.

An dem vom Bundesforschungsministerium geförderten Projekt sind neben dem ULD die Universitäten Hamburg (Prof. Dr. Kollek) und Kiel (Prof. Dr. Luttenberger) beteiligt. Als **Biobank** bezeichnet man eine Sammlung von menschlichen Körperproben, z. B. Blut oder Gewebe, oder der daraus extrahierten Materialien, vor allem DNA. Dieses Material wird zumeist mit soziodemografischen und medizinischen Daten der Spender aufbewahrt. Biobanken gibt es vor allem in Universitätskliniken und bei der forschenden Industrie. Proben und Daten stammen teilweise von Patientinnen und Patienten, teilweise auch von gesunden Menschen, die sich an Forschungsprojekten beteiligen.

Biobanken werden in der Forschung verwendet, um Zusammenhänge zwischen bestimmten genetischen Ausprägungen und dem Vorkommen und dem Verlauf von Krankheiten zu erkunden. Wirkungen und Nebenwirkungen von Medikamenten werden mit ihrer Hilfe in **Beziehung zur genetischen Disposition** gesetzt. Die Erkenntnisse sollen für die Prävention und Heilung von Krankheiten nutzbar gemacht werden.

Vielen dieser Projekte ist eigen, dass derselbe Probengeber zum Teil über viele Jahre hinweg immer wieder zu weiteren medizinischen Untersuchungen gebeten werden muss, um den Verlauf einer Krankheit zu beobachten. Deshalb kann man die früheren Proben und die zugeordneten Daten nicht einfach anonymisieren, sondern muss eine **Möglichkeit der erneuten Zuordnung** vorsehen. Hierbei gilt

es, eine Vielzahl von datenschutzrechtlichen Problemen zu lösen. Vor allem muss das Zusammenspiel der verschiedenen Einrichtungen, die an der Materialgewinnung, der Biobankverwaltung und schließlich der Weitergabe an wechselnde Forschungsprojekte beteiligt sind, effizient und datenschutzgerecht gestaltet werden.

Das Projekt bdc\Audit zielt darauf ab, Methoden und Kriterien zu entwickeln, mit denen die unterschiedlichen bei den Biobanken im Einsatz befindlichen **Datenschutzmanagementsysteme** im Hinblick darauf überprüft werden können, ob sie den datenschutzfachlichen Vorgaben entsprechen. Dabei soll durch einen modularen Aufbau eine große Offenheit für eine Vielzahl unterschiedlicher Organisationsschemata zur Verfügung gestellt werden. Mit der Durchführung eines Audits nach diesen Kriterien können die Betreiber der Biobank nach außen dokumentieren, dass sie rechtskonform mit den Gesundheitsdaten der Probengeber umgehen und diese nicht gefährdet sind. Dies erleichtert es Menschen, sich durch Hergabe einer Probe an der Förderung des medizinischen Fortschritts zu beteiligen. Das Projekt ist im Internet dargestellt unter


www.bdc-audit.de

8.2 AN.ON – ein erfolgreiches Projekt geht (nicht) zu Ende

Das vom Bundesministerium für Wirtschaft und Technologie geförderte Projekt „AN.ON – Anonymität online“, ein Anonymisierungsservice für das World Wide Web, wurde erfolgreich abgeschlossen. Es wird nun ohne Förderung weiterbetrieben.

Seit Anfang 2001 wurde AN.ON vom ULD gemeinsam mit der Technischen Universität Dresden und der Universität Regensburg entwickelt und betrieben (28. TB, Tz. 8.4; 27. TB, Tz. 8.3). Ende November 2006 fand in Berlin im Bundeswirtschaftsministerium im Beisein von Vertreterinnen und Vertretern aus Politik, Behörden und Wirtschaft sowie von der Presse die **Abschlussveranstaltung** statt. Die Kommentare aus dem Verbraucherzentrale Bundesverband, dem Bundeskriminalamt, der Deutschen Telekom und vom eco-Verband der deutschen Internetwirtschaft sowie der sonstigen Teilnehmenden bestätigten, ohne kritische Aspekte auszulassen, die Notwendigkeit, das Internet frei und anonym nutzen zu können.

Die offizielle Förderung ist zu Ende. Deren Ziel war es, hieraus Geschäftsmodelle entstehen zu lassen, die keiner öffentlichen Förderung bedürfen. Unabhängig davon besteht der Bedarf an einer Grundversorgung. Neben dem Aufbau eines kommerziellen Dienstes erfolgt daher weiterhin die Bereitstellung eines **kostenlosen Grunddienstes**, der zwar gegebenenfalls eine geringere Geschwindigkeit bietet, aber jeder Bürgerin und jedem Bürger sofort zur Umsetzung des Rechts auf Anonymität beim Surfen im Internet zur Verfügung steht.

Kurz vor Projektabschluss gab es noch einige arbeitsame und aufregende Monate für die Projektpartner. Zum einen wurde eine **verbesserte Version** der Software, die die Nutzenden noch leichter installieren können, entwickelt.

Zum anderen wurde im September 2006 einer der AN.ON-Server von der Polizei aufgrund eines Beschlusses des Amtsgerichts Konstanz beschlagnahmt. Die beim Provider in Karlsruhe durchgeführte **Beschlagnahme** wurde dem ULD als verantwortlichem Betreiber erst nach eigenen aufwendigen Recherchen einige Tage später mitgeteilt; den Beschlagnahmebeschluss zu erhalten, bedurfte weiterer Nachfragen. Die Beschlagnahme stand offenbar im Zusammenhang mit weiteren Beschlagnahmen bei Betreibern von Anonymisierungsdiensten mit dem Ziel, Nutzer von Kinderpornografie im Internet ausfindig zu machen.

Mit dieser Beschlagnahme wurde von den Strafverfolgern ein **ungeeigneter Weg** gewählt: Bei einem konkreten Anfangsverdacht und Vorliegen eines richterlichen Beschlusses ist es bei AN.ON nämlich möglich, bestimmte Webanfragen – also etwa den Abruf und das Verbreiten von Kinderpornografie – zurückzuverfolgen. Diese Möglichkeit wurde durch die Beschlagnahme verbaut; die Täter waren gewarnt. Die beschlagnahmte Festplatte enthält keine für die Ermittlung der Täter nützlichen Daten, da mit AN.ON ohne vorherige richterliche Anordnung keinerlei Verbindungsdaten gespeichert werden. Wir haben daher gegen den Beschluss des Amtsgerichts Konstanz Beschwerde eingelegt. Eine Entscheidung darüber wurde dem ULD bis zum Redaktionsschluss nicht mitgeteilt. Mit einem Ersatzsystem konnten wir den Dienst zügig wieder aufnehmen.

Vielleicht auch wegen der eingebauten Möglichkeit der Mitprotokollierung von konkreten Einzelfällen nach richterlicher Anordnung scheint AN.ON eine **niedrige Missbrauchsrate** aufzuweisen: Im Jahr 2006 gingen bei den Projektpartnern 44 Anfragen von Strafverfolgungsbehörden ein. Die Zahl der Nutzer im Monat bewegt sich geschätzt zwischen 50.000 und 100.000; ständig ist eine vierstellige Anzahl online.

Für die Politik war und ist AN.ON ebenfalls ein Thema. Auf Anregung des Generalstaatsanwalts forderte der Justizminister des Landes das ULD über die Presse auf, **AN.ON vom Netz zu nehmen**. Hierbei bestanden offensichtlich völlig falsche Vorstellungen von den rechtlichen und technischen Möglichkeiten der Gefahrenabwehr und der Strafverfolgung. Bei einem Treffen unter Einbeziehung des Innenministers des Landes konnten wir diese Möglichkeiten und die Hintergründe des Dienstes sowie die Kooperationsangebote von AN.ON bei der Strafverfolgung in Missbrauchsfällen erläutern und Vorur-

? ***„quick freeze“***

Im Gegensatz zu einer Vorratsdatenspeicherung, die sämtliche Verkehrsdaten der Telekommunikation erfasst, können Strafverfolgungsbehörden bei „quick freeze“ in Verdachtsfällen kurzfristig eine Speicheranordnung gegenüber den Providern erlassen und realisieren. Die routinemäßig erfolgende Löschung der Verkehrsdaten unterbleibt ab sofort. Sobald ein entsprechender richterlicher Beschluss vorgelegt wird, werden diese Daten vom Provider an die Behörde herausgegeben.

teile ausräumen. Wir boten allen Gesprächspartnern an, im Interesse eines angemessenen Ausgleichs zwischen Sicherheits- und Datenschutzbelangen im Gespräch zu bleiben und beratend zur Seite zu stehen.

In diesem Kontext wird zu erörtern sein, wie die Umsetzung der europäischen **Richtlinie zur Vorratsdatenspeicherung** (Tz. 7.1) Anonymisierungsdienste im Internet allgemein und den AN.ON-Dienst konkret betreffen wird. Als Ergebnis darf keine Massenüberwachung der Bürgerinnen und Bürger entstehen. Vielmehr favorisieren wir weiterhin Techniken wie „quick freeze“ (27. TB, Tz. 4.2.3).

Weitere Informationen zum Projekt befinden sich im Internet unter

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

Was ist zu tun?
Der Bürger ist bei der effektiven Wahrnehmung seines gesetzlich garantierten Rechts auf Anonymität im Web weiterhin zu unterstützen. Im Dialog mit Strafverfolgungsbehörden muss die Arbeit an Lösungen fortgesetzt werden, die eine effektive Ermittlung von Missbrauchsfällen ohne gleichzeitigen Eingriff in die Rechte Unbeteiligter ermöglichen.

8.3 ULD-i – das Innovationszentrum Datenschutz und Datensicherheit hat sich bewährt

Das Innovationszentrum Datenschutz & Datensicherheit (ULD-i) berät kleinere und mittlere Unternehmen, wie Datenschutz und Datensicherheit in Produkte integriert werden können. Ziel ist es, die Wirtschaft mit attraktiven Serviceleistungen zu stärken.

In den letzten zweieinhalb Jahren hat sich das ULD-i zu einem wichtigen **Ansprechpartner** für Wirtschaft und Wissenschaft entwickelt, wenn es darum geht, Datenschutz und Datensicherheit in Produkte, Projekte und Prozesse zu integrieren. Als Motivationsförderer für Datenschutz auf hohem Niveau winken **Marktvorteile** für die Unternehmen.

ULD-i >>
Datenschutz innovativ

Das ULD-i versteht sich auch als **Wegweiser** im Dschungel von rechtlichen und organisatorischen Zuständigkeiten, die bei Förderprogrammen eine Rolle spielen. Im Bereich Datenschutz und Datensicherheit werden zunehmend Gelder für innovative Ideen ausgeschüttet. Viele Förderer haben zudem erkannt, dass Projekte, die ohne Datenschutz und Datensicherheit auszukommen glauben, häufig Probleme mit Rechtskonformität und Akzeptanz der Benutzer aufweisen und damit

an diesen Marktbarrieren scheitern. Im schleswig-holsteinischen Förderprogramm e-Region PLUS hat man daher darauf gedrängt, dass sich die Projekte von uns beraten lassen.

Auch ohne den Druck von Förderprogrammen ist bisher eine ganze Reihe von Projekten auf das ULD-i zugekommen und hat sich beraten lassen, wie Datenschutz und Datensicherheit sinnvoll integriert werden können. Ein Teil dieser Projekte hat sich für eine **intensive datenschutzrechtliche und datensicherheitstechnische Begleitung** entschieden.

Das ULD-i wird durch eine Kofinanzierung der Europäischen Union unterstützt. Die Koordination erfolgte durch das Wirtschaftsministerium des Landes über das Regionalprogramm 2000 im Rahmen der Förderung der Technologieregion K.E.R.N.

Was kann das ULD-i für Sie tun?
Nehmen Sie Kontakt mit uns auf:
ULD-i
Holstenstraße 98, 24103 Kiel
Tel.: 0431/988-1399
kontakt@uld-i.de
www.uld-i.de

8.4 PRIME – Identitätsmanagement für den Nutzer immer beliebter

In der Online-Welt muss jeder eine Vielzahl von Benutzerkonten und Datensätzen verwalten. Identitätsmanagementsysteme können dabei helfen. Nutzerzentrierte Ansätze, wie sie beim EU-Projekt „PRIME – Privacy and Identity Management for Europe“ im Vordergrund stehen, setzen sich nun auch in aktuellen kommerziellen und kostenlosen Tools durch.

Als im März 2004 das Projekt PRIME (28. TB, Tz. 8.2.1; 27. TB, Tz. 8.2.1) begann, war noch nicht absehbar, dass sich im Identitätsmanagement ein Trend **weg von zentralisierten Systemen** ohne richtige Kontrolle durch Nutzer und hin zu sogenannten föderierten Lösungen, die Nutzenden mehr Steuermöglichkeiten bieten, herausbilden würde. Wir haben zusammen mit den anderen Partnern aus Wirtschaft und Wissenschaft im Jahr 2006 die Vertreter solch anderer Projekte und Produktentwicklungen eingeladen, gemeinsam an offenen Standards zu arbeiten, und verfolgen die Aktivitäten beispielsweise bei den Normungsgruppierungen ISO oder W3C.

Trotz vieler Gemeinsamkeiten in Grobkonzepten grenzt sich PRIME mit dem Prinzip, das **Maximum an Datenschutz** beim Design und bei der Implementierung anzustreben, von anderen Ansätzen ab. Beispielsweise ermöglicht das Konzept von PRIME die Kombination von anonymem Auftreten und Zurechenbarkeit von Nutzern, wofür Techniken wie Pseudonyme, anonyme Credentials und Anonymisierungstechniken für die Kommunikation zum Einsatz kommen. Auch

auf Serverseite werden neue Wege beschritten, z. B. mit Datenschutzmanagementlösungen zum automatisierten Durchsetzen der Vereinbarungen aus der jeweiligen Privacy Policy.

Das ULD nimmt vielfältige Aufgaben im Projekt wahr: Wir kümmern uns um die rechtliche Evaluation der implementierten Prototypen (z. B. Internetbrowsing, Nutzung von ortsbezogenen Diensten in der Mobilkommunikation, Systeme für kollaboratives Arbeiten) und entwickeln Kriterien für vertrauenswürdige Systemgestaltung. Da wir die **Nutzer in den Mittelpunkt** unserer Betrachtung stellen, liegen uns ihre Rechte besonders am Herzen. Zusammen mit anderen Projektpartnern arbeiten wir mit an Funktionen und Nutzungsoberflächen, die die Nutzer in ihrer informationellen Selbstbestimmung stärken und es ihnen erleichern, ihre Rechte wahrzunehmen, z. B. für Auskunft, Korrektur oder auch Löschung ihrer personenbezogenen Daten.

Besonders empfehlenswert sind die PRIME-**Tutorials** zu Datenschutz und Identitätsmanagement für jedermann, die über die PRIME-Website http://www.prime-project.eu auf Deutsch, Englisch und in mehreren anderen EU-Sprachen verfügbar sind. Mit interaktiven Komponenten lässt sich spielerisch das Verständnis vertiefen – die Tutorials sind auch für Schulen und Universitäten geeignet. Ein Film im Cartoon-Stil macht einem bewusst, wo man überall Datenspuren hinterlässt. Unsere Madrider Kollegen (Agencia de Protección de Datos – Comunidad de Madrid) haben Tutorial und Film ins Spanische übersetzt und nutzen beides für ihre Zwecke.

Das PRIME-Projekt wird bis März 2008 von der Europäischen Kommission im 6. Forschungsrahmenprogramm gefördert. Im letzten Projektjahr werden wir immer mehr Resultate fertigstellen und für Interessierte auf unserer **Projekt-Website** anbieten:

www.prime-project.eu

Was ist zu tun?
Die Entwickler von Identitätsmanagementsystemen sollten bereits beim Systemdesign darauf achten, dass Nutzer ihre Rechte wahrnehmen können; geeignete Systeme sind auszuwählen, die Nutzer sind über ihre Möglichkeiten zu informieren. Die Risiken durch Datenspuren und die möglichen Schutzmaßnahmen sollten in Schulen und anderen Ausbildungsstätten verstärkt vermittelt werden.

8.5 FIDIS – eIDs bestimmen unsere Zukunft

Das von der Europäischen Union geförderte Exzellenznetzwerk FIDIS hat zum Thema „Identität" wichtige Ergebnisse zu elektronischen Identitätsdokumenten, zur RFID-Technik (Radio Frequency Identification) sowie zum Datenschutzmanagement vorgelegt.

Im Projekt „FIDIS – Future of Identity in the Information Society" arbeiten wir mit weiteren 23 Partnern aus 12 Ländern zusammen in einem sogenannten „**Network of Excellence**" (28. TB, Tz. 8.2.2). Ergebnisse des Projektes sind europäische Studien, Berichte und Artikel zu verschiedenen Aspekten von Identität, Identifizierung und Identitätsmanagement, die unter http://www.fidis.net, in Zeitschriften oder über sonstige Medien publiziert werden. Das ULD vertritt dabei aus unterschiedlichen fachlichen Perspektiven grundsätzliche und angewandte Aspekte des Datenschutzes.

Die Arbeit im Projekt ist in Arbeitspaketen organisiert. In zehn dieser Arbeitspakete sind wir aktiv eingebunden, in weiteren übernehmen wir „Reviews" zur Qualitätssicherung. Das Arbeitspaket, das sich mit **Techniken zum Identitätsmanagement und zur Identifizierung** auseinandersetzt, wird von uns koordiniert. Im Jahr 2006 standen im Mittelpunkt unserer Arbeit:

- **Elektronische Identitätsdokumente (eIDs)**: Die eIDs, z. B. der biometrische Reisepass, die kommende Gesundheitskarte und der zukünftige digitale Personalausweis werden in immer mehr Lebensbereichen eingeführt. Leider ist damit nicht unbedingt ein Gewinn an Sicherheit für den Bürger verbunden. In unserer Analyse zum **Reisepass** mussten wir **deutliche Sicherheitsmängel** feststellen, die es z. B. ermöglichen, einzelne Bürger auf ihrer Reise zu verfolgen und teilweise sogar die im Pass gespeicherten Daten unbefugt und ohne Wissen des Betroffenen auszulesen. Wir haben dies in der „Budapest-Erklärung" und einer Studie zu eIDs publik gemacht. Darin fordern wir, dass möglichst schnell ein umfassendes Sicherheitskonzept für den europäischen Pass erstellt und über die technische Gestaltung mit biometrischen Daten und RFID-Technik nachgedacht wird, die in der jetzigen Form auf keinen Fall als ausgereift angesehen werden kann.
- **RFID, Profiling und Ubiquitous Computing**: Zu diesem Themenfeld hat das FIDIS-Netzwerk zwei Studien sowie ein Positionspapier veröffentlicht und die Ergebnisse in den Konsultationsprozess der EU-Kommission zu RFID eingebracht. Hierin werden die kritischen Aspekte der derzeit vor allem in den Bereichen Logistik und Vertrieb eingesetzten RFID-Technologie zusammengefasst und Akteuren in Politik, Wirtschaft und Wissenschaft konkrete Maßnahmenvorschläge gemacht, insbesondere zur Stärkung der **Transparenz für den Nutzer**. Eine Zusammenarbeit gab es in diesem Kontext mit dem Projekt TAUCIS (Tz. 8.11).
- **Datenschutzmanagement**: Dass funktionsfähige Prozesse zur dauerhaften Einhaltung der Datenschutzregelungen in Wirtschaft und Verwaltung international wichtig sind, hat nicht nur die Sommerakademie 2006 gezeigt. Wir

haben einen Musterprozess für Datenschutzmanagement entwickelt, der in das Datenschutzkapitel der IT-Grundschutzkataloge übernommen werden soll. Diese vom Bundesamt für Sicherheit in der Informationstechnik herausgegebenen Kataloge sind ein Standardwerk für die Auswahl und Implementierung von Sicherheitsmaßnahmen für Verwaltung und Wirtschaft in Deutschland (Tz. 6.2).

www.fidis.net/

Was ist zu tun?
Bei der Gestaltung von eID-Systemen müssen Regierungen und Standardisierungsgremien Datenschutz- und Datensicherheitsaspekte von Anfang an einbeziehen. Risiken müssen benannt und Sicherungsmaßnahmen implementiert werden. Beim biometrischen Reisepass können Bürgerinnen und Bürger mit einer Schutzhülle, die den RFID-Chip im Pass abschirmt, unbemerktes Auslesen verhindern.

8.6 PRISE – Schutz der Privatsphäre bei Sicherheitstechnik und -forschung

Datenschutzkonforme Sicherheitsforschung und -technik ist Schwerpunkt des EU-Forschungsprojekts PRISE (Privacy Enhancing Shaping of Security Research and Technology). Die vier Partner entwickeln Kriterien für Grundrechtskonformität bei der Entwicklung und Anwendung von Sicherheitslösungen.

Das Projekt PRISE läuft von Februar 2006 bis Mai 2008 und wird im Rahmen der vorbereitenden Maßnahme auf dem Gebiet der Sicherheitsforschung für das 7. Europäische Forschungsprogramm durch die Europäische Union (EU) gefördert. **Sicherheitstechnologien** werden von Strafverfolgungsbehörden und Geheimdiensten zur Verhinderung von Gefahren und zur Verfolgung von Straftaten eingesetzt. Sie dienen der inneren Sicherheit eines Landes, bewirken aber oft intensive Eingriffe in Grundrechte der Bürgerinnen und Bürger. Unsere Partner sind ausländische Forschungseinrichtungen mit dem Schwerpunkt Technikfolgenabschätzung: das Institut für Technikfolgenabschätzung an der Österreichischen Akademie der Wissenschaften (ITA), der Dänische Technologierat (DBT) und der Norwegische Technologierat (NBT).

PRISE wird Szenarien zur grundrechtskonformen und datenschutzfördernden Gestaltung von Sicherheitstechnik vorstellen. Diese Szenarien werden in Verfahren zur **Technikfolgenabschätzung mit Bürgerbeteiligung** in fünf europäischen Ländern überprüft, um so die Bedenken und Wünsche der Bürgerinnen und Bürger in das Projekt einfließen zu lassen. PRISE wird dann die aufgestellten Kriterien unter Einbeziehung von Anbietern von Sicherheitstechnik, privaten und öffentlichen Anwendern, Gestaltern der Sicherheitspolitik und von Bürgerrechtsorganisationen, die zur Sicherheitspolitik möglicherweise in Konflikt stehende Interessen vertreten, verfeinern.

Unsere Aufgaben sind die rechtliche, vor allem die datenschutzrechtliche Begleitung der Kriterienentwicklung und das Mitwirken beim Erarbeiten technischer, rechtlicher und organisatorischer Maßnahmen, die eine **akzeptable Balance** zwischen Anforderungen der inneren Sicherheit und des Datenschutzes in Forschungsunternehmen, in der Gesellschaft und auf politischer Ebene ermöglichen sollen. Weitere Informationen zum Projekt sind zu finden unter

www.datenschutzzentrum.de/prise/
www.prise.oeaw.ac.at/

Was ist zu tun?
Wir werden mit unseren Partnern auf eine grundrechtskonforme Gestaltung der europäischen und deutschen Forschung im Sicherheitsbereich Einfluss nehmen und dazu die von PRISE entwickelten Kriterien europäischen Entscheidungsträgern vorstellen.

8.7 SpIT-AL – keine Spam-Anrufe über Voice-over-IP

Mit Voice-over-IP billiger telefonieren – das gilt auch für Werbeanrufe, die von vielen Menschen bereits nicht mehr nur als Belästigung, sondern als Telefonterror wahrgenommen werden. Im Kampf gegen diesen Terror hat die Kieler Telefongesellschaft TNG zusammen mit dem ULD im Projekt SpIT-AL eine Abwehrlösung entwickelt.

Werbung für Lotterielose und Telefontarife, Angebote für die Kandidatur in einer Quizsendung oder die automatische Ansage, man hätte einen garantierten Gewinn und solle nur mal eben eine teure Nummer wählen: Täglich klingelt das Telefon – und nervt. Schon in den herkömmlichen Netzen der leitungsvermittelten Telefonie mit noch relativ teuren Gesprächen nimmt die Belästigung zu. Die Durchsetzung rechtlicher Unterlassungsansprüche verspricht in der Praxis kaum Erfolg: Selbst wenn erreicht wird, einem Callcenter die Anrufe zu untersagen, wird schon vom nächsten angerufen. Technische Ansätze, wie sie im Bereich **E-Mail-Spam** praktiziert werden, sind bislang rar.

Von Voice-over-IP, der Übertragung von Telefongesprächen mit Internettechnik, werden **wichtige Impulse** für die Wirtschaft – nicht nur – in Schleswig-Holstein erwartet. Leider ist davon auszugehen, dass diese Impulse auch von den falschen Stellen aufgegriffen werden und zu einer weiteren Flut unerwünschter Anrufe (genannt SpIT – Spam over Internet Telephony) bei Firmen und Privatleuten führen, die die positiven Effekte wieder zunichtemachen könnte.

Die Kieler Telefongesellschaft TNG (The Net Generation) hat daher mit der Idee zur Entwicklung eines **SpIT-Filters** den Zuschlag für die öffentliche Förderung im Rahmen des schleswig-holsteinischen Programms e-Region PLUS bekommen. Das ULD begleitet die Entwicklung von Abwehrmechanismen gegen SpIT innerhalb des Projektes datenschutzrechtlich und -technisch. Das Projekt SpIT-AL (SpIT-Abwehr-Lösung) genießt inzwischen über die nationalen Grenzen hinaus Aufmerksamkeit.

TNG arbeitet daran, die SpIT-AL-Möglichkeiten nicht nur für Voice-over-IP, sondern auch für herkömmliche Telefonie seinen Kunden anzubieten. Darüber hinaus soll die im Projekt erarbeitete Lösung als **Open-Source-Projekt** der Allgemeinheit zur Nutzung und Weiterentwicklung zur Verfügung stehen.

 www.spit-abwehr.de/

Was ist zu tun?
Bei Anti-Spam-Systemen müssen Entwickler und Anwender darauf achten, dass rechtskonforme Lösungen zum Einsatz kommen.

8.8 RISER (Registry Information Service on European Residents)

RISER, der erste E-Government-Dienst für grenzüberschreitende Meldeauskünfte in Europa, hat die Marktevaluierung erfolgreich abgeschlossen und wird nun schrittweise in den Markt eingeführt.

Mit dem Ziel einer datenschutzkonformen Gestaltung haben wir die Einführung der europäischen Melderegisterauskunft RISER (Registry Information Service on European Residents) begleitet (28. TB, Tz. 8.3). Das Projekt eines Konsortiums unter Leitung der Berliner Firma PSI AG befindet sich mittlerweile in der dritten Phase: Nach erfolgreicher Marktevaluierung in Estland und Ungarn (RISERac) startete im September 2006 die Phase der **Markteinführung** (RISERid). Bis zum Jahr 2009 soll dabei der Dienst in weiteren EU-Ländern schrittweise angeboten werden. RISERid wird von der Europäischen Kommission im Rahmen des eTen-Programms gefördert.

Der RISER-Dienst bietet seinen Kunden einen einheitlichen Zugang zu einer sehr heterogenen und damit unübersichtlichen Landschaft von Melderegistern in Europa. Über das **Serviceportal für Meldeanfragen** werden Datei- oder Einzelanfragen über das Internet an die zuständige Meldebehörde weitergeleitet. RISER übernimmt dabei die Funktion eines Zustellers.

Der Schwerpunkt unserer Projektbegleitung liegt auf der **datenschutzgerechten Ausgestaltung** des Dienstes: Welche Daten dürfen in den nationalen Melderegistern abgefragt werden? Wie sind personenbezogene Daten vor unbefugten Zugriffen zu schützen? Was muss ein Dienst datenschutzrechtlich leisten, wenn er personenbezogene Daten im Auftrag abfragt und weiterleitet? Ein wichtiger Meilenstein war die 2. Internationale Konferenz zum Europäischen Meldewesen in Tallinn, Estland, an der Delegierte der öffentlichen Verwaltungen aus 13 Ländern teilnahmen. Bei dieser Diskussion konnten wir das Anliegen des Datenschutzes bei der Weiterentwicklung des Meldewesens in Deutschland und Europa einbringen.

Was ist zu tun?
Die Berücksichtigung einheitlicher hoher datenschutzrechtlicher Standards muss bei der Ausweitung des Dienstes auf das gesamte Gebiet der Europäischen Union gewährleistet bleiben.

8.9 IM Enabled – E-Government per Instant Messaging

Mit der Behörde online und in Echtzeit kommunizieren – dieses ehrgeizige Ziel steht im Mittelpunkt des Projektes IM Enabled E-Government Services, an dem das ULD im Auftrag der Europäischen Kommission mitarbeitet.

Gegenstand des Projektes ist es, Bürgern und Unternehmen E-Government-Dienste über **Instant Messaging** bereitzustellen. Dabei ergeben sich zwangsläufig Datenschutzfragen: Welche Behördeninformationen können datenschutzgerecht über Instant Messaging zur Verfügung gestellt werden? Welche Anforderungen sind an Anbieter von Instant-Messaging-Diensten zu stellen, damit die Bürger sicher mit ihrer Behörde kommunizieren können? Derzeit erfüllen die meisten Anbieter des technischen Basisdienstes die Voraussetzung einer sicheren Übertragung der Informationen nicht. An dem im September 2006 gestarteten Projekt sind unter Führung des Waterford Institutes of Technology Partner aus Irland, Frankreich, Italien und Deutschland beteiligt. Das Projekt wird im Rahmen des eTen-Programms von der Europäischen Union gefördert.

Was ist zu tun?
Personenbezogene Informationen dürfen in Realzeit online erst dann zur Verfügung gestellt werden, wenn die auftretenden technischen und rechtlichen Datenschutzfragen geklärt sind.

8.10 Studie zum Verbraucherdatenschutz

Verbraucherdatenschutz gewinnt immer mehr an Bedeutung. Im Auftrag des Bundesministeriums für Verbraucherschutz hat das ULD die rechtlichen Rahmenbedingungen zusammengestellt und bewertet.

Verbraucherschutz dient der Wahrung der Vertragsfreiheit der Konsumentinnen und Konsumenten. Datenschutz dient der Sicherung der Souveränität bei der Verwendung der eigenen Daten. In beiden Fällen geht es um die Behebung eines **strukturellen Ungleichgewichts** zwischen Unternehmen und Verbraucher bzw. zwischen der Daten verarbeitenden Stelle und dem Betroffenen. Unter dem Begriff „Verbraucherdatenschutz“ sind die beiden Bereiche zusammengeführt. Es geht um den Schutz personenbezogener Informationen der Verbraucher. Diese sollen „auf Augenhöhe“ mit den Unternehmen Verträge schließen und dabei selbst über ihre Daten bestimmen. Sie sollen nicht diskriminiert, manipuliert und ihrer Datenherrschaft beraubt werden. Verbraucherdatenschutz ist eine Grundvoraussetzung, damit Bürgerinnen und Bürger ohne Fremdsteuerung ihre individuellen Bedürfnisse befriedigen können. Er ist aber auch Voraussetzung für einen **fairen**

Wettbewerb zwischen den Anbietern um ihre Kunden, denn es soll niemand wirtschaftliche Vorteile aus der Verletzung von Datenschutzbestimmungen genießen dürfen.

Die im Auftrag des Bundesministeriums für Verbraucherschutz im Frühjahr 2006 erstellte Studie beschreibt erhebliche Mängel in der Durchsetzung des Verbraucherdatenschutzes. Diese sind auf eine unzureichende Aufstellung und Ausstattung der Datenschutzkontrollinstitutionen als auch auf Defizite im Datenschutzrecht zurückzuführen, z. B. auf die unzureichende Sanktionierung von Verstößen gegen Transparenzpflichten. Die Studie zeigt **Lösungen**, wie durch die Stärkung der betrieblichen Eigenkontrolle, eine wirksame Datenschutzaufsicht, eine unabhängige Auditierung von Verfahren der Datenverarbeitung sowie durch die Stärkung der Verbraucherrechte im Wege der Verbandsklage oder des Wettbewerbsrechts das erforderliche Datenschutzniveau im Interesse der Verbraucher gesichert werden kann. Die Studie kann im Internet abgerufen werden unter

www.datenschutzzentrum.de/verbraucherdatenschutz/

Was ist zu tun?
Der Verbraucherdatenschutz muss im Interesse der Verbraucher und eines fairen Wettbewerbes gestärkt werden.

8.11 Folgen und Herausforderungen des Ubiquitären Computing

Ubiquitäres Computing (UC) steht für „Allgegenwart der Informationsverarbeitung“ und beschreibt die Integration von Informationstechnik in Alltagsprodukte, die über Funktechnik miteinander kommunizieren. Durch UC entsteht eine Vielzahl von Datenspuren.

UC eröffnet Möglichkeiten zur **heimlichen Überwachung** der Menschen und ihres Alltagsverhaltens, insbesondere wenn den Betroffenen Steuerungsmöglichkeiten für die Verarbeitung ihrer Daten fehlen. Ungelöst und komplex ist zudem die Sicherheit des Datenaustausches zwischen Objekten (28. TB, Tz. 8.6). In der im Auftrag des Bundesministeriums für Bildung und Forschung (BMBF) im Rahmen des ITA-Programms erstellten Studie „Technikfolgenabschätzung Ubiquitäres Computing und informationelle Selbstbestimmung (TAUCIS)“ haben wir die rechtlichen, technischen und gesellschaftlichen Rahmenbedingungen und Auswirkungen des Ubiquitären Computing, insbesondere auf das Recht auf informationelle Selbstbestimmung, analysiert und beschrieben. Kooperationspartner und Co-Autor an dieser Studie ist das Institut für Wirtschaftsinformatik an der Humboldt-Universität zu Berlin.

Beispiele für UC-Anwendungen sind der „intelligente Kühlschrank“, der die Lebensmittel des täglichen Bedarfs von selbst nachbestellt, das sich selbst wartende Auto oder der „intelligente Arbeitsplatz“, der Kommunikation am Arbeitsplatz durch das Erkennen von Aufgaben proaktiv unterstützt. Wichtige Technolo-

gien, die hier zum Einsatz kommen, sind etwa die RFID-Technik (Radio Frequency Identification) oder das Sensornetz.

Um die **Datenschutzrisiken** für die Nutzerinnen und Nutzer zu minimieren, bedarf es datenschutzkonformer und sicherer UC-Anwendungen. Anonymität und Datensparsamkeit müssen als Standardeinstellungen in den UC-Systemen verankert sein. Sollen dennoch Daten personenbezogen verarbeitet werden, dann gehört die Steuerung der Verarbeitungsprozesse in die Hand der Betroffenen. Damit sind vor allem die Betreiber von UC-Anwendungen in der Pflicht, die für eine datenschutzkonforme Gestaltung sorgen müssen. Wer beispielsweise Lesegeräte aufstellt, UC-Anwendungen betreibt und in Hintergrundsystemen personenbezogene Daten verarbeitet, ist gegenüber den Betroffenen für die Rechtmäßigkeit der Verarbeitung, die Datensicherheit und die Wahrung der Datenschutzrechte (z. B. Information und Auskunft) verantwortlich.

Auf der Basis einer empirischen Untersuchung zeigt unsere Studie, dass die **Menschen grundsätzlich bereit** sind, sich auf technische Systeme einer allgegenwärtigen Datenverarbeitung einzulassen. Es wird aber deutlich, dass das bestehende Technikvertrauen leicht in ein grundsätzliches Misstrauen umschlagen kann, wenn die Nutzer den Einsatz dieser Technik und insbesondere die Erhebung und Verarbeitung ihrer Daten nicht mehr kontrollieren können. Dies ist ein deutlicher Hinweis an die Hersteller und Betreiber von ubiquitären Computeranwendungen, dass sie für vertrauenswürdige Anwendungen Sorge tragen müssen. Eine Datenschutzauditierung durch eine unabhängige Institution wie das ULD kann hierbei eine hilfreiche Rolle spielen.

Die Studie zeigt noch ungelöste Probleme der **Datensicherheit von UC-Anwendungen** auf: Sobald Mikrochips untereinander Informationen austauschen, werden gravierende Sicherheitsfragen der Authentizität, Integrität und Vertraulichkeit aufgeworfen. Es gehört wenig Fantasie zu der Vorstellung, was passiert, wenn z. B. Autos mithilfe von UC automatisch den erforderlichen Sicherheitsabstand einhalten sollen, jedoch die Technik die von Hersteller zu Hersteller, von Auto zu Auto, von Bauteil zu Bauteil unterschiedlichen Signale nicht versteht oder Dritte die Signale manipulieren. Um derartige Risiken auszuschließen und die Innovationen nutzen zu können, bedarf es noch erheblicher Anstrengungen. Hierzu gibt die Studie Hinweise und macht konstruktive Vorschläge.

Die Untersuchung kann abgerufen werden unter

www.taucis.de/

Die Studie wird derzeit im Auftrag des BMBF ins Englische übersetzt.

Was ist zu tun?
Wirtschaft, Wissenschaft und Gesetzgeber müssen die geeigneten technischen Lösungen entwickeln bzw. fördern, damit die informationelle Selbstbestimmung der betroffenen Nutzer in den Anwendungen des Ubiquitären Computing gewährleistet wird.

9 Audit und Gütesiegel

9.1 Datenschutz-Audit konkret

9.1.1 Landesnetz Schleswig-Holstein

Das Verwaltungsnetz des Landes wurde erfolgreich auditiert. Das Finanzministerium und die von ihm beauftragten Dienstleister dataport und T-Systems Enterprise Services GmbH haben mit großem Engagement die mit dem ULD gemeinsam festgelegten Datenschutzziele erreicht.

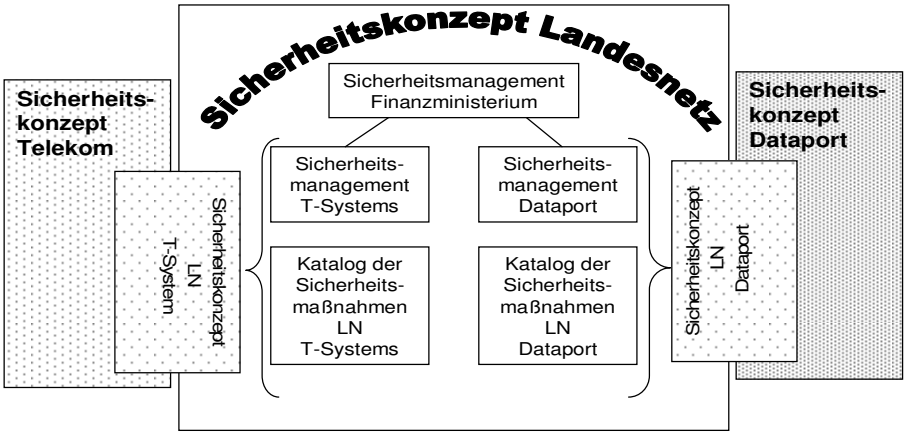
Das Audit für das Landesnetz Schleswig-Holstein (LN) konnte im Rahmen der alljährlichen Sommerakademie an Finanzminister Rainer Wiegard im August 2006 übergeben werden. Das **Finanzministerium als verantwortlicher Betreiber** hat alle Anforderungen umgesetzt, die aus Sicht des ULD für eine sichere Kommunikation notwendig sind (28. TB, Tz. 9.1.1). Das Landesnetz verfügt nun über herausragende Sicherheitsfunktionen, die über die Landesgrenzen hinaus zur Nachahmung einladen.

Besonders hervorzuheben ist die für das LN erstellte **Generaldokumentation**. Sie bildet auf einem hohen qualitativen Niveau die technische und organisatorische Grundlage für die Verfahrensweise und die komplexen Arbeitsabläufe im LN. Darüber hinaus beinhaltet sie die ganzheitliche Sicht der Prozesse aus Kunden- und Betreibersicht für den Transport der Daten. Sie ist sowohl für den Nutzer als auch für den Betreiber nachvollziehbar und verständlich erstellt und besteht aus folgenden Modulen:

- Teil 1: Beschreibung der IT-Systeme
- Teil 2: Sicherheitskonzept
- Teil 3: Weiterführende Dokumentation
- Teil 4: Verträge mit dataport
- Teil 5: Verträge mit T-Systems Enterprise Services GmbH
- Teil 6: Verträge mit den Nutzern

Ein weiteres Highlight im LN sind die integrierten **Revisionswerkzeuge**. Für das LN wurde ein automatisiert eingerichtetes Berichtswesen entwickelt, das die Umsetzung der Kundenaufträge transparent, lesbar und verständlich darstellt. Die Berichte enthalten Informationen über die Kommunikationsparameter zwischen Nutzern des LN untereinander sowie über die Parameter zwischen Nutzern des LN und dataport. Zudem erhalten die Nutzer ein Revisionstool – Landesnetz Router Controll (LNRC) – zur Überwachung der administrativen Aktivitäten auf dem beim Kunden installierten Landesnetzrouter (Übergaberouter).

Über das beim Finanzministerium eingerichtete **Sicherheitsmanagement** besteht die Möglichkeit, die beauftragten und tatsächlich umgesetzten Kommunikationseinstellungen zu kontrollieren.



Zusammenfassend konnten im Auditverfahren folgende **datenschutzfreundliche Aspekte** festgestellt werden:

- Mit dem Einsatz der MPLS-Technologie und der Einrichtung redundanter Netzkomponenten wird durch den vom Finanzministerium beauftragten Netzbetreiber T-Systems Enterprise Services GmbH sichergestellt, dass während des Transports der Daten über das LN die Verfügbarkeit, Vertraulichkeit und die Integrität sowie die Ordnungsmäßigkeit der Datenverarbeitung gewährleistet werden.
- Dataport stellt sicher, dass die im LN eingesetzten Übergaberouter und die Verbindungsfirewall nach den Kommunikationsparametern der Nutzer ordnungsgemäß administriert werden.
- Sicherheitsrelevante Ereignisse können über das automatisierte Berichtswesen sowie den Einsatz eines Revisionstools (LNRC) von den Administratoren der Landesnetznutzer rechtzeitig erkannt und ausgewertet werden.
- Die technischen und organisatorischen Abläufe im LN werden in der Generaldokumentation vollständig beschrieben.
- Das Finanzministerium hat für die Aufrechterhaltung eines hohen Sicherheitsniveaus ein Datenschutz- bzw. Sicherheitsmanagement eingerichtet, das eine umfassende Qualitätssicherung der sicherheitsrelevanten Landesnetzeigenschaften betreibt und auf Sicherheitsvorfälle zeitnah reagiert.
- Alle von dataport und T-Systems Enterprise Services GmbH getroffenen Sicherheitsmaßnahmen sind in dem „Katalog der Sicherheitsmaßnahmen im Landesnetz“ (KdS) festgelegt und damit Bestandteil des Sicherheitskonzepts.

Das ULD stuft das Landesnetz als ein **abgeschlossenes Netzwerk** ein, in dem personenbezogene Daten der Nutzer unverschlüsselt, aber isoliert von anderen

Nutzergruppen transportiert werden können. Eine **Verschlüsselung** der im Rahmen von Fachanwendungen zu transportierenden Daten ist nur erforderlich, wenn die in dem Sicherheitskonzept des Finanzministeriums beschriebenen Restrisiken von der verantwortlichen Stelle als nicht tragbar bewertet werden. Zur Minimierung der Restrisiken bietet es sich an, die Daten vom Absender bis zum Empfänger zu verschlüsseln (Ende-zu-Ende-Verschlüsselung). Für Zweifelsfälle bietet das ULD seine Beratung an.

Das ULD hat zeitgleich zur Auditierung **Hinweise zur Nutzung des Landesnetzes** im Internet veröffentlicht, in dem die Nutzer auf ihre datenschutzrechtliche Verantwortlichkeit für ihr lokales Netz von der Schnittstelle des Übergaberouters an und die Befolgung bestimmter Verhaltensregeln hingewiesen werden. Dazu gehört die Beauftragung von Kommunikationsbeziehungen, die Prüfung und gegebenenfalls Korrektur der Berichte über die erfolgten Einstellungen ihrer Kommunikationsbeziehungen gegenüber dataport sowie die Installation und Nutzung des von dataport bereitgestellten Revisionstool „LandesNetzRouterControl“ (LNRC), um die Einstellungen auf dem Übergaberouter überprüfen zu können. Die Hinweise sind veröffentlicht unter

www.datenschutzzentrum.de/landesnetz/060828-hinweise.htm

Was ist zu tun?
Das Finanzministerium muss das erreichte Sicherheitsniveau dauerhaft aufrechterhalten. Die Nutzer sind verpflichtet, die Berichte über die Einstellungen ihrer Kommunikationsbeziehungen zu prüfen und gegebenenfalls gegenüber dataport zu korrigieren sowie das Revisionstool „LandesNetzRouterControl“ (LNRC) zu installieren und zu nutzen.

9.1.2 Stadt Pinneberg

Das ULD hat der Stadtverwaltung Pinneberg mit der Verleihung eines Auditzeichens bestätigt, dass sie sicherheitstechnisch und datenschutzrechtlich im Bereich ihrer internen Datenverarbeitung sowie des Internetanschlusses gut aufgestellt ist.

Die Bestandsaufnahme vor Ort hat nur wenige und schnell zu behebende Lücken in der IT-Konzeption, Konfiguration und Dokumentation der Systeme ergeben. Auf einem guten und teilweise sehr **hohen Niveau** erfolgt in Pinneberg der Betrieb des Serverraums, die Aufstellung, Konfiguration und Administration der Server sowie das Vorgehen bei der Einführung neuer Fachverfahren. Nach der Bestandsaufnahme musste der bereits gut funktionierende IT-Betrieb nur noch an wenigen Ecken abgerundet werden. Vor allem war das **Datenschutzmanagementsystem** (DSMS) zusammen mit dem neu bestellten Datenschutzbeauftragten, dessen Vorgänger und dem Leiter des IT-Bereichs neu zu definieren und mit Leben zu füllen.

Das Zertifizierungsverfahren wurde dadurch **vereinfacht**, dass sich die Datenverarbeitung der Stadt auf bereits vom ULD zertifizierte Produkte und Dienstleistungen stützen konnte. Die Stadt verfügt für ihre elektronische Kommunikation über einen **zertifizierten Landesnetzanschluss** (Tz. 9.1.1) mit bereits geprüften Sicherheitsfunktionen. Zudem setzt die Stadt Pinneberg das vom ULD im Sommer 2006 rezertifizierte Firewall-System von dataport ein.

Die durch das vorliegende Audit erfassten Verarbeitungsprozesse zeichnen sich insbesondere durch folgende **datenschutzfreundliche Aspekte** aus:

- Der technische Aufbau und Betrieb des Serverraumes ist vorbildlich.
- Alle Fachanwendungen und die mit ihnen verarbeiteten Daten werden strukturiert zentral auf den Servern verwaltet. Die Abschottung der Fachanwendungen untereinander ist sichergestellt. Die Zugriffe auf die Anwendungen sind durch eine transparente Zugriffsregelung gewährleistet.
- Die IT-Systeme sowie die auf ihnen eingesetzten Fachverfahren sind gut dokumentiert. Für jedes Fachverfahren ist ein Verantwortlicher benannt. Die jeweiligen Pflichten des IT-Bereichs und der Fachverfahrensverantwortlichen sind im IT-Konzept nachvollziehbar und eingängig festgelegt.
- Für die Absicherung und Kontrolle des Anschlusses an externe Netze werden Sicherheitskomponenten eingesetzt, die unerwünschte Zugriffe abwehren und den Transport schadhafter Inhalte verhindern.
- Die auf den Arbeitsplatz-PCs enthaltenen Funktionen sind durch den Einsatz von Gruppenrichtlinien auf ein Mindestmaß reduziert. Der Zugriff auf externe Schnittstellen wird über eine Sicherheitssoftware zentral reglementiert.
- Der IT-Bereich verfügt für Test- und Weiterbildungszwecke über eine Testumgebung. In dieser Testumgebung werden auch administrative Änderungen an Fachverfahren durch den Fachverfahrensverantwortlichen vor dem Einsatz in der Produktivumgebung getestet und freigegeben.
- Zur Einführung und Weiterentwicklung von Fachverfahren ist ein Prozess definiert, der für eine umfassende Berücksichtigung möglicher Anforderungen aus den Bereichen Datenschutz und Datensicherheit sorgt.
- Die Auswertung von Protokollen ist geregelt. Die Revisionstools zur Überwachung des Landesnetzzugangs befinden sich im Einsatz.

Was ist zu tun?
Die Stadt Pinneberg wird das erreichte hohe Niveau im Bereich Datensicherheit halten. Über ein Datenschutzmanagementsystem sind Prozesse etabliert, um Datenschutz und Datensicherheit in Zukunft auf dem jetzt nachgewiesenen hohen Niveau zu gewährleisten.

9.1.3 Neues Audit für Personalverwaltungs- und Informationssystem in Norderstedt

Anfang 2007 wurde die Reauditierung des Personalverwaltungs- und Informationssystems der Stadt Norderstedt mit der Verleihung des Datenschutzauditzeichens abgeschlossen.

Das Personalverwaltungs- und Informationssystem der Stadt Norderstedt hat einen **modularen Aufbau** mit verschiedenen Funktionalitäten wie die Verwaltung von Personalstammdaten, Organigrammerstellung, Stellenplanbewirtschaftung, Protokollierung und Datenschnittstellen zu anderen Programmen. Das Reauditierungsverfahren überprüfte erneut dieses System, dessen Einführung 2003 auditiert worden war (26. TB, Tz. 9.2.2).

Im Vordergrund der Untersuchung stand die Funktionsfähigkeit des Datenschutzmanagementsystems. Es zeigte sich, dass die selbst gesteckten Ziele erreicht wurden, einen datenschutzgerechten Betrieb und die laufende Anpassung des Systems und seiner Erweiterungen an die Anforderungen des Datenschutzes sicherzustellen. Bei der Einführung zweier neuer Programmmodule ging die Stadt Norderstedt mit derselben Sorgfalt vor. Die **neu auditierten Module** stellen Funktionen für die Organisation von Fortbildungsveranstaltungen und für die automatisierte Erzeugung von Dokumenten mit Daten aus dem Personalverwaltungs- und Informationssystem bereit. Aus der Auditierung 2003 und dem laufenden Betrieb war bekannt, dass einige datenschutzrechtliche Anforderungen zwar mithilfe der Software erfüllt werden können, dies aber nur manuell erfolgte, z. B. die Löschung nicht mehr benötigter Daten. Notwendige Ergänzungen der Software, die diese Arbeitsschritte automatisieren, wurden von der Stadt Norderstedt beim Hersteller der Software angefordert und durch diesen inzwischen umgesetzt. Sie kommen allen Kunden des Herstellers zugute.

Die von der Stadt Norderstedt vorgelegte **Datenschutzerklärung** zeigt, dass das Personalverwaltungs- und Informationssystem ein gutes datenschutzrechtliches Niveau erreicht hat und dies auch zukünftig beibehalten wird. Dies ist nicht zuletzt der Entscheidung zuzuschreiben, einen behördlichen Datenschutzbeauftragten zu bestellen – dieser hat das Audit maßgeblich unterstützt.

Was ist zu tun?
Die Reauditierung zeigt, dass mit dem Datenschutz-Audit eine dauerhafte Verbesserung des Datenschutzes in öffentlichen Einrichtungen erreicht werden kann, indem die hohen Maßstäbe bei Änderungen und Ergänzungen eingehalten werden. Bereits auditierte Stellen können bei einer Reauditierung auch solche Ergänzungen überprüfen lassen.

9.1.4 Gemeinde Ratekau

Mit seiner offensiven Herangehensweise an das Thema Datenschutz und Datensicherheit tut sich die Gemeinde Ratekau positiv hervor. Der Bürgermeister und seine Mitarbeiterinnen und Mitarbeiter räumen dem Datenschutz und der Datensicherheit einen hohen Stellenwert ein.

Anfang Dezember 2006 wurde der Gemeinde Ratekau vom ULD ein Datenschutzauditzertifikat für den **vorbildlichen Betrieb ihrer IT-Systeme** verliehen. Die Gemeinde hat für ihr Verwaltungsnetz ein Sicherheitskonzept erarbeitet, in dem Maßnahmen für die Absicherung der internen IT-Systeme und des Anschlusses des internen Verwaltungsnetzes an das Internet festgelegt sind. Mit diesen technischen Sicherheitsfunktionen werden die im internen Netz verarbeiteten Daten hinreichend geschützt. Darüber hinaus werden den Mitarbeitern die Internetdienste „E-Mail“ und „WWW“ zur Kommunikation mit Bürgern und anderen Verwaltungen sowie zur Beschaffung dienstlicher Informationen auf sicherem und datenschutzkonformem Wege ermöglicht.

Folgende in dem **Sicherheitskonzept** festgelegte Maßnahmen sind besonders hervorzuheben:

- Die auf den Arbeitsplatz-PCs verfügbaren Funktionen sind auf ein Mindestmaß reduziert.
- Die Disketten- und CD-ROM-Laufwerke sowie der USB-Port sind weitgehend deaktiviert.
- Die Fachanwendungen werden strukturiert zentral auf den Servern verwaltet.
- Der Internetanschluss ist durch eine qualifizierte Viren- und Contentmanagementsicherheitssoftware geschützt.

Grundlage der Überprüfung der IT-Systeme war eine detaillierte Dokumentation. Geprüft wurde im Zusammenwirken mit der bei der Gemeindeverwaltung tätigen **behördlichen Datenschutzbeauftragten**, ob die systemtechnischen Datenschutzvorschriften von den Fachabteilungen beachtet werden.

Bezüglich der Umsetzung und Einhaltung der technischen Sicherheitsmaßnahmen konnte darüber hinaus gewürdigt werden, dass sich der **IT-Koordinator** der Gemeindeverwaltung über die Teilnahme an Seminaren der DATENSCHUTZAKADEMIE besonders qualifiziert hatte. Ihm war kurz vor der Auditierung von der DATENSCHUTZAKADEMIE das Datenschutzzertifikat für Systemadministratoren verliehen worden (26. TB, Tz. 16.4).

Was ist zu tun?
Eine erfolgreiche Zertifizierung bestätigt der Verwaltung, dass sie ihre Hausaufgaben gemacht hat. Die Bürgerinnen und Bürger können sich auf eine sichere Verarbeitung ihrer Daten verlassen. Deshalb sollten sich nicht zertifizierte Kommunen an dem Sicherheitsstandard der Gemeinde Ratekau orientieren.

9.1.5 Kreis Plön

Die IT-Abteilung der Kreisverwaltung Plön setzt mit der angestrebten Auditierung ihres Sicherheitskonzepts zu Kreisnetz, zu Teilbereichen des Rechenzentrums sowie zum Internetzugang für die Kommunen neue Maßstäbe. Schon in der ersten Phase des Auditprozesses ist zu erkennen, dass die IT-Abteilung gute und professionelle Arbeit leistet.

Der Kreis Plön bietet bisher schon auf hohem Sicherheitsniveau für seine Kommunen IT-Dienstleistungen an (27. TB, Tz. 6.6.3). Hierfür wurde beim Kreis ein sternförmig strukturiertes **Kreisnetz** und eine sogenannte Service Area geschaffen. Die IT-Abteilung wirkt darauf hin, dass die Regelungen zur Auftragsdatenverarbeitung und Datensicherheit beachtet werden. Auf der Basis eines Betreibervertrages zwischen Kreis und Netzlieferant werden zwischen den Kommunen und dem Kreis Dienstleistungsverträge geschlossen, in denen die Rechte und Pflichten der Vertragspartner auch im Hinblick auf den Datenschutz festgelegt sind. Die Kunden bzw. Kommunen werden in die Lage versetzt, die vom Kreis angebotenen Leistungen nachzuvollziehen. Sie können ihren Kontrollpflichten gegenüber dem Kreis im Rahmen der Auftragsdatenverarbeitung nachkommen.

Die IT-Abteilung des Kreises möchte ihr Sicherheitskonzept vor allem für das Kreisnetz, Teilbereiche der Service Area sowie den als Dienstleistung für die Kommunen angebotenen Internetzugang auditieren lassen. Zudem soll unter der Berücksichtigung gesetzlicher Regelungen eine praxiskonforme **Dokumentation des Rechenzentrumsbetriebes** erstellt werden. Diese soll als Muster anderen Kreisverwaltungen zugänglich gemacht werden. Eine Zusammenarbeit findet bereits mit dem Kreis Nordfriesland statt (Tz. 9.1.6).

Was ist zu tun?
Die Strategie der IT-Abteilung des Kreises Plön hat Vorbildcharakter.

9.1.6 Kreis Nordfriesland

Die Kreisverwaltung Nordfriesland setzt im Rahmen seiner E-Government-Strategie einen Schwerpunkt auf interkommunale Zusammenarbeit. Die von der Kreisverwaltung betriebenen IT-Systeme werden auf den neuesten Stand der Technik gebracht, um bei der Kooperation mit anderen Kommunen Datenschutz und Datensicherheit gewährleisten zu können.

Das von der Kreisverwaltung Nordfriesland betriebene Kreisnetz und Rechenzentrum wird im Rahmen des Audits nach den Anforderungen der vom Kreis für die Kommunen angebotenen Dienstleistungen **umgestaltet** (28. TB, Tz. 9.1.5). Ziel ist es, unter Wahrung hoher Flexibilität ein Sicherheitsniveau zu erreichen, das die Integrität, Vertraulichkeit und Verfügbarkeit der Daten der Kunden gewährleistet. Dabei geht es um folgende Maßnahmen:

- Virtualisierung der Datenhaltung durch die Einrichtung eines Storage Area Networks (SAN),
- abgeschotteter Einsatz von mehreren Applikationen auf einem Server durch den Einsatz von VMware,
- Einrichtung von sogenannten VLANs, um die Datenkommunikation über das Kreisnetz bis zur Applikation voneinander zu trennen.

Die Kreisverwaltung setzt hauptsächlich die **Terminalservertechnologie** ein, womit die Datenverarbeitung vom Client auf zentrale IT-Komponenten verlagert wird. Dies hat nicht nur wirtschaftliche Vorteile, sondern erleichtert auch die Administration und erhöht die Datensicherheit. Der Einsatz dieser zukunftsgerichteten Technologien erfordert organisatorische Veränderungen im Bereich der IT-Abteilung der Kreisverwaltung.

Was ist zu tun?
Die Kreisverwaltung sollte ihren Weg der Verwaltungsmodernisierung fortführen und die ihr nachgeordneten Kommunen bei dem Betrieb ihrer IT-Systeme mit einem breit angelegten Dienstleistungsangebot unterstützen.

9.1.7 Fördermaßnahmen EAGFL und ELER des Ministeriums für Landwirtschaft, Umwelt und ländliche Räume

Ein beim Ministerium für Landwirtschaft, Umwelt und ländliche Räume (MLUR) durchgeführtes Audit soll bestätigen, dass die Zahlstelle und die dort für die Fördermaßnahmen eingesetzten IT-Systeme (ZIAF) nach den nationalen und europarechtlichen Vorgaben betrieben werden.

Der ländliche Raum wird durch den Europäischen Ausrichtungs- und Garantiefonds für die Landwirtschaft (EAGFL) und den Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) gefördert. Die Kommission der Europäischen Gemeinschaft (EU-Kommission) hat für die **ordnungsgemäße Abwicklung** der zur Verfügung gestellten Finanzmittel **EU-Verordnungen** erlassen, die von den eingerichteten Zahlstellen der einzelnen Bundesländer einzuhalten sind. Für die Umsetzung der Verordnung haben sich die Bundesländer auf die Anwendung des IT-Grundschutzhandbuchs des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verständigt (28. TB, Tz. 9.1.3).

Im Dezember 2006 hat die EU-Kommission in einem anderen Bundesland eine erste Überprüfung einer Zahlstelle durchgeführt. Bereits Art und Umfang der im Rahmen dieser Prüfung **vorzulegenden Unterlagen** verdeutlichen, dass die EU-Kommission hohe Anforderungen an die IT-Sicherheit stellt. Hierzu zählen insbesondere Informationen über die Verantwortlichkeiten, Sicherheitskonzepte, Netzpläne, Hard- und Software sowie Anwendungen, Jahrespläne der Innenrevision, Notfallplan und Katastrophenmanagementkonzept, Softwareentwicklungsmethoden, Verfahrensänderungsmanagement, Verfahrensanweisungen, Checklisten und Datenprotokolle.

Das **Ministerium für Landwirtschaft, Umwelt und ländliche Räume** (MLUR) nimmt die Vorgaben der Europäischen Kommission sehr ernst und hat bereits zu Beginn des Audits eine Lenkungsgruppe sowie Arbeitskreise eingerichtet, um die geforderten Sicherheitsanforderungen bis zum Sommer 2007 erfüllen zu können.

Nach den europäischen Anforderungen muss auch der Dienstleister **dataport** für das Verfahren seine Prozesse der Datenverarbeitung in den Bereichen Rechenzentrum sowie IT-Entwicklung an dem Sicherheitsstandard „IT-Grundschutz“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ausrichten und diese erfüllen. Hierzu hat das ULD im Rahmen seiner Auditierung im Februar 2007 gemeinsam mit dataport eine umfassende Bestandsaufnahme durchgeführt, auf deren Grundlage die erforderlichen Maßnahmen zur Gewährleistung des IT-Grundschutzes getroffen und umgesetzt werden können.

Was ist zu tun?
Die im Rahmen des Audits zu erledigenden Aufgaben müssen zügig und konstruktiv von allen projektbeteiligten Mitarbeitern bearbeitet werden, damit das MLUR bis zum Sommer 2007 die Vorgaben der Europäischen Kommission einhalten kann.

9.1.8 SAP R/3 Kosten- und Leistungsrechnung

Das Finanzministerium hat zur Modernisierung und Steuerung der Verwaltungsprozesse SAP R/3 eingeführt. Das ULD hat im Rahmen eines Audits eine Bestandsaufnahme durchgeführt und aufgezeigt, an welchen Stellen organisatorische und technische Strukturen verbessert werden können.

Das Finanzministerium hat zur Modernisierung und Steuerung der Verwaltungsprozesse SAP R/3 eingeführt und strebt eine Auditierung des Verfahrens an. Aus diesem Grund hat das Finanzministerium das ULD beauftragt, eine Bestandsaufnahme durchzuführen (28. TB, Tz. 9.1.2). Diese wurde im März 2006 abgeschlossen und dem Finanzministerium als Betreiber des Verfahrens in einem umfassenden Bericht dargestellt. Das Finanzministerium beabsichtigt, die Anforderungen aus Datenschutz und Datensicherheit im Rahmen eines **Redesign des SAP R/3-Verfahrens** mit Unterstützung des ULD umzusetzen.

Was ist zu tun?
Auch im Redesign muss das SAP R/3-Verfahren die gesetzlichen Anforderungen aus Datenschutz und Datensicherheit erfüllen.

9.1.9 KITS (Kommunale IT-Standards)

Die Auditierung des Standardsystemkonzeptes für die Bürokommunikation im kommunalen Bereich kommt voran. Zur Lösung sicherheitstechnischer Herausforderungen haben die Beteiligten KomFIT, das Finanzministerium und das ULD einfache und innovative Lösungen gefunden.

Das Finanzministerium als Betreiber der IT-Infrastruktur für KITS („Kommunale IT-Standards“) und den Landesstandard IKOTECH III hat zusammen mit dem Kommunalen Forum für Informationstechnik der Kommunalen Landesverbände in Schleswig-Holstein (KomFIT) das ULD mit der Auditierung des **Standardsystemkonzeptes** für die Bürokommunikation im kommunalen Bereich beauftragt (28. TB, Tz. 9.1.4). Ziel der Auditierung ist das Angebot eines datenschutzgerechten Standards für die Bürokommunikation in den Kommunalverwaltungen.

Technische Unzulänglichkeiten der **am Markt verfügbaren Produkte** (Tz. 6.3) haben zusätzliche aufwendige organisatorische und technische Maßnahmen notwendig gemacht. So ist zur Kontrolle des Microsoft Active Directory das Produkt eines Drittherstellers notwendig. Auch bedarf es zur Absicherung der dezentralen Serversysteme zusätzlicher Sicherheitsmaßnahmen vor Ort. Die Auditierung wird zeitnah erreicht werden können.

Was ist zu tun?
Nach zügigem Abschluss des KITS-Audits kann den Kommunen eine funktionstaugliche und datenschutzkonforme Bürokommunikation angeboten werden.

9.1.10 Christian-Albrechts-Universität

Das ULD wird zusammen mit der rechtswissenschaftlichen Fakultät und dem Rektorat der Christian-Albrechts-Universität die automatisierte Verarbeitung der Studierendendaten zur Durchführung von Studiengängen auditieren.

Die Christian-Albrechts-Universität (CAU) unterwirft als erste Universität im Land Teile ihrer Datenverarbeitung freiwillig einer **externen Sachverständigenüberprüfung**. Die Organisation der Datenverarbeitung sowie die Gewährleistung ihrer Ordnungsmäßigkeit sind an Hochschulen im Vergleich zu anderen öffentlichen Verwaltungen nicht einfach. Die institutionelle Autonomie von Hochschule und Fakultäten erschwert die Umsetzung datenschutzrechtlicher Regelungen und bewährter technischer Praktiken. Wir erhoffen uns von dieser Auditierung eine positive Vorbildwirkung für andere Fakultäten und Hochschulen des Landes.

Was ist zu tun?
Nach erfolgreicher Auditierung sollten auch andere Fakultäten und Hochschulen in Schleswig-Holstein eine Begutachtung ihrer Datenverarbeitung in Betracht ziehen.

9.1.11 Gemeinde Stockelsdorf

Nach einer durch Personalwechsel bedingten Verzögerung befindet sich Stockelsdorf auf der Zielgeraden: Das Auditzeichen ist in Sicht.

Die Gemeindeverwaltung Stockelsdorf lässt ihre **interne Datenverarbeitung sowie ihren Internetanschluss** auf die Konformität mit den datenschutzrechtlichen Vorgaben in einem Auditverfahren überprüfen (28. TB, Tz. 9.1.6). Die Verwaltung wird im Frühjahr 2007 ihre Informations- und Kommunikationsinfrastruktur neu konzeptioniert haben. Dank eines schlanken Konzeptes zur Gliederung der Dokumentation gemäß der Datenschutzverordnung (Tz. 6.5) erhält Stockelsdorf eine aussagekräftige und handhabbare IT-Sicherheitsinfrastruktur.

Was ist zu tun?
Stockelsdorf muss die begonnenen Maßnahmen jetzt zügig umsetzen.

9.1.12 Stadt Flensburg

Die Anbindung eines verwaltungsinternen Netzes an fremde Netzwerke muss sorgfältig geplant und umgesetzt werden.

Die Stadt Flensburg hat für die sichere Anbindung ihres Verwaltungsnetzes an andere Netzwerke ein **zentrales Firewall-System** aufgebaut, das in Eigenregie administriert wird. Über das System wird jegliche Kommunikation mit unsicheren Netzen – etwa dem Internet – geleitet und kontrolliert. Das ULD auditiert dieses Firewall-System. Die Bestandsaufnahme im Rahmen des Auditverfahrens hat ergeben, dass das Konzept dieses Systems gut durchdacht und umgesetzt worden ist. Die Defizite in der Sicherheitsdokumentation werden zurzeit nach den Vorgaben des ULD behoben. Hierzu wurde ein Dokumentationsrahmen erarbeitet, der von den Administratoren der Stadt Flensburg mit den erforderlichen Inhalten ausgefüllt wird.

Was ist zu tun?
Die Stadt Flensburg führt den vielversprechenden Weg einer datenschutzkonformen Dokumentation ihres Firewall-Systems zu Ende.

9.2 Datenschutz-Gütesiegel

9.2.1 Abgeschlossene Gütesiegelverfahren

2006 konnten wir zahlreichen Produkten ein Datenschutz-Gütesiegel verleihen. Fünf Produkte wurden erstmalig zertifiziert. Fünf weitere Produkte wurden nach Fristablauf der ersten Zertifizierung in einem vereinfachten Verfahren rezertifiziert.

Das hohe Interesse an Rezertifizierungen zeigt, dass das Gütesiegel den Herstellern einen **echten Wettbewerbsvorteil** bietet. Zwar blieben die absoluten Zertifi-

zierungszahlen etwas hinter denen des Vorjahres zurück, doch weisen Ankündigungen von Herstellern darauf hin, dass 2007 aller Voraussicht nach eine spürbare Steigerung der Anträge zu verzeichnen sein wird.

Im Einzelnen wurden folgende Produkte **neu zertifiziert**:

- Verfahren zur Vernichtung von Akten und Datenträgern durch die recall Deutschland GmbH,
- e-health.solutions, Version 4.0: Ein klinisches Datenmanagement, das der Integration medizinischer IT-Systeme im Krankenhaus dient und den Workflow am klinischen Arbeitsplatz unterstützt,
- Verfahren der Akteneinlagerung der recall Deutschland GmbH: Im Rahmen eines Auftrags zur Akteneinlagerung erfolgt gemäß dem jeweiligen Schutzbedarf sowohl die reine Archivierung von Akten als auch das Bereitstellen einer externen Akten-/Archivhaltung mit Anforderungsmöglichkeit durch den Kunden,
- Modul „EVA Beitrag“ der „Erweiterten Verwaltungsanwendung – EVA“, Version 2.09: Hierbei handelt es sich um eine Branchenlösung für Industrie- und Handelskammern, die zentral bei der IHK-GfI gehostet und IHKn zur Verfügung gestellt wird; das Modul EVA Beitrag dient der Verwaltung, Veranlagung und Erhebung von Beiträgen,
- Verfahrensregister 2.1 der FinanzIT GmbH: Dient der Unterstützung des betrieblichen Datenschutzbeauftragten bei der Erstellung und Verwaltung eines Verfahrensregisters.

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

- TightGate-Pro, Version 1.2: Softwaresystem mit VNC-Server, der unter einem gehärteten Betriebssystem eine rollenbasierte Rechtevergabe zur sicheren und datenschutzgerechten Internetanbindung von Verwaltungsarbeitsplätzen ermöglicht,
- RDA – Regionale Digitale Automation, Version 2: Verfahren zur Kommunikation und revisionssicheren Langzeitarchivierung von digitalen medizinischen Bildern und Befundberichten,
- Vernichtung von Akten, Datenträgern und Mikrofilmen durch die Firma Reisswolf Akten- und Datenvernichtung GmbH & Co. KG, Hamburg, im Auftrag für Auftraggeber aus dem öffentlichen und nicht öffentlichen Bereich,
- dataport Firewall Altenholz, Version 31.03.2006: Schutz der Resssourcen im Netzwerk der dataport gegen unberechtigte Zugriffe aus dem Internet durch Einschränken der Verbindungen von und zum Internet auf zulässige Dienste,
- Opti.List Professional, Version 7: Archivierung steuerrechtlich relevanter Drucklisten auf Grundlage der Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) sowie der Abgabenordnung.

Es ist festzustellen, dass in einigen Bereichen, in denen ein Hersteller ein Gütesiegel verliehen bekommen hat, auch die **Konkurrenz nachzieht** und Interesse anmeldet. So beweisen auch diese Hersteller ihr besonderes Engagement im Bereich Datenschutz. Zugleich wird dadurch eine generelle Hebung des Datenschutzniveaus in einem Marktsegment erreicht, ohne dass hierfür aufsichtsrechtliche Maßnahmen ergriffen werden müssen.

Weitere Informationen für Hersteller befinden sich im Internet unter

www.datenschutzzentrum.de/guetesiegel/infos_hersteller.htm

Was ist zu tun?
Die Hersteller von Produkten sind weiterhin auf die Vorzüge des Gütesiegels hinzuweisen. Die Verbreitung dieses Instrumentes zur Steigerung des Datenschutzbewusstseins bei den Herstellern sollte auf deutscher und internationaler Ebene vorangetrieben werden.

9.2.2 Erstes Gütesiegel für die Firma Microsoft

Ende 2006 schlossen wir das erste Gütesiegelverfahren zu einem Service der amerikanischen Firma Microsoft ab. Damit wurde diesem Service ein werbewirksames, gutes Zeugnis ausgestellt. Das ULD konnte Erfahrungen bei der Bearbeitung von Großverfahren sammeln, die uns künftig nützlich sein werden.

Zertifiziert wurden die Produkte **Microsoft Updateservice** 6.0 (MU) und **Microsoft Windows Server Update Service** 2.0 (WSUS). Beide dienen dazu, Updates für verschiedene Versionen des Betriebssystems Windows sowie anderer Software der Firma Microsoft bereitzustellen, auf Abruf zum Client zu übermitteln und dort zu installieren. Einzelnutzer verbinden sich in der Regel direkt mittels der Updatefunktion ihrer Windows-Installation mit diesem MU und bekommen so ihre Updates installiert. Bereitgestellt werden durch Microsoft derzeit Updates für die Betriebssysteme Windows 2000, Windows XP und Windows 2003 Server sowie für die Anwendungssoftware Office XP/2003, Exchange Server 2003, SQL Server 2000 und MDSE (Datenbankmodul). Da solche Updates häufig Sicherheitslücken schließen, ist eine zeitnahe und weitestgehend automatisierte Verteilung wichtig.

Größere Stellen und Organisationen haben die Möglichkeit, selbst eine Art Updateserver zu betreiben, der z. B. die Verteilung der **Updates innerhalb eines Firmennetzwerkes** nach Test und Freigabe übernimmt. Was wie verteilt wird, entscheidet dann der Administrator dieses Netzwerkes. Durch diese Eingriffsmöglichkeit verbleibt die Autonomie

? ***Update und Patch***

Ein Software-Update ist eine Nachlieferung von Software, die Programmfehler behebt und meist auch kleinere Programmverbesserungen umfasst. Werden dadurch vorrangig Sicherheitslücken geschlossen, spricht man auch von Patches oder Hotfixes.

über die Softwarekonfiguration bei der Daten verarbeitenden Stelle. Dieses Verfahren ist – im Gegensatz zu früheren Verfahren, die keine Eingriffsmöglichkeiten vorsahen (26. TB, Tz. 6.4) – datenschutzrechtlich nicht zu beanstanden. Um so einen eigenen Updateservice anzubieten, betreiben diese Großkunden den WSUS-Server. Nur dieser verbindet sich mit dem MU von Microsoft und bekommt die Updates übermittelt, die er dann in einem zweiten Schritt an die Einzelrechner im lokalen Netzwerk weiterverteilt und entsprechende Protokolle erstellt.

Begutachtet wurden MU und WSUS durch TÜV IT und die Firma 2B Advice. Im Ergebnis wurde festgestellt, dass beide Systeme den in Schleswig-Holstein geltenden Datenschutzgesetzen entsprechen. Es werden keine personenbezogenen Daten der Nutzer **über die Erbringung des Dienstes hinaus** gesammelt. Sofern Identifikatoren, wie auch IP-Adressen, für die Verarbeitung bzw. Statistik erforderlich sind, werden diese umgehend, d. h. innerhalb weniger Stunden, wieder gelöscht bzw. anonymisiert. Im Fall des WSUS erfolgt die Weiterverteilung im lokalen Netz ohne Rückmeldung von Details (z. B. Art der Server, Nutzer, Fehler, Lizenznummer usw.) an Microsoft. Einzig die Datenschutzerklärung des Dienstes in Verbindung mit der Webseite von Microsoft entsprach nicht in vollem Umfang den gesetzlichen Vorgaben. Microsoft sagte zu, diese entsprechend zu ändern.

Die **Übergabe des Gütesiegels** erfolgte im Februar 2007 in der Landesvertretung von Schleswig-Holstein in Berlin durch Ministerpräsident Peter Harry Carstensen. Von Microsoft wurde in Aussicht gestellt, weitere Produkte dem Gütesiegelverfahren unterziehen zu wollen.

Weitere Informationen für Hersteller befinden sich im Internet unter

www.datenschutzzentrum.de/guetesiegel/

9.2.3 Sachverständige

Das Interesse an der Anerkennung beim ULD als Sachverständiger ist weiterhin hoch.

In den Gütesiegelverfahren erfolgt die Begutachtung der zu zertifizierenden Produkte durch beim ULD anerkannte Datenschutzsachverständige. Je nach Antrag erfolgt die Anerkennung für den Bereich Recht oder den Bereich Technik. Möglich ist auch bei entsprechender **Qualifikation** eine Doppelzulassung sowie die Anerkennung einer ganzen Prüfstelle. Voraussetzungen für eine Anerkennung sind stets neben der Zuverlässigkeit und Unabhängigkeit der Nachweis der erforderlichen Fachkunde. Diese muss sich gerade auch auf den Datenschutzbereich erstrecken.

Hinzugekommen als **Sachverständige** sind 2006 zwei Prüfstellen, ein Einzelsachverständiger für beide Bereiche sowie zwei Sachverstände im Bereich Recht. Inzwischen sind beim ULD 25 Einzelsachverständige registriert. 12 Sachverständige sind für den Bereich Recht und 8 für den Bereich Technik anerkannt. 5 Sach-

verständige machen beides. Hinzu kommen noch 8 Prüfstellen, von denen 3 für Recht, 3 für Technik und 2 für beides bei uns eingetragen sind. Die Sachverständigen sind verpflichtet, im Abstand von jeweils drei Jahren nach dem Datum der Anerkennung Nachweise über die fortbestehende Qualifikation, also über die Wahrnehmung von Fortbildungen und Workshops zum Erfahrungsaustausch, beizubringen.

Im August 2006 schließlich fand der jährliche **Gutachterworkshop** in Kiel statt. Von dieser Möglichkeit des Erfahrungsaustausches machten 14 Sachverständige Gebrauch. Diskutiert wurden nicht nur aktuelle Erfahrungen mit Neu- und Rezertifizierungen, sondern auch Fragen des Marketings des Gütesiegels wie auch Möglichkeiten der Internationalisierung.

In diesem Zusammenhang wurden die Gutachter erneut darauf hingewiesen, dass **E-Mail-Kommunikation** über aktuelle Gütesiegelverfahren **verschlüsselt** erfolgen kann und dass dies unbedingt anzuraten ist. Schon der Umstand, dass überhaupt ein Gütesiegelverfahren stattfindet, kann ein Betriebsgeheimnis darstellen. Bei den auszutauschenden Dokumenten handelt es sich fast durchgängig um Unterlagen, die nicht in falsche Hände geraten dürfen.

Weitere Informationen für Sachverständige befinden sich im Internet unter


www.datenschutzzentrum.de/guetesiegel/akkreditierungsunterlagen.htm

Was ist zu tun?
Sachverständige sind ein zentraler Baustein im Gütesiegelverfahren und hierfür wichtige Multiplikatoren. Ihr Antrieb, neue Produkte für das Gütesiegelverfahren zu gewinnen, wird vom ULD unbedingt unterstützt.

9.2.4 Werbung für das Gütesiegel

Das Gütesiegel stößt bei seiner Vorstellung auf Messen und sonstigen Veranstaltungen auf zunehmendes Interesse.

Wir nutzen die **Übergaben der Gütesiegel** dazu, medienwirksam auf dieses Instrument hinzuweisen. Hersteller von gütesiegelfähigen Produkten werden von uns hierbei direkt angesprochen. Auf der CeBIT 2006 in Hannover konnten wir Ministerpräsident Peter Harry Carstensen für die Überreichung eines Gütesiegels gewinnen. Weitere öffentliche Übergaben fanden auf der ITeG 2006 in Franfurt, auf der Sommerakademie 2006 in Kiel, auf der Messe S-Fit in Berlin und auf der DMS EXPO in Köln statt.

Bei verschiedenen **Veranstaltungen** konnten wir, meist auf Einladung der Initiatoren, in Vorträgen das Gütesiegel präsentieren, so etwa auf dem Heise Forum der CeBIT 2006, auf der Sommerakademie 2006, bei der Luther Rechtsanwaltsgesellschaft Hamburg oder auch bei einer Veranstaltung der ARGE Daten Wien. Im

Rahmen des Förderprogramms e-Region sind die Projektpartner dazu verpflichtet, mit dem ULD über mögliche Datenschutzprobleme und Lösungen zu sprechen, was zwanglos zu der Frage führt, ob für das geförderte Produkt nicht auch ein Datenschutz-Gütesiegel in Betracht kommt.

Anfang 2006 wurde auch unser neuer **Werbeflyer zum Gütesiegel** erstellt und interessierten Gruppen, wie etwa den Gutachtern, für Werbemaßnahmen zur Verfügung gestellt. Die Gütesiegelwebsite wird insbesondere hinsichtlich Aktualität, Übersichtlichkeit und Internationalisierung überarbeitet.

www.datenschutzzentrum.de/guetesiegel/

Was ist zu tun?
Insbesondere im Hinblick auf die anstehende Internationalisierung des Gütesiegels ist die englischsprachige Werbung auszubauen. Messen und andere Veranstaltungen sind ein geeignetes Forum, um potenziell interessierte Hersteller auf das Gütesiegel hinzuweisen.

9.2.5 Nationale und internationale Aktivitäten im Gütesiegelbereich

Die Bedeutung des Gütesiegelverfahrens wird nicht nur im Inland, sondern auch international immer stärker erkannt.

Im Laufe des Jahres haben wir mit verschiedenen Behörden und Organisationen einen intensiven Austausch über das Gütesiegelverfahren gepflegt. Diese waren an uns herangetreten, um **von unseren Erfahrungen zu profitieren**. Umgekehrt konnten wir bei diesen Gesprächen Anregungen für unser Verfahren mitnehmen. Dies betraf z. B. die Etablierung eines Gütesiegels in Mecklenburg-Vorpommern, das sich immer noch in der Planungsphase befindet. Der dortige Datenschutzbeauftragte will sich an die in Schleswig-Holstein entwickelten Kriterien zur Zertifizierung von Produkten und zur Zulassung von Gutachten anlehnen. Auch die Zulassung von Gutachtern für Datenschutzauditverfahren in Bremen wird sich am schleswig-holsteinischen Zulassungsverfahren orientieren.

Im internationalen Bereich erfolgten Gespräche mit der nationalen französischen Datenschutzaufsicht CNIL (28. TB, Tz. 9.2.6) sowie der nationalen schweizerischen Datenschutzaufsicht. Für das in der **Schweiz** im März 2007 startende Gütesiegelverfahren wurden die Kriterien des ULD inhaltlich übernommen. Umgekehrt konnten wir aus dem dortigen Auditverfahren, das wegen der Einbindung externer Experten stärker formalisiert ist, Anregungen für die eigene Strukturierung gewinnen.

Nicht nur Datenschutzbehörden, auch **andere Organisationen** sind an unseren Erfahrungen mit dem Datenschutz-Gütesiegel interessiert. So erhielten wir für einen Erfahrungsaustausch Besuch von der staatlichen Universität Tsukuba in Tokio, da auch in Japan inzwischen Zertifizierungen durchgeführt werden. Das

dortige System „Privacy Mark“ betrifft vor allem firmeninterne Abläufe und keine Produkte. Im November 2006 nahmen wir auf Einladung der europäischen Datensicherheitsbehörde ENISA an einem Workshop von Zertifizierungsstellen teil, um unsere Konzepte vorzustellen und an einem Positionspapier für die EU-Kommission mitzuarbeiten.

Was ist zu tun?
Der Bundesgesetzgeber ist mit einem wachsenden Bedarf an Gütesiegeln und Auditierungen konfrontiert. Eine nationale Regulierung ist überfällig. Zugleich muss zur Etablierung eines europäischen Gütesiegels die grenzüberschreitende Koordination ausgebaut werden.

10 Aus dem IT-Labor

10.1 Datenschutzkonforme Tests durch Virtualisierung

Administratoren müssen Updates und Patches einspielen, um Betriebssysteme und Anwendungsprogramme auf einem aktuellen Sicherheits- und Funktionsstand zu halten. Die Notwendigkeit dieser Fehlerbehebungen hat in den letzten Jahren qualitativ wie quantitativ stetig zugenommen.

Ein geordnetes Sicherheitsmanagement inklusive Test und Freigabe solcher „Bugfixes“ stellt Administratoren vor Herausforderungen. Viele auf den Markt kommende Programme beinhalten derart viele Funktionen, dass es viele Hersteller, wahrscheinlich aus wirtschaftlichen Gründen, mit dem Testen nicht mehr so genau nehmen. Dies führt dazu, dass nach kurzer Zeit **Korrekturen und Ergänzungen** vorgenommen werden müssen. Relativ unbedenklich sind neue „Hilfe“-Dateien mit zusätzlichen Informationen für Systemverantwortliche und Anwender. Häufiger handelt es sich um Updates zu Sicherheits- oder Funktionsaspekten, die versprochene Funktionen fehlerfrei bereitstellen oder Probleme beheben sollen, die bei der Auslieferung der Software noch nicht bekannt waren. Programme werden jedoch nicht mehr isoliert eingesetzt. Schon in kleinen Netzwerken kommunizieren eine Vielzahl von Verfahren in verschiedener Weise miteinander, sodass eine kleine Veränderung in einem Programm dazu führen kann, dass andere Teile eines Verfahrens nicht mehr fehlerfrei funktionieren. Ein Administrator sieht sich in diesen Fällen gezwungen, ein Programm in einer eigentlich veralteten Version durch zeitaufwendige Backup-Prozesse zurückzuspielen.

Administratoren befinden sich dadurch häufig in einer **Zwickmühle**, in der sie schwerlich korrekt handeln können: Einerseits sind Sicherheitsupdates möglichst schnell zu installieren, um keine Sicherheitsvorfälle durch verzögertes Einspielen zu riskieren. Andererseits sind ausführliche Tests notwendig, um ein Zusammenspiel aller Programme und Systeme nach einem Patch oder einem Update zu überprüfen.

Beim Testen in einer realistischen Umgebung, ohne den Produktivbetrieb zu beeinträchtigen, können sogenannte **Virtualisierungstechnologien** helfen. Als virtuelle Systeme bezeichnet man Computer, die nicht fest an eine bestimmte physikalische Hardware gekoppelt sind. Virtualisierungsprogramme simulieren bzw. emulieren Hardware, z. B. Festplatten und Grafikkarten, und bieten somit eine virtuelle technische Umgebung, in der verschiedene Betriebssysteme installiert und eingerichtet werden können, sodass auf einer einzigen physikalischen Hardware eine Vielzahl von virtuellen Computern arbeiten. In einem solchen „virtuellen Sandkasten“ können gefahrlos neue Programmversionen getestet oder die Auswirkungen von Patches und Updates überprüft werden.

Der Vorteil ist klar: Es kann Hardware eingespart werden. Nicht jedes an einem Verfahren beteiligte System muss physikalisch kopiert als Testsystem bereitgehalten werden. In der täglichen Arbeit bieten virtuelle Maschinen noch einen weiteren Vorteil. Sie sind nicht an reale Geräte gebunden. Die Daten virtueller

Maschinen lassen sich dadurch sichern, dass man simulierte Festplatten und die Konfiguration der virtuellen Umgebung als Dateien auf einer (realen) Festplatte kopiert. Diese Daten können wieder zurückgespielt werden, wenn der **Originalzustand** eines Betriebssystems oder eines Programms wiederhergestellt werden muss. Ein Administrator kann dadurch Software und Updates installieren und testen, ohne anschließend den Computer aufwendig neu zu installieren, falls etwas schiefläuft. Ein Zurückspielen der Dateien einer virtuellen Umgebung reicht, um die virtuelle Maschine in den Ursprungszustand zurückzusetzen.

Die Hersteller stellen ihre Virtualisierungssoftware mit vollem Funktionsumfang kostenlos zur Verfügung. Das ULD hat mehrere Virtualisierungslösungen getestet und auf virtualisierten Systemen Szenarien für Tests und Freigabe gemäß der Datenschutzverordnung durchgeführt. Unser Fazit: Testen war noch nie so einfach wie heute. **Virtualisierte Testumgebungen** sind als Maßnahme nach Stand der Technik anzusehen, um effektive Test- und Freigabeszenarien aufzubauen.

Was ist zu tun?
Administratoren sollten Virtualisierungssoftware einsetzen, um Updates und Veränderungen an Systemen schnell, effektiv und kostengünstig unter verschiedenen Bedingungen zu prüfen.

10.2 Terminalserver

Seit wenigen Jahren besteht der Trend, Programme und Betriebssysteme nicht mehr auf Einzel-PCs, sondern wie zu den Zeiten teurer Großrechner auf einem zentralen Server ablaufen zu lassen. Auf diesen sogenannten Terminalservern arbeiten gleichzeitig eine Vielzahl von Benutzern über preiswerte Arbeits-PCs mit diversen Programmen. Aus Datenschutzsicht ist eine solche zentral verwaltete Rechnerinfrastruktur grundsätzlich zu begrüßen.

Allerdings hat dies einen Haken: Administratoren können mit geringem Aufwand und unerkannt die Sitzungen der Benutzer lesen und steuern. Deshalb muss bei der **Konfiguration der Systeme** einiges beachtet werden.

Bis in die 80er-Jahre gab es meist Großrechner, an denen über einfache Textzeichenterminals gearbeitet wurde. Die Großrechner wurden Ende der 80er-Jahre zunehmend durch grafikfähige PCs ersetzt. Programme liefen nicht mehr auf einem Server, sondern lokal ab. Recht kurzfristig darauf folgte die Phase der PC-Vernetzung. Zu Beginn des neuen Jahrtausends begann wieder ein **Rezentralisierungstrend** zum Terminalserver. Die steigende Komplexität der Programme und Workflows sowie die wachsenden Hardwareanforderungen weckten wieder den Wunsch, Programme und Betriebssysteme nur einmal zentral installieren, konfigurieren und pflegen zu müssen.

Moderne Terminalserverlösungen erfüllen diesen Wunsch, indem sie fast alle Arbeitsumgebungen, wie z. B. den Desktop oder Office-Anwendungen, zentral

bereitstellen. Ein weiterer Vorteil ist die längere Nutzbarkeit der Hardware, denn Computer müssen nur ein Bild anzeigen können, anstatt wie bisher alle Programme lokal auszuführen. Bei einer solch zentralen Lösung ist die sogenannte **Spiegelung** zu beachten: Administratoren oder auch andere Benutzer mit der entsprechenden Berechtigung können sich Sitzungen von Terminalserverbenutzern anzeigen lassen und eventuell sogar aktiv steuern. Dies ist implementiert, um Anwendern möglichst effektiv direkt helfen zu können, ohne physikalisch vor Ort sein zu müssen.

Dieser Service kann aber auch zum Nachteil von Benutzern verwendet werden. Denn mithilfe dieser Funktion können **Benutzeraktivitäten unkontrolliert überwacht** werden – also ohne Protokollierung oder Monitoring oder ohne jedes Mal aktiv gegebene Benutzereinwilligung. Eine betroffene Person bemerkt in solchen Fällen nicht, dass ihr gesamter Bildschirminhalt z. B. beim Administrator dupliziert wird. Dies ist ein Problem bei Mitarbeitern mit Vertrauensstellung, etwa beim Personalrat, bei der Personalabteilung oder bei der Leitung. Im Produkt „Citrix Presentation Server“ sollte gleich die Installation so erfolgen, dass eine Protokollierung und eine Benachrichtigung erfolgen. In einer Dienstvereinbarung muss geregelt sein, mit welchen Konsequenzen zu rechnen ist, wenn diese Konfiguration durch die Administration unerlaubt zurückgesetzt oder umgangen wird.

Kann die Spiegelung nicht kontrolliert werden, so empfiehlt sich bei besonders schützenswerter Datenverarbeitung **keine Terminalserverapplikation**. Nur so lässt sich hinreichend sicher eine Kenntnisnahme Dritter ausschließen.

Was ist zu tun?
Die IT-Abteilung muss für eine saubere Protokollierung und Benachrichtigung bei Terminalserverlösungen sorgen.

10.3 Open Source in der öffentlichen Verwaltung

In München, Wien oder Mannheim, in Form einer kompletten Umstellung oder als sanfte Migration: Open Source setzt sich in Verwaltungen zusehends durch.

Das ULD bemerkt auch in Schleswig-Holstein ein gesteigertes Interesse zum Thema Datenschutz und Datensicherheit beim Einsatz von Open-Source-Programmen. Bei Schulungen der DATENSCHUTZAKADEMIE sowie in Beratungs- und Prüfungsgesprächen steht das Thema oft im Fokus. Vielen IT-Verantwortlichen erscheint schon aus **wirtschaftlichen Gründen** der Einsatz der meistens kostenfrei erhältlichen Programme wünschenswert.

Wie bei kommerziellen Programmen müssen auch beim Einsatz von Open-Source-Software stets die folgenden **Fragen** geklärt werden:

- Erfüllt die Software die in sie gestellten Anforderungen?
- Ist die Software sauber programmiert?

- Handelt es sich um Software aus vertrauenswürdigen Quellen?
- Ist die Pflege und Weiterentwicklung der Software mittelfristig sichergestellt?
- Ist innerhalb der Organisation ausreichendes Wissen zum Betrieb der Software vorhanden?
- Gibt es Dienstleister, die bei Planung, Einführung und Betrieb der Software unterstützen können?

Kritisch betrachtet ist festzustellen, dass diese Anforderungen auch von herkömmlichen kommerziellen Anbietern oft nicht zureichend erfüllt werden. Das ULD setzt seit Jahren selbst quelloffene Software ein. Unsere praktischen Erfahrungen beim Einsatz insbesondere in sicherheitskritischen Bereichen erlauben insgesamt ein **positives Zwischenfazit**. Der Einsatz bereits etablierter und renommierter Open-Source-Software bietet einen deutlichen Sicherheitsgewinn gegenüber kommerzieller Software mit unklarer Dokumentationslage oder Zukunftsperspektive.

Was ist zu tun?
IT-Planer müssen jede Art von Software vor dem Einsatz ausreichend prüfen und dabei die Vor- und Nachteile der unterschiedlichen Lösungen gegeneinander abwägen. Grundsätzliche Vorbehalte gegenüber Open-Source-Software sind nicht gerechtfertigt.

10.4 Online-Banking – auf der Suche nach der sicheren Seite

Bankgeschäfte online abzuwickeln, ist ein verlockender Gedanke. Obwohl entsprechende Verfahren schon seit Jahren von den Banken angeboten werden, zeigen sich viele Bürgerinnen und Bürger nach wie vor besorgt über die Sicherheit solcher Online-Transaktionen.

Das meistverwendete Verfahren zur Authentifizierung beim Online-Banking ist nach wie vor das **PIN/TAN-Verfahren** in seinen unterschiedlichen Varianten. Die unter Sicherheitsaspekten vorzuziehende Alternative HBCI fristet noch immer ein Schattendasein (27. TB, Tz. 10.3), zu aufwendig erscheint Nutzern und Banken die Verwendung einer Chipkarte samt extra Lesegerät. An der Installation der notwendigen Treiber und Programme scheitern technisch weniger versierte Anwender. Die Vorteile des PIN/TAN-Verfahrens hingegen liegen oberflächlich betrachtet auf der Hand: Es wird weder Software noch Hardware benötigt; der Nutzer kann seinen gewohnten Browser unverändert verwenden; man ist vom Rechner unabhängig – PIN/TAN funktioniert auf jedem internetfähigen PC; ein lästiger Kartenleser ist nicht notwendig.

Doch PIN/TAN-Verfahren haben einen Nachteil: Wer Kenntnis von PIN und TAN erlangt, kann die zugehörigen Transaktionen ändern. Das bereitet den Boden für sogenannte Phishing-Angriffe (27. TB, Tz. 10.3) und spezialisierte Würmer. Das **HBCI-Verfahren** mit Chipkarte hingegen setzt auf einen externen Kartenleser, dessen eigentliche Funktion vom PC unabhängig ist. So werden die krypto-

grafischen Berechnungen direkt im Kartenleser ausgeführt, und der Nutzer authentifiziert sich durch seine Chipkarte und eine PIN, die direkt am Kartenleser eingetippt wird. Dabei ist es unerheblich, ob ein Schädling den PC befallen hat: Der Kartenleser kommuniziert über Zertifikate direkt mit der Bank, Fälschungen sind hier nach dem Stand der Technik nicht möglich.

Statt HBCI mit Chipkarte großflächig den eigenen Kunden anzubieten, versuchen die Banken mit allerlei Erweiterungsvarianten das PIN/TAN-Verfahren am Leben zu halten. Mit eTAN, iTAN und mTAN will man den Bedrohungen durch Online-Betrüger begegnen. Doch die neuen Verfahren, die entweder auf spezielle Geräte (eTAN), durchnummerierte TAN-Listen (iTAN) oder das Handy des Nutzers (mTAN) setzen, sind nur eine Behandlung von Symptomen. Phishing-Angriffe, bei denen die PIN und eine gültige TAN ergaunert werden sollen, können zwar unterbunden werden. Angriffe wie das Abhören der Verbindung und Verändern von Inhalten („Man in the middle"-Angriff) sind aber auch mit **erweiterten TAN-Verfahren** möglich. Wie fahrlässig manche Banken beim Online-Banking vorgehen, zeigte im Oktober 2006 die Citibank. Die dort ausgegebenen TAN-Listen enthielten keine reinen Zufallszahlen, sondern wiesen eine Systematik auf, die die Wahrscheinlichkeit, einzelne TANs zu erraten, deutlich erhöhte.

Was ist zu tun?
Das HBCI-Verfahren mit Chipkarte ist mit allen Mitteln zu unterstützen! Kunden sollten sich bei ihren Banken nach HBCI erkundigen und sich nicht scheuen, dieses Verfahren trotz geringfügiger Mehrkosten und größerem Installationsaufwand einzusetzen.

10.5 Identitätsdiebe im Internet?

Zunehmend wenden sich besorgte Bürger an das ULD, die unter ihrem Namen Beiträge in Internetforen finden oder Opfer gefälschter E-Mails geworden sind. Oft ist die Unbedarftheit der Nutzer die Ursache für den Missbrauch ihrer Identität durch andere. Manchmal sind es technische Besonderheiten, die Bürger verunsichern.

- **Fall 1: „Google durchsucht/scannt meine Festplatte!"**

Jemand beklagte sich, dass bei einer Google-Suchanfrage nicht nur Webseiten angezeigt wurden, die das Suchwort enthielten, sondern auch seine privaten Dateien und E-Mails, auf die die Suche zutraf. In der Tat kann Google lokale Dateien des Nutzers analysieren, allerdings nur, wenn die Software „Google Desktop" installiert ist. Und auch dann wird zuerst die Suche im Internet durchgeführt und das dort erhaltene Suchergebnis lokal mit den Treffern auf dem eigenen PC angereichert. Für den Nutzer erscheint dies jedoch als ein einziges Suchergebnis (Tz. 10.7).

- **Fall 2: „Bei Google sieht man alle Seiten, die ich besucht habe!“**

Eine besorgte Dame hatte bei einem Bekannten beobachtet, welche Treffer Google bei der Suche nach ihrer Mailadresse anzeigte. Sie hatte daraufhin den Verdacht, ihr Surfverhalten würde aufgezeichnet. Konkret war dem allerdings nicht so. Vielmehr war die Petentin sehr aktiv in Internetforen, wo sie ihre Beiträge stets mit dem gleichen Nutzernamen und derselben E-Mail-Adresse unterschrieb. Internetsuchmaschinen wie Google listen bei einer Suche nach der betreffenden Mailadresse all diese Seiten auf.

- **Fall 3: „Meine Bekannten erhalten Spam-Mails unter meinem Namen!“**

Wer E-Mails von Bekannten erhält, vertraut im Allgemeinen darauf, dass diese seriös sind. Umso irritierter sind viele Nutzer, wenn sie von den vermeintlichen Adressen bekannter Personen Spam-Mails oder gar Viren erhalten. Dabei ist zu beachten, dass die Angabe des Absenders bei einer E-Mail sehr leicht gefälscht werden kann – vergleichbar mit einem Briefumschlag, auf dessen Rückseite man einen falschen Namen als Absender einträgt. Spam-Versender geben oft falsche und vermeintlich vertrauenswürdige Absenderadressen an, um Nutzer zum Lesen ihrer Nachrichten zu bewegen. Adressenlisten zum Spam-Versand werden oft durch Wurmprogramme generiert, die befallene Rechner nach Mailadressen durchsuchen, z. B. durch Auswertung des E-Mail-Programms. So geraten dann Adressen von persönlich miteinander bekannten Menschen auf die Listen von Spam-Versendern. Diese erzeugen ihre Mails dann, indem sie eine Adresse der Liste als Empfänger, die andere als Absender eintragen.

Diese Fälle zeigen eine spürbare Besorgnis bei Bürgerinnen und Bürgern über den Missbrauch ihrer Identität im Internet. Da viele technische Zusammenhänge für Normalanwender nur schwer zu durchschauen sind, stellen sich manche Bedenken bei Anfragen als glücklicherweise unbegründet heraus. Die genannten Beispiele machen jedoch deutlich, wie **arg- und sorglos manche Nutzer** mit Informationen über ihre Person im Netz umgehen. Dass Beiträge unter demselben Nutzernamen von einer Suchmaschine gefunden werden, sollte keine Überraschung sein; schließlich ist es die Aufgabe einer Suchmaschine, Webseiten anhand von Stichworten zu finden.

Nutzer sollten darauf achten, im Internet unter **Pseudonymen** zu agieren, wenn eine Verkettung von personenbezogenen Informationen mit einfachen Mitteln wie Google verhindert werden soll. Anonymisierungsdienste wie AN.ON können dabei nur unterstützen, denn die Anonymisierung der IP-Adresse bringt nichts, wenn der Nutzer seine echte Mailadresse auf der Zielseite angibt. Einwegmailadressen wie www.temporaryinbox.com helfen hier einen Schritt weiter.

E-Mails sind generell mit Skepsis zu betrachten. Bekannte Absendernamen garantieren keine Vertrauenswürdigkeit. Einzig elektronische Unterschriften, sogenannte digitale Signaturen, können die Authentizität belegen, z. B. mittels GnuPG oder X.509-Zertifikat. Obwohl die meisten Nutzer regelmäßig mit gefälschten Absenderadressen konfrontiert werden, hat sich die Nutzung von digitalen Signaturen noch nicht durchgesetzt.

An den Beispielen und Lösungsmöglichkeiten wird deutlich, dass es dem Nutzer überlassen bleibt, das Maß seiner Anonymität im Netz zu bestimmen. Technische Hilfsmittel, die ein wirkungsvolles Management **verschiedener Online-Identitäten** ermöglichen oder unterstützen, befinden sich noch im Entwicklungsstadium, wie z. B. MozPET. Das ULD ist im Projekt PRIME aktiv an der Entwicklung eines Identitätsmanagers beteiligt (Tz. 8.4). Bis zur Marktreife dieser Werkzeuge bleibt es Aufgabe des Nutzers, stets aufs Neue zu entscheiden, welche Informationen er über sich preisgibt und welches Risiko er damit einzugehen bereit ist.

mozpets.sourceforge.net/

10.6 Google

Aufgrund des enormen Wachstums des World Wide Web ist es den Nutzerinnen und Nutzern nicht mehr möglich, den Überblick über die Vielfalt von Angeboten zu bewahren. Als große Hilfe erweisen sich die Internetsuchmaschinen, von denen sich Google als meistfrequentierte Suchmaschine zum Klassenprimus mauserte. Diese Vormachtstellung zementiert Google durch viele zusätzliche Dienste, die bei Datenschützern auf Argwohn stoßen.

Die Konkurrenz ist groß im Suchmaschinengeschäft. Schon lange reicht es nicht mehr aus, die Nutzer über einen reinen Suchdienst an seine Seite zu binden. Über das Angebot **zusätzlicher Dienste** soll dem Nutzer ein Mehrwert bei Inanspruchnahme geboten werden, damit er der Suchseite treu bleibt. Google hat im Laufe der letzten Jahre eine Reihe von Zusatzdiensten ins Netz gestellt, die nicht nur den Nutzern, sondern auch Google einen Mehrwert in Form von Personendaten bieten. Zu diesen Diensten zählen GMail, Google Desktop, Google Maps, Google Analytics und Google Toolbar.

Für sich genommen weist jeder dieser Zusatzdienste schon ein recht hohes Datenschutzdefizit auf, zumal die erfassten personenbezogenen Daten in den Vereinigten Staaten von Amerika (USA) gespeichert werden. Ernsthafte Befürchtungen begründet allerdings die Vorstellung, dass **sämtliche erhobene Daten** der vielen Dienste von Google zusammengeführt werden. Rechtlich verhindern lässt sich das nicht, da die Verarbeitung in den USA erfolgt, wo keine Datenschutzstandards wie in Europa herrschen.

Dem Nutzer selbst ist dieser **Umstand nicht bewusst**. Er weiß in der Regel nicht, welche Daten von ihm erfasst werden und wo diese dann lagern. Ebenso fehlt das Wissen über die mögliche Zusammenführung von Daten, deren Auswertung und der dadurch qualitätssteigernden Aussagekraft. Hier hilft nur eine klare und ausführliche Unterrichtung der Nutzer über die mögliche Bildung von Metaprofilen und deren Informationsgehalt.

Obendrein genießt Google bei den meisten Nutzern immer noch den **Nimbus eines Underdogs**, der an der Seite des kleinen Mannes steht. Durch das Anbieten von hochwertigen Gratisprogrammen wie Picasa oder Google Earth wird diese

Wahrnehmung gefestigt. Dieser Status ist längst überholt, wie aktuellen Fakten zu dem Unternehmen zeigen (Stand November 2006). Der Internetkonzern beschäftigt weltweit mehr als 5000 Menschen und besitzt zurzeit einen Börsenwert von 120 Milliarden Euro. Alteingesessene Industriekonzerne wie BMW oder DaimlerChrysler besitzen nur ein Drittel des Börsenwertes von Google. Jedem sollte bewusst sein, dass der Internetriese im Kampf gegen seine Konkurrenten keinen Anlass hat, etwas zu verschenken, schon gar nicht den enormen Wert seiner vorliegenden Nutzerdaten.

10.7 Google Desktop

Tausende Dateien schlummern auf den Festplatten unserer PCs – Textdokumente, Bilder und Musik. Der Überblick fällt vielen Nutzern schwer. Der Wunsch nach Helfern im Chaos ist daher groß, und wer sollte solch ein Chaos besser zu ordnen wissen als der Suchmaschinenprimus aus dem Internet: Google?

Viele Nutzer haben ein ungutes Gefühl, wenn Google in ihren privaten Dokumenten stöbert – nicht zu Unrecht: Die Suchmaschine verwaltet die gewonnenen Daten nicht nur auf dem Rechner des Nutzers. Die Theorie ist einfach: Ein Programm auf dem eigenen Rechner durchsucht die eigenen Dateien und kann dem Nutzer später sagen, was wo gespeichert ist. Der Brief ans Finanzamt? Hier! Die Bilder von Omas Hochzeit? Da! Aber der Teufel steckt im Detail. Google Desktop erzeugt bei der Installation für den aktuellen Computer eine weltweit einmalige Identifikationsnummer, eine sogenannte GUID (**Globally Unique Identifier**). Diese Nummer wird nach erfolgreicher Installation an Google gesendet. Des Weiteren wird diese Nummer jedes Mal an Google übermittelt, wenn das Programm nach Updates sucht – also sobald der Rechner eingeschaltet wird und ans Datennetz geht.

Google erfährt so umgehend, welches seiner Schäfchen da ins Internet zurückkehrt. Die GUID bleibt gleich. So ist es völlig egal, ob die Nutzer Anonymitätsdienste verwenden oder fleißig ihre Cookies löschen. Google weiß, sobald der Rechner eine gültige IP-Adresse zugewiesen bekommen hat, welcher seiner Nutzer gerade online ist. Da bei der Übertragung der GUID die vom Provider zugewiesene IP-Adresse als Absender mitgeliefert wird, ist **Google stets im Bilde**, welcher PC aktuell mit welcher IP-Adresse im Internet unterwegs ist.

Ein Nutzer, der seine Cookies gelöscht hat, ist beim erneuten Besuch einer Webseite ein „neuer“ unbekannter Nutzer. Die Seite kann nicht erkennen, ob dieser Rechner schon einmal mit ihr verbunden war oder nicht. Dank Googles GUID weiß zumindest der Suchmaschinenriese, welche PCs da durchs Internet geistern. Von der Erzeugung der GUID wird der Nutzer indes **nicht sonderlich auffällig informiert**. Er muss sich die Information aus der allgemeinen Datenschutzerklärung heraussuchen, die zudem auch nicht selbstständig, sondern erst nach entsprechendem Klick geöffnet wird.

Doch die GUID ist nicht alles, was Google in seiner Desktop-Suche versteckt hat. Seit Version 3 ermöglicht Google Desktop eine Übertragung des angelegten Index auf die Server von Google. Mit dieser Funktion ist es einem Nutzer z. B. möglich, von seinem **Büro-PC** mithilfe von Google Desktop auch in den Dokumenten des **Heim-PC**s zu suchen, da der erforderliche Index auf den Google-Servern im Internet liegt. Damit hat Google – zumindest aus technischer Sicht – Zugriff auf alle Daten, die auf dem Nutzer-PC gespeichert sind, denn schließlich enthält der Index nicht nur Dateinamen, sondern auch den Inhalt der Dokumente, um darin Suchoperationen ausführen zu können. Seitens der US-Behörden gab es bereits Begehrlichkeiten in Bezug auf Internetsuchanfragen bei Google. Es ist eine Frage der Zeit, bis die Google-Desktop-Dateien insofern in den Fokus geraten. Da die fraglichen Server ausschließlich in den USA stehen, ist eine Durchsetzung deutscher Datenschutzansprüche schwieriger als hierzulande – bis praktisch unmöglich.

Ein kleiner Trost besteht immerhin im Beitritt und Bekenntnis Googles zum „**Safe-Harbor-Abkommen**“. Die Datensammlung an sich wird dadurch allerdings nicht weniger problematisch.

Immerhin kann die Funktion zum **Übertragen des Suchindex abgeschaltet** werden. Das sollte man auch unbedingt tun, denn unter der Aktivierung der „Erweiterten Funktionen“ von Google Desktop versteht der Hersteller nicht nur die Kopie des Index auf die eigenen Server. Sollte der Nutzer diese Funktion akti-

vieren, *„verschickt Google Desktop gegebenenfalls Informationen über die […] besuchten Webseiten“* und sammelt *„eine begrenzte Zahl nicht personenbezogener Daten“* des Computers: *„Hierzu gehören […] die Anzahl der […] durchgeführten Suchanfragen sowie die Zeit, die Sie bis zum Anschauen der Ergebnisse brauchen, und Anwendungsberichte, die wir benutzen, um das Programm zu verbessern.“*

Google protokolliert also in aller Deutlichkeit das Online-Verhalten seiner Nutzer. Eine technische Notwendigkeit zur Erfassung z. B. der Betrachtungsdauer von Webseiten lässt sich kaum konstruieren. Der brave Hinweis, die Daten enthielten keinerlei Auskünfte zur Person des Nutzers, ist dabei einfach falsch: Die übertragenen Suchindizes sind schon durch ihren Inhalt eindeutig personenbezogen, und aus Nutzerdaten und GUID lassen sich **exzellente Profile** bilden. Hier versteckt sich Google einmal mehr hinter der Behauptung, ein einzelnes Datum habe keinen Personenbezug. Dass dieser Bezug auf den Rechnern von Google durch Kombination mit anderen, für sich genommen ebenfalls unpersönlichen Informationen leicht hergestellt werden kann, verschweigt der Suchmaschinenriese geflissentlich.

Ein weiteres Problem tritt für Nutzer auf, die die Funktion der Desktop-Suche nicht komplett durchschauen. Ist das Programm auf dem eigenen PC installiert, blendet Google Desktop bei jeder Internetsuche die Fundstellen in lokalen Dateien im Browser ein. Wer nach „Quarkstrudel“ sucht, erhält in seinem Browser zuerst alle Dokumente des eigenen PCs, die den Begriff enthalten, und danach die betreffenden Internetseiten. Dass dabei die eine Hälfte der Ergebnisseite vom **lokalen Programm**, die andere Hälfte vom **Google-Server im Internet** erstellt wird, ist für Normalnutzer nicht ersichtlich. Verunsicherte Bürger, die sich beim ULD meldeten, weil „Google auf ihre Festplatte schauen kann“, waren nicht selten. Tatsächlich kann Google zuerst einmal nicht auf die lokalen Daten zugreifen, sondern blendet diese Ergebnisse mithilfe von Google Desktop lokal ein. Erst wenn die oben beschriebenen „Erweiterten Funktionen“ aktiviert werden, landen die Daten des eigenen PCs wirklich bei Google in den USA.

Wer auf Nummer sicher gehen will, deaktiviert diese Funktion daher oder verwendet eine **andere Software**, die das Gleiche leistet, aber kein so ausgeprägtes „Sendungsbewusstsein“ an den Tag legt.

10.8 Google Toolbar

Spezielle Symbolleisten für Browser – sogenannte Toolbars – bieten die Möglichkeit, Spezialfunktionen zu nutzen, die der Browser von Haus aus nicht bietet. Google hat eine solche Toolbar im Angebot. Und wieder bedeutet die Nutzung für den Anwender ein weiteres Stück Verlust der Privatsphäre.

Mit der Google Toolbar lassen sich **nützliche Aufgaben** erledigen. Das Programm dient als Rechtschreibkontrolle im Browser; es vermag Phishing-verdächtige Webseiten zu markieren und zeigt den „PageRank“ an, die Wichtigkeit einer besuchten Internetseite nach Google-Maßstäben.

Dass die Toolbar nicht irgendein kleines Werkzeug ist, ahnt man schon bei der Installation. Hier weist Google darauf hin, dass zur Ausführung bestimmter Funktionen *„Informationen über besuchte Websites an Google übermittelt werden“*. Mit anderen Worten: Wer die Google Toolbar verwendet, surft fortan mit Beifahrer. Um z. B. den PageRank einer Webseite beurteilen zu können, muss Google wissen, um welche Seite es sich handelt, ebenso, um den Nutzer vor Phishing-verdächtigen Seiten zu warnen. Auf diese Weise entsteht bei Google ein komplettes Bild der **Surfgewohnheiten seiner Toolbar-Nutzer**. Wer wann wohin surft, welche Links er anklickt, wie lange er verweilt, welche Suchbegriffe er verwendet, all das wird protokolliert und übermittelt. Wenn man mithilfe der Toolbar seine Lesezeichen zentral bei Google ablegt, erhält Google auch einen Einblick, für was sich die Nutzer dauerhaft interessieren.

Schaltet man die problematischen Funktionen ab, bleiben Extras wie RSS-Abonnement und Rechtschreibprüfung – Funktionen, die moderne Browser wie Firefox schon von Haus aus mitbringen. Ein wahrer **Mehrwert** der Google Toolbar für den Nutzer bleibt somit **fraglich**.

10.9 Google-Szenario

Das Angebot von Zusatzdiensten ist bei Google sehr umfangreich. Um einen Einblick über die mögliche Zusammenführung von Daten aus verschiedenen Google-Diensten zu erhalten, wird im Nachfolgenden ein Szenario entworfen, wie ein beispielhafter Handlungsablauf eines typischen Internetnutzers aussehen kann. Hierbei wird verdeutlicht, welche Daten an Google fließen und welchen Informationsgehalt sie besitzen.

Der Internetnutzer **Herr Mustermann** schaltet seinen Rechner an. In dem Moment, in dem eine Verbindung zum Internet aufgebaut worden ist, verbindet sich das installierte Programm Google Desktop mit dem Google-Server und übermittelt dorthin seine **eindeutige Kennung** – die sogenannte GUID – inklusive der aktuellen IP-Adresse. Herr Mustermann bekommt davon nichts mit; er ist selbst noch nicht im Internet unterwegs. Da er seine Desktop-Suche im „erweiterten Modus“ betreibt, überträgt das Programm seinen Suchindex – ein Verzeichnis aller Begriffe, die in sämtlichen Dokumenten auf seiner Festplatte vorkommen – an Google. Aus diesen Begriffen lassen sich ohne Weiteres Rückschlüsse auf berufliche und private Interessen von Herrn Mustermann ziehen. Herr Mustermann ist immer noch nicht aktiv im Internet tätig gewesen. Eventuell schaltet er seinen Computer wieder aus, hat aber **ohne sein Wissen** seine bei Google gespeicherten Daten aktualisiert.

Nun ruft Herr Mustermann seinen Browser auf. Dessen Startseite ist die Google-Homepage. Der Browser lädt die Webseite und speichert einen **Cookie**, den er von Google erhält. Der Cookie macht den Browser für den Google-Server fortan wiedererkennbar. Alle Google-Suchaktivitäten von Herrn Mustermann können ab jetzt über die IP-Adresse den bereits erfassten Daten zugeordnet werden. Aber zunächst ruft Herr Mustermann sein **Google-Mail-Konto** ab, um zu erfahren, ob neue E-Mails für ihn eingetroffen sind. Seine GMail-Adresse setzt sich wie bei vielen Nutzern aus Vorname, Nachname und der GMail-Endung zusammen. Dadurch bekommen alle bereits gesammelten Daten einen Namen: Die GUID von Google Desktop und der Cookie im Browser gehören zu Herrn Mustermann und dessen Adresse max.mustermann@gmail.com. Spätestens an dieser Stelle erhalten also Daten bei Google einen Personenbezug, die diesen eigentlich gar nicht aufweisen sollten.

Das E-Mail-Postfach von Herrn Mustermann ist von Google im Vorfeld bereits analysiert worden, sodass er bei der Anzeige der Mails auch **Werbebanner** eingeblendet bekommt, die mit dem Inhalt der Nachrichten korrespondieren.

Herr Mustermann surft und gelangt zu einer Seite, auf der kleine Werbeeinblendungen von „**AdSense**“ angezeigt werden. Dieser Dienst von Google blendet auf

diversen Seiten Werbetexte ein, die sich der Browser von Herrn Mustermann vom Google-Server abholt. Google erfährt zum einen dessen Cookie, zum anderen die angesurfte Webseite. Die besuchte Seite kann Herrn Mustermann direkt zugeordnet werden. Da Herr Mustermann noch schnell wissen möchte, was es Neues in der Welt gibt, ruft er seine persönliche Google-**Nachrichtenseite** auf. Hier hat er voreingestellt, dass ihn nur die Themen Politik International und Sport interessieren. Die Themen Gesundheit und Unterhaltung hat er deaktiviert. Google erfährt an dieser Stelle zunächst, dass Herr Mustermann zurückkehrt, denn auch hier wird sein Google-Cookie ausgelesen und weist ihn gegenüber der Webseite aus. Da Google den Cookie intern bereits mit Herrn Mustermanns Namen verknüpft hat, kann auch sein Verhalten auf der Nachrichtenseite exakt zugeordnet werden. Google erfährt, welche Nachrichten ihn generell interessieren und welche speziellen Artikel aus dem Angebot er anklickt und liest.

Schließlich kommt Herr Mustermann auf die Idee, **maps.google.de** aufzurufen. Kollegen haben ihm erzählt, dass auf dieser Webseite sehr schöne und detailgetreue Karten und Luftaufnahmen von fast der gesamten Erdoberfläche zu sehen sind. Neugierig auf diesen Service agiert Herr Mustermann wie die meisten neuen Nutzer von Google Maps: Er gibt seine eigene Adresse ein, um zu sehen, wie sein Wohnort von oben abgelichtet ist. So kann Google seinem Namen eine Adresse und deren Geokoordinate zuordnen, sofern diese nicht als Mailabspann sowieso schon bei GMail vorliegt.

Fassen wir zusammen: Bei einem beispielhaften Gebrauch von Google-Diensten, wie er oben beschrieben ist, **erhält Google folgende Daten**:

- Den vollständigen Namen plus Adresse und Telefonnummer (GMail, Google Desktop, Google Maps),
- einen Index von Begriffen aus Terminkalender, Adressbüchern, Mails, Dokumenten, Tabellen usw. (Google Desktop),
- Stichworte zu Vorlieben, Interessen, Hobbys auch in Bezug auf Politik, Religion und Sex (Google, Google News, Google Toolbar …).

Diese Darstellung ist nicht vollständig; beim Nutzen von weiteren Google-Diensten können noch mehr Daten erhoben werden. Vorausgesetzt wurde eine **sorglose Nutzung des Internets** durch Herrn Mustermann, die aber durch die meisten Nutzer praktiziert wird.

Angegeben sind die Daten, die von den Google-Diensten erhoben werden. Ein Beweis für deren Zusammenführung und Auswertung jedoch existiert bisher nicht. Es liegt allerdings aus marketingstrategischer Sicht nahe, genau diese Profilbildung durchzuführen, zumal wenn sich ein Unternehmen hieran nicht durch strenge Datenschutzregelungen gehindert sieht. Die entstehenden **Nutzerprofile** sind aufgrund ihres Umfangs und ihrer Qualität vor allem auf dem Werbemarkt **Gold wert**. Der Nutzen, den diese Profile zudem für Regierungsbehörden in den USA besitzen können, ist immens. Das US-Justizministerium hat schon bei Google angeklopft und nach Logdateien gefragt. Auch für eine enge Zusammenarbeit mit der CIA gibt es Hinweise.

11 Europa und Internationales

11.1 Transparenzinitiative – es gibt auch kleine Subventionsempfänger

Mit einer „Europäischen Transparenzinitiative“ will die Europäische Kommission durch Veröffentlichung der Subventionsempfänger eine verbesserte Kontrolle der Verwendung von EU-Geldern erreichen. Dabei darf der Datenschutz nicht ausgeblendet werden.

Anlässlich eines Konsultationsverfahrens nahm die Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland (AGID, jetzt IFK; Tz. 12.3) positiv zu der EU-Initiative Stellung, weil diese den Zielen der **Informationsfreiheit** entgegenkommt. Im Bundesrat stieß die Forderung nach mehr Transparenz dagegen auf Kritik wegen Aufwand und Kosten sowie der Befürchtung einer Verzerrung des Wettbewerbs. Auf Bitte des Europaausschusses des Landtags Schleswig-Holstein legte das ULD dar, dass es die Befürchtungen des Bundesrates nicht teilt und das Ziel einer besseren öffentlichen Kontrolle des Mittelabflusses von Steuergeldern unterstützt (Landtagsumdruck 16/1412).

Doch darf die Veröffentlichung von Betriebsdaten etwa von **Kleinunternehmen** nicht zu einem Verzicht auf die Inanspruchnahme von EU-Geldern führen. Gerade in Schleswig-Holstein erhalten viele Einpersonenbetriebe aus der Landwirtschaft und der Fischerei Hilfen aus Brüssel, auf die diese existenziell angewiesen sind. Hilfebedürftigkeit darf nicht zu Diskriminierungen führen. Die Offenbarung personenbezogener Daten muss mit deren Schutzbedürftigkeit abgewogen werden. Daher plädieren wir dafür, eine Bagatellgrenze einzuführen, unterhalb der die Offenlegung von Subventionen nur noch in aggregierter Form erfolgen soll.

Was ist zu tun?
Im Rahmen der Umsetzung der Europäischen Transparenzinitiative in nationales Recht ist bei Kleinsubventionsempfängern ein Ausgleich zwischen Offenlegung und Datenschutz zu suchen.

11.2 Wettbewerbserhebungen bedürfen keiner Kundendaten

Die Kommission der Europäischen Union möchte für ihre Zwecke viel wissen. Dabei muss sie sich streng an den Grundsatz der Erforderlichkeit halten. Personendaten sind bei Markterhebungen nicht nötig.

Über eine Erhebung bei Energieversorgungsunternehmen sollten **präzise Kundenangaben** zu den Lieferverträgen an die Kommission der Europäischen Union (EU) mitgeteilt werden – unter Androhung gewaltiger Strafen (28. TB, Tz. 11.4).

So schnell die Unternehmen zu aufwendigen sensiblen Angaben gezwungen wurden, so langsam arbeiteten die Mühlen der EU-Bürokratie, nachdem das ULD festgestellt hatte, dass hier offensichtlich eine Verletzung europäischer Datenschutzgrundsätze erfolgt: Ziel der Erhebung war offensichtlich, Marktdaten zu erhalten, um zu beurteilen, inwieweit sich die Energieunternehmen an die Wettbewerbsvorschriften halten. Erst nach mehr als einem Jahr konnte der Europäische Datenschutzbeauftragte (EDSB) mitteilen, dass die Abfrage personenbezogener Daten von Elektrizitätskunden unabsichtlich erfolgt sei. Bei der Datenerhebung habe die EU-Kommission unterschiedliche Fragebögen verwendet. Der verwendete Begriff „Endkunde“ hätte nicht so verstanden werden sollen, dass damit Privatpersonen gemeint wären.

Der EDSB forderte nach längeren Verhandlungen mit der Kommission sicherzustellen, dass die erhobenen personenbezogenen Daten nicht weiterverarbeitet und dass sie gelöscht werden. Die zuständige Generaldirektion Wettbewerb hat sich bereit erklärt, dieser Forderung zu entsprechen. Die vom ULD initiierte Kritik war Anlass für den EDSB, mit der Kommission in einem größeren Zusammenhang die Frage zu diskutieren, in welchem Umfang und unter welchen Umständen Personendaten zur **Bekämpfung von Wettbewerbsverletzungen** erhoben werden dürfen. Die Generaldirektion hat dem EDSB mitgeteilt, dass sie künftig keine Erhebungen vornehmen werde, bei denen der Eindruck entstehen könne, es sollten Daten von Elektrizitätsendkunden erhoben werden.

Was ist zu tun?
Die Ermittlungen der für den Binnenmarkt zuständigen Generaldirektion müssen sich auf die Wettbewerbsunternehmen konzentrieren und dürfen keine Privatkunden erfassen.

11.3 Twinning-Projekt mit der Republik Malta

In Kooperation mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) wirkte das ULD daran mit, hohe Datenschutzstandards in anderen Mitgliedstaaten der Europäischen Union zu etablieren.

Seit Ende der 1990-er Jahre führt die Europäische Kommission sogenannte Twinning-Projekte durch, um die seinerzeitigen 10 Beitrittsländer an die **Rechtsstandards** in den alten 15 Mitgliedstaaten **heranzuführen**. Die Grundidee war, dass eine Behörde aus einem Mitgliedstaat sich als sogenannter Twinning-Partner einer entsprechenden Behörde eines Beitrittslandes annimmt. Das Programm wurde nun auf die weiteren neuen EU-Mitgliedstaaten ausgedehnt. Die Projekte werden von der Europäischen Kommission in Brüssel finanziert. Der Know-how-Transfer findet vor allem durch Kurzzeiteinsätze von Experten aus den alten Mitgliedstaaten statt. Diese reisen in die Beitrittsländer und arbeiten dort für eine gewisse Zeit in der Partnerbehörde mit. Dabei geben sie ihre Fachkenntnisse an die Kollegen weiter. Geeignete Aktivitäten sind Berichte zu bestimmten Themen, Präsentationen vor dem einschlägigen Teilnehmerkreis oder die begleitende Teilnahme an der Verwaltungsarbeit.

Das ULD bewarb sich zusammen mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) erfolgreich auf eine Ausschreibung, bei der es um die Unterstützung der **maltesischen Datenschutzbehörde** und des Büros des maltesischen Premierministers – vergleichbar mit der Staatskanzlei in Schleswig – ging. Das Projekt wurde von Oktober 2005 bis Juni 2006 durchgeführt. In dieser Zeit reisten Experten des ULD, des BfDI und anderer deutscher Datenschutzbehörden nach Malta und gaben dort ihr Fachwissen an die beiden maltesischen Partnerbehörden weiter.

Datenschutz ist für die Republik Malta ein völlig neues Sachgebiet, das erst im Zuge des Beitritts zur Europäischen Union 2004 Bedeutung erlangte. Gleichwohl zeigte sich, dass sowohl der maltesische Datenschutzbeauftragte als auch das Büro des Premierministers bereits von Anfang an sehr erfolgreiche Anstrengungen unternommen hatte, den Datenschutz im Land zu etablieren. Die deutschen Experten konnten von ihren Einsätzen auch viele **Anregungen** für ihre Arbeit wieder **mit nach Hause nehmen**. Über Studienreisen machten sich die mit der Aufgabe betrauten maltesischen Kollegen mit der Umsetzung des Datenschutzes in unterschiedlichen Bereichen der Verwaltung und sonstigen öffentlichen Dienstleistungen in Deutschland bekannt. Ein überaus wichtiger Effekt neben dem im Sommer 2006 erfolgreich abgeschlossenen Projekt war nicht nur der Export deutscher Datenschutz- und Verwaltungsstandards, sondern es vertiefte auch die Zusammenarbeit zwischen den europäischen Datenschutzbehörden.

12 Informationsfreiheit

12.1 Novellierung des IFG-SH

Auf Landesebene soll es ein Umweltinformationsgesetz geben. Nach langwierigen Diskussionen besteht Konsens, dass das bisher geltende Informationsfreiheitsgesetz nicht verändert werden soll.

Zunächst war anlässlich der Umsetzung der Europäischen Umweltinformationsrichtlinie eine Novellierung des Informationsfreiheitsgesetzes (IFG-SH) geplant (28. TB, Tz. 12.1). Kein Verständnis hatten wir dafür, dass damit eine erhebliche Einschränkung des Informationszugangs zu allgemeinen Informationen einhergehen sollte. Es war vorgesehen, das privatrechtliche Handeln von Behörden aus dem Anwendungsbereich herauszunehmen. Außerdem sollte die Transparenz bei Privaten, die für Behörden tätig werden, reduziert werden. Das Signal vom ULD, von den Sachverständigen im Innen- und Rechtsausschuss sowie von vielen anderen, dass eine solche Initiative nicht sachdienlich ist, hat das Parlament bewogen, ein **gesondertes Umweltinformationsgesetz** auf den Weg zu bringen und das allgemeine Informationszugangsrecht unangetastet zu lassen.

Das geplante Umweltinformationsgesetz sieht die umfassende Einbeziehung von privaten Stellen vor, die für die öffentliche Verwaltung tätig werden. Diese sind auskunftspflichtig, wenn sie im Zusammenhang mit der Umwelt öffentliche Zuständigkeiten haben, öffentliche Aufgaben wahrnehmen oder öffentliche Dienstleistungen erbringen und dabei der **Kontrolle der öffentlichen Hand** unterliegen. Eine Kontrolle im Sinne des Gesetzes liegt vor, wenn die Person des Privatrechts bei der Wahrnehmung der öffentlichen Aufgabe bzw. Erbringung der Dienstleistung gegenüber Dritten besonderen Pflichten unterliegt oder über besondere Rechte verfügt. Dies ist z. B. bei einem Kontrahierungs- oder einem Anschluss- und Benutzungszwang der Fall. Für eine Kontrolle im Sinne des Gesetzes genügt es, wenn ein oder mehrere Träger der öffentlichen Verwaltung zusammen Eigentümer des Unternehmens sind, über die Mehrheit der Stimmrechte verfügen oder eine Mehrheit der Mitglieder in den Leitungs- bzw. Aufsichtsorganen stellen.

Bei beabsichtigter Ablehnung des Auskunftsersuchens muss immer eine **Abwägung** mit dem Interesse der Allgemeinheit an einer Offenlegung erfolgen. Es ist also relevant, wenn im Einzelfall die gewünschten Informationen aufgrund von besonderen Interessen der Allgemeinheit offenbart werden sollen.

Was ist zu tun?
Im Interesse der Einhaltung europäischer Standards sollte das geplante Landesumweltinformationsgesetz zügig verabschiedet und umgesetzt werden.

12.2 Wirkungen des Bundes-IFG

Die Verabschiedung des Informationsfreiheitsgesetzes des Bundes hat das Bewusstsein der Bürgerinnen und Bürger für die Informationsfreiheit geschärft; andere Bundesländer sind nachgezogen. Dies sind richtige Schritte in Richtung einer umfassenden Informationsfreiheit.

Anfang 2006 ist das Informationsfreiheitsgesetz des Bundes (Bundes-IFG) in Kraft getreten. Einige Bundesländer sind dem **Signal des Bundes gefolgt** und haben ein eigenes Informationsfreiheitsgesetz verabschiedet, z. B. Hamburg, Bremen, Mecklenburg-Vorpommern und das Saarland. Leider orientieren sich einige dieser Gesetze an dem sehr restriktiven Bundes-IFG. Dieses sieht im Verhältnis zum schleswig-holsteinischen IFG und anderen Landesgesetzen „der ersten Stunde“, die sich bewährt haben, weitergehende Ablehnungsgründe vor (28. TB, Tz. 12.3). Einige Länder stehen der Informationsfreiheit weiterhin vollständig ablehnend gegenüber. Es bleibt zu hoffen, dass auch dort der Bedarf nach mehr Verwaltungstransparenz erkannt wird und die Bürgerinnen und Bürger ihr Recht vermehrt einfordern.

Was ist zu tun?
Eine transparente Verwaltung steht jedem Bundesland gut.

12.3 Öffentlichkeit der IFK- und AKIF-Sitzungen

Die Konferenz der Informationsbeauftragten Deutschlands trifft sich zweimal jährlich und beschäftigt sich mit aktuellen Problemen des Informationszugangs in Deutschland und Europa. Diese Sitzungen werden durch den Arbeitskreis Informationsfreiheit vorbereitet. Auch für diese Sitzungen gelten die Grundsätze der Informationsfreiheit.

Die bisherige Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland (AGID) hat sich durch die Aufnahme weiterer Länder zur Konferenz der Informationsbeauftragten (IFK) gemausert. Für das erste Halbjahr 2007 hat das ULD dort den Vorsitz übernommen. Für die IFK und den vorbereitenden Arbeitskreis (AKIF) wurde ein Modus der Öffentlichkeit von Sitzungen mit folgenden **Kernregelungen** beschlossen:

- Die Sitzungen der IFK und des AKIF sind öffentlich. Interessierte Dritte, die nicht bei den Landes- bzw. beim Bundesbeauftragten beschäftigt sind, können an den **Sitzungen teilnehmen**, haben aber kein Mitspracherecht.
- Zum Schutz des Beratungsgeheimnisses bzw. des Willensbildungsprozesses können die Mitglieder die **Öffentlichkeit** von ihren Sitzungen oder Teilen der Sitzungen **ausschließen**. Diese Entscheidung richtet sich nach dem Informationsfreiheitsgesetz des Landes, in dem die Sitzung jeweils stattfindet, und muss gegenüber den Betroffenen begründet werden.

- **Tagesordnungen und Protokolle** der Sitzungen werden ebenso wie dieser Modus im Internet veröffentlicht. Soweit erforderlich, können schutzbedürftige Ausführungen des Protokolls zu den unter Ausschluss der Öffentlichkeit behandelten Themen von der Veröffentlichung ausgenommen werden.

Weitere Einzelheiten des Modus können im Internet abgerufen werden unter

www.datenschutz.de/informationsfreiheit/index.htm
www.datenschutz.de (Stichwort: Informationsfreiheit)

Was ist zu tun?
Informationsfreiheit wird von den Informationsfreiheitsbeauftragten nicht nur eingefordert, sondern auch praktiziert.

12.4 Einzelfragen

12.4.1 Beliehene sind auskunftspflichtig

Private Unternehmen oder Privatpersonen nehmen vielfach als Beliehene Tätigkeiten für die öffentliche Verwaltung wahr, z. B. die Gutachter des TÜV und Schornsteinfeger. Diese Unternehmen sind genauso wie die öffentliche Hand verpflichtet, Auskunft nach dem IFG-SH zu erteilen.

Beliehene sind nach den Vorschriften des Landesverwaltungsgesetzes Schleswig-Holstein **wie Behörden zu behandeln**. Daraus folgt, dass sie den Bürgerinnen und Bürgern ebenso zur Auskunft nach dem Informationsfreiheitsgesetz verpflichtet sind. Sie können sich insofern nicht auf den Schutz eigener Betriebs- und Geschäftsgeheimnisse berufen. Dieser Schutz dient der Sicherung privatwirtschaftlicher Positionen des Unternehmers, die durch Art. 14 Grundgesetz – das Recht am Eigentum – geschützt sind. Dieser Ausschlussgrund von der Informationspflicht ist Personen des Privatrechts vorbehalten und gilt nicht für Träger der öffentlichen Verwaltung. Erhebt der Beliehene für seine hoheitliche Tätigkeit Gebühren, so sind die Kalkulationsgrundlagen, die den Gebühren zugrunde liegen, auf Antrag offenzulegen.

Was ist zu tun?
Sinn und Zweck des IFG-SH ist eine umfassende Transparenz der schleswig-holsteinischen Verwaltung. Dazu gehören alle Träger der öffentlichen Verwaltung – auch Beliehene.

12.4.2 Betriebs- und Geschäftsgeheimnisse I

Befinden sich in den Unterlagen, in die Einsicht genommen werden soll, Betriebs- und Geschäftsgeheimnisse eines Unternehmens, muss die Behörde sorgfältig zwischen dem Geheimhaltungsinteresse des Unternehmers und dem Offenbarungsinteresse der Allgemeinheit abwägen.

Eine Petentin hatte die Herausgabe der Kalkulationsgrundlagen beantragt, die zur **Genehmigung der allgemeinen Stromtarife** bei der zuständigen Behörde vorgelegt worden waren, sowie die Genehmigung selbst. Die Behörde verweigerte die Herausgabe mit dem Hinweis auf Betriebs- und Geschäftsgeheimnisse.

Der Informationszugang darf nicht verweigert werden, wenn dem Geheimhaltungsinteresse des Unternehmers ein überwiegendes Informationsinteresse der Allgemeinheit gegenübersteht. Es gibt keine grundsätzliche Vermutung zugunsten des Geheimhaltungsinteresses. Der Gesetzesvorbehalt beim grundgesetzlichen Eigentumsschutz ermöglicht diesen Interessenausgleich mit anderen Rechtsgütern. Pauschale Hinweise auf den Schutz von Betriebs- und Geschäftsgeheimnissen sind daher nie ausreichend. Für ein **überwiegendes Offenbarungsinteresse** kann die Aktualität, die Bedeutung des Vorgangs und die Betroffenheit einer Vielzahl von Personen sprechen. Die Behörde muss eine entsprechende Abwägung vornehmen und nachvollziehbar begründen. Eine solche Begründung ist möglich, ohne bereits Betriebs- und Geschäftsgeheimnisse zu offenbaren.

Was ist zu tun?
Eine Ablehnung mit dem pauschalen Hinweis auf Betriebs- und Geschäftsgeheimnisse ist unzulässig. Die betroffene Bürgerin bzw. der betroffene Bürger muss nachvollziehen können, warum der Informationsantrag abgelehnt worden ist.

12.4.3 Betriebs- und Geschäftsgeheimnisse II

Der Schutz von Betriebs- und Geschäftsgeheimnissen muss bei der Befriedigung des Informationsinteresses der Bürgerinnen und Bürger nicht leiden.

Ein Petent bat um Einsicht in den **Energieversorgungsvertrag einer Gemeinde** mit einem Energieunternehmen, was zunächst pauschal mit dem Hinweis auf die Interessen des betroffenen Unternehmens abgelehnt wurde (28. TB, Tz. 12.2.1). Das Unternehmen war über den Antrag auf Informationszugang informiert worden und hatte rechtliche Bedenken geltend gemacht. Wir baten die Gemeinde, über das Vorliegen von die Offenbarung ausschließenden Betriebs- und Geschäftsgeheimnissen im Einzelfall selbst zu entscheiden. Der Betroffene ist zwar anzuhören und kann zur Frage, ob ein Betriebs- und Geschäftsgeheimnis vorliegt, wichtige Informationen liefern. Die Entscheidung liegt aber letztlich bei der Behörde. Bestehen nach Auffassung der Behörde solche Geheimnisse, so muss sie in einem zweiten Schritt eine Abwägung zwischen dem Geheimhaltungsinteresse des Unternehmers und dem Offenbarungsinteresse der Allgemeinheit vornehmen.

Nach erneuter Prüfung gewährte die Gemeinde dem Petenten Einsicht in den Energieversorgungsvertrag vor Ort.

Was ist zu tun?
Behörden haben betroffenen Unternehmern bei Informationsersuchen, die Betriebs- und Geschäftsgeheimnisse betreffen, Gelegenheit zur Stellungnahme zu geben. Sie dürfen jedoch nicht deren Kennzeichnung der Unterlagen bzw. deren Vorgaben ungeprüft übernehmen.

12.4.4 Allgemeine Verwaltungshinweise sind zu veröffentlichen

Häufiges Anliegen der Bürgerinnen und Bürger ist die Einsichtnahme in behördliche Verwaltungsanweisungen. Eine Ablehnung mit dem Argument, diese seien ausschließlich für den internen Gebrauch, kommt immer wieder vor.

Die Auskunftssuchenden erhoffen sich mit der Einsicht in allgemeine Verwaltungshinweise in der Regel Aufschluss über das Zustandekommen eines sie betreffenden Bescheids. Durch diese Zusatzinformationen erschließen sich die für sie **oftmals unverständlichen Gesetzesvorschriften**.

Die Behörden müssen über alle bei ihnen vorhandenen Unterlagen Auskunft geben. Die Unterlagen müssen Bestandteil der eigenen Unterlagen und nicht nur vorübergehend hinzugezogen sein. Auch eine in Kürze vorgesehene Vernichtung kann zur Antragsablehnung führen. Allgemeine Verwaltungsanweisungen sind dagegen für den eigenen Dienstgebrauch bestimmt, **Bestandteil der eigenen Unterlagen** und daher zugänglich zu machen.

Eine Ablehnung der Einsichtnahme ist bei Vorliegen eines **gesetzlichen Ausnahmetatbestands** zulässig. In Betracht kommt hierbei, dass der interne Entscheidungsbildungsprozess der Behörde gefährdet wäre oder eine besondere Geheimhaltungsvorschrift eine vertrauliche Behandlung rechtfertigt. Beides ist im Hinblick auf allgemeine Verwaltungsanweisungen kaum denkbar. Diese müssen daher grundsätzlich herausgegeben werden. Nach einem Hinweis von uns auf die klare Rechtslage werden die Verwaltungshinweise im Regelfall unverzüglich bereitgestellt.

Was ist zu tun?
Die Behörden sollten die Verwaltungshinweise im Internet veröffentlichen. Dies ist die einfachste und effektivste Informationsgewährung sowohl für die Behörden als auch für die Bürgerinnen und Bürger.

12.4.5 Gebührenerhebung im Sozialhilfebereich

Gebühren dürfen – nach dem IFG-SH – Informationssuchende nicht abschrecken. Die Erhebung einer Gebühr in Höhe von einem Euro pro Fotokopie ist nicht angemessen und damit unzulässig. Im Einzelfall kann es geboten sein, von einer Gebühr ganz abzusehen.

Behörden können für die Bereitstellung von Informationen nach dem IFG-SH grundsätzlich Gebühren erheben. Dabei ist jedoch zu beachten, dass nach den allgemeinen kostenrechtlichen Grundsätzen die Gebühr in keinem Missverhältnis zu der von der Behörde erbrachten Leistung stehen darf. Insbesondere darf die Gebühr nicht zu einer Abschreckung der Informationssuchenden und in der Konsequenz zum Nichtgebrauch des allgemeinen Informationsanspruches führen; sie darf **keine prohibitive Wirkung** haben. Insofern ist bei der Herstellung von Kopien zu berücksichtigen, dass hierbei der personelle und sachliche Aufwand in der Regel gering ist. Der Preis für die Herstellung von Kopien bewegt sich bei modernen Kopiergeräten bei ca. 5 Cent pro Seite. Eine pauschale Gebührenerhebung von einem Euro pro Kopie ist nicht gerechtfertigt. Die Gebührenverordnung des Bundes zum Umweltinformationsgesetz (Umweltinformationskostenverordnung) hat aus diesem Grunde verbindlich festgelegt, dass pro Kopie nur 15 Cent verlangt werden dürfen.

Von einer Gebührenerhebung kann ganz oder teilweise abgesehen werden, wenn dies im Einzelfall aus Gründen der Billigkeit oder des öffentlichen Interesses geboten ist. Bei sozial bedürftigen Bürgerinnen und Bürgern, d. h. insbesondere bei Anträgen im Sozialbereich, sollte von der Möglichkeit der Gebührenreduzierung bzw. des **Gebührenerlasses** Gebrauch gemacht werden, um das Recht auf Informationszugang nicht zu beschneiden.

Was ist zu tun?
Die Behörden generell und besonders Sozialbehörden sollten darauf achten, dass eine Gebührenerhebung nicht im Einzelfall zu einer Abschreckung des Betroffenen führt. Für die Erstellung von Kopien sind 15 Cent pro Seite eine grobe Orientierung.

12.4.6 Beanstandung der ARGE unumgänglich

Das Problem des Informationszugangs zu Unterlagen der Arbeitsgemeinschaften nach SGB II, der sogenannten ARGEn, ist nach wie vor ungelöst. Einige ARGEn stellen ohne Diskussion ihre Verwaltungsunterlagen den Bürgerinnen und Bürgern gemäß dem IFG-SH zur Verfügung. Im Fall der Weigerung droht eine Beanstandung.

ARGEn sind sogenannte **Mischbehörden**. Sie führen sowohl Aufgaben der Kommunen als auch Aufgaben der Bundesagentur für Arbeit (BA) aus. Die Anwendbarkeit des IFG-SH ist im Gesetz für diese eigene Art von Behörde nicht ausdrücklich geregelt. Aus rechtlichen Erwägungen, z. B. dem Gesetzeszweck, ergibt sich, dass das IFG-SH für die ARGEn des Landes Schleswig-Holstein gilt (28. TB, Tz. 12.2.8). In zwei Fällen hatten verschiedene ARGEn den Antrag einer Petentin mit dem Hinweis auf die Nichtanwendbarkeit des IFG-SH abgelehnt. Auch ein Anspruch nach dem Bundes-IFG bestünde nicht, da dem Anspruch der Schutz von Betriebs- und Geschäftsgeheimnissen entgegenstünde.

Der Anspruch auf Informationszugang beim Ausschlussgrund „**Betriebs- und Geschäftsgeheimnis**“ ist beim Bundes-IFG restriktiver geregelt als beim IFG-SH. Während das Gesetz des Bundes eine Offenbarung der Unterlagen bei Vorliegen eines solchen Geheimnisses vollständig ausschließt, ist nach dem Gesetz des Landes eine Offenbarung möglich, wenn ein überwiegendes Interesse der Allgemeinheit gegeben ist. Die Frage, welches der Informationsfreiheitsgesetze für die ARGEn in Schleswig-Holstein gilt, kann daher nicht offenbleiben.

Was ist zu tun?
Durch Anweisungen sollte im Interesse der Bürgerinnen und Bürger schnellstmöglich Rechtsklarheit geschaffen werden, dass auf schleswig-holsteinische ARGEn das IFG-SH anwendbar ist.

12.4.7 Informationsfreiheit im ULD

Auch für das ULD gelten die Vorschriften des Informationsfreiheitsgesetzes. Transparenzpflichten bestehen für alle öffentlichen Stellen des Landes Schleswig-Holstein, wenn sie verwaltend tätig werden. Selbstverständlich bleiben das Petentengeheimnis und andere gesetzliche Geheimhaltungspflichten unberührt.

Zwei Antragsteller beantragten beim ULD – unter Berufung auf das IFG-SH – die Übersendung eines Berichts über die **datenschutzrechtliche Prüfung** der Datenverarbeitung bei einer Arbeitsgemeinschaft (ARGE) nach dem SGB II (Tz. 12.4.6). Dem haben wir entsprochen. Hierzu waren wir verpflichtet, weil das IFG-SH auf das ULD Anwendung findet und keiner der dort abschließend aufgeführten Ablehnungsgründe vorlag. Das Gesetz findet auch auf das ULD als Anstalt des öffentlichen Rechts Anwendung, auch wenn dies keine ausdrückliche

Erwähnung im Gesetz findet. Nach der Gesetzesbegründung soll der Geltungsbereich des Gesetzes alle Behörden des Landes Schleswig-Holstein erfassen. Nur der Bereich der Gesetzgebung und der Justiz ist aufgrund eigener Regelungen vom Anwendungsbereich ausgeschlossen.

Das IFG-SH sieht eine Reihe von Ablehnungsgründen vor, die aber allesamt nicht einschlägig waren. Nicht offenbart werden dürfen personenbezogene Daten. Sozialdaten genießen einen darüber hinausgehenden Schutz. **Daten von Petenten** genießen absoluten Vorrang und werden in keinem Fall offenbart. Der Datenschutz generell und das Petentengeheimnis speziell werden bei der Bereitstellung von Informationen nach dem IFG-SH durch das ULD gewahrt. Der angeforderte Bericht über die Prüfungen der Datenverarbeitung bei der ARGE enthielt keine Daten der Leistungsempfänger. Andere Ausschlussgründe lagen nicht vor, sodass wir den Anträgen stattgeben konnten.

Was ist zu tun?
Das ULD gewährt Auskunft und Einsicht nach dem IFG-SH. Dabei ist nicht zu befürchten, dass geheimhaltungsbedürftige Tatsachen, die im Rahmen von Prüfungen, Beratungen und Eingaben zur Kenntnis gelangen, offenbart werden.

13 DATENSCHUTZAKADEMIE: Datenschutz macht Schule!

Die stetige Nachfrage nach Weiterbildungskursen der DATENSCHUTZAKADEMIE Schleswig-Holstein (DSA) demonstriert das wachsende Interesse an qualifiziertem Datenschutzmanagement in Verwaltung und Betrieben, in sozialen und medizinischen Einrichtungen.

Die DATENSCHUTZAKADEMIE ist eine vom ULD und dem **Grenzverein e.V.** seit Jahren gemeinsam und erfolgreich betriebene Einrichtung. Mehrtägige Fortbildungen finden in der Regel in der Nordsee Akademie des Grenzvereins in Leck statt. Das dortige Medienlabor bietet nach einem Redesign der Technik Ende letzten Jahres mit 15 technischen Arbeitsplätzen optimale Schulungsvoraussetzungen insbesondere für die Kurse mit sicherheitstechnischen Schwerpunkten.

Wie in der zentralen Veranstaltung der DATENSCHUTZAKADEMIE, der **Sommerakademie**, in diesem Jahr thematisiert wurde, leistet Datenschutzmanagement mehr als „nur“ Datenschutz: Es ist eine unverzichtbare Unterstützung bei der Optimierung der Organisationsstruktur, der Planung von Arbeitsabläufen, der Strukturierung des IT-Einsatzes, der Entwicklung des Produktangebots und der Außendarstellung des Unternehmens bzw. der Behörde. In hochqualifizierten Kursen der DATENSCHUTZAKADEMIE bietet das ULD in diesem Bereich sinnvollen Support für Firmen und Verwaltungen in Schleswig-Holstein an.

- **Schulungsbetrieb 2006**

Vor allem im technischen Bereich konnte die DATENSCHUTZAKADEMIE ihr Angebot erweitern:

- Mit dem neuen Kurs **„Datenschutz und Datensicherheit für SystemadministratorInnen (DS)“** wurde eine gelungene Mischung aus der Vermittlung theoretischer Grundlagen und Bearbeitung aktueller, praxisrelevanter Sicherheitsproblematiken am Rechner realisiert.
- Auch der neu ins Programm aufgenommene Kurs **„Windows Terminal Server mit Citrix Metaframe 4.0“ (WIN-TS)** stieß auf großes Interesse. Er richtet sich an erfahrene Systemadministratoren, die sich mit den unterschiedlichen weitverbreiteten Terminalservertechnologien der Firmen Citrix und Microsoft vertraut machen wollen. Eben diese Techniken ermöglichen eine erhebliche Konsolidierung des administrativen Aufwands in Verwaltungen – eine Tatsache, die von großem Interesse im Rahmen der anstehenden Reformen im kommunalen Bereich ist und zunehmend sein wird. Detailliert ausgearbeitete Schulungsinhalte und ein intensives Vermittlungskonzept erfüllten die Erwartungen der Kursteilnehmerinnen und -teilnehmer. Diesen standen drei

virtualisierte Systeme zur Verfügung, auf denen unterschiedliche Szenarien durchgespielt wurden. Zusätzlich wurden auf dem serverbasierten Teil der Schulungsumgebung zentrale Systeme simuliert, auf welche die Teilnehmer Zugriff hatten.

- Weitere Schwerpunkte der Akademiearbeit bildeten die Kurse zum betrieblichen Datenschutz. Der **„Grundkurs Bundesdatenschutzgesetz" (BDSG-I)** wurde nach drei regulären Durchläufen wegen der starken Nachfrage ein viertes Mal angeboten. Die Grundzüge des für die Wirtschaft geltenden Datenschutzrechts werden den betrieblichen Datenschutzbeauftragten in handlungsoptimierter und praxisbezogener Form vermittelt. Mit den „sieben goldenen Regeln des Datenschutzrechts" – Rechtmäßigkeit, Einwilligung, Zweckbindung, Erforderlichkeit, Transparenz, Datensicherheit und Kontrolle – erhalten die Teilnehmer klare Wegweiser durch die Fülle gesetzlicher Regelungen.
- Die Kurse „Betriebliches Datenschutzmanagement nach dem Bundesdatenschutzgesetz" (BDSG-II), „Technischer Datenschutz/Systemdatenschutz nach dem BDSG" (SIB) und „IT-Revision" (ITR) rundeten die Angebote im Bereich des **betrieblichen Datenschutzes** ab. Der eintägige ITR-Kurs findet ab 2007 in einer erheblich erweiterten Form als „IT-Sicherheitsmanagement" (ITS) in nunmehr drei Tagen statt. An dem langfristigen Projekt eines bundesweit anerkannten Zertifikats für betriebliche Datenschutzbeauftragte wird weiterhin in Abstimmung mit anderen Datenschutzfortbildungseinrichtungen gearbeitet.
- Zunehmende Sensibilisierung im **medizinischen Bereich** in Bezug auf Chancen und Risiken der elektronischen Datenverarbeitung und -sicherung führten bei den Kursen „Datenschutz im Krankenhaus" (DK) und „Datenschutz in der Arztpraxis" (AR) zu steigender Nachfrage.
- Im Anwendungsbereich des Sozialgesetzbuches (SGB) ist eine kontinuierliche Nachfrage nach Datenschutzfortbildungen zu verzeichnen. Soziale Dienstleister, Wohlfahrtsverbände, Werkstätten für Menschen mit Behinderungen suchten in Inhouse-Veranstaltungen um Schulungen ihrer Mitarbeiterinnen und Mitarbeiter zum **„Datenschutz im Sozialhilfebereich"** nach. Der besonderen Bedeutung dieser Problematik trägt die DSA im kommenden Jahr durch das Angebot von Sonderkursen zu folgenden Themen Rechnung: „Hartz IV/Arbeitslosengeld II", „Das Datenschutzrecht der Kranken- und Pflegekassen", „Kinder- und Jugendhilferecht".

Im Jahr 2006 fanden 30 **Kurse, Seminare und Workshops** statt, in denen 423 Personen (2005: 401) Grundlagen- und Spezialwissen zu einem breit gefächerten Spektrum von Datenschutzfragen erlangen konnten. In insgesamt 11 Sonderkursen vermittelten darüber hinaus die Referentinnen und Referenten der DATENSCHUTZAKADEMIE landesweit 193 (2005: 300) Interessierten ihr Fachwissen.

390 Personen besuchten zusätzlich die Sommerakademie am 28.08.2006 im Kieler Schloss zum Thema **„Mach's gut." „Mach's besser!" Datenschutzmanagement in Betrieb und Verwaltung**.

DATENSCHUTZAKADEMIE vor Ort

Die DATENSCHUTZAKADEMIE führt zu Themen Ihrer Wahl auch Inhouse-Veranstaltungen durch, z. B. zu aktuellen Themen wie

- betriebliches Datenschutzmanagement,
- Datenschutz in (Kommunal-)Verwaltungen,
- Datenschutz im Sozial- und Medizinbereich,
- Datenschutz am PC-Arbeitsplatz,
- E-Government,
- Arbeitnehmerdatenschutz.

Ein Vorteil für Sie: Individuelle und qualifizierte Fortbildung!

Sie bekommen in Absprache mit unseren Referentinnen und Referenten auf *Ihre* Bedürfnisse zugeschnittene kostengünstige und qualifizierte Fortbildung.

Haben Sie Interesse?
Dann setzen Sie sich mit uns in Verbindung unter

E-Mail: akademie@datenschutzzentrum.de
oder telefonisch unter 0431/988-1281.

Weitere Informationen zum Programm der DATENSCHUTZAKADEMIE finden Sie unter

www.datenschutzzentrum.de/akademie

- **Datenschutzzertifikat für Systemadministratorinnen und -administratoren**

2006 konnten – nach gründlicher Vorbereitung durch den Besuch mehrerer DSA-Kurse – fünf erfolgreiche Prüflinge ihr „Datenschutzzertifikat für Systemadministratoren“ in Empfang nehmen. In einer eintägigen Prüfung stellten sie ihr theoreti-

sches und praktisches Know-how zur **datenschutz- und gesetzeskonformen EDV-Betreuung** unter Beweis. Dieses hochspezialisierte Schulungs- und Prüfungsangebot zielt darauf ab, Datenschutz und Datensicherheit in Verwaltung und Privatwirtschaft zu optimieren. Langfristiges Ziel ist es, die vermittelten Kenntnisse zu Standardanforderungen an Systemadministratorinnen und -administratoren zu machen. In der Gesamtkonzeption des ULD sind datenschutzrechtlich zertifizierte Administratorinnen und Administratoren von großer Bedeutung.

- **Jahresprogramm 2007 der DATENSCHUTZAKADEMIE**

März	13.03. - 16.03.	WIN-I	Windows 2003 Sicherheit I	
	19.03. - 21.03.	ITS	IT-Sicherheitsmanagement	*NEU*
	20.03.	BDSG-I	Grundkurs Bundesdatenschutzgesetz	
	21.03.	BDSG-II	Betriebliches Datenschutzmanagement	
	22.03.	SIB	Technischer Datenschutz/ Systemdatenschutz nach BDSG	
	23.03.	PD	Datenschutzgerechtes Produktdesign	*NEU*
April	16.04. - 17.04.	DR	Datenschutzrecht für behördliche Datenschutzbeauftragte	
	18.04. - 20.04.	DT	Datensicherheitsrecht für behördliche Datenschutzbeauftragte	
	24.04. - 25.04.	SIKO	Sicherheitskonzepte erstellen	*NEU*
Mai	02.05.	DWBT	Workshop für betriebliche Datenschutzbeauftragte	
	03.05.	IFG	Das neue Informationsfreiheitsgesetz Schleswig-Holstein	
	08.05.	DK	Datenschutz im Krankenhaus	
	09.05.	AR	Datenschutz in der Arztpraxis	
Juni	11.06.	LDSG-R	Landesdatenschutzgesetz Schleswig-Holstein	
	27.06.	ES	Einführung Datenschutz im Schulsekretariat	
Juli	03.07.	BDSG-I	Grundkurs Bundesdatenschutzgesetz	
	04.07.	BDSG-II	Betriebliches Datenschutzmanagement	
	05.07.	SIB	Technischer Datenschutz/ Systemdatenschutz nach BDSG	
August	27.08.		Sommerakademie „Offene Kommunikationsgesellschaft und Terrorbekämpfung – ein Widerspruch?“	
September	04.09. - 05.09.	WIN-NG	Vista und Longhorn für erfahrene AdministratorInnen	*NEU*
	10.09. - 11.09.	DR	Datenschutzrecht für behördliche Datenschutzbeauftragte	
	12.09. - 14.09.	DT	Datensicherheitsrecht für behördliche Datenschutzbeauftragte	
	26.09. - 27.09.	PA	Führung von Personalakten	

Oktober	04.10. - 05.10.	DS	Datensicherheit und Datenschutz für SystemadministratorInnen	
	08.10. - 10.10.	S	Sozialdatenschutzrecht	
	09.10.	BDSG-I	Grundkurs Bundesdatenschutzgesetz	
	09.10. - 12.10.	WIN-II	Windows 2003 Sicherheit II	
	10.10.	BDSG-II	Betriebliches Datenschutzmanagement	
	11.10.	SIB	Technischer Datenschutz/ Systemdatenschutz nach BDSG	
	30.10. - 01.11	ITS	IT-Sicherheitsmanagement	*NEU*
November	06.11. - 07.11	FW	Firewalls: Theorie und Praxis	*NEU*
	13.11. - 15.11	WIN-TS	Windows 2003 Terminal Server mit Citrix Metaframe 4.0	
	26.11.	SDZ	Prüfung zum/zur Systemadministrator/in mit Datenschutzzertifikat	

- **Aktualisierung der Adressverwaltung**

In einer sorgfältig geplanten und durchgeführten Postkartenaktion wurde 2006 der Adressbestand, den die DATENSCHUTZAKADEMIE in den 13 Jahren ihres Bestehens angesammelt hatte, auf Aktualität überprüft. Aus dem bisherigen Bestand von ca. 5000 Adressaten, die zum Teil nicht mehr existent oder nicht mehr interessiert waren, konnte eine nunmehr aktive Anforderung von 1500 Jahresprogrammen der DSA gewonnen werden. Weiteren 500 Personen/Institutionen werden das Jahresprogramm sowie aktuelle Informationen zur DATENSCHUTZAKADEMIE auf elektronischem Wege übermittelt. Konquenzen sind Kostenersparnis und gestiegene Effizienz. Der Kontakt und die Kooperation mit DSA-Interessenten wird so erheblich verbessert.

Praxisforum

Das neue Angebot der DATENSCHUTZAKADEMIE als Diskussionsrunde aus der Praxis für die Praxis.

Erster Themenvorschlag:
„Wie strukturiere ich meine Dokumentation nach LDSG und DSVO?“

In lockerer Folge werden für Interessenten aus Verwaltung und Wirtschaft praxisrelevante Themen im ULD diskutiert.

Themen und Zeitpunkte sind zu erfahren über die DSA-Mailinglist.

Sommerakademie 2007 ∗ Sommerakademie 2007 ∗ Sommerakademie 2007

Offene Kommunikationsgesellschaft und Terrorbekämpfung – ein Widerspruch?

Terrorismusbekämpfung hat seit dem 11. September 2001 eine neue Dimension gewonnen und verändert zunehmend die Arbeit von Sicherheitsbehörden und unseren Alltag. Die Devise heißt „Kontrolle“: vom biometrischen Personalausweis bis zur Vorratsspeicherung der Telekommunikationsdaten; von der Auswertung der Flug- und Banktransaktionen bis zur Antiterrordatei. Auf Bahnhöfen, in Innenstädten, an Firmentoren und bei Großveranstaltungen findet eine präventive Überwachung der Bürgerinnen und Bürger statt.

Die Bürgerrechte – und mit ihnen das Recht auf informationelle Selbstbestimmung – dürfen nicht auf der Strecke bleiben. Dies muss auch nicht sein. Überwachungslösungen sind manchmal nötig, oft aber unwirksam oder sogar selbst ein Sicherheitsrisiko.

Die Sommerakademie 2007 erörtert die Gründe und Hintergründe von Terrorabwehr und Überwachung, die rechtlichen und technischen Grenzen und bürgerrechtsfreundliche Alternativen.

Welchen Beitrag kann der Datenschutz leisten durch

- grundrechtsfreundliche Verfahren,
- intelligente, datensparsame Technik,
- Wahrung von privat(wirtschaftlich)en Freiräumen,
- Transparenz und demokratische Kontrolle der Kontrolle,
- klare Gesetze und effektive Eingriffsbefugnisse …?

Montag, 27. August 2007,
Hotel Maritim in Kiel

Eingeladen sind interessierte Bürgerinnen und Bürger, Vertreter von Wirtschaft und Behörden sowie Techniker, Juristen und Sicherheitsfachleute. Die Teilnahme ist kostenlos.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstr. 98, 24103 Kiel
Tel.: 0431/988-1200
Fax: 0431/988-1223
E-Mail: akademie@datenschutzzentrum.de

Bitte melden Sie sich an unter

www.datenschutzzentrum.de/sommerakademie

14 Neue Publikationen des ULD

Gemäß dem Landesdatenschutzgesetz gehören Beratung und Information der Bürgerinnen und Bürger über alle Fragen des Datenschutzes und der Datensicherheit zu den Serviceaufgaben des ULD. In Erfüllung dieser Zielsetzung sind auch im Jahr 2006 eine Vielzahl von Publikationen erschienen:

- **„Datenschutzrecht in Schleswig-Holstein“** ist inzwischen in der vierten, überarbeiteten Auflage erschienen. Mit dem Landesdatenschutzgesetz, der Datenschutzverordnung, der Gütesiegelverordnung, den Anwendungshinweisen zum Datenschutz-Behördenaudit, dem Bundesdatenschutzgesetz und dem schleswig-holsteinischen Informationsfreiheitsgesetz ist diese Broschüre das Standardwerk des ULD, das Petenten, Teilnehmern der DATENSCHUTZAKADEMIE und anderen Interessenten kostenlos zur Verfügung gestellt wird.
- Die zweite Auflage der BürgerInnen-Infobroschüre **„Vertraulich“** stellt in Form eines persönlichen Notizbuches viele alltägliche Situationen dar, in denen die Frau und der Mann mit Fragen des persönlichen Datenschutzes befasst sind. Zum Einsatz kommt die kleine Broschüre in der Auslage des ULD-Infostandes in der Kieler Fußgängerzone, der Stadtbücherei und des Bürgerbüros.
- Das Faltblatt **„Datenschutz im Melderecht“** ist – auf den neuesten Stand gebracht – den Meldebehörden des Landes in der gewünschten Stückzahl zur Verfügung gestellt worden.
- Das neue Faltblatt des **„Virtuellen Datenschutzbüros“** informiert in deutscher und englischer Sprache über den gemeinsamen Service von Datenschutzinstitutionen in aller Welt unter www.datenschutz.de und präsentiert das vom ULD administrierte Portal als die meistgenutzte deutschsprachige Datenschutzadresse im Internet.
- **„Datenschutz für Verbraucher“** ist eine gemeinsam mit dem Verbraucherzentrale Bundesverband e.V. (vzbv) herausgegebene, 168-seitige Broschüre. Die positive Resonanz auf die erste Auflage hatte eine zweite, überarbeitete Auflage nötig gemacht. Bürgerinnen und Bürger wie auch Unternehmen werden mit anschaulichen Beispielen über ihre Datenschutzrechte und -pflichten informiert. Praktische Verbrauchertipps geben die Möglichkeit, selbst zu reagieren.
- Die **„Blaue Reihe“** stellt ein neues Publikationsformat des ULD dar. In 15-seitigen DIN-A5-Heften werden aktuelle Themen pointiert, unaufwendig und zeitnah an den Adressaten gebracht. Bisher sind erschienen:
  - Videoüberwachung
  - Hartz IV
  - Verbraucherdatenschutz
  - Verbraucher-Scoring

  Beim diesjährigen Schleswig-Holstein-Tag sowie beim Fest zur Deutschen Einheit am 3. Oktober in Kiel erwiesen sich die prägnanten Themenhefte als Publikumsrenner.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z