SCHLESWIG-HOLSTEINISCHER LANDTAG **Drucksache 16/1839**
16. Wahlperiode 08. April 2008

Bericht

des Unabhängigen Landeszentrums
für den Datenschutz Schleswig-Holstein

Tätigkeitsbericht 2008

Tätigkeitsbericht 2008

des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

Berichtszeitraum: 2007, Redaktionsschluss: 15.02.2008
Landtagsdrucksache 16/1839

(30. 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 2007 – Frust und Lust

1.1 Global, multilateral, national ...

Die Zeiten ändern sich: In der öffentlichen Diskussion werden Sinn und Zweck des Datenschutzes **nur noch selten infrage gestellt** – zu offensichtlich ist, dass mit der Informatisierung unserer Gesellschaft eine größer werdende Gefahr für Privatheit und Individualität der Menschen einhergeht. Lippenbekenntnisse zum Datenschutz sind aber kein Garant für tatsächliches Handeln; oft dienen sie der Verschleierung von den Datenschutz beeinträchtigenden Interessen. Als z. B. von der Bundesregierung das Gesetz zur Neuregelung der Telekommunikationsüberwachung und zur Verpflichtung der Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten als Sieg für die Bürgerrechte verkauft wurde, war dies nicht unbedingt Ausdruck der besonderen Wertschätzung dieser Bürgerrechte (Tz. 4.3.1 und Tz. 7.1).

Die international agierende Bürgerrechtsorganisation Privacy International führte im Jahr 2007 zum zweiten Mal ein weltweites Datenschutzranking mit Noten von 1 (endemische Überwachung) bis 5 (konsistente Beachtung menschenrechtlicher Standards) durch. Während Deutschland im Vorjahr – klar – mit der Note 3,9 den ersten Platz belegte, musste es 2007 diesen Platz an Griechenland abgeben und rutschte mit der Note 2,8 auf Platz sieben ab. Diese **drastische Verschlechterung im Ranking** hat – wie aus der transparenten Bewertung leicht entnommen werden kann – einen Hauptgrund in dem schon erwähnten Beschluss zur Vorratsdatenspeicherung. Es kann keine Rede davon sein, dass Deutschland insofern hier nur eine europäische Pflicht erfüllt hätte. Diese wurde übererfüllt; nur acht von den 27 Staaten hatten im Januar 2007 die Vorgaben der Europäischen Union, die mit höherrangigem europäischem Recht im Widerspruch stehen, bisher umgesetzt.

Privacy International weiß wohl die sehr gute verfassungsrechtliche und gesetzliche Sicherung des Datenschutzes in Deutschland zu würdigen, wenn die Organisation feststellt, dass unser Datenschutzgesetz **eines der strengsten weltweit** ist und die Durchsetzung durch unsere Aufsichtsbehörden wohl am effektivsten erfolgt. Doch dann muss sie berichten, dass Deutschland eine der höchsten Telekommunikationsüberwachungsraten Europas aufweist, mit der Speicherung von Fingerabdrücken in Pässen (Tz. 4.1.3) begonnen und eine – trotz Protesten – stark zunehmende Videoüberwachung (Tz. 5.8) hat.

@ www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597

Tatsächlich droht es Deutschland, wenn die Entwicklung so fortgesetzt wird, vom Datenschutzmusterknaben nach hinten durchgereicht zu werden. Diese Feststellung darf und soll nicht als routinemäßiges Wehklagen professioneller Daten-

schützerinnen und Datenschützer verstanden werden, sondern basiert auf objektivierbaren Befunden. Während sowohl die Datenschutzbehörden und die Rechtsprechung – nicht nur des Bundesverfassungsgerichtes – den Schutz des Rechts auf informationelle Selbstbestimmung zu wahren versuchen, wird dies von Teilen der Politik, der Gesetzgebung und der Praxis in Wirtschaft wie Verwaltung **skrupellos ignoriert**: Trotz begrenzender Rechtsprechung wird die sogenannte heimliche Online-Durchsuchung – ohne Rücksicht auf technische Fakten und grundrechtliche Erwägungen – vorangetrieben (Tz. 4.2.4), wurden Protestierende gegen den G-8-Gipfel in Heiligendamm mit einschüchternden Überwachungsmaßnahmen überzogen, werden Jedermannkontrollen, etwa im Luft- (Tz. 11.1) oder im Straßenverkehr (Tz. 4.2.1), forciert. Hierbei erweist sich der Bundesinnenminister als besonders rücksichtslos. In dessen Windschatten sind aber viele am Werk, deren Namen und Wirken durch die medialen Vorstöße des Bundesinnenministeriums öffentlich weniger wahrgenommen werden.

Datenschutzpolitik wird längst nicht mehr nur national bestimmt. **Europa** steht bei praktisch sämtlichen IT-Großprojekten Pate. Dies beginnt mit der Dienstleistungsrichtlinie, geht über die Subventionierung im Landwirtschaftsbereich (Tz. 9.1.1) und Festlegungen zum Binnenmarkt und zum Verbraucherschutz und endet noch lange nicht bei der Gewährleistung der inneren Sicherheit und der Kriminalitätsbekämpfung. In Sachen Datenschutz hat sich einiges auf europäischer Ebene getan: Die Europäische Datenschutzrichtlinie sichert den Grundrechtsschutz im immer größer werdenden Informationsbinnenmarkt. Die Förderung von datenschutzfördernden Technologien (Privacy Enhancing Technologies – PET), von Organisationsstrukturen, z. B. der unabhängigen Datenschutzaufsicht, und von Verfahren, wie z. B. dem europäischen Gütesiegel (Tz. 9.2.1), wären ohne die Europäische Union (EU) in diesem Umfang und in dieser Qualität sicher nicht möglich. Der europäische Druck hat sich äußerst segensreich bei der Überwindung der deutschen Zurückhaltung hinsichtlich der Verwaltungstransparenz und dem Informationszugang zu Behördenakten (Tz. 12) erwiesen.

Doch ist die europäische Perspektive immer zwiespältig gewesen und bis heute geblieben. Jüngste Entwicklungen lassen darauf schließen, dass das Gewicht des Grundrechtsschutzes in Europa abnimmt. Anders lässt sich nicht erklären, dass es überhaupt zur Richtlinie, die zur Vorratsdatenspeicherung verpflichtet, gekommen ist. Weitere Beispiele sind die seit Jahren im rechtlichen Graubereich agierende Europol-Behörde sowie immer mehr Sicherheitsdatenbanken, von Eurodac über das Schengener Informationssystem bis hin zu der Datenbankvernetzung über den Vertrag von Prüm. Jüngstes Beispiel einer fast ungebremsten **Datensammelbereitschaft für Sicherheitszwecke** sind die Planungen für eine langfristige Speicherung der Passenger Name Records von Flugreisenden (Tz. 11.1). Während bei der „Sicherheit“ die deutsche Präsidentschaft der EU im ersten Halbjahr 2007 immer wieder neue Duftnoten setzte, waren und sind diese in Sachen Datenschutz nicht zu verzeichnen. Die Geschichte eines Rahmenbeschlusses für den Datenschutz im Bereich Justiz und Inneres ist insofern ein trauriges markantes Exempel: Der Datenaustausch für Sicherheitszwecke wird immer weiter ausgebaut; die hierfür nötigen grundrechtlichen, prozessualen und verfahrensmäßigen Sicherungen sind weiterhin nicht in Sicht. Die Unzulänglichkeit der kursierenden Texte nimmt eher zu (Tz. 11.2).

Gegen den demokratischen Versuch einer möglichst weitgehenden Kompetenzausweitung zur **Wahrnehmung wichtiger öffentlicher Aufgaben** ist nichts einzuwenden – sei dies das Bestreben nach mehr Sicherheit, nach höheren Steuereinnahmen oder nach gerechter Verteilung von Sozialleistungen. Doch setzt dies voraus, dass auch tatsächlich eine rationale Debatte auf der Basis der technischen, wirtschaftlichen und sozialen Realitäten geführt wird. Insofern ist es ärgerlich und frustrierend, wenn etwa bei der Bekämpfung der Kriminalität im virtuellen Raum des Internets wie im realen Raum in unseren Städten und auf unseren Straßen einfach nicht zur Kenntnis genommen wird, dass populär präsentable Forderungen nicht den angestrebten Nutzen bringen können und werden, wohl aber die Freiheit in der Gesellschaft insgesamt einschränken. Das Angebot der Datenschützer bestand und besteht: Nach einer ernsthaften Evaluation der Fakten lassen wir uns immer auf eine Debatte über neue technische Maßnahmen und neue gesetzliche Regelungen ein. Wird diese aber verweigert wie aktuell bei der Vorratsdatenspeicherung, so nützen unsere besten Argumente nichts und wir sind mit unserem Latein am Ende. Nur über den **rationalen Diskurs** von Meinung und Gegenmeinung kann man gemeinsam eine bestmögliche Lösung erarbeiten.

Diese **aufklärerische Überzeugung** ist der Hintergrund, weshalb sich das ULD der modernen Sicherheitsforschung nicht verweigert, sondern diese mit zu gestalten versucht (Tz. 8.5). Sie ist die Motivation, die präventiven Mittel zum Datenschutz theoretisch, technisch und praktisch weiterzuentwickeln (29. TB, Tz. 11), aktuell in prominenter Position als Leitung des Projektes zur Umsetzung eines europäischen Datenschutz-Gütesiegels (Tz. 9.2.1). Sie motiviert uns, im engen Dialog mit der Wirtschaft, z. B. mit der Versicherungsbranche (Tz. 5.1), nach den besten Lösungen zu suchen und diese dann auch zu verwirklichen.

1.2 ... und regional

Insofern muss und kann erneut die **Sonderrolle des Landes Schleswig-Holstein** herausgestrichen werden. Während andere Beauftragte für den Datenschutz – mit guten Gründen – die Lage des Datenschutzes in ihrem Land beklagen, finden wir im ULD mit unserem Anliegen des Grundrechtsschutzes zumindest Respekt, teilweise sogar nachhaltige Unterstützung. Die Förderung unseres Gütesiegels, insbesondere durch das Wirtschaftsministerium, aber auch von vielen anderen Ressorts, ist geradezu vorbildlich. Die Bereitschaft und das Interesse des Finanzministeriums, sich bei der Gestaltung der Informationstechnik (IT) in der Verwaltung von uns beraten und sogar auditieren zu lassen, forderte uns oft bis über unsere Belastungsgrenzen. Die Kooperation mit dem Innenministerium bei der Konzeptionierung von Anwendungen des E-Governments lässt kaum zu wünschen übrig.

Zwar gibt es die **klassischen Konfliktlinien** zwischen den Informationsbedürfnissen der Polizei oder der Finanzverwaltung einerseits und dem Datenschutz auf der anderen Seite, doch erweisen sich diese – jenseits der Grundsatzdebatten, z. B. zum Polizeirecht (Tz. 4.2) – in der Praxis als gar nicht so klar. So wie der Datenschutz legitime Informationsbedarfe der Ermittlungsbehörden anerkennt, so verstehen diese, dass der gesetzeskonforme und vertrauliche Umgang mit personenbezogenen Daten eine zentrale Erfolgsvoraussetzung für die eigene Arbeit ist.

So angenehm das politische Klima für den Datenschutz im Lande auch sein mag, so findet dies seine Grenzen bei den **Finanzen**. Wäre die Datenschutzbehörde des Landes im gleichen Maße gewachsen wie die Informationstechnologie, so müsste das ULD heute ein mehrfaches an Ressourcen bekommen, als es tatsächlich zur Verfügung hat. Die Haushaltslage des Landes definiert den engen Rahmen, in dem sich der Datenschutz entfalten muss. Die Wahrnehmung der dauernd wachsenden gesetzlichen Kontroll- und Beratungsaufgaben ist mit den im Landeshaushalt zur Verfügung stehenden Mitteln immer weniger möglich. Dies zeigt sich für das ULD insbesondere im Bereich der Wirtschaft, wo trotz höchstem persönlichem Engagement der Mitarbeiterinnen und Mitarbeiter kaum noch akzeptable Bearbeitungszeiten möglich sind.

Die Situation ist in Schleswig-Holstein insofern nicht so dramatisch wie in anderen Ländern, weil das ULD einen großen Bereich der **Drittmittelfinanzierung** hat. Hierzu gehören die organisatorisch teilweise ausgegliederte DATENSCHUTZAKADEMIE (Tz. 13), die gebührenfinanzierten Audit- und Gütesiegelverfahren (Tz. 9), die Durchführung von EU- oder bundesgeförderten Projekten sowie die kostenpflichtigen Beratungen und Gutachten (Tz. 8). Die derart erzielten Einnahmen ermöglichen die Finanzierung von Mitarbeiterinnen und Mitarbeitern, deren Arbeit über Synergien und Effektivitätssteigerungen auch der klassischen Kontrolle und Beratung zugutekommt. Dennoch: Die dadurch bestehende starke Nachfrageabhängigkeit lässt nur begrenzt Sicherheit und Kontinuität zu – Bedingungen, die im äußerst schnelllebigen Datenschutzgeschäft von großer Bedeutung sind. Das ULD ist bemüht, im Rahmen des Möglichen die Bedingungen zu sichern und weiterzuentwickeln.

2 Großes allgegenwärtiges Unbekanntes: das Internet

Das Spannungsverhältnis zwischen Sicherheit und Datenschutz besteht – trotz Verlagerung von thematischen Schwerpunkten – seit den Anfangszeiten des Datenschutzes. Eine qualitativ neue Herausforderung für den Datenschutz ist dagegen seit über zehn Jahren zunehmend das Internet. Hier spielt sich inzwischen gesellschaftlich und gesellschaftspolitisch ein „Second Life“ (so der Name einer großen globalen virtuellen Spielplattform) ab. Das Netz verdrängt zunehmend die klassischen Mittel der Distanzkommunikation Briefpost und Telefon. Es ersetzt teilweise schon vollständig die klassischen Mittel der gegenständlichen Informationsbeschaffung und schickt sich an, selbst die bisherigen elektronischen Medien – Rundfunk und Fernsehen – zu verdrängen. Sämtliche Lebensbereiche – von der geschäftlichen Tätigkeit über den individuellen Konsum bis hin zur Freizeitgestaltung – werden vom Internet berührt, teilweise schon dominiert.

2.1 Herausforderung für Datenschutz und Politik

Es ist also eine Binsenweisheit, dass persönliche Entfaltung, Individualität, die Wahrnehmung der Freiheitsrechte und das soziale Leben sich immer mehr im und um das Internet abspielen – mit gravierenden Konsequenzen für das Grundrecht auf informationelle Selbstbestimmung: Blieben in der realen Welt bei unseren Betätigungen nur wenige körperliche Spuren (z. B. in Form von Schriftstücken) und eine überschaubare Menge an persönlichen Daten zurück, so hinterlassen praktisch **sämtliche Aktivitäten im Internet ihre elektronischen Spuren**.

Die Zukunft scheint dem digitalen Bürger zu gehören. Nicht der gläserne, d. h. der durchsichtige Mensch ist die absehbare Perspektive, sondern der **digitale Mensch**, neben dessen körperliche und geistige Existenz eine diese abbildende digitale Existenz tritt. Diese digitale Existenz bestimmt – mit dem Bedeutungszuwachs des Internets und der sonstigen elektronischen Lebensbegleiter – unser Denken, unseren sozialen Austausch, unser demokratisches Handeln, die Inanspruchnahme unserer Freiheiten.

Dieser sich derzeit abspielende Wandel ist bis heute noch nicht real ins **Bewusstsein der Politikerinnen und Politiker** gedrungen. Diese erkennen wohl das wirtschaftliche Potenzial des Internets, das sich in Umsatz, Arbeitsplätzen und Gewinnen (aber oft genug auch in Verlusten) niederschlägt. Sie erkennen auch die Gefahren für die Sicherheit, wobei dies vor allem für die augenscheinlichen Auswirkungen z. B. bezüglich der Kriminalität zutrifft. Regelmäßig nicht erkannt werden die strukturellen Sicherheitsrisiken, die sich durch die Abhängigkeit von der neuen Netztechnologie ergeben. Erst langsam zieht daher die Politik die Konsequenzen hinsichtlich der dringend notwendigen Schaffung von umfassenden IT-Sicherheitsinfrastrukturen. Dies ist – sozialisationsbedingt – nur verständlich.

Die Generation der heute Regierenden hat (noch) nicht das Verständnis für die technischen Möglichkeiten und Grenzen der digitalen Vernetzung, da sie das Netz nutzt wie ehedem ihre Schreibmaschine, ihre Bibliothek oder wie noch heute ihr Telefon. Die heutige Jugend hat dagegen das Internet oder auch die Mobilkommunikation in ihr soziales Leben vollständig integriert.

Noch wenig erkennt die Politik daher sowohl die positiven wie die negativen **Potenziale für unsere Freiheiten**. Dies sind nicht nur das Recht auf informationelle Selbstbestimmung und – modern formuliert statt „Fernmeldegeheimnis" – das Telekommunikationsgeheimnis. Vielmehr hat jedes unserer – zumeist aus dem 18. Jahrhundert stammenden – Grundrechte einen informationellen Bestandteil: selbstverständlich die Informations- und Pressefreiheit, aber z. B. auch das Recht auf Religionsfreiheit (z. B. bei Ausübung im Internet), den Schutz des Eigentums (z. B. Schutz von Urheberrechten und geistigem Eigentum), die freie Berufsausübung (nicht zuletzt bei IT-Berufen und mit dem Internet verbundenen Berufstätigkeiten) oder gar auf den Schutz vor politischer Verfolgung (die auch über das Internet möglich ist).

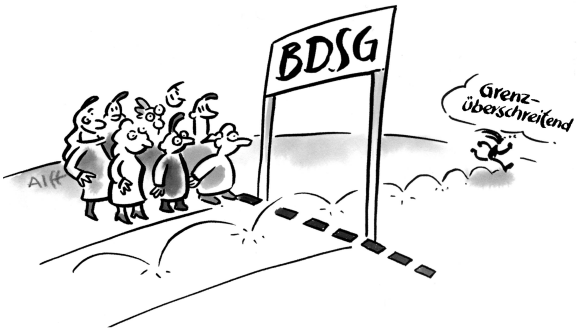
2.2 Neue Instrumente

Angesichts dieses Befundes stellt sich die Frage, ob die digitale Vernetzung unsere Freiheiten nicht nur weiterentwickelt, sondern ob diese nicht auch eine neue eigenständige Qualität bekommen. Dies ist der Ausgangspunkt eines am Horizont auftauchenden neuen Grundrechts – des Rechts auf **Internetfreiheit**. Dieses beinhaltet das Recht der freien Nutzung des Internets, insbesondere zur Kommunikation und zur Informationsbeschaffung. Freie Nutzung bedeutet auch unbeobachtete Nutzung.

Welche praktischen Konsequenzen haben diese Entwicklungen für den Datenschutz? Dieser Frage muss sich die gesamte Gesellschaft immer mehr stellen angesichts der Pflicht zur Vorratsdatenspeicherung, also der langfristigen Aufbewahrung der mehr werdenden digitalen Spuren, und der zunehmenden Quantität und Qualität von personenbezogenen Daten im Internet. Es bedarf einer neuen Kalibrierung des Datenschutzes, wenn globale Unternehmen wie Google oder auch US-amerikanische Geheimdienste einen großen Prozentsatz unserer Netzaktivitäten kontrollieren können. Es macht teilweise ein **Umdenken** nötig, wenn im Netz von unserer gesamten Erde Satellitenbilder bereitgestellt werden, auf denen z. B. erkannt werden kann, dass da jemand im Bikini auf der Veranda meiner Wohnung in der Sonne sitzt. Es macht ein Umdenken nötig, wenn ein Gericht feststellt, dass die anonyme Bewertung durch Schüler von schulischen Lehrkräften im Internet von diesen hingenommen werden muss.

Dem Umdenken muss ein **Umsteuern** folgen. Dieses Umsteuern muss – angesichts der globalen Rahmenbedingungen – **auf technischer Ebene** durch die Schaffung von datenschutzkonformen Angeboten, die Entwicklung und Implementierung datenschutzkonformer Internettechnologien und -infrastrukturen erfolgen. Das ULD arbeitet hieran mit, z. B. durch Teilnahme an zwei internationalen Projekten zum Identitätsmanagement (Tz. 8.2 und 8.3), an einer Expertise zu

Bürgerportalen (Tz. 8.7) oder durch Beiträge zum Datenschutz bei Suchmaschinen (Tz. 7.4). Der Diskussionsbedarf steigt.



Unsere **Gesetze** – in gewisser Hinsicht sogar unser Internetgesetz, das 2007 in Kraft getretene Telemediengesetz – stammen aus der Vorinternetzeit. Das Bundesdatenschutzgesetz (BDSG) ist nicht mehr ansatzweise in der Lage, die Gefahren der Datenverarbeitung für das Persönlichkeitsrecht im globalen Netz zu regulieren. Es ist bereits erkennbar, wie Datenschutz und Privacy-Rechte im Internet rechtlich abgesichert werden können. Hierzu gehören klare und benutzerfreundliche Widerspruchsmöglichkeiten gegen die Datennutzung für Werbung und Marketingzwecke. Rechtliche Anforderungen an die technische Datenlöschung können der „Gnade des Vergessens“ im Internet zum Durchbruch verhelfen. Zur Stärkung des Verbraucherschutzes im BDSG gehören rechtliche Anforderungen an die technische Umsetzung von Korrekturansprüchen einschließlich eines Rechtes auf Gegendarstellung. Weil keiner der Internetuser sich tatsächlich mit allen Details der Datenverarbeitung befassen kann, muss Zertifizierungsmodellen eine größere Rolle zugewiesen werden (Tz. 9). Die Sommerakademie 2008 wird sich dieser Thematik widmen (Tz. 13).

3 Datenschutz im Landtag

Die gute Zusammenarbeit zwischen dem Datenschutzgremium des Landtages und dem ULD ist inzwischen Arbeitsroutine. Hierbei stellen wir gerne unsere Kompetenzen zur Verfügung, etwa wenn es um die **datenschutzgerechte Gestaltung der Telefonanlage** geht. Bei Telefonaten und sonstiger Kommunikation von Abgeordneten muss Vertraulichkeit und Abhörsicherheit besonders groß geschrieben werden. Als Datenlecks im hamburgischen Behördennetz bekannt wurden (Tz. 6.6), informierte das ULD das Datenschutzgremium auf dessen Wunsch hin über die Konsequenzen für das Land Schleswig-Holstein und die Informationstechnik des Landtages.

3.1 Umdruckveröffentlichung

Im Interesse größtmöglicher Transparenz werden Stellungnahmen und allgemeine Eingaben an den Landtag und seine Ausschüsse „verumdruckt", d. h. sie erhalten eine Nummer, werden vervielfältigt und im Internet allgemein zugänglich gemacht. Manchen Absendern solcher Schreiben ist nicht bewusst, dass damit regelmäßig eine Veröffentlichung einhergeht.

Das Internet ist ein ideales Instrument zur Erhöhung der **Transparenz der politischen Arbeit**, vor allem der parlamentarischen Diskussionen. Dieses wird vom Landtag Schleswig-Holstein bewusst und professionell eingesetzt. Ziel ist die umfassende Information der Bevölkerung mit technischen Mitteln geringstmöglicher Beeinträchtigung der Interessierten (25. TB, Tz. 3.2). Oft ist es gerade das Interesse der sich an das Parlament wendenden Verbände, Stellen und Personen, dass ihre Eingabe öffentlich zugänglich gemacht und so zum Ausdruck gebracht wird, dass diese Gegenstand der parlamentarischen Beratung ist.

Das Öffentlichkeitsprinzip kann aber in Konflikt geraten mit dem **Persönlichkeitsschutz** der Menschen, die sich an den Landtag wenden oder über die in den Stellungnahmen berichtet wird. Ab und zu beschweren sich Menschen, dass ihre Zusendung an das Parlament plötzlich über Internetsuchmaschinen weltweit recherchierbar, erschlossen und abrufbar ist. Das Problem ist der Landtagsverwaltung bewusst. Daher weist sie bei der Anforderung von Stellungnahmen darauf hin, dass die Sitzungen der Landtagsausschüsse und die Parlamentsmaterialien öffentlich sind und dass diese Materialien auch im Internetangebot des Landtages der Öffentlichkeit zugänglich sind. Im Übrigen überprüft die Landtagsverwaltung, ob Gründe des Persönlichkeitsschutzes einer Veröffentlichung entgegenstehen. Soweit nötig, etwa bei Gerichtsurteilen, kommt auch eine anonymisierte Veröffentlichung in Betracht. Da die Landtagsverwaltung nicht Adressat, sondern nur Mittler der Schreiben ist, kann von ihr keine vertiefte Abwägung erfolgen, was dann – entgegen dem geheimen Wunsch des Bürgers – zu einer Offenlegung führen kann. Im Einzelfall ist auch eine nachträgliche Löschung bzw. Sperrung veröffentlichter Dokumente möglich. Eingaben an den Petitionsausschuss werden selbstverständlich in einem auditierten Verfahren mit größter Vertraulichkeit behandelt (25. TB, Tz. 3.2).

Möchte ein Bürger nicht, dass seine Eingabe oder Stellungnahme öffentlich verumdruckt wird, so sollte er diese ausdrücklich so **kennzeichnen**. Eine solche Eingabe kann alle Abgeordneten bzw. alle Angehörigen eines Ausschusses auch über eine interne Verumdruckung erreichen.

Was ist zu tun?
Bürger, die sich an den Landtag wenden, sollten es in ihrer Eingabe eindeutig erkennbar zum Ausdruck bringen, wenn sie eine Veröffentlichung als Umdruck nicht wünschen.

3.2 Staatsanwaltliche Vorprüfung gegen Landtagsabgeordnete

Vorabinformationen des Landtages im Fall von staatsanwaltlichen Vorermittlungen sollen eine gesetzliche Grundlage erhalten.

Abgeordnete genießen aus guten Gründen Immunität. Gegen sie dürfen im Interesse des Schutzes vor politisch motivierter Verfolgung nur nach Genehmigung durch den Landtag Ermittlungsmaßnahmen begonnen werden. Hierzu muss der **Landtagspräsident informiert** werden. Wie ist nun in Fällen zu verfahren, in denen die Staatsanwaltschaft bei der Prüfung einer Anzeige keinen Anfangsverdacht feststellt? Eine einfachgesetzliche Rechtsgrundlage für die Unterrichtung des Parlaments besteht in diesen Fällen nicht (29. TB, Tz. 3.2).

In der Praxis nicht ganz selten sind Sammelanzeigen, bei denen das gesamte Parlament oder einzelne Gruppen z. B. wegen ihres Abstimmungsverhaltens angezeigt werden. Für einzelne Abgeordnete können „Ermittlungen“ sehr heikel sein, wenn Informationen über staatsanwaltliche Vorermittlungen bekannt werden, selbst wenn an den behaupteten Vorwürfen nichts dran ist. Der Wissenschaftliche Dienst des Landtages hat dem Parlament einen **Gesetzesvorschlag** gemacht, wonach im Fall eines Vorprüfungsverfahrens sowie bei der staatsanwaltlichen Entscheidung, von der Einleitung eines Ermittlungsverfahrens abzusehen, der Landtagspräsident sowie der Innen- und Rechtsausschuss informiert werden. Außer bei Sammelanzeigen soll künftig regelmäßig auch eine Information der betroffenen Abgeordneten erfolgen.

Was ist zu tun?
Die Annahme des Regelungsvorschlags kann zu mehr Rechtssicherheit für alle Beteiligten bei staatsanwaltlichen Vorermittlungen gegen Abgeordnete führen.

4 Datenschutz in der Verwaltung

4.1 Allgemeine Verwaltung

4.1.1 Online-Meldedatenabruf mit Mängeln gestartet

Ein neues Verfahren für Behörden wie für private Stellen vereinfacht und beschleunigt den Abruf von Meldedaten. Die Inbetriebnahme war ein Kraftakt für die beteiligten Stellen und verursachte erhebliche Datenschutzmängel, deren zugesagte Beseitigung unverzüglich umgesetzt werden muss.

Die Einführung des Online-Meldedatenabrufs von Dataport hat sich verzögert; im November 2007 ist schließlich der offizielle Startschuss gefallen. Zu diesem Zeitpunkt lag allerdings noch nicht die von der Datenschutzverordnung vorgeschriebene Dokumentation vor. Das Fehlen der **Verfahrensbeschreibung**, als „Messlatte“ zwingende Voraussetzung für die notwendigen Funktionstests, hatte besondere negative Folgen. Ohne ausreichende Tests sind keine Aussagen zu eventuellen Mängeln in der Software möglich. Über die nachzuholende Vorabkontrolle, die zunächst auch wegen fehlender Unterlagen nicht erfolgen konnte, werden wir die Sache weiterverfolgen.

- **Datenabruf für Behörden**

Kurz vor dem Start des Verfahrens war noch unklar, auf welche Weise eine Authentisierung der abrufberechtigten Behörden erfolgen sollte. Eine generelle Freischaltung aller Teilnehmer am Landesnetz bzw. an den Kreisnetzen als geschlossene Benutzergruppe musste wegen technischer Probleme auf einen späteren Zeitpunkt verschoben werden. Es blieb nur die Möglichkeit eines **passwortgeschützten Login-Verfahrens**, bei dem durch Dataport zunächst ein sogenannter Master-User bei der abrufberechtigten Behörde freigeschaltet wird. Dieser hat dann in einem Unterauftragsverhältnis das Recht, weitere Mitarbeiter seiner Behörde freizuschalten.

Allerdings wäre es ohne zusätzliche Sicherung möglich gewesen,

- dass Mitarbeiter auch von Zuhause über ihren privaten Rechner Datenabrufe hätten durchführen können oder
- dass der Master-User Personen hätte freischalten können, die nicht Mitarbeiter der Behörde sind.

Um beides auszuschließen, wird auf unsere Forderung hin mit der Anmeldung von Nutzern auch die feste IP-Adresse der jeweiligen Behörde erhoben und voraussichtlich ab dem nächsten Update des Government-Gateways bei Auskünften mit abgeprüft.

- **Polizeiauskunft**

Eigentlich handelt es sich bei der Auskunft an die Polizei nur um eine im Hinblick auf die zu übermittelnden Daten sowie um Listenauskünfte **erweiterte Behördenauskunft**. Um eine komfortable Weiterverarbeitung der Daten im Polizeibereich zu ermöglichen, wurde aber ein eigenständiges Abrufverfahren entwickelt, in welches ein spezielles polizeiliches Modul integriert werden soll, das die Weiterverarbeitung der übermittelten Daten in den polizeilichen Datenbeständen gewährleistet.

Beim Verfahrensstart bestanden insbesondere noch folgende Mängel:

- Der bereits im Jahr 2005 bei der Prüfung des alten Polizeiauskunftsverfahrens festgestellte Fehler, dass zu einer gesuchten Person regelmäßig **alle gespeicherten Daten** übermittelt werden, auch wenn z. B. nur die aktuelle Anschrift benötigt wird, wurde noch nicht beseitigt.
- Es werden Listenauskünfte zugelassen, bei denen die Polizei nach einer unbestimmten Vielzahl von Personen suchen kann, z. B. allen Bewohnern einer Straße, obwohl dafür im Meldegesetz **keine Ermächtigung** vorhanden ist. Eine entsprechende Rechtsänderung ist zwar im Entwurf des Verwaltungsmodernisierungsgesetzes enthalten, befindet sich aber – seit 2006 – noch immer in der parlamentarischen Beratung.

- **Melderegisterauskünfte an Private**

Hier gibt es Probleme beim Verfahren zur Registrierung der Nutzer. Nach dem Melderecht ist eine Registrierung eigentlich nicht erforderlich, da einfache Melderegisterauskünfte an jedermann erteilt werden dürfen. Nur wegen des für die Gebührenzahlung erforderlichen Payment-Verfahrens bedarf es einer **Authentifizierung** der Auskunftsuchenden. Zugelassen ist eine Zahlung durch Lastschriftverfahren ebenso wie durch Kreditkarte. Das Government-Gateway ist allerdings technisch nicht in der Lage, zwischen den Zahlungsarten zu unterscheiden, sodass selbst bei der Kreditkartenzahlung eine Authentifizierung der Nutzer erfolgt, obwohl diese dafür gar nicht benötigt wird. Aus diesem Grund hat man die Möglichkeit einer Vorkassezahlung, die ebenfalls anonym möglich wäre, erst gar nicht weiter geprüft.

Für die Registrierung wird die Notwendigkeit gesehen, dass zur Authentifikation der Nutzer diese unter Vorlage ihres Personalausweises bei einer am Verfahren teilnehmenden Meldebehörde **persönlich** vorsprechen. Während dies für Bürger in Schleswig-Holstein unter Umständen noch mit vertretbarem Aufwand zumutbar ist, dürfte dies für Interessenten aus anderen Bundesländern in der Regel ein Ausschlusskriterium darstellen, was natürlich den Nutzwert des Verfahrens erheblich einschränkt.

Was ist zu tun?
Die an der Einführung des Online-Meldedatenabrufs beteiligten Stellen dürfen nach dem Start des Verfahrens nicht zur Tagesordnung übergehen und müssen die bestehenden „Kinderkrankheiten“ unverzüglich beseitigen.

4.1.2 Melderegistergruppenauskünfte nur bei öffentlichem Interesse

Listenauskünfte aus dem Melderegister für private Stellen haben in der Praxis deutlich zugenommen. Das dafür notwendige öffentliche Interesse muss von den Meldebehörden sorgfältig geprüft werden. Zum Schutz der berechtigten Interessen Betroffener sollte die Auskunft in der Regel mit Auflagen verbunden werden.

Ein örtlicher Freundeskreis zur Erhaltung einer Kirche wollte Mitglieder für einen entsprechenden **Verein** werben, um so die finanziellen Grundlagen für die Renovierung der Kirche zu verbessern. Der ehrenamtliche Bürgermeister hielt dieses Anliegen für eine „gute Sache“ und bat die zuständige Amtsverwaltung um eine sogenannte Gruppenauskunft aus dem Melderegister über die in Betracht kommenden Gemeindemitglieder an den Freundeskreis. Im Meldeamt wurde ohne nähere Prüfung die „gute Sache“ begrifflich dem für die Gruppenauskunft erforderlichen öffentlichen Interesse gleichgestellt. Die anschließend auf der Grundlage der Eingabe eines betroffenen Einwohners durchgeführte Prüfung ergab, dass das öffentliche Interesse im vorliegenden Fall nicht gegeben war.

Unter öffentlichem Interesse ist das Interesse der **Allgemeinheit** zu verstehen, das sich vom Individualinteresse einzelner Personen oder Gruppen abgrenzt. In Betracht kommen insbesondere Datenübermittlungen zum Zwecke der wissenschaftlichen Forschung, soweit diese Forschung aus öffentlichen Mitteln gefördert wird. Rein kommerzielle Interessen, die möglicherweise ein berechtigtes Interesse begründen können, sind dagegen kein öffentliches Interesse. Entsprechendes gilt für die Mitgliederwerbung durch Vereine, und zwar selbst dann, wenn die gesellschaftliche oder kulturelle Bedeutung der Vereinstätigkeit außer Frage steht. Das Interesse liegt in diesen Fällen allein bei dem Verein und nicht bei der Allgemeinheit.

Wird eine Gruppenauskunft aus dem Melderegister erteilt, sind die schutzwürdigen Interessen der Betroffenen zu wahren. Aus diesem Grund sollte bei Datenübermittlungen, z. B. für die wissenschaftliche Forschung, die Erteilung folgender **Auflagen** geprüft werden:

- Die Betroffenen sollten vom Empfänger der Daten auf die **Freiwilligkeit** der Teilnahme an dem Forschungsprojekt schriftlich hingewiesen werden.
- Es sollte eine **Aufklärung** über Inhalt und Zweck der Befragung sowie die beabsichtigte Weiterverarbeitung der Daten beim Forschungsinstitut erfolgen.
- Die übermittelten Daten sollten unverzüglich **gelöscht** werden, falls Betroffene eine Teilnahme am Forschungsvorhaben ablehnen oder auf entsprechende Anfragen nicht reagieren.

Was ist zu tun?
Meldebehörden müssen vor einer Erteilung von Gruppenauskünften sorgfältig prüfen, ob diese tatsächlich im öffentlichen Interesse liegen. Eine Auskunft sollte mit schützenden **Auflagen** verbunden werden.

4.1.3 Fragwürdige Sicherheit bei den neuen biometrischen Pässen

Seit November 2007 werden in Reisepässen Fingerabdrücke als zusätzliches biometrisches Merkmal elektronisch abgespeichert. Für Bürgerinnen und Bürger sind damit neue Datenschutzrisiken verbunden.

Nach den Anschlägen des 11. September 2001 wurde das deutsche Passrecht mehrmals geändert. Ziel war es, den Reisepass sicherer zu machen und mit seiner Hilfe den Schutz vor terroristischen Anschlägen zu verbessern. Zu diesem Zweck werden die Angaben zur Person sowie Gesichtsbild und Fingerabdrücke auf einem Chip im Pass elektronisch gespeichert. Dieser Chip ist mit **Funktechnik** (RFID – Radio Frequency IDentification) auslesbar.

Neue **Datenschutzrisiken** für die Bürgerinnen und Bürger bestehen darin, dass die Passdaten einschließlich biometrischer Angaben nicht nur bei den Behörden, sondern bei Kenntnis der Daten der „maschinenlesbaren Zone“ (MRZ) auch unbemerkt von unberechtigten Dritten ausgelesen werden können, wenn diese mit einem Lesegerät nahe genug an einen ungeschützten Reisepass herankommen. Bei geeigneten Bedingungen ist es möglich, den Ausweis elektronisch zu lesen, wenn der Passbesitzer diesen z. B. in der Hosen- oder Jackentasche mit sich führt.

Welchen Gefahren sind die Bürgerinnen und Bürger bei der Nutzung des Passes ausgesetzt?

Werden die Passdaten über den Funkchip von nicht berechtigten Personen ausgelesen, so können diese auf ein gefälschtes Dokument kopiert werden. Mit diesem Dokument kann dann der Besitzer unter der fremden **Identität** Grenzkontrollen passieren oder sich falsch ausweisen. Möglich ist es auch, eine Person, die ihren Pass mit sich trägt, per Funk zu identifizieren und elektronisch zu verfolgen. Es ist sogar denkbar, dass Kriminelle den elektronischen Pass für einen zielgerichteten Anschlag benutzen, indem sie dessen Funksignal als Auslöser für einen Angriff missbrauchen.

Völlige **Sicherheit** gibt es nicht: Hotels in anderen Staaten können rechtlich verpflichtet sein, Reisepässe vorübergehend einzubehalten. Hierbei lässt sich nicht ausschließen, dass die gedruckten Ausweisangaben mit einem Fotokopierer sowie die Daten auf dem Chip mithilfe eines Scanners ausgelesen und diese dann für

eine Fälschung genutzt werden. Keinen Schutz kann es auch davor geben, dass in einem autoritären Staat die Daten aus dem Reisepass gelesen und gespeichert werden und diese dann zur Überwachung der Person, z. B. während des Aufenthalts in diesem Staat, genutzt werden.

Generell gilt: Als Schutzmaßnahme kann der Reisepass in einer Schutzhülle aus **Aluminiumfolie** aufbewahrt werden. Der dadurch erzeugte sogenannte Faraday-Käfig verhindert das unbemerkte elektronische Auslesen des RFID-Chips, sodass das Speichern für Fälschungen, das Ausspitzeln des Betroffenen sowie das Auslösen von Ereignissen ausgeschlossen wird.

Schutzhüllen sind über das Internet (z. B. https://shop.foebud.org/) sowie ab einer Menge von 10 Stück gegen einen Kostenbeitrag von 6 Euro pro Hülle beim ULD erhältlich. Weitere Hinweise finden sich unter

www.datenschutzzentrum.de/presse/20071031-epass-schutzhuelle.htm

Was ist zu tun?
Der Reisepass sollte nur dann mitgeführt und benutzt werden, wenn dies unbedingt erforderlich ist. Wird der Pass nicht benötigt, so sollte er zu Hause sicher aufbewahrt werden. Er sollte nur aus der Schutzhülle genommen und aus der Hand gegeben werden, wenn gesetzliche Bestimmungen dies z. B. zur Grenzkontrolle oder zur polizeilichen Personenkontrolle erfordern. Im Falle eines Passverlustes sollte dies umgehend der zuständigen Passbehörde gemeldet werden.

4.1.4 Neues Personenstandsrecht erleichtert Familienforschung

Die Änderung des Personenstandsgesetzes führt künftig Personenstandsbücher nach Ablauf gesetzlicher Aufbewahrungsfristen öffentlichen Archiven zu. Diese werden damit insbesondere für die Familienforschung leichter zugänglich.

Das Personenstandsgesetz enthält eine bereichsspezifische Regelung zur Einsichtnahme in Unterlagen der Standesämter, die allgemeinen Vorschriften vorgeht. Einsicht in die Personenstandsbücher, Durchsicht dieser Bücher und Erteilung von Personenstandsurkunden dürfen danach nur von Behörden im Rahmen ihrer Zuständigkeit und von Personen vorgenommen werden, auf die sich der Eintrag bezieht, sowie von deren Ehegatten, Vorfahren und Abkömmlingen. Andere Personen haben nur ein Recht auf Einsicht in die bzw. auf Durchsicht der Personenstandsbücher, wenn sie ein **rechtliches Interesse** glaubhaft machen können. Ein rechtliches Interesse liegt vor, wenn der Antragsteller mit hinreichender Wahrscheinlichkeit darlegen kann, dass die Personenstandsdaten eines anderen zur Verfolgung oder zur Abwehr von Rechten erforderlich sind. Abzugrenzen ist das rechtliche Interesse vom berechtigten Interesse, das auch ideelle, soziale oder wirtschaftliche Interessen erfasst. Gerichte haben dementsprechend festgestellt, dass kein rechtliches Interesse vorliegt, wenn Auskünfte zu privaten Forschungs-

zwecken benötigt werden. Vor diesem Hintergrund war die Ablehnung von Einsichtsanträgen durch Standesbeamte rechtmäßig und von uns nicht zu beanstanden.

Dieses Ergebnis ist aus Datenschutzsicht nicht zwingend. Wenn der Betroffene verstorben ist, ist z. B. ein derart strenger Schutz nicht nötig. Bei der Regelung des Zugangs zu öffentlichen Archiven ist diesem Rechtsgedanken Rechnung getragen worden. Öffentliche Archive dienen der Forschung und Bildung und ermöglichen der Öffentlichkeit die Auseinandersetzung mit Geschichte, Kultur und Politik. Zu diesem Zweck erhält jedermann Zugang zu **öffentlichen Archiven** unter bestimmten Bedingungen, wenn in Unterlagen Daten inzwischen Verstorbener vorhanden sind. Nach dem Landesarchivgesetz darf personenbezogenes Archivgut 10 Jahre nach dem Tod Betroffener oder – wenn das Todesdatum nicht bekannt oder nur mit unvertretbarem Aufwand feststellbar ist – 90 Jahre nach deren Geburt genutzt werden. Ist weder ein Todes- noch ein Geburtsdatum feststellbar, endet die Schutzfrist für personenbezogenes Archivgut 60 Jahre nach Entstehung der Unterlagen.

Aus unserer Sicht ist es gerechtfertigt, die Unterlagen der Standesämter entsprechend den Grundsätzen des Archivrechts zugänglich zu machen. Es handelt sich um Unterlagen der Verwaltung, die von erheblichem Interesse für die **Familienforschung** sind. Werden diese in ein öffentliches Archiv aufgenommen, besteht ein Einsichtsrecht nach dem Archivrecht, wenn die Schutzfristen abgelaufen sind. Die grundsätzlichen Voraussetzungen dafür hat der Bundesgesetzgeber jetzt durch die Novellierung des Personenstandsgesetzes geschaffen. Danach endet künftig die Pflicht zur Fortführung der Personenstandsregister nach Ablauf folgender Fristen:

- für Eheregister und Lebenspartnerschaftsregister 80 Jahre,
- für Geburtenregister 100 Jahre und
- für Sterberegister 30 Jahre.

Nach Ablauf dieser Fristen sind die Personenstandsregister bzw. die Sammelakten den zuständigen öffentlichen Archiven anzubieten. Diese Änderungen werden die Zugangsvoraussetzungen für die Familienforschung verbessern, wenngleich die im Gesetz vorgesehenen **Fristen** großzügiger bemessen sind als die des Archivrechts. Die geänderten Normen treten erst zum Jahresbeginn 2009 in Kraft, sodass es noch einige Zeit dauern wird, bis die Möglichkeit zur Einsichtnahme in Personenstandsdaten in der Praxis Realität wird.

Was ist zu tun?
Die Standesämter sollten zu Beginn 2009 ihre Personenstandsregister, für die keine Pflicht zur Fortführung mehr besteht, unverzüglich den für sie zuständigen öffentlichen Archiven zuführen.

4.1.5 Niederschlagswassereinleitungsgebühr nicht ohne besondere Satzung

Soll eine neue kommunale Abgabe eingeführt werden, ist dafür eine satzungsrechtliche Grundlage zwingend erforderlich. Dies gilt auch, wenn vor Erlass einer solchen Regelung Daten von den Betroffenen zu Kalkulationszwecken erhoben werden sollen.

Eine Gemeinde beabsichtigte die Einführung einer Niederschlagswassereinleitungsgebühr. Die betroffenen Grundstückseigentümer sollten hierfür eine Erklärung über die **bebauten und befestigten Flächen** ihres Grundstückes abgeben. Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn entweder der Betroffene eingewilligt hat oder eine Rechtsvorschrift sie erlaubt. Auch kommunale Satzungen kommen als Befugnisgrundlage in Betracht. Die zuständige Amtsverwaltung musste allerdings einräumen, dass eine Niederschlagswassereinleitungsgebührensatzung für die betreffende Gemeinde noch gar nicht vorlag. Die vorhandene Abwassersatzung kam als Ermächtigung nicht in Betracht, weil sie keinen entsprechenden Gebührentatbestand enthielt.

Wegen fehlender Befugnisgrundlage war die Datenerhebung durch das Amt von uns formell zu **beanstanden**. Die laufende Fragebogenaktion musste bis zum Erlass einer neuen Satzung zurückgestellt werden. Für die Überarbeitung der Satzungsgrundlagen gaben wir folgende Empfehlungen:

- In der Satzung sollte normenklar beschrieben werden, welcher **Zweck** mit der Satzung erreicht werden soll, z. B. „Erhebung einer Niederschlagswassereinleitungsgebühr“.
- Es sollte festgelegt werden, aufgrund welcher **Angaben** eine Berechnung der Gebühr erfolgen soll.
- Ist eine Festlegung des auf den Gebührenmaßstab anzuwendenden **Hebesatzes** noch nicht möglich, weil zwar das beabsichtigte Gesamtgebührenaufkommen, nicht jedoch die umlagefähigen Flächen bekannt sind, so kann dies in der Satzung kurz dargelegt werden mit dem Hinweis, dass der Hebesatz erst in einer späteren Nachtragssatzung festgelegt wird.
- Es sollte klargestellt werden, ob sich das **Veranlagungsverfahren** auf eine bloße Selbsteinschätzung der Betroffenen stützt oder ob und gegebenenfalls in welcher Weise die Angaben verwaltungsseitig kontrolliert werden sollen bzw. können, etwa durch eine Plausibilitätskontrolle unter Heranziehung der Bauakten. Soweit regelmäßig eine Kontrolle vor Ort durch Mitarbeiter der Verwaltung erfolgen soll, müsste auch ein entsprechendes Betretungsrecht für das jeweilige Grundstück in die Satzung aufgenommen werden.

Was ist zu tun?
Kommunen sollten insbesondere bei neuen kommunalen Abgaben oder bei deren Änderung sorgfältig prüfen, ob dafür ausreichende **Satzungsgrundlagen** vorhanden sind. Ist eine Überarbeitung notwendig, sollten die vorstehenden Hinweise beachtet werden.

4.1.6 Behandlung von Bauanträgen und -voranfragen in kommunalen Gremien

Der Ausschluss der Öffentlichkeit bei Sitzungen kommunaler Vertretungskörperschaften steht nicht im freien Ermessen der Mandatsträger. Soweit berechtigte Interessen Einzelner es erfordern, ist die Öffentlichkeit zwingend auszuschließen.

Bei einer Gemeinde sollten Bauanträge und -voranfragen grundsätzlich öffentlich beraten werden. Die Betroffenen waren aufgefordert, der **öffentlichen Beratung** zuzustimmen. Anderenfalls sollten sie ihre berechtigten Interessen schriftlich darstellen, verbunden mit der Aussicht, dass das Vertretungsorgan diese nach Einzelfallabwägung nicht akzeptiert.

Zu den berechtigten Interessen Einzelner gehört insbesondere der Schutz von Persönlichkeitsrechten. Die Verarbeitung personenbezogener Daten – und dazu gehört auch deren Bekanntgabe in öffentlicher Sitzung – steht unter **Erlaubnisvorbehalt** („zulässig, wenn"). Eine generelle Befugnis für die Veröffentlichung personenbezogener Daten existiert nicht.

Bei Bauanträgen und -voranfragen handelt es sich durchweg um Daten aus Verwaltungsverfahren. Die Beteiligten haben nach dem Landesverwaltungsgesetz einen Anspruch darauf, dass ihre Geheimnisse, insbesondere zum persönlichen Lebensbereich gehörenden Vorgänge sowie Betriebs- und Geschäftsgeheimnisse, von der Behörde nicht unbefugt offenbart werden. Als Ermächtigung zur öffentlichen Verhandlung kommt deshalb nur die Einwilligung der Betroffenen in Betracht. Wird diese nicht erteilt, fehlt die notwendige Ermächtigung zur Datenverarbeitung mit der Folge, dass die Interessen Einzelner einen **Ausschluss der Öffentlichkeit** zwingend erfordern. Es bestehen selbstverständlich keine Bedenken dagegen, dass Betroffene selbst an der Sitzung teilnehmen, soweit es lediglich um ihre eigenen Anträge und nicht um die Dritter geht.

Was ist zu tun?
Kommunale Vertretungskörperschaften sollten darauf achten, dass personenbezogene Daten aus Verwaltungsverfahren nur dann in öffentlicher Sitzung beraten werden, wenn dafür eine **schriftliche Einwilligung** der Betroffenen vorliegt.

4.1.7 Unsicherheiten bei Zielvereinbarungen für die leistungsorientierte Bezahlung

Mit der leistungsorientierten Bezahlung im öffentlichen Dienst soll jetzt Ernst gemacht werden. Die notwendigen Instrumente zur Leistungsbemessung gehören zunächst auf den datenschutzrechtlichen Prüfstand.

Die neuen Tarifverträge für den öffentlichen Dienst enthalten erstmalig konkrete Regelungen, wonach in die Gehälter der Mitarbeiterinnen und Mitarbeiter jährlich festzusetzende **erfolgsbezogene Bestandteile** aufgenommen werden sollen. Das bisherige Beurteilungswesen für die Beschäftigten erscheint als Grundlage für die

Leistungsbemessung wenig geeignet. Bisher wurden in der Landesverwaltung praktisch nach jeder Beurteilungsrunde neue Beurteilungsrichtlinien erlassen, weil sich die jeweils geltenden Regelungen offensichtlich nicht ausreichend bewährt hatten. Es hätte zudem einen beträchtlichen Verwaltungsaufwand zur Folge, wollte man jeden Bediensteten jedes Jahr neu formell beurteilen. Viele Verwaltungen sehen deshalb Zielvereinbarungen als Schlüssel zum Erfolg an. In einer Reihe von Fällen wurden damit in der Vergangenheit gute Erfahrungen gemacht. Allerdings waren diese Zielvereinbarungen nicht mit leistungsbezogenen Gehaltsbestandteilen verknüpft.

Diese neue Qualität führt zu einer geänderten rechtlichen Bewertung beim Umgang mit den darin enthaltenen Daten. Wenn Zielvereinbarungen als **individueller Bemessungsmaßstab** bereits rechtsgestaltende Wirkung für das Beschäftigungsverhältnis der Mitarbeiter entfalten, sind sie als sogenannter materieller Bestandteil der Personalakte zu qualifizieren. Das Dienstrecht legt fest, dass alle Unterlagen, die in einem unmittelbaren inneren Zusammenhang zum Dienstverhältnis der Betroffenen stehen, in ihre Personalakte gehören. Die mit Beschäftigten abgeschlossenen Zielvereinbarungen sind damit vertraulich zu behandeln und vor unbefugter Einsicht zu schützen. Eine „verwaltungsöffentliche“ Behandlung solcher Unterlagen scheidet aus.

Problematisch erweisen sich Zielvereinbarungen, die gemeinsam für mehrere Mitarbeiter im Team abgeschlossen werden sollen. In einer Zielvereinbarung mag zwar der Teamfähigkeit eines Mitarbeiters besondere Bedeutung beigemessen werden; eine gleichsam „gesamtschuldnerische“ Verantwortung für eine **Teamleistung** kann jedoch – wenn überhaupt – nur dem jeweiligen Teamleiter bzw. Vorgesetzten, nicht aber einzelnen Teammitgliedern übertragen werden. Die Gehaltszahlung ist schließlich ein Individual- und kein Kollektivanspruch. Die Entscheidung über die Zielerreichung einer Teamleistung wäre automatisch mit der Diskussion von Beurteilungs- und Leistungsdaten statusmäßig gleichgestellter Kollegen untereinander verbunden. Dies allein würde schon einen Verstoß gegen das Personalaktengeheimnis bedeuten. Es ist übrigens ebenso nicht zulässig, dass bisherige Beurteilungen offiziell im Kollegenkreis bekannt gegeben und inhaltlich diskutiert werden. Zielvereinbarungen sollten deshalb nur als individueller Maßstab zur Leistungsbemessung im Rahmen der leistungsorientierten Bezahlung eingesetzt werden.

Was ist zu tun?
Personalverwaltungen sollten darauf achten, dass Zielvereinbarungen im Rahmen der leistungsorientierten Bezahlung vertraulich behandelt und nach deren Abschluss zur Personalakte genommen werden. Auf die Nutzung gemeinschaftlicher Zielvereinbarungen für Teams sollte ganz verzichtet werden.

4.1.8 Kernpunkte des betrieblichen Eingliederungsmanagements

Das durch das Gesetz zur Förderung der Ausbildung und Beschäftigung schwerbehinderter Menschen eingeführte „betriebliche Eingliederungsmanagement" hält zunehmend Einzug in die Verwaltung. Wegen der Sensibilität der zu verarbeitenden Daten ist die Beachtung datenschutzgerechter Rahmenbedingungen unabdingbar.

Das betriebliche Eingliederungsmanagement umfasst alle Aktivitäten, Maßnahmen und Leistungen, die zur **Wiedereingliederung** nach konkreter längerer Arbeitsunfähigkeit erforderlich sind. Sein Ziel ist es, Arbeitsunfähigkeit zu überwinden, erneuter Arbeitsunfähigkeit vorzubeugen, chronische Krankheiten und Behinderungen der Beschäftigten, die am Arbeitsplatz entstehen können, zu vermeiden und den Arbeitsplatz betroffener Mitarbeiter zu erhalten.

Die Durchführung des Eingliederungsmanagements ist von der **Zustimmung** der Betroffenen abhängig und kann von diesen jederzeit widerrufen werden. Da in erster Linie sensible Daten der Mitarbeiter verarbeitet werden, setzt die notwendige Akzeptanz für die Maßnahme bei den Betroffenen einen datenschutzkonformen Umgang voraus.

In der Praxis besteht das zentrale Problem oft darin, dass Mitarbeiter zwangsläufig auch vertrauliche Daten aus dem **persönlichen Umfeld** bzw. Gesundheitsdaten offenbaren müssen, die der Dienststelle sonst nicht bekannt werden würden (z. B. Details über familiäre Schwierigkeiten, Alkoholprobleme und Ähnliches) und die zu nachteiligen Personalentscheidungen der Dienststelle führen könnten. Widerruft der Betroffene seine Einwilligung zum Eingliederungsmanagement, z. B. weil der angestrebte Erfolg nicht eintritt, kann eine physikalische Löschung der inzwischen verarbeiteten Daten verlangt werden. Soweit jedoch personalverantwortliche Mitarbeiter davon Kenntnisse erlangt haben, ist nicht auszuschließen, dass sie diese später gegebenenfalls nachteilig gegen die Betroffenen einsetzen.

Für die Beihilfegewährung, bei der ein ähnlicher **Interessenkonflikt** auftritt, hat das Dienstrecht eine Lösung in der Weise getroffen, dass an Personalentscheidungen beteiligte Mitarbeiter keine Einsicht in die betreffenden Beihilfeunterlagen dieser Mitarbeiter erhalten dürfen. Diese Regelung sollte soweit möglich auf das betriebliche Eingliederungsmanagement übertragen werden. Unmittelbare Vorgesetzte wie auch Mitarbeiter der Personalverwaltung sind vor diesem Hintergrund als Ansprechpartner für das Eingliederungsmanagement denkbar ungeeignet. Mit der Durchführung des Verfahrens sollte die Dienststelle deshalb nur Beschäftigte beauftragen, die im Übrigen nicht bzw. möglichst wenig selbst an Personalentscheidungen beteiligt sind. Es kann sogar daran gedacht werden, den behördlichen Datenschutzbeauftragten zum „**Eingliederungsmanager**" zu bestellen. Wenn der Betroffene durch entsprechende Verfahrensregelungen darauf vertrauen kann, dass seine Daten nicht in belastender Weise gegen ihn verwendet werden, wird er eher bereit sein, die notwendigen Informationen für ein erfolgreiches Verfahren zu liefern.

Die Bestellung eines unabhängigen „Eingliederungsmanagers“ hat gegenüber dem Fachvorgesetzten als Ansprechpartner zudem den Vorteil, dass der nicht unbeträchtliche **Schulungsaufwand** für die ordnungsgemäße Durchführung des betrieblichen Eingliederungsmanagements nur einmal erbracht werden muss; die einzelnen Mitarbeiter werden zudem nach einheitlichen Maßstäben behandelt.

Was ist zu tun?
Die Dienststellen sollten mit der Durchführung des Eingliederungsmanagements einen von der Personalverwaltung unabhängigen Mitarbeiter bestellen, um **Interessenkonflikte**, die bei der Offenbarung besonders sensibler Daten durch die Betroffenen im Verfahren entstehen können, von vornherein auszuschließen.

4.1.9 Wer darf dienstliche E-Mail-Konten kontrollieren?

Dienstliche E-Mail-Accounts unterliegen der Kontrolle des Dienstherrn. Gehen dort private Mails ein, sind sie unverzüglich auf ein privates Konto des Mitarbeiters weiterzuleiten oder zu löschen. Personalratsmitglieder sollten für die Erfüllung dieser Aufgabe ein eigenes Konto erhalten.

Der Mitarbeiter einer Stadtverwaltung war für längere Zeit erkrankt. Sein Stellvertreter wurde vom Bürgermeister angewiesen, alle vorhandenen Mails auf seinem dienstlichen E-Mail-Konto zu sichten und gegebenenfalls zu bearbeiten. Gegen diese „Aktion“ wollte sich der erkrankte Mitarbeiter wehren und bat uns um eine Bewertung. Er würde den E-Mail-Account zwar selbst nicht privat nutzen können, es gleichwohl aber nicht verhindern, dass Dritte ihm **private Mails auf diesen dienstlichen Account** senden. Schließlich habe er verschiedene Ehrenämter in der Gemeindevertretung sowie in örtlichen Vereinen inne, und ein großer Absenderkreis würde ihn über die allgemein bekannte dienstliche Mailadresse ansprechen, ohne dass er darauf Einfluss habe.

Ebenso wie sonstige dienstliche Verwaltungstätigkeiten unterliegt die Kontrolle eines dienstlichen E-Mail-Accounts der **Weisungsbefugnis** des Bürgermeisters als Leiter der Verwaltung. Es ist deshalb nicht zu beanstanden, wenn er im Krankheitsfall Vertretungsregelungen trifft, die eine Kenntnisnahme aller eingegangenen E-Mails durch einen Vertreter mit einschließt. Anders wäre auch eine Bearbeitung der dienstlichen E-Mails durch einen Vertreter nicht zu gewährleisten. Insoweit muss sich auch der Absender einer privaten E-Mail im Klaren darüber sein, dass bei einer Adressierung der E-Mail an den dienstlichen Account einer Behörde eine Kenntnisnahme der Inhalte durch Dritte möglich ist. Im Übrigen würde auch ein an die Stadt adressierter Brief mit privatem Inhalt zulässigerweise von der Posteingangsstelle der Stadt geöffnet und von Dritten zur Kenntnis genommen. Insoweit entspricht die E-Mail-Regelung nur der Handhabung des sonstigen Postverkehrs.

Selbstverständlich dürfen die privaten E-Mails durch die Stadt nicht sofort gelöscht werden. Betroffene sollten die Möglichkeit erhalten, in geeigneter Weise darüber zu verfügen. Dies kann z. B. durch **Weiterleitung** der E-Mails an eine private Mailadresse geschehen.

Etwas anderes gilt für den E-Mail-Verkehr von Personalratsmitgliedern. Diese Tätigkeit unterliegt grundsätzlich nicht der Kontrolle des Bürgermeisters als Leiter der Verwaltung. Der Personalrat ist sogar verpflichtet, die ihm von den Beschäftigten zur Verfügung gestellten Daten auch gegenüber der Dienststelle vertraulich zu behandeln. Für den E-Mail-Verkehr bedeutet dies, dass der Personalrat wegen der Kontrollkompetenz des Bürgermeisters den normalen dienstlichen E-Mail-Account nicht für die **Personalratstätigkeit** nutzen sollte. Es ist vielerorts gängige Praxis, für Personalräte ein eigenes E-Mail-Konto einzurichten, das nicht von den üblichen Vertretungsregelungen erfasst wird.

Was ist zu tun?
Behörden sollten darauf achten, dass Personalratsmitglieder für diese Funktion eine eigene E-Mail-Adresse erhalten, um im Vertretungsfall bzw. bei einer dienstlichen Kontrolle der sonstigen Aufgabenerfüllung eine ausreichende Vertraulichkeit der Personalratsdaten gewährleisten zu können.

4.2 Polizei und Nachrichtendienste

Datenschutz bei Polizei- und Verfassungsschutzbehörden – das bedeutete für das ULD im vergangenen Jahr die Begleitung neuer IT-Verfahren und die Durchführung von Kontrollen, vor allem aufgrund von Eingaben betroffener Bürgerinnen und Bürger.

Die **Verfahren der Polizei** – @rtus und INPOL, die schon länger unter Beobachtung und Begleitung des ULD stehen –, werden weiter ausgebaut. Daneben werden weitere Verfahren geplant und eingerichtet. Das Landeskriminalamt (LKA) unterrichtete uns von neuen Planungen, z. B. zu einer elektronischen Kriminalakte.

Insbesondere im Bereich Polizei und Nachrichtendienste ist es wegen der hohen Sensibilität für das Leben der Menschen ein Anliegen des ULD, Eingaben betroffener Bürgerinnen und Bürger umfassend und zeitnah zu bearbeiten. Anlass hierfür sind oft polizeiliche Kontrollen, bei denen für die Betroffenen der Eindruck entsteht, etwas über sie sei in polizeilichen Dateien gespeichert, ohne dass ihnen dies ehrlich mitgeteilt wurde. In diesen Fällen stellen wir zunächst – durch **Kontrollen** vor Ort – fest, welche Daten zum Petenten gespeichert sind. Immer wieder führen diese Kontrollen zur Löschung gespeicherter Daten. Im Rahmen dieser Kontrolltätigkeit zeigte sich die zunehmende Bedeutung des Vorgangsbearbeitungssystems @rtus der Landespolizei. Es ergab sich Nachbesserungsbedarf bei den Löschfristen und wegen der fehlenden Möglichkeit der vorzeitigen Löschung einzelner Datensätze (Tz. 4.2.8).

Als besonders delikate Form polizeilicher Datenverarbeitung kann sich die Pressearbeit erweisen. Bei einer **polizeilichen Pressemitteilung** fehlt es an hinreichender Anonymisierung. Ein Petent aus einem kleinen Ort war bereits anhand der in der Pressemeldung genannten markanten Fahrzeugmarke für alle Einwohner identifizierbar. Dies muss und darf nicht sein, meint auch das Innenministerium.

4.2.1 Neues Polizeirecht – Verfassung und Auslegung

Das neue Polizeirecht des Landes, das „Gesetz zur Anpassung der gefahrenrechtlichen und verwaltungsverfahrensrechtlichen Bestimmungen", ist in Kraft getreten. Im Gesetzgebungsverfahren konnten einige verfassungsrechtlich kritischen Punkte entschärft werden. Andere bestehen fort und sind nun eine Herausforderung für die Rechtspraxis.

Erfreulich ist, dass gegenüber den Ursprungsentwürfen die Eingriffsschwelle für die Telekommunikationsüberwachung zur Gefahrenabwehr angehoben wurde. Diese Überwachung darf nur durchgeführt werden, wenn eine gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person vorliegt. In Schleswig-Holstein dürfen Polizeibehörden daher nicht aufgrund vager Verdachtslagen im sogenannten „Vorfeld" Telefongespräche abhören. **Nachgebessert** wurden auch die Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung.

Sehr weitgehend ist nach wie vor die allgemeine Regelung zur Erhebung von Daten zur vorbeugenden Straftatenbekämpfung. Das Gesetz erlaubt solche **Vorfelderhebung** immer, wenn eine möglicherweise geplante Tat durch „Täterschaft und Teilnahme organisiert" ist. Dies gilt nach dem Gesetzeswortlaut selbst für die Bagatellkriminalität, etwa bei spontanen Ladendiebstählen aus einer Gruppe von Jugendlichen heraus, selbst bei geringen Schäden. Von dieser Regelung darf bei verfassungskonformer Anwendung aber nur Gebrauch gemacht werden, wenn es um Straftaten von erheblicher Bedeutung geht und der Verdacht der bevorstehenden Straftat hinreichend konkretisiert ist. Ähnliches gilt für die neu per Gesetz erlaubten lagebildabhängigen Kontrollen. Bei unseren kommenden Kontrollen werden wir eine verhältnismäßige, d. h. restriktive Gesetzesanwendung einfordern. Auch bei der Videoüberwachung wurde gegenüber dem Ursprungstext eine Verbesserung durch eine höhere, nunmehr verfassungsrechtlich akzeptable Eingriffsschwelle erreicht.

Dagegen blieb die Regelung der **Kfz-Kennzeichenerfassung** im Hinblick auf Normenklarheit, Verhältnismäßigkeit und Gesetzgebungskompetenz Not leidend. Das Gesetz erlaubt den Abgleich von Kfz-Kennzeichen mit dem gesamten polizeilichen Fahndungsbestand, der auch der Strafverfolgung dient. Dies hätte aber nur der Bundesgesetzgeber regeln dürfen. Aufgrund der kritischen Anmerkungen – u. a. des Wissenschaftlichen Dienstes des Landtages und des ULD – beschränkt die Landespolizei den für das Kennzeichenscanning verwendeten Fahndungsbestand auf reine Gefahrenabwehrdaten – also vorrangig bei Verstößen gegen die Versicherungspflicht und bei der Suche gestohlener Autos. Ob dies ausreicht, um den verfassungsrechtlichen Vorgaben zu genügen, was wir bezweifeln, wird demnächst das Bundesverfassungsgericht in Karlsruhe anlässlich einer Klage gegen die Neuregelung entscheiden.

Im letzten Tätigkeitsbericht hatten wir in Bezug auf die Regelung der **Vorgangsbearbeitungssysteme** die fehlende Zweckbindung moniert (29. TB, Tz. 4.2.1). Dieser Missstand wurde nicht behoben. Eine verfassungskonforme Nutzung solcher Systeme setzt voraus, dass bei der Verwendung der erhobenen und gespeicherten Daten der ursprüngliche Zweck beachtet wird.

Was ist zu tun?
Die zu weit geratenen Vorschriften des neuen Polizeirechtes sind verfassungskonform, d. h. einschränkend auszulegen.

4.2.2 Verweigerungshaltung bei Antiterrordatei

Die Antiterrordatei ist in Betrieb. Die Vorschläge der Datenschützer wurden vom Gesetzgeber übergangen. Daher musste das ULD erneut eine Stellungnahme zum Antiterrordateigesetz abgeben – gegenüber dem Bundesverfassungsgericht. Zwecks deren Erstellung erhielt das ULD von den zuständigen Behörden des Landes nicht die erfragten Informationen. In der Praxis zeichnet sich ein mangelhaftes Auskunftsverfahren gegenüber den Betroffenen ab.

Zur Vorbereitung unserer Stellungnahme – und als Vorlauf einer späteren Kontrolle – hatten wir der Verfassungsschutzbehörde und dem Landeskriminalamt einen **Fragenkatalog** übersandt und hofften, die nötigen Angaben auf kooperativem Wege zu erhalten, ohne sogleich zum Mittel der förmlichen Kontrolle zu greifen. Das Innenministerium zog als übergeordnete Stelle die Beantwortung an sich und beantwortete die Fragen nur auszugsweise – mit dem erläuternden Hinweis darauf, dass die Weitergabe der Daten an das Bundesverfassungsgericht beabsichtigt sei. Diese Verweigerungshaltung können wir nicht nachvollziehen. Im Ergebnis mussten wir uns daher weitgehend darauf beschränken, dem höchsten deutschen Gericht unsere rechtliche Bewertung der abstrakten Regelungen mitzuteilen.

Die in dem Gesetz vorgesehene weitgehende Aufhebung der informationellen **Trennung zwischen Polizei und Nachrichtendiensten** birgt massive Gefahren für die informationelle Selbstbestimmung. Das Trennungsgebot verpflichtet zur Abgrenzung der Aufgaben von Polizei und Geheimdiensten und der von diesen genutzten Daten. Für die Nachrichtendienste gelten nicht die Eingriffsschwellen der Polizei- bzw. Strafverfolgungsbehörden. Die Ausforschung der Bürgerinnen und Bürger setzt keinen Tatverdacht und keine illegalen Handlungen voraus. Die Antiterrordatei und die noch unbefriedigender geregelten Projektdateien sind darauf angelegt, das Trennungsgebot zu umgehen und Polizeibehörden Zugriff auf Daten trotz fehlenden Tatverdachts zu gewähren. Unglücklich geregelt ist der weite und nicht hinreichend präzisierte Kreis der gespeicherten Personen. Dies sind nicht nur Terroristen, sondern selbst „Befürworter“ rechtswidriger Gewalt und Kontaktpersonen – all das auf der vagen Grundlage „tatsächlicher Anhaltspunkte“. Gespeichert werden nicht nur Grunddaten, sondern sogenannte erweiterte Grunddaten. Hierzu gehört ein nach dem Gesetzeswortlaut praktisch unbegrenztes Freitextfeld (29. TB, Tz. 4.2.6). Nicht hinnehmbar sind die unbestimmten Regelungen zu Löschfristen und zur Auskunft an Betroffene.

Für die Antiterrordatei ist in der Praxis ein **mangelhaftes Auskunftsverfahren** zu den verdeckt gespeicherten Daten geplant. Die aktuelle Rechtsprechung der höchsten deutschen Gerichte stellt immer wieder heraus, dass der Auskunftsanspruch für die informationelle Selbstbestimmung der Betroffenen von grund-

legender Bedeutung ist. Jede Bürgerin und jeder Bürger muss grundsätzlich in Erfahrung bringen können, bei welcher Stelle welche Daten über sie bzw. ihn gespeichert sind. Schon die Regelung des Antiterrordateigesetzes ist insofern eine Zumutung: „Die Auskunft zu verdeckt gespeicherten Daten richtet sich nach den für die Behörde, die die Daten eingegeben hat, geltenden Rechtsvorschriften." Die Betroffenen sollen einen Hinweis auf diese Regelung und eine Adressenliste der beteiligten Stellen erhalten, um dort jeweils die Auskunft einzeln zu beantragen. Die Bürgerinnen und Bürger haben unter Umständen **keine leise Ahnung**, welche der zurzeit mehr als 40 beteiligten Stellen Daten über sie gespeichert haben. Sie sind so gezwungen, mehr als 40 Anträge zu stellen. Im Zweifel sind ebenso viele Widerspruchs- und Klageverfahren „ins Blaue hinein" nötig, ohne die Erfolgsaussichten ansatzweise vorher abschätzen zu können. Dieses Auskunftsverfahren ist weder mit den Grundrechten noch mit der Rechtsweggarantie des Grundgesetzes zu vereinbaren.

Was ist zu tun?
Solange keine Entscheidung des Bundesverfassungsgerichts vorliegt, sind die Vorschriften des Antiterrordateigesetzes restriktiv anzuwenden, vor allem hinsichtlich des gespeicherten Personenkreises. In Zweifelsfällen sollte auf die Speicherung verzichtet werden. Das Auskunftsverfahren ist nicht akzeptabel. Die Betroffenen müssen sich an eine zentrale Stelle wenden können.

4.2.3 Zuverlässigkeitsüberprüfungen – Neuer Standard am Gesetzgeber vorbei?

Fernab von jeder politischen Diskussion breitet sich ein neues Verfahren mit wechselnden Namen aus: „Sicherheitsüberprüfung", „Zuverlässigkeitsüberprüfung", neuerdings „Akkreditierungsverfahren".

Dahinter verbirgt sich ein umfassender **Datenabgleich** der Betroffenen **bei Polizei und Geheimdiensten**. Dessen Ergebnis bestimmt, ob der Betroffene eine bestimmte Aufgabe wahrnehmen darf, seinen Beruf ausüben kann, zu einer Veranstaltung zugelassen wird. All diese potenziellen Nachteile basieren auf „Einwilligungen" der Betroffenen. Sicherheitsüberprüfungen sind im Sicherheitsüberprüfungsgesetz geregelt, weitere Zuverlässigkeitsüberprüfungen in Spezialgesetzen wie dem Atomgesetz oder dem Luftverkehrsgesetz. Daneben regelt das Bundeszentralregistergesetz, welche Daten in ein Führungszeugnis aufgenommen werden, das Arbeitgebern in begründeten Fällen die Möglichkeit gibt, bei der Besetzung sicherheitsrelevanter Stellen Wichtiges aus dem „Vorleben" des Arbeitnehmers zu erfahren. Das Bundeszentralregister schafft Transparenz für den Betroffenen, da ohne dessen Mitwirkung die Arbeitgeber grundsätzlich keine Möglichkeit haben, dessen Daten zu erhalten.

Diese etablierten und praktisch bewährten Regelungen werden zunehmend durch **Fantasieverfahren** ohne jegliche Rechtsgrundlage ersetzt. Sie berufen sich allein auf die „Einwilligung" der Betroffenen. Hiermit werden Datenabgleiche gerechtfertigt, an denen Polizei- und unter Umständen Verfassungsschutzbehörden beteiligt sind. Dies ist nicht akzeptabel. Die Verfahren umgehen den Willen des Gesetz-

gebers. Dieser hat abschließend entschieden, in welchen Fällen nach welchen Verfahren Zuverlässigkeits- und Sicherheitsüberprüfungen durchgeführt werden dürfen. Vorgesehen ist neben anderen Voraussetzungen – zusätzlich – die Einwilligung der Betroffenen. Allein dies zeigt: Bloße Einwilligungserklärungen können für derart weitgehende Eingriffe nicht ausreichen. In Arbeitsverhältnissen kann zudem von einer echten Freiwilligkeit der Einwilligung oft keine Rede sein. Wer befürchtet, seinen Job zu verlieren, wenn er nicht einwilligt, der gibt diese Erklärung nicht freiwillig ab.

Diese Fantasieverfahren – erdacht von der Verwaltung, gegebenenfalls gemeinsam mit einer Interessengruppe oder einem Veranstalter – stellen die fein austarierte Systematik des Bundeszentralregistergesetzes und der Sicherheitsüberprüfungsgesetze auf den Kopf. Wenn eine Sicherheitsüberprüfung vom Gesetz nicht erlaubt ist, dann muss sie unterbleiben. Erlaubt das Gesetz dem Arbeitgeber nur das **Verlangen eines Führungszeugnisses**, so kann er nur dieses verlangen, nicht aber eine Überprüfung durch Polizei und Verfassungsschutz.

Den Anfang der Aufweichung bildete das „Akkreditierungsverfahren“ zur **Fußballweltmeisterschaft** (29. TB, Tz. 4.2.5). Dieses Verfahren entwickelt sich zunehmend zum Standard. Zunächst bezog es sich auf Großveranstaltungen, inzwischen neigen erste Bundesbehörden dazu, Mitarbeiter mit ähnlichen Verfahren zu prüfen. Das Innenministerium hat bisher nicht erkannt, dass diese Verfahren auf eine schiefe Bahn des Grundrechtsentzugs führen.

Was ist zu tun?
Zuverlässigkeitsüberprüfungsverfahren dürfen nicht am Gesetzgeber vorbei ohne gesetzliche Grundlage durchgeführt werden. Sie stellen einen Grundrechtseingriff dar, der einer normenklaren und verhältnismäßigen Rechtsgrundlage bedarf.

4.2.4 Online-Durchsuchung – Keine rechtsstaatlichen Standards aufgeben!

Bundesweit wird die sogenannte Online-Durchsuchung diskutiert. Gesetzlich erlaubt ist sie nicht. Der Bundesgerichtshof hat festgestellt, dass sie im Strafverfahren verboten ist. Für andere Bereiche gilt nichts anderes. Dies sollte in Zukunft so bleiben.

Seit 1877 sieht die Strafprozessordnung vor, dass Wohnungsdurchsuchungen im Strafverfahren nur offen erfolgen dürfen. Gegenüber Beschuldigten müssen die Ermittlungsbehörden mit „**offenem Visier**“ vorgehen. Der Bundesgerichtshof hat ausdrücklich klargestellt, dass es für darüber hinausgehende heimliche Durchsuchungen von Computern keine rechtliche Grundlage gibt. Für die Gefahrenabwehr und nachrichtendienstliche Zwecke gilt nichts anderes.

Einige Sicherheitspolitiker wollen diese **rechtsstaatliche Tradition aufgeben** und fordern die sogenannte Online-Durchsuchung. Diese übertrifft in Bezug auf die Eingriffsintensität für die Betroffenen die auch nicht gerade harmlose Wohnungs-

durchsuchung. Mit ihr sollen an das Internet oder ein anderes Netzwerk angeschlossene Computer, Festplatten oder sonstige elektronische Geräte ohne Wissen der Betroffenen durchforstet werden. Dies wirft schwerwiegende verfassungsrechtliche Fragen auf und führt zur Verunsicherung bei der Nutzung von vernetzter Informationstechnik.

Nach der inzwischen gefestigten Rechtsprechung des Bundesverfassungsgerichts müssen heimliche Ermittlungsmaßnahmen stets den **Kernbereich privater Lebensgestaltung** respektieren. So dürfen z. B. innerste Gedankengänge der Betroffenen unter keinen Umständen zum Gegenstand einer staatlichen Überwachung gemacht werden. Die Wahrung dieses Kernbereichs ist bei der Online-Durchsuchung praktisch unmöglich. Sobald Computer in einer Wohnung stehen, berührt die heimliche Ausforschung das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 GG). Das Grundgesetz erlaubt jedoch – abgesehen von der akustischen Wohnraumüberwachung – nicht das heimliche Eindringen. Schon allein die Schranken des Art. 13 GG lassen diese Maßnahme also nicht zu.

Für die Bürgerinnen und Bürger bedeutet das: Niemand ist davor gefeit, in ein Ermittlungsverfahren verwickelt zu werden. Zunächst sind die derart Betroffenen nur „Beschuldigte“, noch nicht „Täterinnen“ oder „Täter“. Ob sich der Tatverdacht erhärtet, muss sich im Strafermittlungsverfahren erst noch erweisen. Die Betroffenen wie die Strafverfolger haben ein Interesse daran, dass die erhobenen Indizien und Beweise sicher sind und keinem **Risiko der Verfälschung** unterliegen. Daher gilt in der Praxis bislang der unabdingbare Grundsatz, dass Datenträger nach der Beschlagnahme „eingefroren“ werden. Im Ermittlungsverfahren dürfen keine Veränderungen daran durchgeführt werden, um die Beweiskraft der Daten nicht zu gefährden. Die Online-Durchsuchung wird jedoch im laufenden Betrieb durchgeführt. Dabei kann es den Ermittlern unter Umständen entgehen, dass ein Rechner von unbekannten Dritten mit einer Schadsoftware „gekapert“ und dann für kriminelle Zwecke missbraucht wurde. Versehentliche wie auch gezielte Veränderungen an den Daten sind nicht auszuschließen.

In **Schleswig-Holstein** sind wir der Frage nach der tatsächlichen Anwendung bzw. Handhabung dieser Eingriffsmethode nachgegangen. Bei unseren Recherchen ergaben sich keine Anhaltspunkte für eine Überschreitung der gesetzlichen Befugnisse durch Stellen des Landes.

Was ist zu tun?
Von der Einführung der sogenannten Online-Durchsuchung sollte Abstand genommen werden. Unsere rechtsstaatliche Tradition und handwerklich saubere Polizeiarbeit sind zu wahren.

4.2.5 Auskunftsverfahren bei der Polizei

Aufgrund von Mängeln bei der polizeilichen Auskunftserteilung an die Betroffenen hat das ULD den Verantwortlichen im Land in einem „13-Punkte-Papier“ ein datenschutzrechtliches Anforderungsprofil an das „Auskunftsmanagement“ bereitgestellt. Jetzt ist Bewegung in die Sache gekommen; unsere Anregungen wurden weitgehend aufgegriffen.

Das ULD stellte anlässlich vieler Beschwerdefälle in der Vergangenheit fest, dass Auskunftsersuchen von der Polizei an die Betroffenen falsch waren, vor allem weil sie unvollständig beantwortet wurden (28. TB, Tz. 4.2.5; 29. TB, Tz. 4.2.2). Den anfragenden Bürgerinnen und Bürgern wurden oft unter Missachtung der gesetzlichen Pflicht keine umfassenden Auskünfte erteilt oder gar die Mitteilung verweigert, dass keine Daten zum Anfragenden in polizeilichen Dateien gespeichert sind. Jede Person, die Behörden des Landes Schleswig-Holstein um Auskunft über gespeicherte personenbezogene Daten bittet, muss korrekte Angaben hierüber erhalten. Dies ist ein **verfassungsrechtlich begründeter Anspruch**. Nur wenn sie weiß, ob Daten über sie verarbeitet werden, hat sie die Möglichkeit, ihre Datenschutzrechte auszuüben, und kann sich gegebenenfalls zur Wehr setzen. Können die Bürgerinnnen und Bürger nicht darauf vertrauen, dass die ihnen gegebene Auskunft vollständig und korrekt ist, sind sie insoweit an ihrer Rechtsausübung gehindert.

In einem „**13-Punkte-Papier**“ haben wir festgehalten, wie in der Praxis mit Auskunftsansprüchen umgegangen werden sollte. Dazu gehört u. a., dass

- die behördlichen Datenschutzbeauftragten eingebunden werden,
- sichergestellt wird, dass alle relevanten Dateien überprüft werden,
- auch die Verbunddateien beim BKA berücksichtigt werden,
- keine Speicherungen im Zusammenhang mit einem Auskunftsersuchen in polizeilichen Datensammlungen erfasst werden,
- der Schriftwechsel getrennt von polizeilichen Unterlagen bei der bzw. dem behördlichen Datenschutzbeauftragten aufbewahrt wird.

Das Innenministerium hat mitgeteilt, dass viele der Forderungen des ULD in der Praxis beim Landeskriminalamt (LKA) umgesetzt sind. Bei anderen Punkten besteht noch **Gesprächsbedarf**, z. B. bezüglich der elektronischen Aufbewahrung des Schriftwechsels in einem besonders geschützten Bereich einer Datenbank. Wir sehen das Thema inzwischen in guten Händen und sich positiv entwickeln.

Was ist zu tun?
Die begonnenen Bemühungen zur datenschutzfreundlichen Umgestaltung des Auskunftsverfahrens sollten konsequent fortgeführt werden. Das ULD ist bereit, diesen Prozess weiterhin konstruktiv zu unterstützen.

4.2.6 Kontrolle beim Staatsschutz des LKA

Die datenschutzrechtliche Kontrolle des ULD bei der Abteilung 3 des Landeskriminalamtes (LKA) aus dem Jahre 2005 konnte lange nicht abgeschlossen werden. Zu gravierenden Feststellungen wurden nur vage, nicht hinreichend substanziierte Absichtserklärungen gegeben. Nachhaltige Interventionen des ULD brachten nun Bewegung in die Sache; das Innenministerium scheint um Schadensbegrenzung bemüht und hat erste Entscheidungen getroffen.

Vor etwa drei Jahren führte das ULD eine datenschutzrechtliche Kontrolle bei der Abteilung 3 – Staatsschutz – des LKA Schleswig-Holstein durch. Sachverhalte wie die **Speicherung erlaubten Verhaltens** (bloße Teilnahme an Demonstrationen), die umfangreiche Informationsverarbeitung nach sich ziehen, wurden von uns beanstandet. Gewisse Datenverarbeitungsverfahren der Staatsschutzabteilung erwiesen sich aus Datenschutzsicht als sehr bedenklich. Wir baten um zusätzliche Angaben und Errichtungsanordnungen. Trotz förmlicher Rügen erfolgte bisher noch keine befriedigende Reaktion (28. TB, Tz. 4.2.7; 29. TB, Tz. 4.2.9). In Vorbereitung dieses Tätigkeitsberichtes erhielt das ULD auf erneute Mahnung nun eine Auflistung der anstehenden Maßnahmen der Abteilung 3.

Die Polizei hält die amtsinternen Dateien „Indexdatei Kalender“, „Innere Sicherheit Schleswig-Holstein“ (ISSH), „Warndatei Rechts“ für weiterhin erforderlich und will die gesetzlich vorgeschriebenen Errichtungsanordnungen dem ULD vorlegen. Leider hat das LKA bisher darauf verzichtet, dem ULD rechtlich nachvollziehbare Begründungen für die Fortführung der genannten Verfahren zu geben. Die Datei „COMPAS“ wurde in das Verfahren „@rtus“ überführt. Der Datenbestand von 16.740 Datensätzen mit insgesamt 31.408 Personalien wurde sukzessive auf weitere Speicherungswürdigkeit überprüft. Das Konzept sah wöchentlich eine Durchsicht von 250 Vorgängen vor. Das LKA zeigte sich zuversichtlich, dass alle **Vorgänge kurzfristig bereinigt** sein werden. Die COMPAS-Rechner bei den Polizeidienststellen werden nach und nach deinstalliert und nur noch für Auskunftszwecke genutzt. Ein Rechner befindet sich bei der Abteilung 3 des Landeskriminalamtes und wird dort ausschließlich zur Verwaltung und Bearbeitung eines noch offenen Verfahrens eingesetzt, da die Falldaten nicht in @rtus migriert werden konnten.

Was ist zu tun?
Die bei der Datenschutzkontrolle im Jahre 2005 begonnene Diskussion über die rechtlichen Grenzen der polizeilichen Beobachtung von politischen Aktivitäten sollte endlich zu einem grundrechtlich akzeptablen Ergebnis geführt werden.

4.2.7 Protokollierung bei polizeilicher Datenverarbeitung

Das Landesverwaltungsgesetz schreibt Protokollierungen von Zugriffen auf automatisierte Datenverarbeitungssysteme vor. Das ULD sieht sich von der Praxis mit der unerwarteten Frage konfrontiert, ob wirklich alle oder nur ein bestimmter Prozentsatz der getätigten Abrufe für die im Gesetz genannten Zwecke aufzuzeichnen und welche Daten hierfür notwendig sind.

Bei der Befassung mit der Errichtungsanordnung für die Datei „INPOL-SH“ (27. TB, Tz. 4.2.4; 28. TB, Tz. 4.2.2) war die Ausgestaltung und die Nutzung von Protokolldaten bei automatisierter Informationsverarbeitung bei der schleswig-holsteinischen Polizei ein wichtiger Schwerpunkt. Das Landesverwaltungsgesetz bestimmt, dass **Abrufe in überprüfbarer Form** automatisiert zu protokollieren sind und dass diese Daten nur für Zwecke der Datenschutzkontrolle, der Datensicherheit, zur Sicherstellung eines ordnungsgemäßen Betriebes der Datenverarbeitungsanlage sowie zur Ausübung von Aufsichts- und Kontrollbefugnissen durch Dienst- und Fachvorgesetzte verwendet werden dürfen. Um diese Vorschrift ihrem Sinn und Zweck entsprechend anwenden zu können, bedarf es einer Aufzeichnung sämtlicher Abrufe von Daten aus der Datei – eine reduzierte Protokollierung von durchschnittlich jedem zehnten Abruf reicht nicht aus. Zudem bedarf es der klaren Festlegung des erforderlichen Umfangs der zu protokollierenden Daten, um den Zweck der Protokollierung zu erreichen.

Das ULD hat sich in Zusammenarbeit mit dem Landeskriminalamt und dem Innenministerium des Landes Schleswig-Holstein – ausgehend vom Verfahren INPOL-SH – auf einen Datensatz verständigt. Diese Vorgabe muss nun im Wirkbetrieb umgesetzt werden. Die Polizei hat ein eigenes starkes Interesse an einer revisionsfesten Protokollierung. Das ULD hat angeregt, dieses **Protokollierungsmodell** für alle automatisierten Datenverarbeitungsverfahren bei der Polizei des Landes einzuführen. Dies verspricht Synergieeffekte durch verminderten Aufwand bei der Softwareentwicklung. Das Verfahren könnte in einer eigenen Errichtungsanordnung beschrieben und festgelegt werden, wodurch die weiteren Errichtungsanordnungen vereinfacht würden.

Was ist zu tun?
Die gemeinsam mit dem Innenministerium und dem Landeskriminalamt entwickelten Vorstellungen zur Protokollierung sollten nun zügig realisiert werden.

4.2.8 @rtus – die neue Datei der Polizei in Schleswig-Holstein

Das Vorgangsbearbeitungs- und Dokumentationssystem „@rtus“ der schleswig-holsteinischen Polizei ist seit mehr als einem Jahr in Betrieb. Das Gesetz wurde geändert, um @rtus zu legalisieren; nun muss @rtus geändert werden, damit es dem Gesetz entspricht.

Das ULD hatte bereits im Jahre 2005 auf gravierende konzeptionelle Defizite des Systems @rtus hingewiesen und Lösungswege aufgezeigt, welche zu einer verbes-

serten technischen Ausgestaltung von @rtus geführt hätten. Dies betrifft insbesondere die gemeinsame Bestandsführung von Daten aus der „Vorgangsbearbeitung“ und der „Dokumentation“ und die damit verbundenen unterschiedlichen Zweckbestimmungen. Die notwendigen Änderungen wären aus unserer Sicht problemlos vor der Implementierung des Systems möglich gewesen. Einer Gesetzesnovellierung hätte es nicht bedurft (28. TB, Tz. 4.2.3; 29. TB, Tz. 4.2.3). Es wurden **technische Fakten geschaffen**, die zur Rechtsunsicherheit führen.

Die Landespolizei stellt inzwischen praktisch **sämtliche laufenden Fälle** im Rahmen der Bearbeitung in das System ein. Zusätzlich werden die Datenbestände älterer Verfahren wie COMPAS in den Datenbestand von @rtus überführt (Tz. 4.2.6). Der Gesamtbestand ist bereits auf ca. 2.000.000 Datensätze angewachsen. Im jetzigen Stadium noch datenschutzrechtliche Verbesserungen einzubringen erscheint fast unmöglich, soweit dabei technische Anpassungen nötig sind. Die Trennung und differenzierte Verarbeitung der Datensätze je nach ihrem Verwendungszweck sollte nach 30 Jahren Datenschutz eigentlich eine Selbstverständlichkeit sein. Das Gesetz differenziert zwischen Vorgangsbearbeitung und Vorgangsverwaltung. Die Lösung des Problems der Trennung der Datensätze sowie die nachträgliche Zuordnung der bereits gespeicherten Datensätze stellt die Polizei vor eine zunehmend schwieriger werdende Aufgabe. Bei frühzeitiger Befassung hiermit hätte viel überflüssige Polizeiarbeit vermieden werden können.

Zu der **Errichtungsanordnung** zu @rtus ist in den vergangenen Jahren viel zwischen ULD und Innenministerium hin- und hergeschrieben worden. Bis heute hat sich die Polizei aber nicht bereit gezeigt, auf unsere Argumente einzugehen. Das ULD hat den wirkungslosen Schriftwechsel nicht weitergeführt. Die Hoffnungen ruhen nun darauf, dass die Diskussion über das zu novellierende Polizeirecht und praktische Erfahrungen der Landespolizei mit dem neuen Verfahren das Problembewusstsein schärfen werden.

Bei Prüfungen haben wir nun festgestellt, dass der für die Berechnung der **Speicherdauer** relevante Beginn der Laufzeit oft nicht den gesetzlichen Vorgaben entspricht. In der Praxis beginnt die Frist regelmäßig mit der Speicherung der personenbezogenen Daten in der Datei. Der Gesetzgeber hat zur Fristberechnung dagegen eine klare Regelung getroffen, wonach die Frist regelmäßig mit dem letzten Anlass, der zur Speicherung personenbezogener Daten geführt hat, beginnt. Ausgangspunkt für die Fristberechnung ist das Datum des Ereignisses, z. B. eine Straftat. Nicht relevant ist der manchmal sehr zufällige Zeitpunkt, an dem der Sachbearbeiter den Fall in das System eingibt. Auch in anderen Bereichen, wie bei der Berechnung von Verjährungsfristen, bedarf es der Bezugnahme auf das Datum des Deliktes.

Die Polizeibehörden sind auch nach dem neuen Gesetz verpflichtet, bei jeder Einzelfallbefassung die **Erforderlichkeit** der weiteren Verarbeitung von gespeicherten personenbezogenen Daten zu **überprüfen**. Dieser wichtige Datenschutzgrundsatz findet in der Praxis offensichtlich wenig Beachtung. Es genügt nicht, die Erforderlichkeit nur in den Fällen des Fristablaufes, einer Betroffeneneingabe oder einer externen Datenschutzkontrolle zu überprüfen. Die Polizei müsste ein

Eigeninteresse an einem Datenbestand haben, der verlässliche, für die künftige Aufgabenerfüllung relevante Informationen enthält. Alles andere wäre unnötiger, eventuell Arbeit auslösender Ballast.

Bei ersten **Kontrollen** bei Polizeidirektionen haben wir u. a. Folgendes festgestellt:

- Datensätze werden nicht entsprechend der gesetzlichen Vorgaben verarbeitet, sobald sie in den Bereich der Vorgangsverwaltung übergehen.
- Die datenschutzrechtlich verantwortlichen Polizeidirektionen können aus technischen Gründen keinen Einfluss auf die Speicherungsdauer von Datensätzen nehmen. Die Speicherungsfristen werden automatisch vom System vergeben und können nicht entsprechend den Anforderungen des Einzelfalls festgesetzt werden.
- Die Vergabe der Zugriffe auf @rtus erfolgt auf der Ebene der Fachdienststellen undifferenziert.

Was ist zu tun?
Das Verfahren @rtus muss nun im laufenden Betrieb rechtlich und technisch so modifiziert werden, dass das Verfahren den gesetzlichen Anforderungen genügt. Die Bereitschaft des ULD, seine Vorschläge zu erläutern und zu präzisieren und das technisch verantwortliche Landespolizeiamt zu beraten, besteht nach wie vor.

4.3 Justizverwaltung

Datenschutz bei der Justiz bedeutet derzeit die Behandlung grundlegender Themen wie Vorratsdatenspeicherung, StPO-Novelle, Auskunftserteilung und Datenschutzkontrollbefugnis. Anlassbezogen gerieten weitere „kleinere" Themen in unseren Fokus.

Oft war es der konkrete **unkorrekte Umgang mit Informationen**, der Bürgerinnen und Bürger zu Eingaben veranlasste. So war es nicht in Ordnung, dass die Zustellung einer Benachrichtigung des Gerichtsvollziehers über eine bevorstehende Vollstreckung offen, d. h. sogar ohne verschlossenen Briefumschlag, im Briefkasten der Nachbarn landete. Ärgerlich war die Nachlässigkeit eines Gerichtsvollziehers, der seine „abzuarbeitende" Liste mit Namen auf dem Beifahrersitz seines Fahrzeugs so offen liegen ließ, dass deren Inhalt für Passanten zugänglich war. Es sind oft kleine Dinge im Alltag, die zu Beeinträchtigungen für die Betroffenen führen können. Manche durch Nachlässigkeit offenbarte Umstände sprechen sich in der Nachbarschaft herum. Dies kann nur verhindert werden, wenn stets die erforderliche Sorgfalt waltet.

4.3.1 Vorratsdatenspeicherung und StPO-Novelle – Generalverdacht gegen alle

Das Gesetz zur Vorratsdatenspeicherung wurde verabschiedet – eine schwerwiegende Weichenstellung zulasten der informationellen Selbstbestimmung und des Telekommunikationsgeheimnisses aller Bürgerinnen und Bürger. Nicht erlangt wird das erklärte Ziel bei der Änderung der Strafprozessordnung (StPO), eine „harmonische Gesamtregelung" zu erreichen.

Wir haben immer wieder und mit nachdrücklichen rechtlichen wie lebenspraktischen Argumenten – letztendlich im Ergebnis vergeblich – an den Gesetzgeber appelliert, von der **Vorratsdatenspeicherung** Abstand zu nehmen. Wir mussten zur Kenntnis nehmen, dass das Land und insbesondere der Innen- und Rechtsausschuss des Landtages die Einflussmöglichkeiten über den Bundesrat ungenutzt ließ. Die Folgen werden wir alle, also auch die Bürgerinnen und Bürger in Schleswig-Holstein, zu tragen haben.

- **Vorratsdatenspeicherung**

Die Vorratsdatenspeicherung, also die **sechsmonatige Speicherung sämtlicher Telekommunikationsverbindungsdaten**, ist unverhältnismäßig und damit verfassungswidrig. Sie verstößt gegen das national durch Art. 10 Grundgesetz (GG) sowie europarechtlich durch Art. 8 Europäische Menschenrechtskonvention (EMRK) geschützte Fernmeldegeheimnis. Im Volkszählungsurteil von 1983 und später immer wieder erklärte das Bundesverfassungsgericht die Speicherung „nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken" für unzulässig. Die Zwecke der Vorratsdatenspeicherung sind unbestimmt, weil die Verkehrs- und Standortdaten aller Teilnehmer und Nutzer öffentlicher elektronischer Kommunikationsdienste pauschal und ohne jeden konkreten Anhaltspunkt für eine konkrete Straftat der betroffenen Personen gespeichert werden sollen.

- Die **Einbeziehung aller Kommunikationsteilnehmer** qualifiziert die Vorratsdatenspeicherung als eine Maßnahme mit einer außerordentlich hohen Eingriffsintensität. Sie gefährdet die Unbefangenheit der Nutzung der Telekommunikation und in der Folge die **Qualität der Kommunikation einer Gesellschaft**, weil die Maßnahmen dazu beitragen, dass Risiken des Missbrauches und ein Gefühl des Überwachtwerdens entstehen.
- Die Vorratsdatenspeicherung ist unverhältnismäßig und damit verfassungswidrig, weil sie die Speicherung von Verkehrs- und Standortdaten aller Kommunikationsteilnehmer **ohne jeden Verdacht** anordnet. Nach dem Grundsatz der Verhältnismäßigkeit dürfen intensive Grundrechtseingriffe erst von bestimmten Verdachts- oder Gefahrenstufen an vorgesehen werden. Grundrechtseingreifende Maßnahmen „ins Blaue hinein" sind unzulässig.
- Die **Zugriffsmöglichkeit der Nachrichtendienste** steigert die Unverhältnismäßigkeit in unerträglicher Weise. Schon das bestehende Recht der Nachrichtendienste lässt die Beobachtung gesetzestreuer Bürgerinnen und Bürger zu. Diese müssen nicht illegal gehandelt haben. Nunmehr gerät die gesamte Bevöl-

kerung in den Fokus der Nachrichtendienste. Es droht eine extensive Überwachung ganzer Bevölkerungsgruppen.

- Angesichts der Missbrauchsmöglichkeiten warnen wir dringend vor der Verankerung eines **zivilrechtlichen Auskunftsanspruches** auf die Vorratsdaten. Private Dritte haben das Interesse, die Kommunikationsprofile auch außerhalb ihrer Zweckbestimmung einzusetzen. Adresshändler zahlen heute für weit belanglosere Daten teilweise erhebliche Summen. Dem kommerziellen Gebrauch darf der Gesetzgeber nicht Vorschub leisten – es geht um das Telekommunikationsgeheimnis (Tz. 7.1).

- **Änderungen der Strafprozessordnung**

Das Ziel, im Bereich der **Strafprozessordnung** (StPO) eine „harmonische Gesamtregelung" der verdeckten Ermittlungsmaßnahmen zu schaffen, ist grundsätzlich zu begrüßen. Hierfür wäre eine umfassende Evaluation zu wünschen gewesen. Eine solche ist bislang nur für die Wohnraumüberwachung und die Telekommunikationsüberwachung durchgeführt worden. Im Hinblick auf das verfolgte Ziel sind insbesondere folgende Punkte problematisch:

- Die Regelungen des Gesetzes senken **Eingriffsschwellen**, nicht nur bei der Telekommunikationsüberwachung. Es wird voraussichtlich zu einer erheblichen Ausweitung von Eingriffen kommen. Der Entwurf räumt tatsächlichen oder vermeintlichen Sicherheitsinteressen den Vorrang ein. Besonders heikel ist die zu umfangreiche Einbeziehung von Kontakt- und Begleitpersonen.

Zweifel an der Verfassungsmäßigkeit gelten insbesondere für den Zugriff auf die im Rahmen der Vorratsdatenspeicherung erfassten **Verkehrsdaten**. Das Gesetz überschreitet die Grenzen der Verhältnismäßigkeit und der umzusetzenden Europäischen Richtlinie. Es erlaubt die Herausgabe der Daten schon in Fällen der Bagatellkriminalität. Jede „mittels eines Telekommunikationsendgerätes" begangene Straftat soll für die Datennutzung genügen – darunter fällt schon die telefonische Beleidigung. Im Bereich der Internetdaten wird praktisch auf jede Eingriffsschwelle verzichtet.

Der **Anlasstatenkatalog** zur Telekommunikationsüberwachung wird ohne hinreichende Begründung erweitert. Aus dem Katalog wurden nur Straftatbestände gestrichen, die keine praktische Bedeutung haben.

- Der Schutz des **Kernbereichs privater Lebensgestaltung** wird durch die geplante Regelung ausgehöhlt. Wenn nur Inhalte geschützt sind, die „allein" den Kernbereich betreffen, wird nichts geschützt. Denn ein solcher Fall wird in der Praxis kaum vorkommen. Die Vorgaben aus Karlsruhe blieben unbeachtet. Der Schutz muss über den Bereich der Telekommunikationsüberwachung hinausgehen. Andere Maßnahmen können den Kernbereich ebenfalls berühren, so etwa das vertrauliche Gespräch außerhalb von Wohnungen. Notwendig ist eine „vor die Klammer gezogene" Regelung.

- Die Schutzansprüche der **Zeugnisverweigerungsberechtigten** drohen durch weiche Abwägungsklauseln verwässert zu werden. Die Differenzierung nach verschiedenen Klassen von Zeugnisverweigerungsberechtigten ist nicht nachvollziehbar und untergräbt einen wirksamen Grundrechtsschutz. Der Geheimnisschutz soll erst eingreifen, wenn sich die Überwachungsmaßnahme „gegen" den Zeugnisverweigerungsberechtigten richtet; dies verringert den Schutz zusätzlich.
- Den **Verfahrenssicherungen** fehlt eine Begründungspflicht für richterliche Beschlüsse. Auf die in wissenschaftlichen Studien festgestellten aufsehenerregenden Praxisdefizite wurde nicht reagiert.
- Die **Benachrichtigungsregel** enthält Schlupflöcher, die eine Information der Betroffenen im Einzelfall umgehen oder ausschließen. Die Benachrichtigungspflicht ergibt sich aus der Rechtsweggarantie und hat darüber hinausgehend grundrechtswahrende Bedeutung. Sie darf nach unserem Verfassungsrecht nur in eng begrenzten Fällen unterbleiben. Die bestehenden Defizite in der Praxis werden verstärkt.

Was ist zu tun?
Es ist darauf hinzuarbeiten, dass der Europäische Gerichtshof und das Bundesverfassungsgericht das Gesetz und die zugrunde liegende Richtlinie im Hinblick auf die Kritikpunkte umfassend beurteilen und dann zurückweisen.

4.3.2 Kontrollbefugnis

Beschränkungen der Kontrollbefugnis des ULD bei den Staatsanwaltschaften waren bisher oft Auslöser von Konflikten. Es ist zwar noch keine förmliche Klärung erreicht, doch wurde dem ULD jüngst in verschiedenen Fällen gesetzeskonform Akteneinsicht bzw. Auskunft erteilt. Das Thema beschäftigte in den letzten Jahren nicht nur das ULD und den Generalstaatsanwalt, sondern auch das Innenministerium und den Landtag.

Anlass waren Verweigerungen bzw. Einschränkungen unserer Kontrollmöglichkeiten in Einzelfällen (29. TB, Tz. 4.3.3). Der Generalstaatsanwalt meinte, das ULD dürfe nur dann prüfen, wenn es um die Anwendung datenschutzrechtlicher Vorschriften im engeren Sinne gehe. Dies sei nicht der Fall, wenn sich ein „datenschutzrechtlicher Reflex" aus einzelnen Ermittlungen ergibt. Der Begriff des „datenschutzrechtlichen Reflexes" hat keine gesetzliche Grundlage und ist nicht definierbar; er löst allenfalls Rechtsunsicherheit aus. Wir haben als Kompromiss angeboten, das **Ermittlungsermessen als praktische Grenze** unserer Kontrollen zu nehmen. Die Strafprozessordnung regelt vor allem Datenerhebungen – z. B. im Rahmen einer Telekommunikationsüberwachung – und den Schutz der Betroffenen hiervor; sie enthält somit datenschutzrechtliche Vorschriften. Würde etwa ein erforderlicher Richtervorbehalt nicht beachtet, müssten wir dies im Rahmen unserer Kontrollbefugnis beanstanden. Die Beurteilung, ob die Maßnahme ermittlungstaktisch sinnvoll ist, überlassen wir der Staatsanwaltschaft, ebenso die Frage, ob der Verdacht eines bestimmten Straftatbestands hinreichend ist. Eine schriftliche Reaktion des Generalstaatsanwalts auf unser Angebot erfolgte bisher nicht.

Ungeachtet dessen wurde uns im Rahmen der letzten Kontrolle die Akteneinsicht bei der Staatsanwaltschaft Kiel in Abstimmung mit dem Generalstaatsanwalt ermöglicht. Es besteht also **Hoffnung** auf eine künftige tragbare praktische Handhabung.

Was ist zu tun?
Der Generalstaatsanwalt sollte unseren Kompromissvorschlag akzeptieren.

4.3.3 Datenübermittlung an Interessenverband der Unterhaltungsindustrie

Die Polizei hat nach Rücksprache mit der Staatsanwaltschaft einen beschlagnahmten Personalcomputer mit zahlreichen persönlichen Informationen eines Petenten an einen Interessenverband der Unterhaltungsindustrie übergeben. Diese Datenübermittlung war unzulässig.

Der Computer des Petenten war im Rahmen eines Strafverfahrens beschlagnahmt worden. Der ursprüngliche Tatvorwurf erwies sich als nicht haltbar, doch wurden auf dem Rechner verschiedene urheberrechtlich geschützte Filmdateien gefunden. Darauf übergab die Polizeibehörde nach Rücksprache mit der sachleitenden Staatsanwaltschaft den vollständigen Rechner einem Interessenverband, der sich der gezielten **Bekämpfung von Urheberrechtsverletzungen** verschrieben hat. Außerdem wurde der ursprüngliche Tatvorwurf mitgeteilt. Auf dem Rechner befanden sich zahlreiche private Dateien des Petenten, die mit dem Tatvorwurf der Urheberrechtsverletzung in keinem Zusammenhang standen. Der Rechner wurde vollständig durch einen technischen Mitarbeiter des Interessenverbandes ausgewertet. Insbesondere nahm dieser den gesammelten E-Mail-Verkehr des Betroffenen in Augenschein. Die Staatsanwaltschaft erhielt hierüber einen umfassenden „Auswertungsbericht“, fast zeitgleich fertigte die Rechtsabteilung des Verbandes einen Strafantrag gegen den Petenten.

Grundsätzlich ist eine Datenübermittlung an **Sachverständige** im Strafverfahren nicht ausgeschlossen, wenn die Strafverfolgungsbehörden auf diese Hilfe angewiesen sind. Dabei hat die Staatsanwaltschaft jedoch auf die strikte Wahrung der **Neutralität** und Zuverlässigkeit der Sachverständigen zu achten. Das Landgericht Kiel hat im Jahr 2006 klar entschieden, dass ein Interessenverband nicht neutral ist. Besondere Brisanz hatte der Fall dadurch, dass der Rechner ohne klare Festlegung der Tätigkeit des Interessenverbandes übergeben wurde; ein schriftlicher Gutachtenauftrag fand sich in der von uns geprüften Akte nicht. Die Mitarbeiter des Verbandes sollten selbst beurteilen, welche möglichen Verstöße sie feststellen und zur Ahndung bringen wollen.

Die Staatsanwaltschaft teilte uns mit, dass die Entscheidung des Landgerichts Kiel bei allen Dezernentinnen und Dezernenten besonders bekannt gemacht wurde, um den Blick für die Belange des Datenschutzes zu schärfen. Über zusätzliche Gespräche sollte das **Problembewusstsein** verstärkt werden. Der Einzelfall wurde als kritisch angesehen. Allerdings begegne es Bedenken, wenn und soweit generell die Rechtmäßigkeit der Hinzuziehung von Mitarbeitern eines Interessenverbandes

angezweifelt werde. Es bestehe das Problem einer hohen Auslastung der Beweissicherungsstellen der Polizei, was zu langen Wartezeiten führen könne.

Eine Beanstandung im konkreten Fall durch das ULD sei nicht angemessen; die Tätigkeit der Staatsanwaltschaft weise generell eine **Gefahrenneigung** auf. Die Aufgabenerfüllung der Staatsanwaltschaft bringe typischerweise mehr Grundrechtseingriffe mit sich als in anderen Bereichen der Verwaltung. Daher laufe nahezu jede Entschließung der Staatsanwaltschaft Gefahr, als besonders schwer wiegender Datenschutzverstoß qualifiziert zu werden. Der konkrete Fall sei auch auf die Hektik des Tagesgeschäfts zurückzuführen, in der die Anweisung zur Weitergabe des Rechners nur telefonisch erteilt worden sei.

Trotz dieser Darlegung bleiben wir bei der Qualifizierung des Einzelfalls als besonders schwer wiegende Verletzung datenschutzrechtlicher Vorschriften. Der Umstand besonders intensiver Grundrechtseingriffe muss bei der Staatsanwaltschaft gerade zur Anwendung eines extrem hohen Sorgfaltsmaßstabes führen. Der Fall lässt sich aus unserer Sicht nicht auf die Hektik des Einzelfalles zurückführen, sondern offenbart ein **strukturelles Problem** im Umgang mit den Interessenverbänden. Die hohe Auslastung der Polizeibehörden kann kein Grund sein, Teile der Ermittlungsarbeit in den – parteiischen – Privatbereich auszulagern.

Der Informationsaustausch mit Interessenverbänden ist rechtlich stark eingeschränkt, aber nicht generell ausgeschlossen. Im konkreten Fall hätte die Möglichkeit bestanden, die bereits vorhandene Liste der aufgefundenen Dateien **zunächst anonymisiert** zu übermitteln. Im Falle einer konkret festgestellten Urheberrechtsverletzung hätte dann eine auf den relevanten Sachverhalt begrenzte Auskunft an die verletzten Rechteinhaber bzw. eine Akteneinsicht erfolgen können. Nach Vorlage einer Vollmacht hätte diese auch durch den Interessenverband wahrgenommen werden können. Die Strafprozessordnung erlaubt eine solche – hierauf begrenzte – Datenübermittlung an die Opfer einer Straftat.

Was ist zu tun?
Das strukturelle Problem der Überlastung der Beweissicherungsstellen der Polizei darf nicht zur Auslagerung von Ermittlungsarbeit in den Privatbereich führen. Sachverständige sind nach dem Grundsatz der Unparteilichkeit auszuwählen. Interessenverbände dürfen personenbezogene Daten nur unter den Voraussetzungen erhalten, unter denen Opfer einer Straftat bzw. deren Bevollmächtigte Akteneinsicht erhalten können.

4.4 Verkehr

4.4.1 Online-Anbindung der Fahrerlaubnisbehörden an Kraftfahrt-Bundesamt

Das Chaos bei der Zentralisierung der Führerscheindaten beim Kraftfahrt-Bundesamt (KBA) lichtet sich langsam. Ein neuer Datenabgleich zwischen den Fahrerlaubnisbehörden und dem KBA soll zur Korrektur der fehlerhaften Informationen führen. Weiterhin gefährdet das nicht genügend durchdachte technische Konzept den Bestand und die Rechtsverbindlichkeit der gespeicherten Informationen.

Die Zentralisierung der Führerscheindaten beim KBA brachte große Datenschutzprobleme mit sich (29. TB, Tz. 4.4.2). Unter Federführung des ULD erarbeitete die Konferenz der Datenschutzbeauftragten ein Gutachten zu rechtlichen und technischen Fragen, die sich mit der Online-Anbindung der Fahrerlaubnisbehörden an das KBA stellen. Dieses dem Bundesministerium für Verkehr, Bau und Stadtentwicklung zugeleitete **Gutachten** soll die Bundesregierung dazu bringen, die defizitären rechtlichen Regelungen an die technischen Notwendigkeiten für eine sichere elektronische Datenverarbeitung anzupassen. Dabei sind verbindliche Sicherheitsstandards festzulegen. Die Richtigkeit der ausschließlich automatisiert gespeicherten Daten sowie die Sicherheit der elektronischen Kommunikation der Fahrerlaubnisbehörden mit dem KBA müssen langfristig garantiert werden. Derartiger Standards bedarf es auch für die ab September 2008 beginnende Online-Kommunikation der Kfz-Zulassungsbehörden mit dem KBA.

Was ist zu tun?
Der Bundesgesetzgeber muss den Rechtsrahmen an die Notwendigkeiten von Rechtsverbindlichkeit und Sicherheit der beim KBA zentral gespeicherten Führerscheindaten anpassen.

4.4.2 Fachaufsicht über Kfz-Zulassungsbehörden auf Tauchstation

Wenn Datenschutzverstöße festgestellt werden, ist die zuständige Aufsichtsbehörde zu unterrichten. Diese soll im Zweifel per Weisung an die geprüfte Stelle erreichen, dass der Datenschutz zukünftig beachtet wird. Das Verkehrsministerium verfolgt eine andere Praxis.

Wie schon bei Fahrerlaubnisbehörden werden künftig auch die Kfz-Zulassungsbehörden ihre Daten im Online-Dialog mit dem Kraftfahrt-Bundesamt (KBA) verarbeiten. Gemäß dem ursprünglichen technischen Konzept sollte der Nachweis der ordnungsgemäßen und richtigen Datenverarbeitung durch die **Protokollierung der Tätigkeit jedes Sachbearbeiters** erfolgen. Hierfür werden vom KBA an die lokalen Behörden Chipkarten ausgegeben, die einzelnen Mitarbeiterinnen und Mitarbeitern dieser Stelle zugeordnet werden.

Vor einigen Jahren musste das KBA allerdings die Einrichtung sogenannter Kopfstellen bei den Zulassungsbehörden akzeptieren. Dies sind zentrale Rechner, an

die mehrere Sachbearbeiter-PCs angeschlossen werden können. Die Bündelung in Kopfstellen führt dazu, dass das KBA nicht mehr die Aktivitäten einzelner Sachbearbeiter feststellen kann, da protokollierte Vorgänge nicht mehr den einzelnen handelnden Personen zugerechnet werden, sondern nur noch der Behörde, die die Kopfstelle betreibt. Um dennoch eine revisionsfähige Protokollierung der Zugriffe zu ermöglichen, machte das KBA die Einrichtung und den Betrieb solcher Kopfstellen von einer **Selbstverpflichtung der Behörde** abhängig, wonach diese u. a. intern protokollieren muss, welcher Sachbearbeiter welche personenbezogenen Daten elektronisch verarbeitet hat. Wir haben bei mehreren Behörden die Umsetzung der Vorgaben für solche Kopfstellen angeschaut. Die Ergebnisse waren erschreckend. Lediglich bei einer Stelle war es überhaupt möglich, die erzeugten Protokolldaten zu überprüfen. Die weiteren Vorgaben des KBA zur Datensicherheit und zur Dokumentation der Verfahren waren in keiner der geprüften Behörden umgesetzt worden.

Gemeinsam mit dem KBA haben wir daraufhin **Hinweise für die Behörden** erarbeitet und das Verkehrsministerium gebeten, diese im Erlasswege den Behörden im Land bekannt zu geben. Das Ministerium erteilte unserer Bitte jedoch eine Absage mit dem Hinweis, man würde mit dem geforderten Erlass in die Selbstverwaltungsautonomie der Kommunen eingreifen. Uns wurde der Rat gegeben, die festgestellten Mängel jeweils im Einzelfall zu beanstanden und dann die Kommunalaufsicht des Innenministeriums zu informieren. Diese möge sich dann um die Angelegenheit kümmern. Diese Haltung ist für uns nicht nachvollziehbar. Es ist Aufgabe des Ministeriums als Fachaufsichtsbehörde, sich um die Abstellung festgestellter Mängel im Zusammenhang mit personenbezogener Datenverarbeitung zu kümmern.

Der Vorgang zeigt die dringende Notwendigkeit **einheitlicher bundesgesetzlicher Regelungen** für die Online-Kommunikation der Fahrerlaubnisbehörden und der Kfz-Zulassungsbehörden. Das Verkehrsministerium hätte die Durchsetzung gesetzlicher Vorgaben wohl weniger verweigert als unsere fachlich und datenschutzrechtlich begründeten praktischen Anforderungen.

Was ist zu tun?
Das Verkehrsministerium kann und muss als einzige Stelle im Land verbindlich eine rechtskonforme Kommunikation der Zulassungsbehörden mit dem KBA sicherstellen.

4.5 Soziales

4.5.1 Sozialgesetzbuch II – Was hat sich jüngst getan?

Noch immer erreicht das ULD eine wahre Eingabenflut rund um das **Arbeitslosengeld II** (ALG II). Dauerbrenner sind die Anforderung von Kontoauszügen (Tz. 4.5.2) oder Hausbesuche (Tz. 4.5.3); uns beschäftigen zudem neue Fragestellungen zu Eingliederungsmaßnahmen (Tz. 4.5.5).

Die Zusammenarbeit mit den **Arbeitsgemeinschaften** (ARGEn) hat sich verbessert. Deren Geschäftsführer haben erkannt, dass das ULD, wenn dies berechtigt ist, scharf kritisiert, gleichwohl aber stets mit konstruktivem Rat zur Seite steht. Die gemeinsam mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) herbeigeführte Klärung der Zuständigkeiten war für diese konstruktive Wende wichtig (29. TB, 4.5.1).

Sehr zu unserer Freude wurde über den BfDI erreicht, dass die Bundesagentur für Arbeit für ihre zentralen Verfahren **Berechtigungs- und Löschungskonzepte** erarbeitet hat (28. TB, Tz. 4.5.1). Wir werden die Installation vor Ort nachprüfen.

4.5.2 Anforderung von Kontoauszügen – Zurückhaltung ist gefragt

Ob und in welchem Umfang bei der erstmaligen Beantragung oder Weiterbewilligung von ALG II die Vorlage von Kontoauszügen gefordert wird, entscheidet beinahe jeder Leistungsträger anders. Wie sollen sich da die Hilfesuchenden zurechtfinden?

Das hatte unser ULD-Mitarbeiter nicht erwartet. Vor ihm saßen Vertreter von 26 verschiedenen Arbeitsgemeinschaften und Optionskommunen aus ganz Deutschland und diskutierten aufgeregt die Erforderlichkeit der Anforderung von Kontoauszügen. Einige sahen im Anfordern und Kopieren von Kontoauszügen eine überflüssige und sinnlose **Arbeitsbeschaffungsmaßnahme**, hätte sich doch in der Vergangenheit gezeigt, dass diese kaum neue Informationen enthielten. Andere beharrten darauf, dass, solange Hilfesuchende Leistungen beziehen würden, diese jeden Kontoauszug ungeschwärzt vorlegen müssten, da nur so wirksam dem **Leistungsmissbrauch vorzubeugen** wäre.

Das Gesetz sieht vor, dass Sozialdaten nur erhoben werden dürfen, wenn dies zur **Aufgabenerfüllung erforderlich** ist. Darüber, was fachlich erforderlich ist, scheinen sich die Leistungsträger aber uneinig zu sein.

Zunächst müssen die Leistungsträger für sich klären, welchem **Zweck** die Kontoauszüge dienen sollen. Geht es lediglich darum festzustellen, ob jemand aktuell bedürftig ist, so dürften nur wenige Kontoauszüge, z. B. des letzten Monats, erforderlich sein, können doch Einkünfte und Ausgaben vor mehreren Monaten für die Feststellung kaum noch berücksichtigt werden. Anders verhält es sich, wenn Angaben des Betroffenen auf ihre Vollständigkeit und Richtigkeit kontrolliert werden müssen. Ob ein Anlass für diese Kontrollen besteht, kann nur bezogen auf den **konkreten Einzelfall** festgestellt werden. Alle Antragsteller und Leistungsempfänger unter einen Generalverdacht zu stellen, ist datenschutzrechtlich nicht zulässig. Das Schleswig-Holsteinische Landessozialgericht sieht dies in einer Entscheidung vom Juli 2007 ebenso wie wir.

Die Leistungsträger sind dringend gefordert, ihre Verwaltungspraxis auch unter datenschutzrechtlichen Gesichtspunkten aufeinander abzustimmen. Die bestehende **Uneinigkeit** darf **nicht zulasten der Hilfesuchenden** gehen.

Das ULD hat seine Rechtseinschätzung bereits 1998 in einer **Bekanntmachung** hierzu veröffentlicht (21. TB, Tz. 4.7.4). Diese wurde fortgeschrieben in den „Gemeinsamen Hinweisen zur datenschutzgerechten Ausgestaltung der Anforderung von Kontoauszügen bei der Beantragung von Sozialleistungen der Landesbeauftragten für den Datenschutz der Länder Berlin, Brandenburg, Hamburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und Schleswig-Holstein“ (28. TB, Tz. 4.5.1). Die dort dargestellte Bewertung berücksichtigt sowohl den Informationsbedarf der Leistungsträger als auch das Interesse der Betroffenen, keine überflüssigen Daten preisgeben zu müssen. In Schleswig-Holstein richten sich die Leistungsträger überwiegend nach diesen Hinweisen und haben uns immer wieder bestätigt, dass die Hinweise einen praktikablen Lösungsansatz darstellen. Diese Hinweise sind im Internet abrufbar unter

www.datenschutzzentrum.de/materialien/themen/bekannt/kontoaus.htm

Was ist zu tun?
Die Leistungsträger müssen ernsthaft klären, welche Angaben und Unterlagen aus fachlicher Sicht jeweils erforderlich sind. Zu viele Daten zu erheben ist gesetzlich nicht zulässig, bindet unnötig Arbeitskraft und belastet die Betroffenen über Gebühr. Verbindliche Vorgaben für die Anforderung von Unterlagen, z. B. von Kontoauszügen, sollten bundesweit abgestimmt werden.

4.5.3 Unberechtigte Befragung des vermeintlichen Arbeitgebers

Nach dem Sozialgesetzbuch sind die ARGEn berechtigt, von Arbeitgebern Auskunft über Tatsachen zu verlangen, die für die Entscheidung über einen ALG-II-Leistungsanspruch erheblich sein können. Dies berechtigt sie nicht zu Fragen, die keinen Bezug zum Arbeitsverhältnis haben.

Eine Promotionsstudentin hatte einen Antrag auf ALG II gestellt, in dem sie wahrheitsgemäß angab, Diplomdoktorandin an einer Universität in Norddeutschland zu sein. Der zuständige Sachbearbeiter des Leistungszentrums der ARGE überprüfte die Angaben im Internet und fand sie bestätigt: Die Antragstellerin war tatsächlich (nur) als Diplomdoktorandin auf der Seite der Universität verzeichnet. Er ging jedoch fälschlicherweise davon aus, dass eine Doktorandinnenstelle von der Uni entlohnt werde. Aufgrund dieses Irrtums stellte er ein **Auskunftsverlangen** an den die Doktorarbeit **betreuenden Universitätsprofessor**. Dabei unterstellte er nicht nur dessen Arbeitgebereigenschaft, sondern verlangte zudem Auskünfte über Sachverhalte, die in keinerlei Bezug zu dem fälschlicherweise angenommenen Arbeitsverhältnis standen. Insbesondere bat er darum, der ARGE mitzuteilen, ob der Universitätsprofessor etwa von der Bewilligung eines Stipendiums für die Antragstellerin durch dritte Stellen wisse.

Dieses Vorgehen war unzulässig und wurde bei dem für die Fachaufsicht zuständigen Sozialministerium beanstandet. Im Rahmen des Auskunftsverlangens darf der Arbeitgeber nur über Tatsachen befragt werden, die das Arbeitsverhältnis betreffen. Es ist unzulässig, vom Arbeitgeber Auskunft über Umstände zu verlangen, die nichts mit dem konkreten Arbeitsverhältnis zu tun haben und von denen er nur zufällig erfahren hat, etwa in der Kaffeepause oder auf dem Betriebsausflug. Die Erheblichkeit des Verstoßes ergab sich im benannten Fall zudem aus dem Umstand, dass die ARGE auch nach unserer rechtlichen Information **kein Problembewusstsein** erkennen ließ. Sie sah keine Veranlassung, uns Maßnahmen zur Vermeidung derartiger rechtswidriger Befragungen zu beschreiben oder anzukündigen.

Die Bekämpfung von Leistungsmissbrauch ist ein wichtiges Anliegen im Bereich des Sozialrechts. Ungezielte Befragungen greifen unnötigerweise erheblich in die Persönlichkeitsrechte der Betroffenen ein und stehen wegen ihrer abschreckenden Wirkung dem gesellschaftlichen Interesse entgegen, durch die berechtigte Inanspruchnahme von Sozialleistungen Notlagen zu vermeiden. Derartige **investigative Ermittlungsmethoden im Sozialbereich** können das Vertrauen der Bürger untereinander und gegenüber dem Staat nachhaltig beeinträchtigen. Wenn die Befragten angehalten werden, umfassende Angaben zu den Lebensumständen ihrer Mitmenschen zu machen, wird jeder zur potenziellen Auskunftsperson über private Angelegenheiten seiner Mitbürger. Dies kann zu einer Vergiftung des gesellschaftlichen Klimas führen. In diesem sensiblen Bereich ist im besonderen Maße für ein ausgewogenes Vorgehen Sorge zu tragen.

Was ist zu tun?
Die ARGEn müssen Maßnahmen zur Qualitätssicherung einführen, z. B. das Vieraugenprinzip bei speziellen Fallgestaltungen. Die durch unberechtigte Befragungen bewirkte Rufschädigung der Betroffenen ist keine Bagatelle.

4.5.4 Das „SEK“ des Jobcenters

Obwohl unsere „Hinweise zur datenschutzgerechten Ausgestaltung von Hausbesuchen“ in die maßgebliche Handlungsempfehlung der Bundesagentur für Arbeit Eingang fanden, schildern uns Hilfesuchende immer wieder haarsträubende Begebenheiten.

Im letzten Jahr berichteten wir über **problematische Hausbesuche** (29. TB, Tz. 4.5.3). Es scheint fast, als würde dieses Thema eine Never ending story. Montagmorgen kurz vor 9 Uhr klingelte es an der Haustür. Nur mit einem Top und einem Slip bekleidet, öffnet die junge Frau die Tür. Sie wird später erklären, man habe ihr nicht erlaubt, sich etwas überzuziehen. Auch ihr Nachbar wird aufgesucht. Im Bericht wird über ihn zu lesen sein: „Zu Beginn des Besuches wirkt Herr XY entspannt und ausgeruht, sein Gesicht ist eher blass. Er erscheint weder verschwitzt noch abgehetzt. Dagegen bilden sich zum Ende des Gespräches Schweißperlen auf seiner Oberlippe.“ Der Nachbar wird intensiv zu seinem bisherigen Leben befragt. Dezidiert werden Angaben zu einem Unfall und den

daraus resultierenden Kopfverletzungen vermerkt. Akribisch notiert der Außendienst jede Beobachtung in dem umfangreichen Prüfbericht. Es finden sich Notizen wie: „Sechs Zigaretten im Aschenbecher in der Küche, im Flur befindet sich in einem Schrank eine Plastikdose mit Weihnachtskugeln, im Wohnzimmerschrank vier Medikamentenschachteln." Selbst die Glühbirne an der Küchendecke wird festgehalten.

Was sich wie ein Protokoll der Stasi der DDR liest, ist der **Prüfbericht des Außendienstes einer ARGE**. Dieser sollte feststellen, ob die Frau, die mit ihren zwei Kindern eine Zweizimmerwohnung bewohnt, eventuell mit ihrem Nachbarn, der eine Einzimmerwohnung hat, in „eheähnlicher Gemeinschaft" lebt. Dass der Nachbar die junge Frau ins Amt begleitete, reichte dem Sachbearbeiter aus, um den Prüfdienst loszuschicken.

Die **Liste der Beschwerden** ist lang. In einem anderen Fall berichtete das Ministerium für Justiz, Arbeit und Europa von einem äußerst kreativen Außendienstmitarbeiter, der sich in Abwesenheit des Hilfesuchenden mithilfe des Hausmeisters bzw. eines Nachschlüssels Zugang zu der Wohnung verschaffte. Eine Mutter schilderte uns, dass die Befragung ihrer Nachbarn dazu führte, dass nun ihre Kinder gehänselt werden. In einem anderen Fall berichtete uns ein Ehepaar, dass sogar der im benachbarten Dorf lebende Großvater befragt worden sei.

Was genau ist die Ursache für diese Entgleisungen? Ein **Blick ins Gesetz** lässt Schlimmes ahnen: Die Leistungsträger sind verpflichtet, einen Außendienst „zur Bekämpfung von Leistungsmissbrauch" einzurichten. Primäres Ziel der Außendienstmitarbeiter soll es also sein, möglichst viele Betrüger ausfindig zu machen. Der Außendienst mutiert so zu einem Sondereinsatzkommando (SEK). Anders als bei der Polizei werden jedoch nicht speziell ausgebildete und geschulte Mitarbeiter mit dieser Tätigkeit beauftragt. Es sind normale Verwaltungsmitarbeiter, die von Wohnung zu Wohnung eilen, um vermeintliche Betrügerinnen und Betrüger zu überlisten.

Verantwortungsbewusste Leistungsträger müssen erkennen, dass es nicht ausreicht, unerfahrenen jungen Mitarbeitern eine Dienstanweisung in die Hand zu drücken. Fernsehsendungen wie „Tatort" oder „CSI Miami" dürfen nicht zur Arbeitsgrundlage des Außendienstes werden. Die Mitarbeiter müssen den Unterschied zwischen Hausbesuchen und Hausdurchsuchungen, einer Befragung und einem Verhör kennen. Andernfalls bleibt das Sozialgeheimnis auf der Strecke und die Mitarbeiter des Außendienstes werden der Gefahr strafrechtlicher Konsequenzen ausgesetzt. Die Tätigkeit im Außendienst erfordert eine **fortlaufende Schulung**. Die Leistungsträger sind gefordert, entsprechende Schulungsmöglichkeiten aufzuzeigen.

Was ist zu tun?
Die rechtliche Verantwortung dafür, dass Hausbesuche – wenn überhaupt erforderlich – unter Beachtung der einschlägigen Gesetze durchgeführt werden, liegt bei jeder einzelnen Arbeitsgemeinschaft bzw. Optionskommune. Diese sind gefordert, ihre Mitarbeiterinnen und Mitarbeiter ausreichend auf die schwierige Tätigkeit im Außendienst vorzubereiten. Nur geschultes und verantwortungsbewusstes Personal darf eingesetzt werden. Die Tätigkeit des Außendienstes muss fortwährend einer internen Qualitätsprüfung unterzogen werden.

4.5.5 Eingliederungsmaßnahmen – Was darf gefragt werden?

Unter Eingliederungsmaßnahmen versteht man jene Angebote und Hilfen der Leistungsträger, die dazu beitragen sollen, dass Hilfesuchende möglichst schnell wieder in den Arbeitsmarkt integriert werden. Mit der Durchführung der Eingliederungsmaßnahmen werden häufig private Unternehmen beauftragt.

Wir schilderten, unter welchen **rechtlichen Rahmenbedingungen** die Leistungsträger mit den Maßnahmeträgern Daten austauschen dürfen (29. TB, Tz. 4.5.7). Im Folgenden soll näher beleuchtet werden, wie welche Daten von den Maßnahmeträgern erhoben und verarbeitet werden dürfen.

- **Erfordernis einer Einwilligung des Betroffenen**

Die bzw. der Betroffene muss in die Datenerhebung einwilligen. Diese Einwilligung kann Gegenstand eines Maßnahmevertrages (nicht zu verwechseln mit der Eingliederungsvereinbarung) sein. Aber aufgepasst: Wenn besondere Arten von personenbezogenen Daten, also z. B. Daten über die Gesundheit, erhoben werden sollen, bedarf es unter Umständen einer gesonderten bzw. ausdrücklichen Einwilligung. Die Wirksamkeit der Einwilligung setzt voraus, dass dem Betroffenen der **konkrete Inhalt** der Eingliederungsmaßnahme **dargelegt** wird.

- **Umfang der Datenerhebung**

Grundsätzlich gilt, dass nur die Daten erhoben werden dürfen, **die erforderlich sind**, um die konkrete Maßnahme durchzuführen. Es dürfen umso mehr Daten erhoben werden, je umfangreicher und komplexer die Maßnahme ist.

Bei umfangreichen Maßnahmen kann, ähnlich wie schon zuvor bei dem Leistungsträger, ein **Profiling** durchgeführt werden. Welche Fragen zur Schul- und Berufsausbildung, zur familiären Situation, zu gesundheitlichen Einschränkungen, zu Drogen und Vorstrafen erforderlich sind, hängt maßgeblich vom Einzelfall ab. Pauschalisierte Fragenkataloge bergen stets die Gefahr, dass Daten erhoben werden, die nicht erforderlich sind. Hier sind in besonderem Maße die Mitarbeiterinnen und Mitarbeiter bei den Maßnahmeträgern gefragt. Diese müssen geschult und sensibilisiert werden, auch mal eine Frage nicht zu stellen, wenn diese nicht erforderlich ist.

Manche **Fragebögen** zielen auf alle denkbaren Fallgestaltungen und gehen so zu weit, z. B. ein uns überreichter Vordruck „Freiwillige Selbstauskunft“. In diesem wurden Frauen nach „Zyklusstörungen/erheblichen Menstruationsbeschwerden“ gefragt. Es sollte angegeben werden, ob gelegentlich Alkohol konsumiert wird oder ob man raucht. Es wurde gefragt, in welchem Verein man sich sportlich betätigt und welche Medikamente eingenommen werden. Auch dass genau abgefragt wurde, ob innerhalb der Familie Krankheiten wie Anfallsleiden, Allergien, Behinderungen oder Hautkrankheiten bekannt sind, wurde von uns als datenschutzrechtlicher Verstoß bewertet.

- **Transparenz der Datenerhebung**

Daten sind grundsätzlich mit Kenntnis des Betroffenen zu erheben. Feststellungen über das Verhalten und die erbrachten Leistungen sind offenzulegen. Gibt es Defizite, z. B. im Erscheinungsbild, oder lässt eine Fahne am Morgen auf ein Alkoholproblem schließen, so dürfen diese Erkenntnisse nur vermerkt werden, wenn der **Betroffene unterrichtet** wird.

- **Das besondere Berufsgeheimnis beim Maßnahmeträger**

Ein privater Maßnahmeträger muss die Vorschriften des Bundesdatenschutzgesetzes beachten. Aber aufgepasst: Erfolgt eine Schuldner- oder Suchtberatung als Eingliederungsmaßnahme, oder führt ein Mitarbeiter als staatlich anerkannter Sozialarbeiter oder staatlich anerkannter Sozialpädagoge eine psychosoziale Betreuung durch, dann gilt zusätzlich ein besonderes Berufsgeheimnis. Wie Ärzte unterliegen diese Mitarbeiter einer strafbewehrten **persönlichen Schweigepflicht** (Patientengeheimnis). Diesem besonderen Berufsgeheimnis unterfallende Daten dürfen beim Maßnahmeträger anderen Mitarbeitern nur zur Verfügung stehen, wenn der Betroffene hiermit ausdrücklich einverstanden ist. Der Leistungsträger darf aber keine Kenntnis davon erhalten.

- **Datenübermittlung vom Maßnahmeträger an den Leistungsträger**

Ein Maßnahmeträger ist nicht nur berechtigt, sondern sogar verpflichtet, dem Leistungsträger Daten zu übermitteln. Es gibt jedoch noch keine **verbindliche Vorgaben** darüber, wie und in welcher Form diese Rückmeldung erfolgen soll (29. TB, Tz. 4.5.7). Einzelne Arbeitsgemeinschaften haben auf diese Mangelfeststellung reagiert. So wurden wir u. a. von der Geschäftsführung der ARGE Stormarn eingeladen, bei der inhaltlichen Ausgestaltung des durchzuführenden Datenaustausches mit den regionalen Maßnahmeträgern aus datenschutzrechtlicher Sicht mitzuwirken. Über das Ergebnis werden wir berichten.

- **Aufbewahrung der Daten beim Maßnahmeträger**

Die bei den Maßnahmeträgern erhobenen **Daten sind zu löschen**, sobald diese für die weitere Aufgabenerfüllung nicht mehr erforderlich sind. Dies ist regelmäßig der Fall, wenn die Maßnahme beendet wurde, spätestens jedoch zwei Jahre danach. Auch die Bundesagentur für Arbeit bzw. deren Regionaldirektion Nord

sieht keine Erforderlichkeit für eine längere Aufbewahrung. Die Aufbewahrungsfrist ist in dem Vertrag des Leistungsträgers mit dem Maßnahmeträger zu definieren.

Was ist zu tun?
Die Maßnahmeträger dürfen nur Daten erheben, soweit der Betroffene einwilligt. Sie sind gesetzlich verpflichtet, die Datenerhebung auf das erforderliche Mindestmaß zu beschränken. Bestimmte Eingliederungsmaßnahmen, wie z. B. eine Suchtberatung, unterliegen einem besonderen Berufsgeheimnis. Leistungs- und Maßnahmeträger müssen ein datenschutzgerechtes Konzept für den beabsichtigten Austausch erarbeiten. Nach Beendigung der Maßnahme sind die erhobenen Daten spätestens nach zwei Jahren vom Maßnahmeträger zu löschen.

4.5.6 Die neue Aktenführung bei der Deutschen Rentenversicherung Nord

Bei einem Rentenversicherungsträger wurden medizinische Daten – eingereichte Atteste, Gutachten und Untersuchungsberichte – nicht getrennt von der Verwaltungsakte aufbewahrt, sodass Verwaltungsmitarbeiter ohne medizinische Ausbildung Zugang zu den zum Teil hochsensiblen Daten der Antragsteller hatten. Dies ändert sich nun.

Unsere Kollegen vom Hamburgischen Datenschutzbeauftragten stellten die bisherige Praxis als Erste infrage. Wer eine **Rentenleistung aus gesundheitlichen Gründen** beantragt, muss zum Nachweis ärztliche Atteste einreichen, auf deren Grundlage die Ärzte des sozialmedizinischen Dienstes des Rentenversicherungsträgers (SMD) ein Gutachten erstellen. Dieses Gutachten ist Grundlage für die Entscheidung der jeweiligen Leistungsabteilung (Verwaltung). Bislang wurden alle Unterlagen, also auch die ärztlichen Unterlagen, von den Mitarbeitern der Leistungsabteilung verwaltet.

Zugegebenermaßen brauchen manche Dinge viel Zeit, aber oft lohnt es sich, einen langen Atem zu behalten: Nachdem die Landesversicherungsanstalten der Länder Hamburg, Mecklenburg-Vorpommern und Schleswig-Holstein zur **Deutschen Rentenversicherung Nord** fusionierten, übernahm das ULD, unterstützt vom hiesigen Ministerium für Soziales, Gesundheit, Familie, Jugend und Senioren in enger Absprache mit den Kollegen aus Hamburg und Mecklenburg-Vorpommern die Klärung dieser Frage.

Nach anfänglichem Zögern akzeptierte die Geschäftsführung unser Anliegen. Zukünftig werden bei der Deutschen Rentenversicherung Nord die **Unterlagen des SMD** getrennt von den Akten der Leistungsabteilung geführt. Mitarbeiter der Leistungsabteilung sollen auf konkrete Anforderung und erst nach Freigabe durch den SMD nur noch die medizinischen Daten erhalten, die wirklich erforderlich sind, um über den jeweiligen Antrag entscheiden zu können.

Die Anstrengungen, die die Deutsche Rentenversicherung seitdem unternimmt, sind ausdrücklich zu loben. Mit großem personellem und finanziellem Aufwand

hat die Deutsche Rentenversicherung Nord begonnen, an allen drei Standorten die Archive und die dort befindlichen Akten neu zu strukturieren. Bei der **Trennung der Aktenbestände** werden zugleich Unterlagen, die nicht mehr benötigt werden, aussortiert und vernichtet. Künftig wird der SMD gesonderte Gutachtenakten getrennt von der Verwaltungsakte gesichert aufbewahren.

Die Deutsche Rentenversicherung Nord hat auch nicht bei den Papierakten haltgemacht. Es wurde ein neuartiges **Gutachteninformationssystem** – GIS – mit einem ausgeklügelten Berechtigungskonzept entwickelt. Das GIS ermöglicht eine elektronische Datenerfassung und -speicherung und, was aus Datenschutzsicht sehr wichtig ist, eine abgestufte Datenweitergabe an die Leistungsabteilung. Wir haben der Deutschen Rentenversicherung Nord empfohlen, ihre Bemühungen mit einem Audit bzw. einem Gütesiegel für das GIS zu krönen.

Was ist zu tun?
Das Sozialgeheimnis gilt auch innerhalb eines Sozialleistungsträgers. Nicht jeder Mitarbeiter darf auf alle Daten zugreifen können. Bei Rentenversicherungsträgern sind die Datenbestände des sozialmedizinischen Dienstes getrennt vom Leistungsbereich aufzubewahren.

4.5.7 Kinderschutzgesetz Schleswig-Holstein

Der Schutz von Kindern vor Vernachlässigung und Misshandlung ist ein wichtiges gesellschaftliches Anliegen. Zu diesem Schutz der betroffenen Kinder und Familien gehört auch, dass beim berechtigten Einsatz verstärkter Kontrollmaßnahmen die Verwendung von persönlichen Daten auf ein Minimum beschränkt wird und die Betroffenenrechte gewahrt bleiben.

Die Landesregierung und der Landtag erarbeiteten ein Gesetz zur Weiterentwicklung und Verbesserung des Schutzes von Kindern und Jugendlichen in Schleswig-Holstein, das im Dezember 2007 verabschiedet wurde. Das Gesetz enthält u. a. Vorschriften zur Verbesserung der Information und der Förderung, zur Gewährung von Leistungen und Hilfen für betroffene Kinder und Familien und zur Inobhutnahme von gefährdeten Kindern. Informationell besonders bedeutsam ist eine Ergänzung des Gesetzes über den öffentlichen Gesundheitsdienst (GDG). Die Regelung knüpft an die für Kleinkinder von den Krankenkassen angebotenen **Früherkennungsuntersuchungen** (U1 bis U9) an. Diese Untersuchungen finden erstmals unmittelbar nach der Geburt und dann bis zum Alter von 5½ Jahren in bestimmten, immer länger werdenden Abständen statt und sollen die gesunde Entwicklung der Kinder sicherstellen. Wohlgemerkt: Es gibt auch weiterhin keine Pflicht zur Teilnahme. Die Wahrnehmungsquote ist bei diesen Früherkennungsuntersuchungen aber traditionell recht hoch.

Die Früherkennungsuntersuchungen sollen mit der Neuregelung dazu genutzt werden, Vernachlässigung oder Misshandlung von kleinen Kindern zu entdecken, ohne aber direkten Zwang auszuüben. Es wird davon ausgegangen, dass Kinderärzte bei einer Untersuchung Anzeichen für solche Missstände erkennen können.

Daher soll die schon hohe **Teilnahmequote weiter erhöht** werden. Auch künftig verbleibt jedoch voraussichtlich eine gewisse Zahl von Kindern, die innerhalb der ersten sechs Lebensjahre nie von einer unabhängigen Stelle auf Gesundheit bzw. etwaige Anzeichen für Vernachlässigung untersucht werden. Das Ausbleiben eines Kindes bei einer Untersuchung soll als Anlass genommen werden, behördlicherseits zu überprüfen, ob die Nichtteilnahme etwa mit einer Vernachlässigung des Kindes einhergeht.

Zu diesem Zweck wird ein **Einladungs- und Rückmeldeverfahren** festgelegt. Eine sogenannte zentrale Stelle übernimmt die Adressdaten der gesetzlichen Vertreter von Kindern im Alter vom dritten Lebensmonat (U4) bis zu 5½ Jahren (U9) von den Meldebehörden. Die Aufgabe der zentralen Stelle wird vom Landesamt für soziale Dienste wahrgenommen. Es lädt die Kinder zur Teilnahme an der Früherkennungsuntersuchung ein bzw. erinnert an die Teilnahme, wenn diese nicht innerhalb eines vorgesehenen Zeitraums nach der ersten Einladung erfolgt. Schließlich werden die Daten der Nichtteilnehmer an die zuständige kommunale Stelle weitergemeldet. Beim Kreis bzw. einer kreisfreien Stadt wird schließlich das Jugendamt tätig und überprüft, ob die Nichtteilnahme im Zusammenhang mit einer Vernachlässigung des Wohlergehens des Kindes steht. Ein solches Verfahren wirft natürlich aus Datenschutzsicht viele Fragen auf.

Das ULD war bereits frühzeitig in die Gestaltung des Verfahrens einbezogen. Im Konsens konnten so wichtige Festlegungen getroffen werden. Dazu gehört, dass die **zentrale Stelle**, die die Einladungen versendet und die Rückmeldungen entgegennimmt, Daten von den Meldeämtern jeweils zeitnah vor dem Stichtag der Untersuchung übermittelt bekommt und nach Abschluss einer Einladungsrunde für eine bestimmte Untersuchung wieder löscht. Sie hält selbst keine parallelen Bestände zum Melderegister vor und speichert nicht über eine längere Dauer Daten über die (Nicht-)Teilnahme an den Untersuchungen. Die Einladungen werden mit einer eindeutigen Kennung (Barcode-Aufkleber) versehen. Auf diesem Schriftstück bestätigt der Arzt die Durchführung der Untersuchung. Dieses wird an die zentrale Stelle zurückgeschickt, entweder durch die Eltern oder durch den Arzt. Dabei ist zum Zeitpunkt der Abfassung des Berichtes noch offen, ob die Rücksendebögen lediglich den Barcode oder auch noch weitere Daten des Kindes im Klartext enthalten. Im ersten Fall können die Rückmeldungen als offene Postkarte versandt werden. Enthalten die Rücksendekarten dagegen offen lesbare persönliche Daten der Kinder, so muss ein verschlossener Briefumschlag benutzt werden.

Bei der zentralen Stelle werden die eingehenden Rückmeldekarten elektronisch erfasst und den zuvor angeschriebenen Personen eindeutig zugeordnet. Geht eine **Rückmeldung** ein, so werden die betreffenden Personen zeitnah aus dem Datenbestand gelöscht. Eine weitere Speicherung und Verarbeitung erfolgt in diesem Fall nicht. Erfolgt bis zu einem bestimmten Zeitraum nach Versendung der Erinnerung noch keine Rückmeldung, so werden die Daten an die Kommunen weitergegeben. Auch in diesem Fall werden die Daten bei der zentralen Stelle gelöscht.

Das ULD hatte vorgeschlagen, dass die Meldungen unmittelbar an die **kommunalen Jugendämter** erfolgen, welche ohnehin zur Sachverhaltsaufklärung tätig werden. Mit diesem Vorgehen sollten Probleme vermieden werden, die sich in einem gestuften Verfahren bei der Einschaltung einer weiteren Stelle ergeben, wie sie in einigen Bundesländern vorgesehen ist. Wenn die zentrale Stelle das Fehlen des Rücklaufs festgestellt hat, spricht dort zunächst das zuständige kommunale Gesundheitsamt eine weitere Einladung zur Untersuchung aus; erst wenn dies keinen Erfolg hat, soll das Jugendamt tätig werden. Aus Sicht des ULD sollte ein derartiger Umweg über das Gesundheitsamt vermieden werden. Mit Blick auf den Zweck der Regelung kann er in tatsächlichen Fällen von Misshandlung oder Vernachlässigung zu einer unnötigen Verzögerung führen.

Mit der vorrangigen Einschaltung des **Gesundheitsamtes** ergeben sich auch Datenschutzprobleme, weil ein sehr sensibler Datenbestand letztlich bei zwei unterschiedlichen kommunalen Stellen gespeichert wird und sich eine Synchronisierung und Aktualisierung dieser Daten in der Praxis als schwierig erweisen kann. In einer Vielzahl von Fällen, in denen die Kinder nicht zur Früherkennungsuntersuchung vorgestellt werden, gibt es hierfür Gründe, die mit Vernachlässigung nichts zu tun haben. Darüber hinaus sind Probleme in den grenznahen Regionen in Betracht zu ziehen. Eltern können z. B. einen Kinderarzt in Hamburg, Niedersachsen oder einem anderen Bundesland in Anspruch nehmen. Ärzte außerhalb des Landes Schleswig-Holstein können nicht durch Schleswig-Holsteinisches Landesrecht verpflichtet werden, die Bestätigungen zurückzusenden. Auch bei Ärzten im Land Schleswig-Holstein kann es vorkommen, dass eine Rücksendung nicht erfolgt. In all diesen Fällen landen die Daten der Eltern letztlich bei den kommunalen Stellen. Diese müssen daraufhin tätig werden, um den zunächst im Raum stehenden Verdacht der Kindeswohlvernachlässigung auszuschließen oder zu bestätigen.

Eine korrekte Vorgehensweise ist wichtig; nicht nur zur Abwendung etwaiger Gesundheitsgefahren, sondern auch im Hinblick auf den äußerst relevanten Eingriff in das informationelle Selbstbestimmungsrecht der ins Visier geratenen Eltern und Kinder. Dieser Eingriff ist nur zu rechtfertigen, wenn sichergestellt ist, dass konkrete Fälle von **Kindeswohlgefährdung schnell aufgedeckt und abgewendet** werden. Nicht akzeptabel wäre es, wenn auf kommunaler Seite Datenmeldungen entgegengenommen würden, ohne dass daraus ein konkretes Tätigwerden erwächst. Eine solche Praxis würde das gesamte, mit erheblichen informationellen Eingriffen verbundene Verfahren wegen fehlender Erforderlichkeit unverhältnismäßig machen.

Künftig wird von Bedeutung sein, dass von den Kommunen das Verfahren sensibel und zugleich zielsicher etabliert und praktiziert wird. Die Regelung im Gesundheitsdienstgesetz deutet zwar auf die Einschaltung der Gesundheitsämter hin. Das ULD empfiehlt aber weiterhin dringend, auf **kommunaler Ebene** ausschließlich die Jugendämter mit dem Thema zu befassen. Bei der konkreten Umsetzung muss zudem darauf geachtet werden, dass es in der weitaus überwiegenden Mehrzahl von Fällen, die sich als unproblematisch erweisen, zu einer zeitnahen Löschung sämtlicher Daten kommt. Es wäre z. B. unverhältnismäßig, die

Daten von Eltern und Kindern in einer Datei potenzieller Kindeswohlvernachlässiger zu speichern, nur weil die Eltern einen Kinderarzt außerhalb der Landesgrenzen von Schleswig-Holstein aufgesucht haben.

Was ist zu tun?
Bei der Ausgestaltung des Verfahrens durch die Kommunen ist die Verarbeitung der äußerst sensiblen personenbezogenen Daten auf ein Mindestmaß zu beschränken. Das Jugendamt sollte ausschließlich damit befasst werden. Bei der zentralen Stelle sind die erforderlichen Maßnahmen der Datensicherheit zum Schutz der sensiblen Datenbestände zu ergreifen.

4.5.8 ELENA – Datenmonster, nicht schöne Göttin

Das bisherige JobCard-Verfahren wird von der Bundesregierung unter dem hübschen Kürzel ELENA weiterbetrieben. Dabei wird weiterhin das Konzept einer gefährlichen Vorratsdatenverarbeitung verfolgt, obwohl es verfassungsverträgliche Alternativen gibt.

Über Jahre hinweg wehren sich die Landesbeauftragten für den Datenschutz gegen die Einrichtung einer gewaltigen Datenbank mit den Einkommensdaten sämtlicher in Deutschland abhängig Beschäftigten. Wurde das Konzept bisher unter dem freundlich klingenden Titel „JobCard“ betrieben (28. TB, Tz. 4.5.2), so wurde es nun ohne inhaltliche Änderung noch euphorischer zu „ELENA“ umgetauft – **Elektronischer Einkommensnachweis**. Erklärtes Ziel ist es, das bisherige sehr aufwendige und fehleranfällige Papierbelegverfahren für Einkommensnachweise in Sozialverfahren durch Auskünfte aus einem Zentralregister zu ersetzen. Die Datenschutzkritik richtete sich dagegen, dass unter staatlicher Verfügungsgewalt Einkommensdaten langjährig gespeichert würden, von denen nur ein geringer Prozentsatz benötigt wird. Die Begehrlichkeiten an dieser Datenbank – von Bekämpfern der Schwarzarbeit und der organisierten Kriminalität bis hin zum Finanzamt – waren von Anfang an erkennbar.

Von August 2007 datiert ein **Referentenentwurf für ein ELENA-Gesetz**, der fast identisch ist mit einem Kabinettsentwurf vom Februar 2007. Dieser kam vor allem wegen des Widerstandes der Bundesländer nicht zustande. Der einzige Unterschied liegt darin, dass nur die bei der Bundesanstalt für Arbeit durchgeführten Sozialleistungsverfahren tangiert sein sollen. Eine Öffnungsklausel sieht aber vor, dass weitere Sozialbehörden den Antrag stellen können, zum ELENA-Verfahren zugelassen zu werden. Damit drängt sich der Eindruck geradezu auf, dass mit der reduzierten Anwendungsregelung nur der Widerstand der Bundesländer im Bundesrat ausgehebelt werden soll.

Inzwischen wurde uns ein **neues technisches Konzept** vorgelegt, das den Datenschutzbedenken weitgehend Rechnung trägt, ohne dass wesentliche Ziele des elektronischen Nachweisverfahrens aufgegeben würden, das aber mit den bisherigen Gesetzesvorschlägen nicht übereinstimmt. Danach werden die Einkommensdaten verschlüsselt von den Arbeitgebern einer zentralen Stelle angeliefert. Dabei

können die Arbeitgeber auf die aus dem Besteuerungsverfahren bekannte und inzwischen bewährte ELSTER-Technologie zurückgreifen (27. TB, Tz. 4.9). In der zentralen Stelle erfolgt umgehend eine Umverschlüsselung mit dem öffentlichen Schlüssel des Arbeitnehmers. Der Abruf dieser Daten könnte somit nur mit dessen privatem Schlüssel erfolgen, den er anlässlich einer Antragstellung beim Sozialleistungsträger zum Zweck der Abfrage bereitstellt. Nur für gesetzlich definierte Ausnahmefälle würde ein Recovery-Verfahren für die privaten Schlüssel bei einer vertrauenswürdigen Stelle vorgesehen. Eine Entschlüsselung der sensiblen Einkommensdaten wäre damit nur noch im Einzelfall technisch möglich. Überzogene Begehrlichkeiten an den Daten ließen sich wirksam zurückweisen. Dennoch würde die angestrebte Verfahrensvereinfachung und die Verbesserung der Datenbasis bei Sozialverfahren erreicht. Über das Recovery-Verfahren würde zwar die alleinige Verfügungsbefugnis der Betroffenen über ihre Daten empfindlich eingeschränkt. Der Makel der offensichtlichen Verfassungswidrigkeit wäre aber ausgeräumt.

Was ist zu tun?
Das bisherige ELENA-Konzept muss aufgegeben werden. Eine Ende-zu-Ende-Verschlüsselung macht das Nachweisverfahren verfassungskonform.

4.6 Schutz des Patientengeheimnisses

4.6.1 Neues von der elektronischen Gesundheitskarte

Die neuen Funktionen der eGK werden endlich getestet. Derweil wächst in der Ärzteschaft eine Fundamentalopposition gegen das Projekt. Mängel am Datenschutz können dafür nicht als Begründung herhalten.

Die Einführung der elektronischen Gesundheitskarte (eGK) ist für das ULD zu einem Dauerbrenner geworden. In der Testregion Flensburg begann die Testung des sogenannten **Release 1**. Dies beinhaltet den Einsatz von echten eGK und Heilberufeausweisen aufseiten der Ärzte. Zunächst wird die elektronische Verordnung von Arzneien sowie die Speicherung von Notfalldaten auf der Karte ohne Rückgriff auf die sogenannte Telematikinfrastruktur, d. h. das dahinter liegende Netzwerk, erprobt.

Wie bei solchen Tests üblich, zeigten sich Schwierigkeiten, die aber weitgehend im weiteren Verlauf der Testung überwunden werden konnten bzw. bei der Systemgestaltung aufgefangen werden können. Als schwerwiegend erwiesen sich die Probleme für die Testpersonen bei der **Verwendung der PIN-Nummer**. Bei der Verwendung der eGK reicht für den Zugriff auf bestimmte Informationen die Vorlage der Karte, z. B. bei der Übertragung des elektronischen Rezepts von der Arztpraxis zur Apotheke oder beim Auslesen von Notfalldaten durch Ärzte. Einzige Voraussetzung ist in beiden Fällen neben dem Einlesen der eGK das gleichzeitige Einschieben eines autorisierten Heilberufeausweises (HBA) eines Arztes oder Apothekers in den speziellen Kartenleser. Das technische Konzept für die eGK fordert aber bei den weiteren freiwilligen Anwendungen ein zusätzliches Sicherheitsmerkmal: Der Versicherte muss die Karte nicht nur in das Lesegerät

einschieben, sondern durch Eingabe einer sechsstelligen PIN-Nummer freigeben. Nur bei Vorhandensein dieser beiden Sicherheitsmerkmale – Besitz der Karte und Wissen der PIN-Nummer – wird z. B. das Aufspeichern oder Ändern von Notfalldaten auf der Karte ermöglicht; Entsprechendes gilt für später zu testende freiwillige Anwendungen wie die elektronische Patientenakte. Die dabei verwendete PIN ist nicht vorgegeben; sie muss beim ersten Einsatz der Karte in einer Arztpraxis festgelegt und dort eingegeben werden.

Zur Absicherung der Karten vor diesem Ersteinsatz gibt es ein sogenanntes **Transport-PIN-Verfahren**, dessen Ziel es ist, die Karte vor ihrem Einsatz gegen missbräuchliche Nutzung abzusichern. Dieses Verfahren unterscheidet sich allerdings auf technischer Ebene von Krankenkasse zu Krankenkasse und zudem auch noch zwischen den verschiedenen Kartenherstellern. Zum Teil werden die Karten mit sogenannten PIN-Briefen ausgeliefert, die – nur für den Transport – eine willkürlich festgelegte PIN vorgeben, zum Teil ist die Transport-PIN aus Angaben erstellt worden, die bei den die Karte ausgebenden Krankenkassen über den Versicherten vorhanden sind; teilweise fehlt eine Transport-PIN gänzlich. Diese Vielfalt rührt daher, dass die Transportabsicherung von jeder Krankenkasse eigenständig gewählt werden konnte.

In der Testung hat sich gezeigt, dass vor allem ältere und an verschiedenen Krankheiten leidende Teilnehmer mit den PIN-Verfahren oft nicht zurechtkamen. Zudem wird die Karte bei Fehleingaben komplett unbrauchbar und muss ersetzt werden, was während des Übergangs von der Transport-PIN zur Echt-PIN sehr schnell geschehen kann. Dies hat die Leitung des Testprojekts in Flensburg dazu bewogen, gegenüber der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (Gematik, 28. TB, Tz. 4.6.1) anzuregen, als Übergangsverfahren eine sogenannte Default-PIN fest in die eGK einzuprogrammieren. Dies würde es besonders älteren und multimorbiden Versicherten ermöglichen, die Karte auch für die Speicherung von Notfalldaten zu verwenden, ohne sich eine spezielle PIN merken zu müssen. Die freiwillige Nutzung der wichtigsten medizinischen Daten sollte gerade bei solchen Karteninhabern, die davon am meisten profitieren können, nicht daran scheitern, dass diese Personen mit der Handhabung der Technik nicht vertraut sind.

Die Sicherheit des Gesamtsystems wäre durch solch eine Ergänzung nicht beeinträchtigt. Zwar könnten die nur mit einer **Default-PIN** gesicherten Daten theoretisch von einem Unbefugten, der sich die Karte verschafft, ausgelesen werden. Dies gelänge aber nur, wenn gleichzeitig der HBA eines Arztes oder Apothekers verwendet wird. Es kann davon ausgegangen werden, dass bei Letzterem eine Prüfung der Identität mithilfe der auf der Karte gespeicherten Daten erfolgt. Die Sicherheit liegt dabei auf dem gleichen Niveau wie beim elektronischen Rezept, für dessen Verwendung auch keine PIN-Eingabe des Versicherten vorgesehen ist. Namentlich für die Anwendung des Speicherns von Notfalldaten auf der Karte lässt sich kaum ein realistisches Angriffsszenario denken, das auf dem Vorhandensein einer Default-PIN basiert. Weiterhin würden alle Versicherten beim ersten Einsatz der mit einer Default-PIN abgesicherten Karte sowie bei allen Folgeeinsätzen automatisch darauf hingewiesen, dass sie für erhöhten Schutz eine individuelle PIN einsetzen können.

Das ULD hat der Leitung der Testregion Flensburg seine Unterstützung dieses Vorschlages signalisiert. Hohe Standards bei der Datensicherheit sind grundsätzlich zu begrüßen. Sie dürfen jedoch nicht gegen die mit dieser Technik befassten Nutzer eingesetzt werden. Für diese muss es eine Möglichkeit geben, die Technik hinreichend sicher, aber auch ohne übermäßige Anforderungen an Verfahren, die ihnen nicht bekannt sind und mit denen sie nicht zurechtkommen, anzuwenden. Es bleibt abzuwarten, ob die Gematik eine entsprechende Erweiterung der Spezifikationen der Karte vornimmt, bevor die Karte wie vorgesehen in der ersten Hälfte des Jahres 2008 nach und nach „ausgerollt“ wird.

Unabhängig von den konkreten Ergebnissen der Testung ist verstärkt **Kritik aus der Ärzteschaft** an der Einführung der eGK zu hören: Die Vertraulichkeit der ärztlichen Dokumentation sei nicht gewährleistet. Die Speicherung auf sogenannten zentralen Servern belaste das Arzt-Patienten-Verhältnis, da sie unsicher sei. Die eGK ermögliche die Einteilung der Bevölkerung in Risikoklassen.

Alle diese Argumente sind falsch. Die im Rahmen des Projektes eGK geplante **Telematikinfrastruktur** weist einen bemerkenswert hohen Grad von Datensicherheit auf. Tatsächlich dürfte die Sicherheit in diesem System deutlich höher liegen als die in manchen Arztpraxen, in denen es erfahrungsgemäß mit Datensicherheit nicht immer so genau genommen wird. Unzutreffend ist auch, dass die Speicherung auf sogenannten zentralen Servern besondere Sicherheitsrisiken und Auswertungsmöglichkeiten für die Serverbetreiber mit sich bringt. Jeder einzelne Datensatz der Patienten ist mit einem speziellen Schlüssel digital verschlüsselt. Die technische Sicherheit dieser Speicherung ist so hoch, dass ein Aufbrechen der Schlüssel praktisch unmöglich ist. Selbst wenn es mit der geballten Rechenkraft aller Geheimdienstcomputer nach Jahren gelingen sollte, einen Schlüssel zu knacken, ist damit lediglich ein einzelner Datensatz entschlüsselt. Die Speicherung der Daten erfolgt auf einer großen Zahl von Servern bei den unterschiedlichsten Stellen; dabei handelt es sich in der Regel um sicherheitsgeprüfte Rechenzentren. Schließlich ist die Teilnahme an den meisten Anwendungen der eGK den Versicherten freigestellt. Lediglich das elektronische Rezept stellt eine Pflichtanwendung dar. Alle weiteren medizinischen Informationen werden nur dann im System der eGK gespeichert, wenn der Patient dies ausdrücklich wünscht.

Weiterhin ist nicht erkennbar, warum gerade die eGK zu einer **erweiterten Profilbildung** führen soll. Bereits seit 2004, seit Inkrafttreten des sogenannten GKV-Modernisierungsgesetzes, erhalten die Krankenkassen nicht nur – wie zuvor – die Behandlungsdaten arztbezogen, sondern auch die Versicherungsnummer mitgeteilt. Entsprechendes gilt für die Abrechnung vonseiten der Apotheken über die Apothekenrechenzentren. Die Krankenkassen sind also seit einiger Zeit bereits im Besitz der Daten, die für eine Profilbildung der einzelnen Versicherten und eine Einteilung in Risikoklassen benutzt werden können. Dies ist aus Datenschutzsicht äußerst kritisch zu beurteilen, hat allerdings mit der eGK nichts zu tun.

Uns scheint, dass ein **rationaler Diskurs** über diese Probleme zunehmend schwieriger wird. Nicht alle Akteure in der Debatte scheinen daran interessiert zu

sein, auf der Basis der bestehenden Gesetze und der tatsächlich geplanten technischen Umsetzung zu diskutieren. Von Ärzteseite wird zutreffend geltend gemacht, dass bestimmte Prozeduren erhöhten Aufwand erfordern und die großen Einsparpotenziale durch den Einsatz der eGK für die Krankenkassen entstehen. Die Vertreter der kritischen Ärzteschaft sollten es jedoch – auch im Interesse der eigenen Glaubwürdigkeit – vermeiden, mit nicht zutreffenden Datenschutzargumenten gegen die Einführung der Karte zu Felde zu ziehen.

Was ist zu tun?
Bei der Einführung der Karte sich ergebende Probleme der Benutzbarkeit von Sicherheitsmerkmalen können zu Anpassungen in der Standardisierung führen. Es ergibt wenig Sinn, eine hochsichere Systemumgebung zu erzeugen, die letztendlich von einer großen Zahl von Bürgerinnen und Bürgern nicht benutzt werden kann. Die rechtlichen und technischen Fakten sollten als Grundlage der Diskussion über die eGK genommen werden.

4.6.2 Mammografie-Screening Schleswig-Holstein hat begonnen

Mit dem Start des Mammografie-Screenings beginnt auch die Verarbeitung von medizinischen und sonstigen Daten der Teilnehmerinnen. Bei allen beteiligten Institutionen ist auf eine penible Umsetzung des Datenschutzes zu achten.

Bei den Vorbereitungen des Mammografie-Screenings lag das Augenmerk auf dem bei der sogenannten zentralen Stelle geplanten Datenverarbeitungsverfahren (29. TB, Tz. 4.6.3). Deren Aufgabe wurde von der **Kassenärztlichen Vereinigung Schleswig-Holstein** übernommen. Dort werden Daten der zur Teilnahme am Screening berechtigten Frauen von den Melderegistern entgegengenommen. Die Frauen werden mit einem Einladungsschreiben und gegebenenfalls einer Erinnerung auf die Möglichkeit der Teilnahme am Screening aufmerksam gemacht. Weiterhin werden Rückmeldungen über die Teilnahme von den Screening-Einheiten an die zentrale Stelle verarbeitet. Mit der zentralen Stelle wurde das Sicherheitskonzept für dieses Verfahren weiter konkretisiert. Die in dem Sicherheitskonzept vorgesehenen Maßnahmen sind nun korrekt in der Praxis umzusetzen.

Beteiligt sind neben der zentralen Stelle vor allem die vier sogenannten **Screening-Einheiten**, die jeweils für eine Region in Schleswig-Holstein zuständig sind. In den vier Screening-Regionen finden sich verschiedene Mammografie-Einheiten – Einrichtungen, in denen das eigentliche Mammografie-Screening durchgeführt wird. Die meisten davon sind stationär in Krankenhäusern oder Arztpraxen untergebracht. Es gibt jedoch auch Mammobile; das sind mobile Screening-Einheiten, die als Sattelzuganhänger zu festgelegten Terminen an verschiedene Orte gefahren werden. Eine Übersicht ist zu finden unter

www.mamma-screening-sh.de/einheiten.htm

Das Screening in jeder Screening-Einheit wird von einem oder mehreren sogenannten **programmverantwortlichen Ärzten** (PVA) geleitet. Diese sind u. a. für die Einhaltung des Datenschutzes bei den Screening-Einheiten verantwortlich. Dazu gehört, dass die elektronischen Aufnahmen für den Erst- bzw. Zweitbefunder, die die Bilder unabhängig voneinander bewerten, auf einem sicheren Weg zur Verfügung gestellt werden. Die Ergebnisse der Befundungen werden in dem von der Kassenärztlichen Vereinigung Bayern (KV Bayern) entwickelten Programm Mammasoft dokumentiert. Auch wenn die technische Infrastruktur hierzu von der Kassenärztlichen Vereinigung Schleswig-Holstein (KV Schleswig-Holstein) als der zentralen Stelle zur Verfügung gestellt wird, bleibt für die hier gespeicherten medizinischen Daten jeweils der PVA verantwortlich. Außerhalb dieses Verfahrens werden die beim Screening erzeugten Bilddaten gespeichert. Durch das jeweils vor Ort verwendete Verfahren ist sicherzustellen, dass kein Zugriff Unberechtigter stattfinden kann.

In die Verantwortung des PVA fällt auch die fristgemäße Löschung der bei der Untersuchung erzeugten Daten. Dabei gilt die **10-jährige Aufbewahrungsfrist** für medizinische Unterlagen. Es ist davon auszugehen, dass jede neue Teilnahme am Screening nach zwei Jahren eine erneute Behandlung darstellt, welche jeweils die Aufbewahrungsfrist in Gang setzt. Kommt es aus in der Vergangenheit durchgeführten Screenings nicht zu weiteren medizinischen Maßnahmen, so sind diese Unterlagen jeweils nach 10 Jahren zu löschen.

Schließlich hat der PVA den Frauen das **Ergebnis** der Untersuchung **schriftlich mitzuteilen**. Auch wenn der Befund negativ ist und keine Anzeichen für einen Tumor gefunden wurden, handelt es sich um die Übersendung sensibler medizinischer Daten. Diese darf nur in einem verschlossenen Umschlag erfolgen; eine Versendung mit offener Postkarte ist unzulässig. Es würde weiterhin einen Verstoß gegen die ärztliche Schweigepflicht darstellen, wenn diese Daten an Auftragsdatenverarbeiter weitergegeben würden, ohne dass dafür eine Einwilligung der Betroffenen vorliegt. Das ULD plant, eine datenschutzrechtliche Prüfung einzelner Verfahrensteile vorzunehmen, wenn der Komplettbetrieb erreicht ist.

Was ist zu tun?
Die zentrale Stelle sowie die programmverantwortlichen Ärzte haben beim Mammografie-Screening die Vorgaben des Datenschutzes genauestens umzusetzen. Das ULD steht für Nachfrage und Beratung gerne zur Verfügung.

4.6.3 Neue Aufgaben für das Krebsregister?

Das Krebsregister spielt eine wichtige Rolle bei der epidemiologischen Forschung über das Vorkommen von Krebserkrankungen. Diese Aufgabe kann es nur erfüllen, wenn die strikte Vertraulichkeit der dort gespeicherten Daten außer Zweifel steht. Aktuellen Wünschen, aus dem Krebsregister personenbezogene Rückmeldungen über Einzelheiten der Erkrankung zu erhalten, stehen erhebliche Datzenschutzbedenken entgegen.

Wie im 28. Tätigkeitsbericht (Tz. 4.6.3) berichtet, kam es vor Kurzem zu gewissen Änderungen in der Verfahrensweise beim Krebsregister. Das wesentliche Element dieses für die epidemiologische Forschung so wichtigen Instruments blieb die **Trennung der gespeicherten Daten** zwischen der Vertrauensstelle, die die Meldungen entgegennimmt, und der Registerstelle, die die medizinischen Daten verwaltet. Die Weitergabe von medizinischen Daten an Stellen, die damit bisher nicht befasst waren, scheidet aus.

Dieser Schutzmechanismus erweist sich bei der medizinischen Forschung: Das Krebsregistergesetz ermöglicht grundsätzlich das Durchführen von sogenannten **Kohortenstudien**. So kann z. B. für bestimmte, namentlich bekannte Mitglieder von zuvor definierten Personengruppen über das Krebsregister festgestellt werden, ob für deren Gruppe ein erhöhtes Vorkommen von Krebserkrankungen vorliegt. Solche Personengruppen können z. B. Beschäftigte aus besonderen Industriezweigen sein. Die strengen gesetzlichen Voraussetzungen für die Durchführung einer solchen Kohortenstudie verlangen, dass es der forschenden Stelle nicht möglich ist, die vom Krebsregister zurückgemeldeten krankheitsbezogenen Daten einzelnen Mitgliedern der Kohorte zuzuordnen; etwas anderes gilt nur, wenn die Betroffenen dieser Zuordnung zugestimmt haben. Im Berichtszeitraum erarbeitete das Ministerium für Soziales, Gesundheit, Familie, Jugend und Senioren des Landes Schleswig-Holstein gemeinsam mit dem ULD und den Verantwortlichen beim Krebsregister den Entwurf einer Landesverordnung mit Einzelheiten über diesen Kohortenabgleich. Diese Verordnung sichert die Vorgaben zur Nichtidentifizierbarkeit der Personen, für die epidemiologische Daten zurückgemeldet werden.

Weiter gehende Forderungen an das Krebsregister nach zusätzlichen individuellen Datenabgleichen wurden nun vonseiten der Kooperationsgemeinschaft Mammografie, die das bundesweite **Mammografie-Screening** koordiniert (Tz. 4.6.2), aufgestellt. Dabei sollen vor allem zwei Zwecke verfolgt werden:

Zum einen geht es um die **Evaluation der Mortalität** insbesondere solcher Frauen, die an dem Mammografie-Screening teilgenommen haben. Entwickelt sich die Mortalität für diese Gruppe besser als für den Rest der Bevölkerung, sodass sich daher der hohe Aufwand beim Mammografie-Screening lohnt? Dies kann nur nachgewiesen werden, wenn von den Screening-Einheiten Daten über die Teilnehmerinnen, bei denen Brustkrebs entdeckt wird, an das Krebsregister weitergeleitet werden. Dieses Element der Qualitätskontrolle ist akzeptabel. Das Krebsregistergesetz sieht die Verwendung der Daten nicht für individualisierte

Qualitätskontrollen vor. Außerdem sind die Screening-Einheiten nach dem Krebsregistergesetz zur Meldung von Krebsfällen verpflichtet. Entscheidend ist, dass die Daten über die Mortalität in der Vertrauensstelle des Krebsregisters verarbeitet werden und so die Krebsmeldungen das Krebsregister nicht verlassen.

Problematisch ist jedoch ein zweites Ansinnen der Kooperationsgemeinschaft Mammografie. Als weiteres Element der Qualitätskontrolle der Befundung soll festgestellt werden, wie viele sogenannte **Intervallkarzinome** auftreten und insbesondere, ob diese nicht bereits im Mammografie-Screening hätten erkannt werden können. Intervallkarzinome sind Tumore, die in der Zeit zwischen zwei Screening-Untersuchungen auftreten. Zwar lässt sich relativ einfach eine statistische Zahl von Intervallkarzinomen errechnen, ohne dass Daten über Krebserkrankungen das Krebsregister verlassen müssen. Der Wunsch der Kooperationsgemeinschaft Mammografie geht jedoch dahin, zu den einzelnen Fällen, bei denen Intervallkarzinome aufgetreten sind, sämtliche dazugehörigen Daten über die Einzelheiten der Erkrankung aus dem Krebsregister zu erhalten. Damit sollen die im letzten Screening vor Auftreten des Intervallkarzinoms befundeten Röntgenaufnahmen erneut abgeglichen werden, um zu untersuchen, ob nicht doch Anhaltspunkte für den Tumor hätten erkannt werden können.

Ein solches Verfahren lässt sich rechtlich nur auf die Einwilligung der Teilnehmerinnen im Mammografie-Screening stützen; diese könnten darin einwilligen, dass ihre krankheitsbezogenen, im Krebsregister gespeicherten Daten zu Qualitätskontrollzwecken den Screening-Einheiten zur Verfügung gestellt werden. Diese Einwilligungslösung ist allerdings nicht vorgesehen. Mit gutem Grund verbieten die Krebsregistergesetze der Länder, dass ohne die Einwilligung der betroffenen Personen Einzelheiten über die Erkrankungen an dritte Stellen weitergegeben werden. So würde unter der Hand eine Zweckänderung des Registers erfolgen. Es ginge nicht mehr um die Erkenntnis epidemiologischer Gegebenheiten. Vielmehr würde auf eine Qualitätskontrolle im Einzelfall abgezielt. Dafür ist das Krebsregister jedoch nicht geschaffen, und die dort zur Identifikation von Personendatensätzen verwendeten Instrumente sind dafür nicht geeignet. Bei der Zuordnung von Personendatensätzen im Krebsregister wird regelmäßig keine 100%ige Übereinstimmung der Daten erreicht, die die Personen identifizieren; diese ist auch für epidemiologische Zwecke nicht erforderlich. Ein raffinierter Algorithmus sichert bei einer zweiten Meldung zu einem bestimmten Patienten auch dann die richtige Zuordnung, wenn Ungenauigkeiten in der Schreibweise des Namens oder der Adresse vorkommen. Allerdings gibt es für die Richtigkeit der Zuordnung keine 100%ige Garantie. Für **epidemiologische Zwecke** ist die erreichte hohe Wahrscheinlichkeit ausreichend.

Etwas anderes gilt für **individualisierte Rückmeldungen**. Ein schlimmer Fall läge in folgendem Szenario: Aufgrund einer Personenverwechslung durch die beschriebene Ungenauigkeit werden Krankheitsdaten aus dem Krebsregister fälschlich einer Frau zugeordnet, die am Screening teilgenommen hat und bei der kein Tumor gefunden wurde. Diese könnte dann von der zuständigen Screening-Einheit angesprochen und darum gebeten werden, im Hinblick auf das bei ihr vermeintlich festgestellte Karzinom dem programmverantwortlichen Arzt den

Zugang zu ihren medizinischen Behandlungsunterlagen zu erlauben. Die Auswirkungen einer solchen Fehlzuordnung können fatal sein. Daher sollte der Abgleich zwischen Mammografie-Screening und Krebsregister zum Zwecke der individualisierten Qualitätskontrolle nur stattfinden, wenn die betroffene Frau nach ausführlicher Aufklärung beim Mammografie-Screening eingewilligt hat.

Was ist zu tun?
Bei Kohortenstudien im Krebsregister ist künftig die dazu erlassene Landesverordnung zu beachten. Ein Abgleich zwischen Mammografie-Screening und Krebsregister zur individualisierten Qualitätskontrolle sollte nur mit Einwilligung der betroffenen Frau stattfinden.

4.6.4 Patientenakten und Computer im Müll

Patientendaten sind besonders sensibel. In der Theorie dürfte hier weitgehend Einigkeit bestehen. In der Praxis sieht es manchmal anders aus.

Keine Ärztin und kein Physiotherapeut würden sich auf die Straße stellen und aussortierte Patientenakten an Passanten verteilen. Bei der Entsorgung von Patientenunterlagen mag häufig keine böse Absicht vorliegen. Aber die Patientenakten ordnungsgemäß mit dem **Schredder zu vernichten** oder die Festplatte des Praxiscomputers zu zerkleinern, scheint der Mühe nicht wert. Also landen Patientenakten im Müllcontainer und Praxiscomputer im Sperrmüll. Das spart Zeit. Wer sollte sich schon für die Informationen über den Gesundheitszustand von Unbekannten interessieren?

Von Unbekannten? Jüngste Fälle in Schleswig-Holstein zeigten, dass das Interesse, solche Patientendaten einzusehen, sehr wohl vorhanden war, selbst bei Passanten. Schnell ist zufällig eine Information über einen Bekannten gefunden; zumal dann, wenn der Datenmüll in der Nachbarschaft abgeladen wird. Für alle Beteiligten bleibt ein schaler Beigeschmack bestehen; für die betroffenen Patientinnen und Patienten ist der **Schaden** am größten: Es muss gar nicht unbedingt Missbrauch mit den Patienteninformationen betrieben werden – die Verunsicherung ist für die Beteiligten belastend genug. Was stand in den Akten alles drin? Was wissen jetzt andere über mich? Der Arzt, der eine Datenstreuung zu verantworten hat, wird die leichtsinnige Entscheidung, seine Patientenakten aus Bequemlichkeit nicht fachgerecht entsorgt zu haben, mehr als einmal bereuen. Solche Vorfälle sprechen sich schnell herum. Geschädigt ist dann nicht nur der Ruf des betreffenden Arztes, sondern indirekt der der ganzen Ärzteschaft. Der Standesethos wird verletzt. Unsachgemäße Datenbeseitigung ist mit Geist und Wortlaut des hippokratischen Eides nicht vereinbar und verstößt gegen Straf- und Bußgeldtatbestände.

Was ist zu tun?
Werden Patientenakten in größerem Umfang, etwa bei einer Praxisaufgabe nach Ablauf der Aufbewahrungsfristen, entsorgt, sind sie am besten einem professionellen Aktenvernichter zu übergeben. Zur Entsorgung des Praxiscomputers oder anderer elektronischer Datenträger genügt eine einfache Löschung der Daten nicht aus; die Datenträger müssen physisch zerstört werden.

4.6.5 Aufbewahrungsfristen bei Patientenakten

Immer wieder wenden sich Stellen aus dem medizinischen Bereich an das ULD, um die für ihren Berufszweig maßgeblichen Aufbewahrungsfristen zu erfahren. Zwei Fragen müssen auseinandergehalten werden: Wie lange müssen Patientenakten aufbewahrt werden? Wie lange dürfen sie aufbewahrt werden?

Allgemeingültige Antworten können hierauf nicht gegeben werden. Es kommt darauf an, wer welche Daten zu welchem Zweck speichert. Den **rechtlichen Rahmen** ergeben das jeweilige Standesrecht, verschiedene Spezialgesetze und subsidiär das Bundesdatenschutzgesetz (BDSG).

Bis zum Ablauf des **Behandlungsvertrages** dürfen die Daten gespeichert werden. Während dieser Zeit ist entsprechend dem Vertragszweck die Speicherung aller für das operative Geschäft erforderlichen Daten zulässig. Nach Beendigung des jeweiligen Vertragsverhältnisses fällt der ursprüngliche Vertragszweck als Rechtfertigung für die Datenspeicherung weg. An seine Stelle treten berufsrechtliche **Aufbewahrungspflichten**; diese können jedoch nur eine Datenaufbewahrung außerhalb des operativen Geschäfts rechtfertigen. Zu solchen standesrechtlichen und -gesetzlichen Spezialregelungen gehören z. B.:

- die Berufsordnung der Ärzte in Schleswig-Holstein: 10 Jahre für ärztliche Unterlagen,
- das Heimgesetz: 5 Jahre für Daten über den Betrieb eines Pflegeheims,
- die Rahmenempfehlung für Physiotherapeuten: 3 Jahre für die physiotherapeutische Verlaufsdokumentation.

Daneben sind hier gegebenenfalls auch handelsrechtliche Aufbewahrungsfristen nach dem **Handelsgesetzbuch** zu berücksichtigen:

- 5 Jahre für handelsrechtliche Unterlagen,
- 10 Jahre für Handelsbücher und Ähnliches,
- 6 Jahre für Handelskorrespondenz.

Die detaillierten Patientendokumentationen gehören nicht zu den handelsrechtlichen Dokumenten.

Die aufzubewahrenden Daten sind nach Möglichkeit gemäß den Löschfristen **getrennt in Akten** zu führen, sodass diese ohne Aufwand zum frühstmöglichen Zeitpunkt gelöscht werden können. Die Daten sind so aufzubewahren, dass nur Berechtigte Zugang haben. Nach dem Ablauf der Aufbewahrungsfristen sind gemäß den spezialgesetzlichen Regeln oder dem Bundesdatenschutzgesetz die Patientendaten grundsätzlich zu löschen. **Haftungsrechtlich** ergeben sich aus der fristgemäßen Vernichtung von Unterlagen keine Beweislastverschiebungen zulasten der Ärztinnen und Ärzte.

Ausnahmsweise dürfen die Patientendaten aus folgenden Erwägungen länger gesperrt aufbewahrt werden:

- Wenn die weitere Aufbewahrung aus medizinischen Gründen im Einzelfall erforderlich ist, ist dies möglich, aber schriftlich zu begründen.
- Im Falle eines konkreten Prozessrisikos dürfen Unterlagen aus Beweissicherungsgründen trotz des grundsätzlichen Löschungsgebotes über die gesetzlich oder standesrechtlich vorgeschriebenen Aufbewahrungsfristen hinaus aufbewahrt werden.

Was ist zu tun?
Patientenakten müssen und dürfen nur bis zum Ablauf der jeweiligen berufsspezifischen Aufbewahrungsfristen aufbewahrt werden. Unter besonderen Umständen ist eine längere Aufbewahrung zulässig.

4.6.6 Novellierung des Maßregelvollzugsgesetzes

Im Maßregelvollzug kommt es zu intensiven Grundrechtseingriffen durch staatliche Stellen. Erfreulicherweise hat die Landesregierung durch eine Änderung des entsprechenden Gesetzes für mehr Klarheit und Rechtssicherheit gesorgt.

Im Maßregelvollzug werden Straftäter untergebracht, die aufgrund einer psychischen Erkrankung schuldunfähig oder vermindert schuldfähig sind, bei denen aber zugleich von einer weiteren Gefährlichkeit auszugehen ist. Zudem gibt es suchtkranke Delinquenten. Durchgeführt wird der Maßregelvollzug in der forensischen Abteilung eines psychiatrischen Krankenhauses. Seit der Privatisierung der Landeskrankenhäuser in Schleswig-Holstein werden auch die **forensischen Abteilungen von privaten Kliniken** betrieben. Durch sogenannte Beleihung dieser Stellen wird sichergestellt, dass öffentlich-rechtliche Standards und die Grundrechtsbindung erhalten bleiben.

Diese Rechtsformänderung und andere rechtliche und tatsächliche Entwicklungen waren Anlass zur Novellierung des Landesgesetzes über den Maßregelvollzug. Das ULD wurde von Anfang an durch das Sozialministerium des Landes Schleswig-Holstein einbezogen. Die Vorarbeiten begannen bereits im Jahr 2006. Das Gesetz wurde vom Landtag Ende 2007 verabschiedet. Es wurde eine detaillierte und normenklare Regelung über die zulässigen Datenübermittlungen

aufgenommen. Das **Recht auf Akteneinsicht** für die im Maßregelvollzug untergebrachten Personen wurde überarbeitet. Konform mit der Rechtsprechung des Bundesverfassungsgerichts kann dieses Recht nur ausnahmsweise beschränkt werden. Die Ärzte können sich grundsätzlich nicht darauf berufen, der vollständigen Einsicht stünden deren eigene Rechte entgegen. Wohl können aber berechtigte Interessen anderer dritter Personen eine Grenze für die Akteneinsicht darstellen. Durch entsprechende Aktenführung kann dafür gesorgt werden, dass Informationen über Dritte von der Kernakte zum Betroffenen abtrennbar sind. Den Betroffenen soll eine weitestgehende Aktenkenntnis ermöglicht werden.

Was ist zu tun?
Die neuen Vorschriften müssen in der Praxis in datenschutzfreundlicher Weise angewendet werden.

4.6.7 Das Universitätsklinikum Schleswig-Holstein und der Datenschutz

Als wichtigster Anbieter medizinischer Leistungen in Schleswig-Holstein verfolgt das UK S-H ehrgeizige Projekte mit Auswirkungen auf den Patientendatenschutz und die Einhaltung der ärztlichen Schweigepflicht. Der Abbau der Ressourcen des betrieblichen Datenschutzes wäre ein falsches Signal.

Das Universitätsklinikum Schleswig-Holstein (UK S-H) kann **Superlative** vorweisen. Es ist mit ca. 2.400 stationären Betten, über 240.000 ambulanten und ca. 100.000 stationären und teilstationären Patientinnen und Patienten eine der drei größten Universitätskliniken in Deutschland und zugleich das einzige Krankenhaus in Schleswig-Holstein mit sogenannter Maximalversorgung, die in 51 Kliniken und 26 Instituten realisiert wird. Mit etwa 10.000 beschäftigten Mitarbeiterinnen und Mitarbeitern ist es der größte öffentliche Arbeitgeber im Land.

Der Datenschutz wird beim UK S-H bisher durch ein Team wahrgenommen, das aus einem internen behördlichen Datenschutzbeauftragten sowie einem externen Berater besteht. Dieses Team hat zurzeit alle Hände voll zu tun. Viele datenschutzrelevante Vorhaben stehen an. Es soll ein neues Krankenhausinformationssystem eingeführt werden. Aus dem Klinikum heraus wurden und werden eine zunehmende Anzahl von Organisationseinheiten rechtlich verselbstständigt und in den Privatrechtsbereich überführt. Nach der Verselbstständigung darf es keine gemeinsame Führung der Datenbestände mehr geben. Daneben ist das laufende Geschäft dieses großen Unternehmens zu begleiten.

Angesichts dessen überraschte es, dass das UK S-H die Initiative startete, die verfügbaren Ressourcen für das Datenschutzteam signifikant zu kürzen. Die wirtschaftlichen Probleme des Klinikums sind bekannt. Allerdings darf bezweifelt werden, dass hier kurzfristig erzielte Einsparungen einen relevanten und nachhaltigen Spareffekt hätten. Zu befürchten ist, dass eine weitere **Reduzierung der Ressourcen** zu erhöhten Risiken und zu Verstößen bei der Wahrung des Patientengeheimnisses führt. Negative, auch finanzielle Folgen für das UK S-H sowie

Imageverluste drohen. Die Kürzungen müssen daher zurückgenommen werden. Die Ausstattung des behördlichen Datenschutzes muss der Größe der Einrichtung und dem Umfang der Aufgaben entsprechen.

Was ist zu tun?
Alle Krankenhäuser im Land Schleswig-Holstein müssen sicherstellen, dass den bestellten Datenschutzbeauftragten für deren Datenschutzmanagement zur Wahrnehmung ihrer wichtigen Aufgabe ausreichende Ressourcen zur Verfügung gestellt werden.

4.7 Wissenschaft und Bildung

4.7.1 Landesnetz Bildung (LanBSH) jetzt auf sicheren Beinen

Es wurde ein zentrales Konzept für eine einheitliche Informationstechnologie in den Schulverwaltungen fertiggestellt. Nach Abschluss der Pilotierungsphase beginnt – angefangen bei den Gymnasien – die Einführung datenschutzkonformer IT-Systeme in den Schulverwaltungen.

Das vom ULD eingeforderte IT-Konzept (29. TB, Tz. 4.7.2) wurde in enger Zusammenarbeit zwischen Finanzministerium, Bildungsministerium, den kommunalen Landesverbänden, den Schulträgern und dem Unabhängigen Landeszentrum für Datenschutz erarbeitet. Auf der Basis der vereinbarten Systemkonzepte gehen nun Rechnersysteme in vielen Schulverwaltungen des Landes in den Echtbetrieb. Diese Schulverwaltungsrechner sind **standardisiert konfiguriert** und in das Landesnetz eingebunden. So ist auch eine sichere Internetanbindung der Schulverwaltungen möglich.

Die bisher beim Institut für Qualitätsentwicklung an Schulen Schleswig-Holstein (IQSH) vorliegenden **Anmeldungen** für einen solchen Anschluss zeigen, dass viele Schulleitungen und Schulträger inzwischen von diesem Konzept überzeugt sind.

4.7.2 Wissensdefizite bei Schulleiterinnen, Schulleitern und Schulsekretärinnen

Eingaben von Betroffenen und Anfragen aus Schulleitungen und von Schulsekretärinnen zeigen uns, dass Informationsdefizite in Bezug auf die bestehende Rechtslage und die Umsetzung dieser Normen bestehen.

So erfreulich die Umsetzung des LanBSH-Konzepts (Tz. 4.7.1) auch ist, bei der konkreten Anwendung der Technik in den Schulverwaltungen dürfen die Möglichkeiten des Datenschutzes nicht durch fehlendes Wissen über das Datenschutzrecht und die technischen Sicherungen konterkariert werden. Das Angebot der DATENSCHUTZAKADEMIE (DSA), Schulsekretärinnen in diesem Sektor fortzubilden, findet derzeit immer weniger Resonanz, offensichtlich weil die Schulträger immer weniger Geld für Fortbildungsmaßnahmen zur Verfügung stellen. Schulsekretärinnen scheinen insofern am Ende der Prioritätenkette zu stehen,

obwohl sie tagtäglich mit sensiblen personenbezogenen Daten umgehen. Ein Eckpfeiler des LanBSH-Konzepts ist die datenschutzrechtliche **Schulung**. Ohne diese ist eine sichere und datenschutzkonforme elektronische Datenverarbeitung nicht möglich.

Auch bei den für die Datenverarbeitung verantwortlichen **Schulleitungen** besteht ein erhöhter Ausbildungsbedarf. So existiert z. B. eine große Unsicherheit, welche Daten von Schülerinnen und Schülern auf der Schulhomepage präsentiert werden dürfen. Die Schulleiterschulung der DSA wurde bis vor einigen Jahren regelmäßig und mit großem Erfolg in Zusammenarbeit mit dem IQSH durchgeführt, aber inzwischen nicht mehr finanziell unterstützt. Schulverwaltungen beginnen damit, die Daten der Schülerinnen und Schüler ausschließlich automatisiert zu speichern. Dabei sind genaue Kenntnisse der Vorschriften zum Datenschutz und zur Datensicherung sowie deren Beachtung für eine sichere personenbezogene elektronische Datenverarbeitung unabdingbar.

? LanBSH

In den letzten Jahren nahm die Notwendigkeit der Online-Kommunikation der Schulverwaltungen mit anderen öffentlichen Stellen (z. B. dem Statistischen Amt, Bildungsministerium usw.) immer mehr zu.

Dieser Entwicklung wurde durch die Schaffung des Landesnetzes Bildung (LanBSH) Rechnung getragen. In Zusammenarbeit des Bildungs- und Finanzministeriums, des IQSH, den Schulträgern und des ULD wurde ein technisches Konzept entwickelt, welches die sichere Anbindung der Schulverwaltungsrechner über das Landesnetz an das Internet möglich macht. Es umfasst neben der technischen Ausgestaltung der Hardware nach genau festgelegten Kriterien auch die Bereitstellung der erforderlichen schriftlichen Verfahrensdokumentation für das EDV-Verfahren. Daneben enthält eine Dienstanweisung detaillierte Regelungen für die Nutzer der Schulverwaltungsrechner.

Um den Beteiligten eine günstige und einfache Möglichkeit der Wissensbeschaffung zu geben, hat das ULD ein „**Praxishandbuch Schuldatenschutz**“ herausgegeben, das den Verantwortlichen in den Schulen des Landes unentgeltlich zur Verfügung gestellt wird und in dem versucht wird, in allgemein verständlicher Form alle relevanten Fragen zu beantworten. Die Broschüre ist auch im Internet verfügbar unter

www.datenschutzzentrum.de/schule/praxishandbuch-schuldatenschutz.pdf

Was ist zu tun?
Ministerium und Schulträger sollten sicherstellen, dass genügend finanzielle Mittel bereitgestellt werden, damit die Schulleitungen, die Schulsekretärinnen und sonstige Personen, die für den Datenschutz in Schulen verantwortlich sind, die nötige Fortbildung in Anspruch nehmen können.

4.7.3 Zentrale Schülerdatenbank

Nach wie vor ist es geplant, die Bildungsverläufe jeder Schülerin und jedes Schülers von der Einschulung bis zur Schulentlassung zu verfolgen. Allerdings werden die Argumente der Datenschützer zunehmend von den Verantwortlichen zur Kenntnis genommen.

Die Kultusministerkonferenz (KMK) ist nach den von der Konferenz der Datenschutzbeauftragten vorgebrachten Einwänden (29. TB, Tz. 4.7.1) von der Einrichtung einer bundesweiten Schüler- bzw. genauer gesagt **Schuldatenbank** abgerückt. Es besteht aber kein Grund zur Entwarnung. Es wird daran festgehalten, die Bildungsverläufe aller Schülerinnen und Schüler in Deutschland auf Landesebene zu speichern und zu verfolgen. Statt der bisher geplanten Schüler-Identifikationsnummer sollen die einzelnen Schülerdatensätze nunmehr mittels einer Hashwert-Verschlüsselung versehen werden, womit Datensätze Jahr für Jahr derselben Person zugeordnet werden können. Damit, meint die KMK, sei den Einwänden der Datenschutzbeauftragten Genüge getan. Wir mussten aber signalisieren, dass dieses Abspecken der Pläne nicht ausreicht. Mit den Informationen aus den jährlich zu bildenden Gesamtdatensätzen lässt sich ohne größeres Zusatzwissen weiterhin feststellen, für welche Person diese stehen. Die KMK hält außerdem an ihrem Plan fest, für nicht näher definierte Zwecke die in den Bundesländern gespeicherten Daten temporär zusammenzuführen. Diese Planungen erscheinen uns weiterhin zu unbestimmt und unverhältnismäßig.

Was ist zu tun?
Die KMK sollte von dem Großerfassungsvorhaben gänzlich abrücken. Für die dargelegten Informationsinteressen bedarf es keiner Totalerhebung; Stichprobenerhebungen dürften genügen.

4.8 Steuerverwaltung

4.8.1 Zustellung von Schriftstücken durch dänische Finanzverwaltung

Grenzüberschreitende Steuerhinterziehung und Steuerumgehung führen zu Einnahmeverlusten, verletzen das Prinzip der Steuergerechtigkeit und können Verzerrungen des Kapitalverkehrs und des Wettbewerbs verursachen. Datenschutz hindert nicht die Inanspruchnahme mitgliedstaatlicher Hilfe in der Europäischen Union für steuerstrafrechtliche Ermittlungen.

Ein in Dänemark wohnhafter Petent beschwerte sich über die **Zustellung eines Schreibens** eines deutschen Finanzamtes durch die dänische Finanzverwaltung. Das Schreiben eröffnete dem Petenten rechtliches Gehör in einem gegen ihn eingeleiteten Steuerstrafverfahren. Der Petent meinte, das deutsche Finanzamt hätte das Schreiben direkt an die dänische Adresse schicken müssen und die dänische Finanzverwaltung sei nicht befugt gewesen, dieses als einfachen Brief zu versenden.

Tatsächlich ist den deutschen Finanzbehörden erlaubt, bei der Bekanntgabe von Schriftstücken gegenüber im EU-Ausland lebenden Empfängern, welche dem deutschen Steuerrecht unterliegen, die Hilfe ausländischer Finanzbehörden in Anspruch zu nehmen. Dabei leistet das Bundeszentralamt für Steuern **internationale Amtshilfe** in den Bereichen der Umsatzsteuer und der Ertragssteuer; insbesondere Auskunftsersuchen und Zustellungsbegehren werden so koordiniert. Rechtsgrundlage hierfür ist die Verordnung über die Zusammenarbeit der Verwaltungsbehörden auf dem Gebiet der indirekten Besteuerung. Danach sendet die deutsche Finanzbehörde ihre Verwaltungsakte, Entscheidungen und auch sonstige Mitteilungen, wie etwa die Anhörung in einem eingeleiteten Steuerstrafverfahren, an das Bundeszentralamt, das den anderen EU-Staat um eine Zusendung des Schriftstückes auf dem ausländischen Territorium ersucht.

Im konkreten Fall erfolgte die Zusendung des deutschen Finanzamtes an das Bundeszentralamt in verschlossenem Umschlag. Dieses ersuchte die dänische Finanzbehörde um Zusendung des Umschlages an die dänische Adresse. Datenschutzrechtliche Vorschriften wurden nicht verletzt. Dem deutschen Finanzamt konnte auch nicht vorgeworfen werden, dass die dänische Finanzbehörde die Zusendung mittels einfachem Brief vornahm. Dort gelten die dänischen Zustellungsvorschriften. Die EU-Verordnung verlangt ausdrücklich **Angaben über den Gegenstand** der zuzustellenden Verwaltungsakte oder Entscheidungen, Namen und Anschrift des Empfängers sowie alle weiteren zur Identifizierung des Empfängers notwendigen Informationen.

Was ist zu tun?
Im Rahmen der Bekämpfung der Umsatzsteuerhinterziehung ist eine enge Zusammenarbeit der Verwaltungsbehörden der EU-Mitgliedstaaten vorgesehen. Damit einhergehende Datenübermittlungen sind bei Wahrung der Vorschriften erlaubt.

4.8.2 Speicherung von Lohnsteuerabzugsmerkmalen – Bundes-Steuerdatei

Mit dem Entwurf des Jahressteuergesetzes 2008 wird die Ablösung des Lohnsteuerkartenverfahrens durch ein elektronisches Abrufverfahren ab 2011 eingeleitet. Die damit verbundenen gesetzlichen Änderungen halten einer datenschutzrechtlichen Beurteilung nicht stand.

Die zentralisierte Erfassung der deutschen Bevölkerung für steuerliche Zwecke geht ohne Rücksicht auf das Verbot der Vorratsdatenspeicherung voran. Die für Juli 2007 vorgesehene Einführung der **Steuer-Identifikationsnummer** (Steuer-ID) hat sich wegen praktischer IT-Probleme verschleppt (29. TB, Tz. 4.8.3) und nicht aufgrund der Einsicht, dass diese aus Grundrechtssicht nicht akzeptabel ist.


https://www.datenschutzzentrum.de/presse/20070629-steuer-id.htm

Im Rahmen des Entwurfes eines Jahressteuergesetzes 2008 ist geplant, in einer beim **Bundeszentralamt für Steuern** befindlichen Datenbank mit den Steuer-IDs

weitere personenbezogene Daten zu speichern, z. B. die rechtliche Zugehörigkeit zu einer steuererhebenden Religionsgemeinschaft, bei Verheirateten die Steuernummer des Ehegatten, Kinder und ihre Identifikationsnummern, der Familienstand und die gewählte Steuerklasse.

Bereits heute werden die entsprechenden Lohnsteuerabzugsmerkmale auf den Lohnsteuerkarten eingetragen. Künftig soll die Speicherung der Daten auch bei Personen erfolgen, die sich **nicht in einem Beschäftigungsverhältnis** befinden. Nach Ansicht der Bundesregierung könne das Bundeszentralamt nur auf diesem Wege die elektronischen Abzugsmerkmale ohne zeitliche Verzögerungen automatisiert bilden und dem Arbeitgeber zur Verfügung stellen. Durch manuelle Bearbeitung einer Meldung im Einzelfall ausgelöste Verzögerungen rechtfertigen die voraussetzungslose Sammlung von personenbezogenen Daten nicht. Die Speicherung von personenbezogenen Daten muss stets dem Erforderlichkeitsgrundsatz genügen.

Der Gesetzentwurf sieht weiterhin vor, dass sich der **Arbeitgeber für den Abruf** der Lohnsteuerabzugsmerkmale authentifizieren und hierfür seine Wirtschaftsidentifikationsnummer sowie die Steuer-ID und den Tag der Geburt des Arbeitnehmers mitteilen muss. Eine solche Authentifizierung kann den unberechtigten Zugriff Dritter auf die Lohnsteuerabzugsmerkmale nicht ausschließen. Bei der Erbringung elektronischer Informations- und Kommunikationsdienste muss der Arbeitgeber nach den Vorschriften des Telemediengesetzes seine Wirtschaftsidentifikationsnummer allgemein ständig verfügbar halten. Ehemalige Arbeitgeber oder sonstige unbefugte Dritte können die zum Abruf nötigen Informationen unter Umständen leicht in Erfahrung bringen und damit sensible Informationen abrufen.

Die 74. **Konferenz der Datenschutzbeauftragten** des Bundes und der Länder hat im Oktober 2007 eine Entschließung verabschiedet, das im Gesetzentwurf geplante Vorhaben der Umstellung auf ein elektronisches Verfahren vom Jahressteuergesetz 2008 zu trennen.

www.thueringen.de/datenschutz/74_konferenz/zentrale_steuerdatei

Was ist zu tun?
Ein derart bedeutsames Projekt bedarf einer gründlichen fachlichen Analyse sowie einer öffentlichen politischen und verfassungsrechtlichen Diskussion.

4.8.3 Insolvenzhinweis als Adresszusatz

Eine zustellfähige Adresse besteht gewöhnlich aus dem Vor- und Nachnamen des Empfängers, Straße und Hausnummer sowie Postleitzahl und Ortsname. Ein lesbarer Hinweis auf die Insolvenz des Adressaten darf hingegen nicht im Adressfeld erscheinen.

Ein Petent erhielt von einem Finanzamt einen Steuerbescheid, in dessen Adressfeld der Zusatz „In Insolvenz“ zu lesen war. Auf die Datenschutzproblematik

hingewiesen, entschuldigten sich die Mitarbeiter des Finanzamtes bei dem Betroffenen umgehend für diese Adressierung. Bei den entsprechenden Adressangaben handelte es sich um einen **Eingabefehler**, wobei der Hinweis auf die Insolvenz nicht einmal zutreffend war. Das Finanzamt sicherte zu, den fehlerhaften Datenbestand sofort zu bereinigen.

Das Finanzamt erklärte, die Aufnahme des Adresszusatzes erfolge aus verfahrenstechnischen Gründen. Das Insolvenzverfahren sei ein öffentliches Verfahren, daher müsste die Aufnahme eines entsprechenden Adresszusatzes möglich sein. Gleichwohl verpflichtete sich das befragte Finanzamt, künftig eine Adressierung mit dem Hinweis „In Insolvenz“ auch in begründeten Fällen zu unterlassen. Dies ist auch nötig, da die Postadressierung einen anderen Adressatenkreis zu einem anderen Zweck erreicht als die Mitteilung über Insolvenzverfahren. Das Finanzministerium des Landes unterstützte die **datenschutzgerechte Gestaltung der Adressierung** durch ein klärendes Schreiben an alle Finanzämter in Schleswig-Holstein. So wird eine landesweit einheitliche Handhabung der Adressierung von Steuerbescheiden erreicht.

Was ist zu tun?
Finanzämter sind zur Wahrung des Steuergeheimnisses verpflichtet. Verhältnisse, die im Rahmen eines Besteuerungsverfahrens bekannt geworden sind, dürfen nicht unbefugt offenbart werden, auch nicht durch Verwendung von Zusätzen im Adressfeld von Schreiben.

5 Datenschutz in der Wirtschaft

5.1 Arbeitsgruppe Versicherungswirtschaft

Das ULD hat im Jahr 2006 den Vorsitz der Arbeitsgruppe Versicherungswirtschaft des Düsseldorfer Kreises übernommen und führt seitdem die Verhandlungen zwischen Datenschutzbehörden und Versicherungswirtschaft.

Seit mehreren Jahren bestand Uneinigkeit zwischen der Versicherungswirtschaft, vertreten durch den **Gesamtverband der deutschen Versicherungswirtschaft** (GDV), und den Datenschutzaufsichtsbehörden zum Einsatz einer neuen, in der Versicherungswirtschaft fast einheitlich verwendeten Einwilligungserklärung zur Verarbeitung personenbezogener Daten. Dabei handelt es sich um eine kombinierte Klausel, die auch eine Entbindung von der Schweigepflicht enthält, sodass die Versicherungen zur Antrags- oder Leistungsprüfung bei den behandelnden Ärzten nachfragen können. Zudem soll sie die eingesetzten Verfahren der Datenverarbeitung durch die Zustimmung des Versicherungsnehmers legitimieren. Größter Kritikpunkt der Datenschützer war bisher, dass die Information der Versicherungsnehmer über die teilweise sehr komplexen Verfahren unzureichend war und die Einwilligungserklärung letztlich nicht freiwillig erteilt werden kann, da ohne Einwilligung in der Regel auch kein Vertragsabschluss zustande kommt.

Schützenhilfe erhielten die Datenschützer Ende 2006 vom Bundesverfassungsgericht. Das Gericht bekräftigte, dass immer dann, wenn ein Vertragspartner den Vertragsinhalt aufgrund seines Gewichtes faktisch selbst bestimmen kann, dem Recht die Aufgabe

Der Düsseldorfer Kreis und seine Arbeitsgruppen

Die Kontrolle des Datenschutzes bei nicht öffentlichen Stellen ist föderal organisiert, d. h., jedes Bundesland hat eine Behörde, welche die Aufsicht über die dort ansässigen Unternehmen führt. Für Schleswig-Holstein nimmt das Unabhängige Landeszentrum für Datenschutz (ULD) die Aufgaben der Aufsichtsbehörde wahr.

Sind in der Praxis datenschutzrechtliche Fragen zu klären, die branchenweit, d. h. überregional eine Vielzahl von Unternehmen und Verbraucher bzw. Mitarbeiter oder große Konzerne betreffen, die in vielen Bundesländern einen Geschäftssitz haben, so erfolgt ein Austausch im sogenannten „Düsseldorfer Kreis". Hierüber wird eine einheitliche Linie in der Aufsichtspraxis angestrebt. Die Beschlüsse des Düsseldorfer Kreises haben zwar nur informellen Charakter, aber hohe praktische Relevanz.

Da der Düsseldorfer Kreis nur zweimal im Jahr zusammentrifft und eine detaillierte Prüfung in dem Gremium dessen Rahmen sprengen würde, haben die Aufsichtsbehörden die Erörterung von branchenspezifischen Fragen in Arbeitsgruppen ausgelagert. Die Arbeitsgruppen (z. B. AG Kreditwirtschaft, AG Auskunfteien, AG Internationaler Datenverkehr usw.) führen auch die Verhandlung mit den betreffenden Unternehmensvertretern oder Wirtschaftsverbänden und versuchen auf diesem Wege datenschutzrechtliche Probleme zu lösen. Zu einzelnen Fragen werden Beschlussvorlagen erstellt, die dem Düsseldorfer Kreis dann zur Abstimmung vorgelegt werden.

zukommt zu verhindern, dass sich für den anderen Vertragsteil die informationelle Selbstbestimmung zur Fremdbestimmung verkehrt. Dies ergibt sich insbesondere, wenn die angebotene Leistung des einen Vertragsteiles für den anderen so elementar ist, dass die denkbare Alternative, nämlich von einem Vertragsabschluss abzusehen, weil der Versicherer eine zu weitgehende Preisgabe von persönlichen Informationen einfordert, unzumutbar ist. Eine solche Sachlage sah das Bundesverfassungsgericht für den Bereich der Versicherungen gegeben, wo Vertragsbedingungen zumeist in der Praxis nicht verhandelbar sind. Es hat festgestellt, dass die Einholung einer pauschalen **Entbindung von der Schweigepflicht** unzulässig ist, wenn dem Versicherungsnehmer nicht die Möglichkeit gegeben wird, in jedem Einzelfall über die Entbindung zu entscheiden.

Im Nachgang zu dieser Entscheidung ist die Versicherungswirtschaft mit der AG Versicherungswirtschaft in einen neuen Dialog eingetreten. Ziel der Verhandlungen, die vom ULD geführt werden, ist es, den Einsatz einer Einwilligungserklärung auf solche Bereiche zu beschränken, in denen die Betroffenen tatsächlich unabhängig von einem Vertragsabschluss oder der Leistungsgewährung frei entscheiden können (z. B. im Falle der Nutzung und Übermittlung zu Werbezwecken), und alle andere Verarbeitungsverfahren auf die nach **gesetzlichen Rechtsvorschriften** erlaubten Verarbeitungen zu begrenzen.

Ein erster Schritt in diese Richtung wurde bereits für den Einsatz eines **Hinweis- und Informationssystems** (HIS) in der Versicherungswirtschaft gemacht. Das System dient der Risikoprüfung und der Aufdeckung bzw. Prävention von Versicherungsbetrug und wird bereits seit Jahren über eine Software mit dem Namen „Uniwagnis“ innerhalb der dem GDV angeschlossenen Versicherungsunternehmen betrieben. Lange Zeit herrschte Unklarheit darüber, wie dieses System tatsächlich funktioniert, welche Daten verarbeitet werden, wie die Versicherungsunternehmen den Datenaustausch betreiben usw. Die AG Versicherungswirtschaft hat nunmehr unter Federführung des ULD und in Zusammenarbeit mit dem GDV eine Sachverhaltsdarstellung veröffentlicht, die das herkömmliche System transparent beschreibt.

www.datenschutzzentrum.de/wirtschaft/20070703-his.htm

Es gilt nun, das System datenschutzkonform umzugestalten. Im Wesentlichen geht es dabei darum, das grundsätzlich anzuerkennende Interesse der Versicherungswirtschaft an **Betrugsprävention** mit den schutzwürdigen Belangen der betroffenen Versicherungsnehmer, insbesondere auch mit deren Transparenzbedürfnissen, in Einklang zu bringen. Aus Datenschutzgründen dürfen nur solche Daten in das System eingemeldet werden, denen eine tatsächliche Aussagekraft für die Frage eines Versicherungsmissbrauches zukommt. Die Berechtigung eines Abrufs dieser Daten durch ein anderes Versicherungsunternehmen muss auf bestimmte Fälle beschränkt und kontrollierbar sein, und die Betroffenen müssen über eine Einmeldung informiert bzw. in die Lage versetzt werden, Auskünfte über die eingemeldeten Daten zu erhalten. Die Versicherungsunternehmen sind insbesondere verpflichtet, Dritte, z. B. Zeugen eines Unfalles, die gemeldet werden, nachträglich zu benachrichtigen.

Was ist zu tun?
Sämtliche Datenverarbeitungsverfahren der Versicherungswirtschaft sind anhand der gesetzlichen Verarbeitungsmöglichkeiten zu überprüfen. Einwilligungserklärungen haben nur dort eine Berechtigung, wo für die Betroffenen echte Entscheidungsfreiheit gegeben ist, sodass ein Wettbewerb über datenschutzrechtliche Konditionen entstehen kann. Alle anderen Datenverarbeitungsverfahren, die z. B. für die Abwicklung des Versicherungsvertrages notwendig sind, müssen sich den beschränkten gesetzlichen Verarbeitungsmöglichkeiten unterwerfen.

5.2 BDSG-Änderungsentwurf: Gut gemeint genügt nicht!

Das Bundesinnenministerium will das Bundesdatenschutzgesetz (BDSG) für die Bereiche Auskunfteien und Scoring-Verfahren ändern. Sein Entwurf enthält positive Ansätze für mehr Transparenz beim Einsatz von Scoring-Verfahren. Auf der anderen Seite würde er Abfragemöglichkeiten bei Auskunfteien eröffnen, die angesichts der schutzwürdigen Interessen der Betroffenen nicht angemessen wären.

Der Entwurf setzt sich zum Ziel, angesichts einer anonymer werdenden Geschäftswelt der steigenden Bedeutung von Auskunfteien Rechnung zu tragen durch verbesserte Transparenz der Verfahren bei Auskunfteien und mehr Rechts- und Planungssicherheit für die Unternehmen. Was dabei herausgekommen ist, geht aber leider teilweise erheblich zulasten der Verbraucherinnen und Verbraucher. Mit Transparenz allein können diese nicht hinreichend vor den Gefahren immer umfangreicherer branchenübergreifender Datensammlungen bei den Auskunfteien bewahrt werden.

Angesichts der hohen Komplexität von Scoring-Verfahren (29. TB, Tz. 5.8) kann sich Verfahrenstransparenz als stumpfes Schwert erweisen. Die Kenntnis darüber, welche Kriterien bei so einem Verfahren eine Rolle spielen, ist begrüßenswert, bringt dem Betroffenen in der Praxis allerdings dann nichts, wenn die Bank und insbesondere der Kreditsachbearbeiter die Bewertungsmaßstäbe des Systems im konkreten Fall nicht kennt. Im Zweifel wird einem nach angeblich objektiven Maßstäben berechneten Scorewert vertraut und etwaige **Gegendarstellungen des Betroffenen** ignoriert.

Der Entwurf würde die Auskunfteiabfrage erheblich erleichtern. Bisher berechtigt nach Überzeugung der Aufsichtsbehörden allein ein **kreditorisches Risiko**, d. h. ein durch Vorleistung des Unternehmens bewirktes finanzielles Ausfallrisiko, zur Erhebung von Zahlungsinformationen über den Betroffenen bei einer Auskunftei. Der Gesetzesvorschlag lässt darüber hinausgehend jedes allgemeine Vertragsrisiko für eine Abfrage ausreichen. Überspitzt formuliert: Mit dieser Öffnung könnten Brötchenverkäufer branchenübergreifend Zahlungserfahrungsdaten über mich erfragen. Realistisch und existenziell für den Einzelnen ist der Fall, dass die Anmietung einer Wohnung verweigert wird, weil der Betroffene seine Handyrechnung – vielleicht aus guten Gründen – nicht bezahlt hat.

Verschwänden die Begrenzungen der Abfrageberechtigung, so könnte der Betroffene sich nicht mehr davor schützen, dass seine Daten an verschiedene Stellen in unterschiedlichen Geschäftskreisen gestreut werden. Das allgemeine unternehmerische Risiko, das bereits bei der Kosten- und Preisgestaltung Berücksichtigung findet, würde abgewälzt zulasten der informationellen Selbstbestimmung. Da die Systeme der Auskunfteien zum Teil (z. B. bei der Schufa) auf dem Gedanken der Gegenseitigkeit beruhen, werden die angeschlossenen abfragenden Vertragspartner auch angehalten, selbst Daten einzumelden. Dadurch fließen Daten aus den unterschiedlichsten Bereichen zu den Auskunfteien. Deren Wissensmacht wird immer weiter erhöht und lädt zu umfassenden Profilbildungen geradezu ein. Ein negativer Wert oder ein negatives Merkmal im Bestand kann dazu führen, dass dem Einzelnen der **Zugang zu einer Vielzahl von Wirtschaftsbereichen** verwehrt bleibt.

Das vorrangige Problem sind nicht die Gesetze, sondern deren **mangelnde Umsetzung**. Die bestehenden Regelungen wären auf die Wirklichkeit anwendbar. Das Bundesinnenministerium geht unzutreffend davon aus, dass unterschiedliche Gesetzesauslegungen der Aufsichtsbehörden das Problem wären. Vielmehr fehlt es den Unternehmen häufig an Kenntnis der Regeln und an der Bereitschaft, Datenschutz als gesetzliche Verpflichtung zu beachten. Die Aufsichtsbehörden können mangels personeller Ausstattung nicht den notwendigen Kontrolldruck aufbauen. Das Schutzniveau für den Einzelnen darf angesichts der in der Praxis ständig erfolgenden Unterlaufungen nicht auch noch auf gesetzlicher Ebene angegriffen werden. Eine Anpassung an die Praxis käme einer Kapitulation eines Grundrechtes gleich.

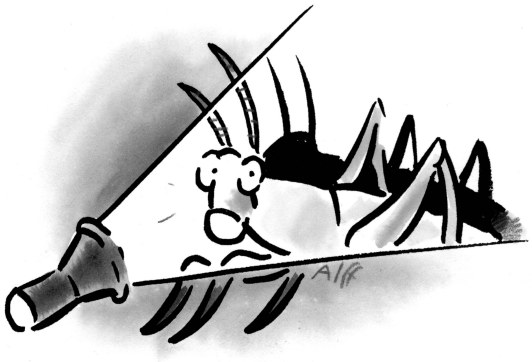
Was ist zu tun?
Es gilt bei der Erhöhung der Kontrolldichte anzusetzen. Dann ist systematisch zu eruieren, welche Regelungen verändert, ergänzt bzw. mit Blick auf die Praxis und nah an der Praxis effektiver zum Schutze der Betroffenen gestaltet werden können.

5.3 Heuschrecken – Erschrecken nach Darlehensverkauf

Eine Horrorvorstellung für jeden Sparkassenkunden mit einem Darlehensvertrag: Ihm wird mitgeteilt, dass sein Kredit an eine ausländische Firma verkauft ist, die Sparkasse habe damit nichts mehr zu tun. Auch die gesamten persönlichen Unterlagen wären dort.

Was hat ein Darlehensverkauf mit dem Datenschutz zu tun? Mit dieser irritierenden Nachfrage wurden wir immer wieder konfrontiert, als wir Beschwerden von Sparkassenkunden nachgingen, deren Kredit an ein Unternehmen verkauft wurde, das nun versuchte, die mit übertragenen Sicherheiten zu versilbern. Mit der Übertragung von Darlehensforderungen werden teilweise hochsensible **persönliche Unterlagen an Dritte** weitergegeben: Vermögensaufstellung, Einkommensnachweise, Erlös- und Gewinnrechnung, Wertgutachten, Betriebs- und Geschäftsgeheimnisse, wirtschaftliche Korrespondenz, teilweise sehr private Hintergrundinformationen. Besonders heikel ist es, wenn diese Unterlagen bei völlig unbe-

kannten Stellen im Ausland landen, wo es keinen oder nur rudimentären Datenschutz gibt.



Darlehensverkäufe von zwei Sparkassen haben nicht nur das ULD intensiv beschäftigt, sondern auch den Landtag und die Staatsanwaltschaft. Während Strafverfolger und Parlament vor allem der Frage nachgingen, inwieweit Mitarbeiter einer Sparkasse dem besonders strafbewehrten Amtsgeheimnis unterliegen, stand bei uns das Übermittlungsverbot im Vordergrund, wenn der Datenweitergabe **schutzwürdige Betroffeneninteressen** entgegenstehen. Der Bundesgerichtshof vertrat in einer Entscheidung im Februar 2007 noch die Ansicht, Verstöße gegen den Datenschutz durch Entsorgung der Darlehen und Darlehensunterlagen an Dritte hätten keine zivilrechtlichen Auswirkungen. Das Bundesverfassungsgericht stellte dagegen aber wenig später klar, dass der Datenschutz seinen Schutzgehalt auch im Privatrecht entfaltet, was zur Folge hat, dass bei einer Forderungsabtretung die Interessen des Gläubigers an der Verkehrsfähigkeit von Forderungen in jedem Einzelfall mit Geheimhaltungsinteressen des Schuldners abgewogen werden müssen. Handelt es sich um einen sogenannten notleidenden Kredit, so ist das schutzwürdige Interesse geringer zu bewerten, als wenn Zins und Tilgung bisher korrekt bedient wurden.

Besonders schutzwürdig sind die Interessen des Schuldners, wenn dieser nicht mehr weiß, wer die Verfügung über seine Unterlagen hat, und wenn er hierzu seine Datenschutzrechte nicht mehr geltend machen kann. Dies kann bis zu einem Totalverlust des Datenschutzes führen, wenn in dem Land, wo der neue Gläubiger seinen Sitz hat, keine Datenschutzkontrolle besteht und **Betroffenenrechte nicht durchsetzbar** sind. Besteht dagegen hinreichend Transparenz für den Kreditnehmer und gelten bei dem neuen Gläubiger adäquate Datenschutzregelungen, so kann der Datenschutz einem Kreditverkauf nicht entgegengehalten werden. Dass dies der Fall war, stellten wir bei einigen Eingaben fest. In anderen Fällen wollten wir das Ermittlungsergebnis der eingeschalteten Staatsanwaltschaft abwarten.

In einem Fall mussten wir dagegen einen Datenschutzverstoß beanstanden. Der Schuldner hatte den Kredit immer korrekt bedient. Dennoch kündigte die Sparkasse den Darlehensvertrag mit der Begründung, sie sei über Sicherheiten falsch informiert worden. Obwohl diesbezüglich noch keine rechtliche Klärung herbeigeführt war, veräußerte die Sparkasse den Kredit in einem größeren Paket an eine irische Tochter des US-amerikanischen Lone Star Fonds und teilte mit, man habe mit der Sache nichts mehr zu tun. Zwar hatte der handelnde Treuhänder seinen Sitz in Deutschland und der Empfänger seinen Sitz in Irland, also in einem Land der Europäischen Union und damit im Geltungsbereich der Europäischen Datenschutzrichtlinie. Dennoch standen hier der Übertragung Datenschutzgründe entgegen, weil **keinerlei Garantien für den Schutz des Betroffenen** bestanden.

Was ist zu tun?
Darlehen dürfen nicht ohne Berücksichtigung des Datenschutzes übertragen werden, da damit die Weitergabe sensibler Daten einhergeht. Vor der Übertragung muss mit pseudonymisierten Unterlagen gearbeitet werden. Die Betroffenen müssen umfassend informiert werden und die Chance haben, ihre Belange geltend zu machen. Das übertragende Kreditunternehmen muss in jedem Fall eine Interessenabwägung vornehmen. Verstöße können dazu führen, dass selbst das Grundgeschäft unwirksam ist.

5.4 Versandhandelskunden bei der Auskunftei

Die Datenschutzaufsichtsbehörde eines anderen Landes fand heraus, dass ein Versandhändler Angaben über vertragsgemäßes Zahlungsverhalten sowie Scorewerte seiner Kundinnen und Kunden ohne Einwilligung oder auch nur Informationen an eine Auskunftei weitergab. Eine Prüfung in Schleswig-Holstein brachte keine entsprechenden Verstöße zutage.

Es ist unbestritten, dass Versandhändler bei kreditorischen Risiken berechtigt sein können, ohne ausdrückliche Zustimmung der Kunden nach negativen Zahlungserfahrungen zu fragen. Voraussetzung ist, dass die potenziellen Kunden über die Abfrage vorab hinreichend konkret informiert werden und sich so rechtzeitig gegen einen Vertragsabschluss entscheiden können. Demgegenüber ist die Einmeldung von Informationen bei einer Auskunftei über das Bestehen oder Nichtbestehen eines Vertragsverhältnisses bzw. über **vertragsgemäßes Kundenverhalten** immer von einer wirksamen Einwilligung der betroffenen Kunden abhängig. Ohne Einwilligung ist die Weitergabe solcher Informationen durch den Versandhändler schlichtweg unzulässig.

Durchweg alle in **Schleswig-Holstein** vom ULD befragten Versandhändler gaben an, lediglich Identifizierungsdaten zum Zwecke einer Bonitätsabfrage und damit keine Daten über vertragsgemäßes Zahlungsverhalten an Auskunfteien weiterzugeben. Die befragten Firmen hatten alle entsprechende Hinweise in ihre allgemeinen Geschäftsbedingungen aufgenommen, wobei bei der Gestaltung der Datenschutzhinweise hier und da Nachbesserungsbedarf bestand. Sollte einem Kunden nicht gefallen, was er liest, bzw. wird ihm die Information über den Umgang mit seinen Daten komplett vorenthalten, so sollte er sich an uns wenden. Wer verunsichert ist, was ein Unternehmen über ihn gespeichert hat bzw. an andere weitergibt, darf und sollte beim Unternehmen nachfragen. Jede Person hat ein Recht darauf zu erfahren, welche Daten über sie gespeichert sind, woher diese stammen und an wen diese Daten übermittelt wurden.

Was ist zu tun?
Die Kunden sind vor Abschluss eines Vertrages auf den Zweck der Datenverarbeitung und über die etwaigen Empfänger der Daten zu unterrichten. Es lohnt sich, den Datenschutzhinweis und die allgemeinen Geschäftsbedingungen eines Unternehmens unter dem Gesichtspunkt des vernünftigen Umgangs mit personenbezogenen Daten zu überprüfen.

5.5 Datenschutz im Autohaus?

Das ULD untersuchte die Datenflüsse in einem Autohaus und fand dabei weitreichende problematische Datenübermittlungen zum Hersteller und wenig Transparenz für die Kundinnen und Kunden.

Die IT-Struktur eines Autohauses ist in der Regel von den Applikationen und dem **Systemaufbau von dem Kfz-Hersteller** geprägt, zu dem eine vertragliche Bindung besteht. Selbst wenn ein Autohaus eigene IT-Anwendungen nutzt, verpflichtet es sich meistens zur Bereitstellung von Datenschnittstellen zwischen dem eigenen System und dem des Herstellers. Hierüber wird dem Hersteller ein weitgehender Zugriff auf die Systeme der Vertragshändler und somit auf die Kundendaten eröffnet.

Das Bundesdatenschutzgesetz (BDSG) privilegiert Datenflüsse innerhalb eines Konzerns bzw. Unternehmensverbundes nicht. Für Datenübermittlungen zwischen den **Vertragshändlern** und dem **Herstellerkonzern** muss ebenso wie für Datenübermittlungen an andere dritte Stellen eine Rechtsgrundlage vorhanden sein. Eine Übermittlung von Kundendaten bei einer Neuwagenbestellung kann gerechtfertigt sein, wenn der Hersteller diese z. B. für Rückrufaktionen oder für eine zentralisierte Meldung beim Kraftfahrt-Bundesamt benötigt. Auch für die Gewährleistungsabwicklung kann eine Weitergabe erforderlich sein, wenn der Vertragshändler sich beim Hersteller für die Regulierung der einzelnen Gewährleistungsfälle schadlos halten möchte und die Abwicklung gegenüber dem Hersteller im Einzelfall beweisen muss. In der Regel, z. B. für die Durchführung des Kundendienstes, ist aber eine personenbezogene Datenübermittlung an den Hersteller nicht erforderlich. Der Vertragshändler ist für den Kunden tätig, ohne dass es z. B. einer personenbezogenen Bestellung von Ersatzteilen beim Hersteller bedarf. Anderweitige Nutzungen der Kundendaten beim Hersteller – z. B. für Werbezwecke oder für vom Hersteller durchgeführte telefonische Kundenzufriedenheitsanalysen – setzen zumeist die schriftliche Einwilligung der Kunden voraus. Insbesondere der Aufbau einer konzernweiten Kundenbindungsdatenbank, die sich aus den Datenübermittlungen der einzelnen Vertragshändler speist, ist ohne freiwillige und widerrufliche Einwilligungserklärungen unzulässig.

Die Datenverarbeitung in den Autohäusern selbst ist auch oft nachbesserungsbedürftig. Die für den **Verkauf von Fahrzeugen** genutzten Datenverarbeitungssysteme sehen zum Teil Datenfelder vor, die nur mit Einwilligung der Kunden ausgefüllt werden dürfen. Wenn der Kunde im Beratungs- und Kaufgespräch private Informationen zu Hobbys, Familie oder Lebensumständen mitteilt, so muss er nicht damit rechnen, dass diese aufgenommen, elektronisch gespeichert und zur weiteren Kundenakquise bzw. Kundenbindung genutzt werden. Für die Erhebung und Speicherung von Daten, die mit der eigentlichen Verkaufsabwicklung in keinem Zusammenhang stehen, ist daher die ausdrückliche Zustimmung erforderlich.

Was ist zu tun?
Die Vertragshändler müssen ihren gesetzlichen Unterrichtungsverpflichtungen nachkommen und die Kundinnen und Kunden über die Speicherung bzw. Übermittlung ihrer Daten und die Zwecke der Datenverarbeitung informieren. Sie sind für die Einholung von Einwilligungen bei Übermittlungen an den Hersteller verantwortlich, wenn diese nicht für die Abwicklung der Vertragsverhältnisse erforderlich sind. Fehlt die Einwilligung, so darf die Weitergabe der Daten nicht erfolgen. Autohäuser haben sich bei Datenerhebung und -speicherung auf das erforderliche Maß zu beschränken.

5.6 Einzelfälle im Verbraucherdatenschutz

5.6.1 Wer hört mit? Aufzeichnungen von Telefongesprächen im Bankgeschäft

Wer unbefugt das vertraulich gesprochene Wort eines anderen aufnimmt, macht sich strafbar. Wollen Unternehmen ihre Telefongespräche mit den Kunden aufzeichnen, so benötigen sie die Einwilligung der Betroffenen. Entsprechendes gilt für die angestellten Mitarbeiter.

Verträge werden zunehmend im Fernabsatz über Telefon geschlossen. Die Unternehmen sind bei solchen Verträgen dafür beweispflichtig, dass sie den Kundinnen und Kunden gegenüber bestimmte Informationspflichten erfüllt haben, und wollen daher dies nachvollziehbar dokumentieren. In einzelnen Bereichen, z. B. im Wertpapierhandel, treffen die Unternehmen gesetzliche Verpflichtungen zur **Dokumentation von telefonischen Aufträgen** und Anweisungen der Kunden. Daher greifen Unternehmen oft zum Mittel des vollständigen Mitschneidens der Telefonate, um sie zu Beweiszwecken einsetzen zu können. Die gesetzlichen Vorgaben erlauben allerdings keine Tonbandaufnahmen. Vielmehr handelt es sich hier um Nachweise, die auch auf anderem Wege ohne Belastung der Persönlichkeitsrechte von Kunden und Mitarbeitern erbracht werden können. Sollen Telefonate legal aufgezeichnet werden, so geht kein Weg an der wirksamen Einwilligung der Betroffenen vorbei.

Bei zwei Finanzdienstleistern aus Schleswig-Holstein stellten wir Mängel fest. Im ersten Fall wurde den Kunden zu Beginn des Gespräches mitgeteilt, dass eine Aufzeichnung durchgeführt wird. Allerdings bestand keine Möglichkeit für die Kunden, die Aufzeichnung abzulehnen oder ihr zuzustimmen. Im zweiten Fall wurde den Kunden eine Einwilligungserklärung bei Vertragsabschluss vorgelegt. Die Zustimmung zur Aufzeichnung der Telefonate wurde jedoch zur Voraussetzung für den Vertragsabschluss gemacht, sodass die Betroffenen sich nicht frei entscheiden konnten, eine Aufzeichnung per Telefon zuzulassen oder nicht.

Was ist zu tun?
Die Einwilligung in die Aufzeichnung eines Telefongesprächs muss bei telefonischen Geschäftsvorgängen ausnahmsweise nicht schriftlich erklärt werden, doch muss die Erklärung durch den Betroffenen ausdrücklich erfolgen und dokumentiert werden. Vor dem Start der Aufnahme müssen die Kundinnen und Kunden über die Absicht der Telefonaufzeichnung unterrichtet werden. Es muss ihnen die Gelegenheit gegeben werden, sich mit der Aufzeichnung einverstanden zu erklären. Das Einverständnis sollte zu Beginn des Mitschnittes noch einmal ausdrücklich bestätigt werden.

Für die Bediensteten kommt allerdings eine Einwilligung meistens nicht in Betracht, da sie sich im Rahmen eines Arbeitsverhältnisses nicht wirklich frei für oder gegen Tonaufzeichnungen entscheiden können. Sie haben zu befürchten, dass sich eine ablehnende Entscheidung negativ auf das Arbeitsverhältnis auswirken kann bzw. sanktioniert wird. Aufgrund des existenziellen Charakters des Arbeitsverhältnisses kann man daher in der Regel nicht davon ausgehen, dass der Mitarbeiter sich ohne Zwang für die eine oder die andere Variante entscheidet. Es empfiehlt sich daher, die Durchführungen von Tonaufzeichnungen und deren Ausgestaltung in einer **Betriebsvereinbarung** zwischen dem Betriebsrat und dem Arbeitgeber festzuhalten. Der Betriebsrat vertritt die Rechte des Arbeitnehmers gegenüber dem Arbeitgeber, ist in dieser Stellung unabhängig und daher in der Verhandlungsposition dem Arbeitgeber ebenbürtig. Eine Betriebsvereinbarung kann, soweit sie die Wahrung der schutzwürdigen Interessen der Mitarbeiter ausreichend berücksichtigt, die Aufnahme von Telefonaten datenschutzrechtlich legitimieren.

Was ist zu tun?
Die Betriebsvereinbarung muss den Mitarbeitern deutlich machen, wann welche Aufzeichnungen zu welchen Zwecken vorgenommen und wie lange diese vorgehalten werden. Zudem sollte festgehalten werden, dass die Aufnahmen nicht zu anderen Zwecken, wie etwa zur Leistungs- und Verhaltenskontrolle, genutzt werden dürfen.

5.6.2 Keine „Schufa-Klauseln“ für alle Fälle

Ein Kunde beschwert sich: Warum muss er bei der Beantragung eines Girokontos auch eine „Schufa-Klausel“ für die Beantragung einer Kreditkarte unterzeichnen, obwohl er diese gar nicht haben möchte?

Die „Schufa-Klausel“ ist eine Einwilligungserklärung, die nur für die Einmeldung von sogenannten Positivdaten gilt. Das sind Informationen über die Beantragung, die Aufnahme und die Beendigung von Vertragsverhältnissen, die als neutrale Daten letztlich keine Aussagekraft für die Frage der Zahlungswilligkeit und Zahlungsfähigkeit, d. h. der Kreditwürdigkeit des Betroffenen haben. Ohne Einwilligung besteht für die Übermittlung solcher Informationen keine Rechtfertigung. Der Einsatz der Schufa-Klausel wird von jeher von Datenschützern kritisch betrachtet, da eine Einwilligungserklärung grundsätzlich freiwillig sein

muss. Die Unterschrift unter der Schufa-Klausel ist aber in der Regel Bedingung für den Vertragsabschluss. Bei einem Antrag auf ein Girokonto müssen die Kunden deswegen fast immer die Einwilligung erteilen, dass Informationen über die Beantragung, Aufnahme und Beendigung des Girokontovertrages an die Schufa übermittelt werden dürfen.

Das Problem ist nach derzeitiger Rechtslage nicht ohne Einwilligungserklärung zu lösen: Einerseits besteht ein anerkennenswertes Interesse der Kreditwirtschaft, Informationen über die Anzahl von Girokonto-, Kreditverträgen usw. zu erhalten, um einschätzen zu können, ob der Betroffene angesichts anderer Verpflichtungen in der Lage sein wird, z. B. einen neuen Kredit ordnungsgemäß zu bedienen. Andererseits gibt es keine Rechtsvorschrift, die eine Übermittlung legitimieren könnte. Der Betroffene hat auch im Hinblick auf den Schutz des Bankgeheimnisses einen Anspruch darauf, dass Bankdaten nicht ohne seine Zustimmung weitergegeben werden. Insofern bleibt es derzeit bei einer **Einwilligungserklärung**, die faktisch **nicht freiwillig** ist.

Unzulässig ist es allerdings, die Einwilligungserklärung nicht nur an den Vertrag mit dem vom Kunden gewünschten Produkt zu **koppeln**, sondern zusätzlich eine Einwilligungserklärung in Bezug auf ein Produkt zu verlangen, dass der Kunde gar nicht haben möchte. Im konkreten Fall war dem Kunden von einer Bank aus Schleswig-Holstein mitgeteilt worden, dass der Girokontoantrag nur bearbeitet würde, wenn der Kunde nicht nur die Schufa-Einwilligung zum Girokontoantrag unterzeichnet, sondern zusätzlich einwilligt, dass auch Daten über eine etwaige Beantragung, Aufnahme und Beendigung eines Kreditkartenvertrages an die Schufa weitergegeben werden dürfen. Der Kunde hatte aber gar keine Kreditkarte für das Konto beantragt. Das ULD forderte die Bank auf, die Schufa-Klausel zur Datenübermittlung von Informationen über einen Kreditkartenvertrag nicht mit dem Giro-

? *Schufa*

Die Schufa wurde ursprünglich von der kreditgebenden Wirtschaft getragen und betrieb für diese ein reines Kreditinformationssystem, das auf dem Prinzip der Gegenseitigkeit beruhte. Ziel war es, den angeschlossenen Unternehmen die Beurteilung der Kreditwürdigkeit des Einzelnen zu erleichtern. Dazu wurden von den angeschlossenen Unternehmen Bonitätsinformationen über Kunden bei der Schufa eingemeldet und abfragenden anderen Instituten weitergegeben.

Inzwischen hat sich die Schufa schrittweise zu einer allgemeinen Auskunftei entwickelt. Die Beauskunftung mit Informationen, die Rückschlüsse auf die Zahlungswilligkeit und -fähigkeit des Einzelnen zulassen sollen, erfolgt auch an andere Branchen. Dies sind mittlerweile z. B. Telekommunikationsunternehmen, Wohnungswirtschaftsunternehmen, Versandhandelsunternehmen, Inkassofirmen und Versicherungsunternehmen.

Um eine Bonitätsinformation zu erhalten, müssen die angeschlossenen Unternehmen ein berechtigtes Interesse glaubhaft darlegen. Ein solches kann in der Regel nur bei einem kreditorischen Ausfallrisiko gegeben sein, d. h. immer wenn Unternehmen in Vorleistung gehen. Problematisch ist, dass beim Anschluss neuer Vertragspartner (z. B. aus dem Bereich der Wohnungs- bzw. Versicherungswirtschaft) zuvor keine Zulässigkeitsprüfung durch die Datenschutzaufsichtsbehörden erfolgt.

kontoantrag zu verknüpfen. Die Bank hat ihr Vorgehen entsprechend geändert.

Werden Einwilligungen zur Datenübermittlung an die Schufa auf Vorrat eingeholt, so verlieren die ohnehin faktisch nicht freiwilligen Einwilligungen auch ihre **Warnfunktion**. Ein Ziel der Einwilligung ist es, dem Kunden bewusst zu machen, welche Daten an wen übermittelt werden sollen, sodass er sich im sachlichen und zeitlichen Kontext mit der Übermittlung auseinandersetzen kann. Eine Einwilligungserklärung aus Vorzeiten und ohne Bezug zum beantragten Produkt hat der Kunde im Zweifel vergessen und entfaltet keine Warnfunktion. Eine spätere Übermittlung erfolgt dann, ohne für den Betroffenen transparent zu sein.

Was ist zu tun?
Auf Vorratseinwilligungen ist zu verzichten.

? Schufa-Klausel

Die Schufa-Klausel stellt nicht nur eine Einwilligungserklärung für die Übermittlung von Vertragsdaten an die Schufa dar. Die Klausel enthält darüber hinaus einen Informationsteil, mit welchem die Kunden über das Schufa-Verfahren unterrichtet werden. Unabhängig von der erteilten Einwilligung dürfen die Unternehmen nach dem Bundesdatenschutzgesetz auch negative Informationen über das Zahlungsverhalten der Kunden bei der Schufa einmelden. Diese Informationen dürfen ohne ausdrückliche Zustimmung von anderen Unternehmen zwecks „Bonitätsprüfung" im Vorfeld von Vertragsabschlüssen mit kreditorischem Risiko abgerufen werden. Das berechtigte Interesse für die Abfrage muss glaubhaft dargelegt werden. Zudem ermittelt die Schufa auf der Grundlage ihrer Datenbasis Scorewerte, die in der Regel im Rahmen der Bonitätsauskunft mit beauskunftet werden. Wie die Werte zustande kommen und welche Faktoren dabei eine Rolle spielen, ist nicht hinreichend transparent. Der Einsatz der Schufa-Klausel muss von Anfang an kritisch bewertet werden: Einwilligungserklärungen müssen grundsätzlich freiwillig sein; die Unterschrift bei der Schufa-Klausel wird aber in der Regel zur Bedingung für den Vertragsabschluss gemacht. Über die Formulierung der Schufa-Klausel wird mit dem Ziel einer datenschutzkonformen Gestaltung intensiv verhandelt. Die Schufa hat sich trotz eindeutiger Rechtslage nicht auf eine rechtskonforme Lösung eingelassen.

5.6.3 Datenschutz im Tank!

Die Nutzung fremder Kundendaten zur Akquise neuer Abnehmer unter Verwendung der Telefonnummer (Cold-Calling) ist wettbewerbs- und datenschutzwidrig.

Der langjährige Kunde eines Heizöllieferanten erhielt, so sein erster Eindruck, einen Telefonanruf seines Unternehmens. Ihm wurde eine Reinigung seines Tankes offeriert. Er ging darauf ein und erbat sich eine schriftliche Bestätigung. Diese wurde ihm am selben Tag per Fax zugesandt. Aus dem Fax ergab sich, dass das Angebot nicht vom Heizöllieferanten stammte, sondern von einem anderen Unternehmen. Dieses hatte auf die Daten des Heizöllieferanten zugegriffen und zur Telefonwerbung genutzt. Eine Einwilligung des Kunden in die Weitergabe und Nutzung seiner Daten zur Telefonwerbung lag nicht vor. Daraufhin machte der Kunde gegenüber den betreffenden Unternehmen seine Rechte auf Auskunft und Sperrung geltend. Die Auskunft wurde vom Tankreini-

gungsunternehmen nur unvollständig beantwortet. Diese und weitere Hinweise auf ein **mangelhaftes Datenschutzmanagement** veranlassten uns zu einer intensiveren Prüfung.

Tatsächlich griffen die Mitarbeiter des Tankreinigungsunternehmens nicht nur auf die **Kundendaten des Heizöllieferanten** inklusive technische Angaben, wie z. B. Tankgröße, zu. Eine solche „Kooperation" erfolgte mit verschiedenen weiteren Firmen, deren Kunden ebenso per Telefon beworben wurden. Einwilligungen der Kunden konnten nicht vorgelegt werden. Wir mussen diese illegale Praxis beanstanden.

Was ist zu tun?
Telefonwerbung ohne vorherige Einwilligung, das sogenannte „Cold-Calling", ist eine datenschutzrechtlich unzulässige Nutzung personenbezogener Daten.

5.6.4 Kreative Kundenbindung: Bonuspunkte nur gegen Grundbuchauszug

Ein Kunde eines Baubedarfgeschäftes beschwerte sich, dass er für den Erhalt einer Bonuskarte mit der Bereitstellung eines Auszugs aus dem Grundbuch beweisen musste, dass er Hauseigentümer ist.

Zwecks Abschluss eines Vertrages über eine Bonuskarte verlangte ein Geschäft für Baubedarf vom Kunden den Beweis, dass er Hauseigentümer ist – über einen Auszug aus dem Grundbuch. Die Bonuskarte ist ein spezielles Produkt des Bauhandels für Kunden mit einem **besonders hohen Einkaufsvolumen**, also für gewerbliche Kunden oder Hauseigentümer. Zur Überprüfung dieser Voraussetzungen verlangte das Geschäft in dem Bonuskartenvertrag unter Benennung der berechtigten Kundengruppen bestimmte Nachweise.

Die Bonuskarte ist eine freiwillige zusätzliche Leistung des Baumarktes. Die Vertragsfreiheit erlaubt den Unternehmen grundsätzlich selbst zu entscheiden, mit welchen Kunden derartige Bonusverträge abgeschlossen werden sollen. Auch die Forderung eines Nachweises der Zugehörigkeit zu einem privilegierten Kundenkreis ist grundsätzlich zulässig. Es ist aber nicht erforderlich und unzulässig, dass Einblick in sensible Unterlagen gefordert, Kopien angefertigt und beim Unternehmen in der jeweiligen Kundenakte aufbewahrt werden. Der Grundbuchauszug enthält Angaben zu Nutzungs- und Wohnrechten, die für den Nachweis der Hauseigentümerschaft uninteressant sind und deshalb hätten geschwärzt werden können. Als Rechtfertigung für das **Aufbewahren von Kopien** kann nicht die Notwendigkeit der Mitarbeiterkontrolle durch den Arbeitgeber herangezogen werden.

Was ist zu tun?
Grundsätzlich genügt im Wirtschaftsverkehr die Vorlage von Unterlagen, z. B. des Personalausweises oder eines offiziellen Dokuments. Das Anfertigen und die Aufbewahrung von Kopien ist zumeist nicht erforderlich. Bei der Vorlage sensibler Unterlagen sollten die Kunden auf ihr Recht hingewiesen werden, bestimmte irrelevante Informationen zu schwärzen.

5.6.5 Nepper, Schlepper, Bauernfänger – SMS umsonst?

Im Internet finden sich viele dubiose Angebote für scheinbar kostenlose Dienstleistungen, die sich am Ende als Abonnementfalle entpuppen. Ziele der Begierde der Anbieter sind neben dem Geldbeutel der Betroffenen deren Daten.

Die Eingaben im ULD zu SMS-Versanddiensten im Internet nehmen zu. Die Petenten nutzten diese Angebote in dem **Glauben, sie seien kostenlos**. Durch Verwendung von Begriffen wie „free“ in der Internetadresse und die grafische und textliche Seitengestaltung der Seiten wurde dies gezielt suggeriert. Bei genauerem Hinsehen entpuppten sich die Angebote jedoch als Abonnementverträge für den Versand von SMS über eine Laufzeit von zwei Jahren und zu einem jährlichen Preis von circa 100 Euro. Betroffene, die nach Aufforderung nicht zahlten, wurden durch zahlreiche E-Mails und die Einschaltung von Inkassounternehmen massiv bedrängt, die Forderungen zu begleichen.

Um den Versanddienst nutzen zu können, mussten die Betroffenen **umfangreiche Angaben zu ihrer Person** machen. Neben Name und Adresse wurden E-Mail-Adresse, Mobilfunknummer und Geburtsdatum abverlangt. Zusätzlich wurde auch die IP-Adresse der Nutzer gespeichert. Die Betreiber der Angebote protokollierten die Telefonnummern der Empfänger der SMS. Im Fall der Zahlungsverweigerung wurden diese Verbindungsdaten zusammen mit anderen Daten an Inkassounternehmen zwecks Beitreibung der Forderungen übermittelt. Wir beanstandeten in einem ersten Verfahrensschritt die umfangreiche Erhebung und Speicherung der Daten. Insbesondere die Speicherung der IP-Adressen war unzulässig und wurde von uns beanstandet.

Zudem monierten wir die Missachtung des Auskunftsrechts der Betroffenen durch die Betreiber. Datenschutzrechtliche Anfragen der Betroffenen wurden entweder gar nicht oder nur unzureichend beantwortet. Die Geltendmachung des Auskunftsrechts wurde zusätzlich dadurch erschwert, dass die Versanddienstbetreiber als Firmensitz eine Adresse in Großbritannien nannten. Nach unseren Erkenntnissen sitzen die Betreiber aber tatsächlich u. a. in Schleswig-Holstein. Die Verschleierung der Identität der Betreiber stellte einen Verstoß gegen das **Transparenzprinzip** dar und war ein weiterer Datenschutzverstoß.

Was ist zu tun?
Die Aufsichtsbehörden tun ihr Bestes bei der Verfolgung illegaler und betrügerischer Datenverarbeitungen im Internet. Zuallererst sind aber die Verbraucherinnen und Verbraucher gefordert, sich durch umsichtigen Umgang mit ihren Daten im weltweiten Netz vor der Verletzung ihrer Persönlichkeitsrechte zu schützen.

5.6.6 Datenschutz? Kein Anschluss unter dieser Nummer!

Ein Telekommunikationsunternehmen erwies sich als das Schlusslicht in Sachen Datenschutz. Die vielen Beschwerden zu fingierten Vertragsabschlüssen und nicht beantworteten Datenschutzanfragen weisen auf systembedingte Mängel hin.

Die Betroffenen erhielten Bestätigungsschreiben zu Verträgen bzw. Bestellungen, die sie niemals abgeschlossen bzw. vorgenommen hatten. Zum Teil waren die Petenten zuvor telefonisch kontaktiert worden. Allesamt versicherten sie glaubhaft, dass sie am Telefon keine Verträge abgeschlossen hätten. Trotzdem tauchten dann Bestätigungsschreiben auf, die auch die Kontoverbindungsdaten der Betroffenen enthielten, ohne dass diese preisgegeben worden waren. In einem Fall erhielt ein Betroffener dreimal hintereinander eine Bestätigung zu einer Bestellung, die er nicht vorgenommen hatte. Machten die Petenten dann ihre Datenschutzrechte geltend und fragten an, welche Daten gespeichert sind und woher diese stammen, erhielten sie keine Antwort. Das Unternehmen erklärte auf Anfrage durch das ULD, dass es sich hier um einzelne Fälle von Datenmissbrauch durch Vertriebspartner handele. Ein paar schwarze Schafe unter den Franchisenehmern, die einen Shop zu diesem Telekommunikationsunternehmen betrieben, würden Vertragsverhältnisse fingieren. Die Masse der Beschwerden macht allerdings deutlich, dass das Problem mit dem Verweis auf den jeweiligen Einzelfall nicht abgetan werden kann. Das Unternehmen ist mit verantwortlich für die **Vertriebswege und -partner**, die sorgfältig auszuwählen, zu kontrollieren und immer wieder zu hinterfragen sind.

Nachbesserungsbedarf besteht insbesondere auch im eigenen **Datenschutzmanagement**. Wenn das Unternehmen organisatorisch nicht in der Lage ist, Datenschutzanfragen von Betroffenen an die zuständige Stelle im Betrieb weiterzuleiten, bestehen tief greifende strukturelle Probleme, die potenzielle Neukunden verprellen und Altkunden spürbar unzufrieden machen. Solche Anfragen können bei kleinen Unternehmen vom betrieblichen Datenschutzbeauftragten selbst beantwortet werden. In anderen Unternehmen wird die Beantwortung möglicherweise vom Kundenservice übernommen; dies sollte dann aber vom Datenschutzbeauftragten koordiniert und angeleitet werden.

Was ist zu tun?
Unternehmen müssen dafür Sorge tragen, dass Datenschutzanfragen wie z. B. Auskunftsersuchen, Löschungsbegehren, Widersprüche usw. an die zuständigen Stellen im Unternehmen weitergeleitet werden, sodass eine Beantwortung sichergestellt ist. Vertriebspartner sollten im Wege von Vertragsstrafenregelungen verpflichtet werden, sorgfältig mit Kundendaten umzugehen. Bei Datenmissbrauch sollte der Franchisevertrag gekündigt werden.

5.6.7 Ohne Daten keine Muckis!

Über Jahre war es ein zwangloses Kommen und Gehen im Fitnessstudio. Doch nach einem Diebstahl wollte der Betreiber des Studios schon gerne wissen, wer sich wann in seinen Räumlichkeiten aufhielt.

Er legte eine Check-in/-out-Liste aus, in die sich die Studiomitglieder freiwillig eintragen konnten und – nach ein paar Jahren – eintragen mussten. Als einige Mitglieder auf das Eintragen „verzichteten", kam es zum Streit. Der Betreiber fühlte sich mit Verweis auf die von ihm erlassene Hausordnung im Recht – ein Trugschluss. Der Wunsch des Betreibers, einen Überblick darüber zu erhalten, wer sich zu welchen Zeiten im Fitnessstudio aufhält, ist nachvollziehbar. Dies muss jedoch datenschutzrechtlich auf sichere Beine gestellt werden: In den Verträgen wurde ein Passus aufgenommen, in dem die Mitglieder sich zur Beachtung der **Hausordnung** verpflichten. Die Hausordnung wird künftig bei Vertragsabschluss ausgehändigt und liegt an geeigneter Stelle im Fitnessstudio jederzeit zur Einsichtnahme aus. Die erhobenen Daten werden spätestens am Tag nach der Erhebung vernichtet. So wird die Datenerhebung für die Mitglieder transparent, und es erfolgt keine übermäßige Datenspeicherung; der Betreiber kann künftig bei Neumitgliedern auf sein „Recht pochen". Da die Altverträge so leicht nicht zu kündigen sind, muss er bei den bisherigen Mitgliedern auf deren Verständnis hoffen.

Was ist zu tun?
Vor der Erhebung von personenbezogenen Daten ist der Zweck genau zu definieren. Die Betroffenen sind über den Zweck der Datenverarbeitung und die Speicherdauer vorab zu informieren.

5.6.8 Der Wolf im Schafspelz

Wen nerven unangekündigte Werbeanrufe nicht? Tagtäglich werden Verbraucher mit scheinbar lukrativen Geldanlagen, Zeitungsabos, gewinnträchtigen Lotteriespielen am Telefon konfrontiert. Doch unerbetene Werbeanrufe sind gesetzlich verboten!

Genau auf diesen Zug sprang ein junges dynamisches Unternehmen auf. Circa 30 Euro sollen die Verbraucherinnen und Verbraucher dafür zahlen, dass ein Eintrag auf Telefon- und Handysperrlisten, eine Weiterleitung der Beschwerde an den Verbraucherschutz, eine Rechtsanwaltsvermittlung und das Bereithalten einer Servicehotline erfolgt. Das Perfide an der Sache: Die **vermeintlichen Verbraucherschützer** bedienten sich selbst des Telefons, um ihre fragwürdigen Verträge an die Frau/den Mann zu bringen.

Zwei Betroffene teilten uns ihre Erfahrungen mit. Sie hatten bei den Anrufen des Unternehmens einen Vertragsabschluss abgelehnt und ihre Bankverbindung nicht preisgegeben. Trotzdem war die Abbuchung der oben genannten „Gebühr" erfolgt. Das Unternehmen behauptete, die Petenten hätten ihre Bankverbindung am Tele-

fon mitgeteilt. Die telefonische Kontaktaufnahme sei gerechtfertigt gewesen, da die Petenten sich auf einer **Gewinnspielkarte** mit der telefonischen Entgegennahme interessanter Angebote bereit erklärt hätten. Wir forderten die Gewinncoupons an und legten sie den Petenten vor. Diese versicherten glaubhaft, dass sie an dem Gewinnspiel niemals teilgenommen hatten; es handele sich auch nicht um ihre Unterschrift auf den Coupons. In einem Fall war sogar der Name falsch geschrieben. Dies waren für uns ausreichende Anhaltspunkte für die Annahme einer Straftat durch den Geschäftsführer, sodass wir den Vorgang an die Staatsanwaltschaft abgaben.

Unerbetene Werbeanrufe sind verboten!

Das Gesetz gegen unlauteren Wettbewerb sowie das Datenschutzrecht verbieten Telefonanrufe zu Werbezwecken. Das gilt auch, wenn mit dem Unternehmen eine Geschäftsbeziehung besteht. Anderes gilt nur, wenn eine Einwilligung vorliegt, am Telefon über Produkte des Unternehmens informiert zu werden.

Für die Werbeansprache per Post ist dagegen eine ausdrückliche Zustimmung des Betroffenen nicht erforderlich. Der Betroffene kann allerdings der Nutzung und Weitergabe seiner Daten zu Werbezwecken widersprechen und muss auf dieses Recht bei der Werbeansprache hingewiesen werden. Im Fall des Widerspruchs dürfen die Daten nicht mehr zu Werbezwecken genutzt oder übermittelt werden. Wer von vornherein weiß, dass er keine Werbung bekommen möchte, kann bereits zum Zeitpunkt des Vertragsabschlusses widersprechen.

Was ist zu tun?
Bei der Preisgabe eigener Daten ist Vorsicht und Zurückhaltung geboten, auch bei Telefonnummern, vor allem aber bei Bankverbindungsdaten. Bei Vertragsabschlüssen kann der Nutzung und Übermittlung der Daten zu Werbezwecken widersprochen werden. Unerbetene Werbeanrufe sind verboten. Beim Telekommunikationsprovider kann beantragt werden, dass Anrufe mit unterdrückter Rufnummer nicht durchgestellt werden. Gewinnspielkarten und -coupons sollten sorgfältig gelesen werden. Der Teufel steckt oft im Kleingedruckten!

5.6.9 Öfter mal was Neues – Datenschutz in der Wohnungswirtschaft

Neue technische Entwicklungen im Bereich der Wohnungswirtschaft und nicht mehr so ganz neue Fragen der Zusammenarbeit der Vermieter mit Auskunfteien beschäftigten das ULD.

Wohnungsunternehmen in Schleswig-Holstein sind dazu übergegangen, Verbrauchswerte wie **Heizenergie und Wasserverbrauch** elektronisch abzulesen und per Funk zu übertragen. Das spart Personalkosten; die Mieter müssen zudem die Ableser nicht mehr in die Wohnung lassen. Funkfähige Erfassungsgeräte können taggenau den jeweiligen Energie- oder Wasserverbrauch aufzeichnen. Sie ermöglichen damit eine Protokollierung der verbrauchten Ressourcen je nach Bedarf. Was dem Mieter und dem Vermieter einerseits entgegenkommt, nämlich die präzise und unkomplizierte Ablesung und Berechnung der Nebenkosten, birgt andererseits Gefahren für die Privatsphäre der Mieter. Eine hochauflösende Erfas-

sung des Verbrauches erlaubt Rückschlüsse auf deren Lebensgewohnheiten. So ist ohne Weiteres erkennbar, wann ein Mieter im Urlaub bzw. längere Zeit abwesend ist. Auch andere Schlüsse, z. B. auf Besuch durch erhöhten Verbrauch im Gästezimmer, sind möglich.

Die unbestreitbaren Vorteile der Technik können von allen Beteiligten in vollen Zügen nur genossen werden, wenn die Persönlichkeitsrechte der Betroffenen gewahrt werden. Dies ist nur der Fall, wenn die Verbrauchsdaten **in zusammengefasster Form** für den gesamten Abrechnungszeitraum übermittelt und ausgewertet werden. Eine unterjährige Erfassung ist nur datenschutzkonform, wenn dies im Rahmen der Erfüllung der mietvertraglichen Pflichten erforderlich ist, also z. B. eine Betriebskostenabrechnung bei Mieterwechsel. Die Vermieter müssen die Betroffenen über die neuen Erfassungs- und Abrechnungsmodalitäten genau informieren. Die Mieter müssen wissen, in welchen Intervallen von wem und zu welchem Zweck der Verbrauch erfasst wird. Die erfassten Daten dürfen nur zweckgebunden für die Erstellung der Betriebskostenabrechnung verwendet werden. Darüber hinausgehende Nutzungen bedürfen einer auf den jeweiligen Zweck ausgerichteten Rechtsgrundlage.

Dauerthema schriftlicher Eingaben und der telefonischen Beratung ist die Abfrage und Einmeldung von Informationen über Mietinteressenten durch die Vermieter bei **Auskunfteien**. Vermieter gehen vermehrt dazu über, vor dem Abschluss von Mietverträgen derartige Auskünfte einzuholen und im Gegenzug Informationen über ihre Mieter einzumelden. Teilweise wird die Erteilung einer Einwilligung in die Abfrage und in die Einmeldung von Informationen bei Auskunfteien zur Bedingung gemacht, ohne die sich die Betroffenen überhaupt nicht für eine Wohnung bewerben können, auch wenn am Ende nicht der Abschluss eines Mietvertrages steht.

Die Einholung von Auskünften über die Bonität potenzieller Mieter ist nur zulässig, soweit es zur **Wahrung der berechtigten Interessen** der Wohnungswirtschaftsunternehmen erforderlich ist. Außerdem darf kein Grund zu der Annahme bestehen, dass durch die Abfrage schutzwürdige Interessen der zukünftigen Mieter verletzt werden. Ein berechtigtes Interesse auf der Seite der Vermieter ist in der Minimierung des betriebswirtschaftlichen Risikos von Mietausfällen zu sehen. Dem stehen die schutzwürdigen Interessen der potenziellen Mieter an der Geheimhaltung von privaten Informationen gegenüber. Bei dieser Abwägung muss die existenzielle Bedeutung von Wohnraum für die Betroffenen, die von der Rechtsordnung vorgesehenen Bindungen des sozialen Mietrechts und die Möglichkeit der Vermieter, sich durch Direktbefragung der potenziellen Mieter, durch Mietkautionen, Vermieterpfandrechte oder Einschaltung der Sozialbehörden wirtschaftlich abzusichern, einfließen. Im Ergebnis sehen wir nur die Einmeldung und Erteilung von Auskunft sogenannter **harter Negativmerkmale** unter Beachtung der Besonderheiten des Mietrechts als zulässig an. Vermieter und Auskunfteien dürfen danach nur folgende Informationen melden bzw. beauskunften:

- Informationen aus öffentlichen Schuldnerverzeichnissen,
- Vollstreckungsbescheide wegen Mietzahlungsrückständen in Höhe von mindestens zwei Monatmieten einschließlich Nebenkosten, ausgenommen Fälle, in denen Mietminderung geltend gemacht wurde,
- Bescheinigung eines Gerichtsvollziehers über die fruchtlose Pfändung einer titulierten Forderung aus einem Mietverhältnis,
- rechtskräftige Urteile, die eine fristlose Kündigung wegen der Vernachlässigung der Mietsache oder unbefugte Überlassung an Dritte oder gesetzlich vorgesehener wichtiger Gründe bestätigen, ausgenommen Fälle, in denen Mietminderung geltend gemacht wurde,
- rechtskräftige Räumungsurteile nach fristloser Kündigung wegen vertragswidrigen Verhaltens der Mietpartei, ausgenommen Fälle, in denen vor Kündigung wegen Zahlungsverzugs Mietminderung geltend gemacht wurde.

Der Einmeldung und der Beschaffung von über harte Negativmerkmale **hinausgehenden Informationen** stehen in der Regel schutzwürdige Betroffeneninteressen entgegen. Die wirtschaftlichen Interessen der Vermieter an der Minimierung ihrer Risiken – angesichts der genannten Sicherungsmöglichkeiten der Vermieter, der Bedeutung des Wohnraums und den mietrechtlichen Vorschriften – müssen zurücktreten.

Für die Beschaffung und Einmeldung von sogenannten **Positivmerkmalen**, d. h. Informationen über die Eingehung eines Mietverhältnisses oder Ähnliches, fehlt ebenso eine datenschutzrechtliche Rechtfertigung. Die Erhebung und Übermittlung solcher Daten wäre nur über die freiwillige Einwilligung der Betroffenen zulässig. An der Freiwilligkeit bestanden in den vom ULD zu prüfenden Fällen jeweils erhebliche Zweifel. Den Mietinteressenten verblieb aufgrund der Lage auf dem Wohnungsmarkt und der eigenen finanziellen Möglichkeiten häufig keine Alternative zur Einwilligung, weil sie bei einer Weigerung von der Auswahlentscheidung ausgeschlossen worden wären. Unfreiwillig erteilte Einwilligungen sind ungültig. Eine darauf basierende Datenverarbeitung kann eventuell als Ordnungswidrigkeit sanktioniert werden.

Häufig missachtet wurde durch Vermieter die Verpflichtung, die Betroffenen vor der Abfrage oder Einmeldung solcher Informationen zu **informieren**. Transparenz im Umgang mit sensiblen Daten und die Beachtung des Erforderlichkeitsprinzips sind vom Gesetz her geboten, verbessern das Bild des eigenen Unternehmens in der Öffentlichkeit und schaffen Vertrauen bei den Mietern.

Was ist zu tun?
Vermieter müssen bei der Verfolgung ihrer berechtigten wirtschaftlichen Interessen die Persönlichkeitsrechte ihrer Mieter und der Interessenten beachten.

5.6.10 Anonym auf die Insel?

Die Bewohner einer Insel waren empört: Sie sollten ihren Hauptwohnsitz per Meldebescheinigung gegenüber der Fährgesellschaft nachweisen, um den verbilligten Insulanerfahrpreis zu erhalten. Zudem wurden die Überfahrtdaten – Datum, Uhrzeit, Kfz-Kennzeichen und bei Vorabbuchung auch Namen – langfristig gespeichert und im Einzelfall zur Überprüfung des Insulanerstatus herangezogen.

Die Frage der Verpflichtung zur **Vorlage einer Meldebescheinigung** war einfach zu beantworten: Das Landesmeldegesetz sieht die Ausgabe von Meldebescheinigungen an die Einwohner vor. Diese dienen aber nur zur Vorlage bei einer Behörde, das Vorlageverlangen durch ein privates Unternehmen ist nicht vorgesehen. Um den Einwohnerstatus gegenüber einer Fährgesellschaft nachzuweisen, muss die Sichtvorlage des Personalausweises ausreichen.

Die Überfahrtdaten dürfen nur solange gespeichert werden, wie sie für die Abwicklung des Transportes benötigt werden. Für Fährnutzer, die eine Hin- und Rückfahrkarte gebucht haben, hängt die Gültigkeit der Rückfahrkarte davon ab, wann die Hinfahrt in Anspruch genommen wurde. Die Reisedaten dürfen dann für diesen Zeitraum gespeichert werden, aber nicht länger. Die Datennutzung zwecks Feststellung der Insulanereigenschaft ist weder geeignet noch angemessen. Die allgemeinen Tarifbestimmungen des Unternehmens sahen vor, dass der verbilligte Insulanertarif nicht nur den Hauptwohnsitz, sondern auch den tatsächlichen **Lebensmittelpunkt auf der Insel** voraussetzten. Die Transportdaten eines Fahrzeuges lassen aber keinen aussagekräftigen Rückschluss auf den Lebensmittelpunkt zu, der sowieso mit den Mitteln einer Fährgesellschaft schwerlich erfassbar ist. Der Standort des Fahrzeuges, der aus den Reisedaten ablesbar ist, ist allenfalls ein Indiz. Die Feststellung des Lebensmittelpunktes muss weniger datenintensiv und die Privatsphäre weniger beeinträchtigend erfolgen. Die Fährnutzer haben ein überwiegendes Interesse an einer unbeobachteten und undokumentierten freien Reise gegenüber dem Kontrollinteresse der Fährbetreiber. Die Einwohnerzahl der Insel ist überschaubar; die Reisenden sind den Mitarbeitern der Fährgesellschaft zum Teil persönlich bekannt. Deren gesammelte Überfahrten sollten nicht zum Inselgespräch werden.

Das Unternehmen erklärte, dass eine kurzfristige Änderung der automatisierten Löschung nicht möglich sei. Wir räumten daher eine angemessene Frist zur datenschutzkonformen Umgestaltung des Systems ein, verbunden mit der Auflage, dass die Daten zwischenzeitlich nur zum Zwecke der Prüfung der Gültigkeitsdauer von Fahrkarten und nicht zu anderen Zwecken, insbesondere nicht zum Zwecke der Missbrauchskontrolle, genutzt werden. Das Unternehmen wurde verpflichtet, die Fährbenutzer über die Datenerhebung, -speicherung und -nutzung hinreichend konkret zu informieren. Die nun nötige lästige, aufwendige und teure Systemnachbesserung wäre vermeidbar gewesen.

Was ist zu tun?
Datenvermeidung und Datensparksamkeit sowie Rechtmäßigkeit der Datenverarbeitung müssen bereits bei der Konzipierung bzw. der Auswahl eines Kontrollsystems berücksichtigt werden.

5.6.11 Freundlicher Hinweis zum Reifenwechsel

Das Serviceangebot eines bundesweit agierenden Autowerkstattunternehmens erfreute eine Petentin überhaupt nicht. Sie hatte eine Werbepostkarte erhalten mit Anschrift, Kfz-Kennzeichen, Automarke und TÜV/AU-Fälligkeit.

Die Petentin hatte keine Einwilligung für eine Speicherung und Weitergabe ihrer Daten zu Werbezwecken erteilt. Zudem monierte sie die öffentliche Preisgabe ihrer Daten durch das Versenden auf einer Postkarte. Die schutzwürdigen Interessen der Petentin, keine unerwünschte Werbung zu erhalten, standen somit dem „berechtigten“ wirtschaftlichen Interesse des Unternehmens an der Durchführung der Werbemaßnahme gegenüber. Dieses akzeptierte letztlich unsere Feststellung, dass die schutzwürdigen Kundeninteressen verlangen, dass bereits bei Datenerhebung über die geplante Werbenutzung **hinreichend Transparenz** geschaffen wird. Nur wenn die Kundinnen und Kunden informiert sind, können und müssen sie mit einer Bewerbung rechnen. Das Unternehmen äußerte seine Absicht, künftig seine Kunden bereits beim Erteilen des Werkstattauftrages über die beabsichtigte Nutzung der erhobenen Daten zu informieren.

Auch die Gestaltung der **Erinnerungspostkarten** wurde geändert. Künftig wird auf die Angabe des Kfz-Kennzeichens verzichtet. Die Kundinnen und Kunden werden auf die bestehende Möglichkeit eines Widerspruchs zur Nutzung der Daten zu Werbezwecken hingewiesen.

5.6.12 Lektüre in der Warteschlange

Die Einführung eines neuen Kassensystems in einem großen Einkaufsmarkt hatte einen interessanten Nebeneffekt: Nach dem Einlesen der Kundenkarte wurde der Name und die vollständige Adresse des Kundenkarteninhabers für alle in der Warteschlange stehenden Kunden am Display der Kasse sichtbar. Dieses „EDV-Problem“ konnte kurzfristig behoben werden.

Was ist zu tun?
Vor der Inbetriebnahme neuer Verfahren ist zu prüfen, ob damit Risiken für das informationelle Selbstbestimmungsrecht der Betroffenen verbunden sind. **Vor** dem Realbetrieb sind die Maßnahmen zu treffen, die eine Gefährdung des Persönlichkeitsrechts der Betroffenen ausschließen.

5.7 Arbeitnehmerdatenschutz

Ein **Arbeitnehmerdatenschutzgesetz**, das seit über 20 Jahren auf Bundesebene von Datenschützern wie auch von Vertretern der Arbeitnehmerseite gefordert wird, ist nicht in Sicht. Inzwischen erfolgen auch keine Ankündigungen der Bundesregierung mehr, ein solches Gesetz auf den Weg bringen zu wollen. Dies mag zur Bewältigung der im Tagesgeschäft anfallenden Konfliktfälle angesichts einer datenschutzbewussten Arbeitsgerichtsrechtsprechung hinnehmbar sein.

Wer aber angesichts des zunehmenden **Einsatzes von Telekommunikation** in Unternehmen besonders unter dem Fehlen einer bereichsspezifischen Regelung zum Arbeitnehmerdatenschutz leidet, sind die Unternehmen: Sie werden derzeit wie Telekommunikationsprovider mit einer Vielzahl von Pflichten behandelt, wenn sie ihre Unternehmenskommunikation auch nur ein wenig für die private Nutzung freigeben. Eventuell in Betrieben sinnvolle begrenzte Stichprobenkontrollen bei der Telekommunikationsnutzung sind gesetzlich unzulässig. So wählen viele Unternehmen die Alternative eines absoluten Nutzungsverbotes für private Zwecke – keine wirklich mitarbeiterfreundliche Alternative.

Es gibt aber eine Vielzahl weiterer – angesichts der technischen Entwicklung – dringend werdender Regelungsnotwendigkeiten: die verstärkte Nutzung von biotechnologischen Verfahren, z. B. bei der Einstellung, die Praxis illegaler Drogentests, der konzernweite Austausch von Arbeitnehmerdaten usw.

5.7.1 Bewerber ahnungslos – über die Einstellung entscheiden andere

Ein Stellenbewerber beschwerte sich über die Weitergabe seiner Unterlagen an eine Zeitarbeitsfirma. Er hatte sich bei einem Unternehmen auf eine Stellenanzeige hin beworben und keine Antwort erhalten.

Auf eigene mehrmalige telefonische Nachfrage hin wurde dem Betroffenen mitgeteilt, dass die Stelle anderweitig vergeben worden ist. Er bat daraufhin um Rücksendung seiner Bewerbungsunterlagen. Ihm wurde mitgeteilt, dass zwecks Rücksendung seiner Unterlagen diese **an eine Zeitarbeitsfirma weitergeleitet** worden waren und er diese in zwei Wochen zurückerhalten würde. Nach zwei Wochen meldete sich die Zeitarbeitsfirma tatsächlich, bestätigte den Eingang der Unterlagen und fragte nach, ob er Interesse daran hätte, in die Kartei der Firma aufgenommen zu werden.

Das Unternehmen hatte, so seine Darstellung, die Zeitarbeitsfirma mit der logistischen Abwicklung des Bewerbungsverfahrens beauftragt und daher die Unterlagen übermittelt. Die betroffenen Bewerber waren hierüber vorab nicht informiert

worden. Das ULD beanstandete diese Praxis gegenüber dem Unternehmen. Bei der **Beauftragung Dritter** mit der logistischen Abwicklung eines Bewerbungsverfahrens muss das Unternehmen sicherstellen, dass die Unterlagen vertraulich behandelt werden und der Dienstleister die Angaben der Bewerber nur in dem erforderlichen Umfang zur Kenntnis nimmt. Konkret hatte das Unternehmen seine Aufsichtspflicht dahin gehend verletzt, dass es nicht verhinderte, dass die Zeitarbeitsfirma die Bewerbungen **für eigene Zwecke nutzte**. Bewerbungsunterlagen sind hochsensitiv; sie zielen darauf ab, ein umfassendes Bild von der eigenen Qualifikation und Persönlichkeit zu zeichnen. Sowohl die fehlende Information der Bewerber über die Einschaltung der Zeitarbeitsfirma wie auch die unterlassene Überwachung dieser Firma verstießen gegen den Datenschutz.

Die Übermittlung von Bewerbungsunterlagen an Dritte für deren eigene Zwecke, z. B. zur Besetzung offener Stellen, ist nur mit vorheriger ausdrücklicher **Einwilligung der Betroffenen** zulässig. Unerheblich ist, ob die Übermittlung im vermuteten Interesse des Bewerbers ist. Dieser hat selbst darüber zu entscheiden, wer von seinen Unterlagen Kenntnis nehmen darf.

Was ist zu tun?
Werden Dritte in die Durchführung des Bewerbungsverfahrens durch das ausschreibende Unternehmen eingeschaltet, müssen Bewerber darüber in geeigneter Weise informiert werden. Das Unternehmen muss sicherstellen, dass die Vertraulichkeit der Bewerberdaten gewahrt bleibt und nicht Dritte davon unbefugt Kenntnis nehmen können.

5.7.2 Was mein Chef wissen darf

Unternehmen erheben in Personalfragebögen umfangreiche personenbezogene Daten. Oft ist nicht alles, was gefragt wird, erforderlich.

Grundsätzlich ist die Erhebung der personenbezogenen Daten in einem Arbeitsverhältnis zulässig, die **zur Durchführung des Arbeitsverhältnisses erforderlich** sind oder soweit eine Rechtsvorschrift dies erlaubt. Vor diesem Hintergrund mussten wir in einem konkreten Fall die Erhebung folgender Daten beanstanden:

- Angabe der Personalausweis-/Reisepassnummer zur Prüfung/Feststellung der Identität: Zur Prüfung der Identität ist die Sichtvorlage des Personalausweises ausreichend.
- Angaben zu den Eltern des Beschäftigten, wenn dieser minderjährig ist und keine eigene Bankverbindung hat oder familienversichert ist: Falls der Beschäftigte keine eigene Bankverbindung besitzt, kann er eine Bankverbindung angeben, deren Inhaber nicht zwingend ein Elternteil sein muss. Es ist daher ausreichend, bei der Angabe der Bankverbindung in einem zusätzlichen Feld gegebenenfalls nach dem abweichenden Namen des Kontoinhabers zu fragen.
- Sollte der Beschäftigte nicht selbst Mitglied einer Krankenkasse sein, reicht die Angabe „familienversichert“ aus. Durch wen die Familienversicherung erfolgt, ist für die Durchführung des Arbeitsverhältnisses unerheblich.

- Angabe über den Bezug von Sozialhilfe: Die Verpflichtung zur Angabe des Einkommens bei Bezug von Sozialhilfe liegt beim Betroffenen und nicht beim Arbeitgeber.
- Frage nach einer Schwerbehinderteneigenschaft: Auch nach Inkrafttreten des Allgemeinen Gleichbehandlungsgesetzes ist die Frage nach einer Behinderung allenfalls dann zulässig, wenn deren Fehlen oder Vorhandensein wesentliche und entscheidende Voraussetzung für die Tätigkeit ist. Das ist nur ausnahmsweise der Fall.
- Angaben zum Arbeitgeber bei weiteren sozialversicherungspflichtigen oder geringfügigen Beschäftigungen: Es genügt, die Frage nach einer sozialversicherungspflichtigen Tätigkeit zu beantworten.

Das Unternehmen hat alle Beanstandungen akzeptiert und den Fragebogen überarbeitet und datenschutzgerecht gestaltet.

Was ist zu tun?
Personalfragebögen sind so zu gestalten, dass die Betroffenen erkennen können, welche Angaben zwingend erforderlich sind bzw. warum die Angaben erfragt werden und welche Antworten freiwillig sind.

5.7.3 Never ending story – Internet & Co. am Arbeitsplatz

Wieder gab es viele Anfragen und Beschwerden zur Kontrolle privater E-Mail und Internetnutzung am Arbeitsplatz.

Verbietet der Arbeitgeber die private E-Mail- und Internetnutzung, so sollte dieses Verbot eindeutig und umfassend formuliert werden. Selbst die Zulassung einer eingeschränkten privaten Nutzung eröffnet altbekannte Probleme. Der Arbeitgeber wird zum Telekommunikationsanbieter, und eine Missbrauchskontrolle der privaten Nutzung, z. B. durch Auswertung der Verkehrsdaten, ist unter Beachtung des Fernmeldegeheimnisses unzulässig.

In einem Fall hatte ein Arbeitgeber bestimmte Ausnahmen vom Privatnutzungsverbot gemacht, allerdings umfangreiche Kontrollen von E-Mail-, Internet- und Telefonnutzung durchgeführt. Zusätzlich fehlte es in diesem

Worum geht's?

Lässt ein Arbeitgeber die private Nutzung von E-Mail und Internet zu, wird er zum Diensteanbieter im Sinne des Telekommunikationsgesetzes. Für die Verarbeitung der hierbei anfallenden Daten gilt dann das Fernmeldegeheimnis, sodass eine Nutzung dieser Daten zum Zwecke der Kontrolle des Inhaltes und des Umfanges der privaten Nutzung unzulässig ist. Es ist in der Regel schwierig, die private Kommunikation eindeutig von der dienstlichen zu unterscheiden, zumal nicht nur das Fernmeldegeheimnis der Arbeitnehmer, sondern auch das der außen stehenden Kommunikationsteilnehmer zu wahren ist. Im Zweifel fällt die gesamte Kommunikation am Arbeitsplatz unter das Fernmeldegeheimnis und ist für Kontrollen und sonstige Einsichtnahmen tabu. Nur für Abrechnungszwecke dürfen die Daten verwendet werden.

Unternehmen an einer individuellen Benutzerkennung, sodass eine eindeutige Zuordnung eines bestimmten Nutzungsverhaltens zu einem individualisierten Mitarbeiteraccount unmöglich war. Derartige Verfahren sind eine dauernde **Quelle von Konflikten**.

Immer wieder bereitet auch die **Abwesenheit von Mitarbeitern** bzw. die Beendigung des Arbeitsverhältnisses Probleme. Es fehlt dabei häufig an eindeutigen Regeln zur Vertretung bzw. zur Umleitung dienstlicher E-Mails. Das Thema der E-Mail- und Internetnutzung am Arbeitsplatz wird uns auch zukünftig weiter beschäftigen. Telekommunikationsgesetz und Telemediengesetz lassen bisher die Sondersituation in einem Unternehmen völlig unberücksichtigt.

Was ist zu tun?
Die private Nutzung sollte nicht über die dienstlichen E-Mail-Adressen, sondern nur über sogenannte Webmailer (z. B. E-Mail über WEB.DE oder GMX) zugelassen werden. So wird den Arbeitnehmern private vertrauliche Korrespondenz ermöglicht; andererseits bleibt dem Arbeitgeber die Kontrolle der dienstlichen Kommunikation erhalten.

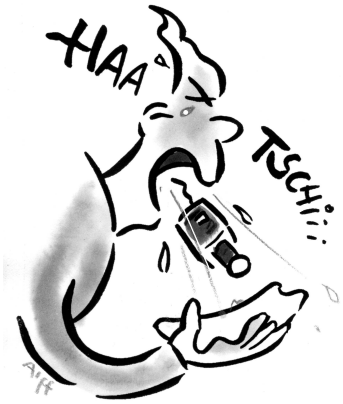
5.8 Videoüberwachung

War vor wenigen Jahren noch nicht Alarmstufe angesagt bei der Videoüberwachung, so ändert sich nunmehr rapide die Situation: Videokameras sind inzwischen derart billig, dass für Datenschutzaufsichtsbehörden dem Wildwuchs kaum noch etwas entgegengesetzt werden kann. Dieser Wildwuchs ist **Auslöser dauernder Streitigkeiten**, z. B. unter Nachbarn, zwischen Unternehmen und deren Beschäftigten, zwischen Wohnungsverwaltern und Mietern. Das ULD ist immer mehr als Streitschlichter gefordert.

5.8.1 Kamera – die erste: das elektronische Auge isst mit

Durch einen Hinweis wurde das ULD auf die exzessive Videoüberwachung eines größeren Cafébetreibers aus dem norddeutschen Raum in Gasträumen, den Außenbereichen und den nicht frei zugänglichen Küchen- und Büroräumen einer Filiale aufmerksam.

Die Prüfung vor Ort wies eine fast lückenlose Videoüberwachung der Tätigkeit der Angestellten hinter dem Tresen und des Freizeitbereichs der Kunden aus unterschiedlichsten Perspektiven durch mehrere Kameras auf. Zudem waren Teile der biergartenähnlichen Außenanlagen erfasst. Es war unmöglich, die Filiale zu betreten, ohne gefilmt zu werden. Besonders gravierend war die Überwachung im hinteren, nicht öffentlich zugänglichen Bereich der Filiale. Die Bediensteten im Küchenbereich waren bei der Zubereitung von Speisen **dauerhaft und vollständig unter Kamerakontrolle**. Gefilmt wurden der Eingangsbereich zu den Mitarbeitertoiletten und der für das Umkleiden vorgesehene Raum, in dem sich u. a. ein Tresor befand. Auf die Videoüberwachung wurde durch ein kaum sichtbares Schild am Haupteingang und Hintereingang der Filiale hingewiesen.



Diese Vollüberwachung wurde von uns als unzulässig beanstandet. Mitarbeiterinnen und Mitarbeiter haben einen Anspruch darauf, nicht dauernd unter Kamerabeobachtung zu sein. Lediglich eine punktuelle und auf besonders sensitive Bereiche begrenzte Videoüberwachung ist zulässig. Dabei muss jedoch sichergestellt sein, dass den Mitarbeitern ein **Rückzugsraum** während der Ausübung der Tätigkeit verbleibt und eine Erfassung nur kurzzeitig und nicht zielgerichtet auf einzelne Personen erfolgt. Die Arbeitgeber haben die Privatsphäre und Persönlichkeit der Mitarbeiter zu achten. Dies gilt erst recht für die Kundinnen und Kunden. Die Erfassung von Gästen eines Cafés trifft diese zumeist in ihrer Freizeit, d. h., wenn deren private Lebensgestaltung im Vordergrund steht. Die flächendeckende und dauerhafte Überwachung ist absolut unzulässig.

In jedem Fall muss ein **berechtigter Grund** für die Installation der Überwachung vorliegen. Dieser muss gegenüber den Interessen der Betroffenen am Schutz ihrer Privatsphäre überwiegen. Die im vorliegenden Fall durch die Geschäftsführung des Unternehmens vorgebrachte pauschale Begründung, mit der Videoüberwachung sollten Vandalismus und Einbrüche verhindert werden, kann derart gravierende Eingriffe in die Rechte der Mitarbeiter und Kunden nicht legitimieren.

Was ist zu tun?
Die Mitarbeiterüberwachung per Kamera bedarf einer spezifischen Rechtfertigung. Zweck, Dauer und Umfang der Überwachung müssen genau geregelt und den Betroffenen gegenüber transparent gemacht werden.

5.8.2 Kamera – die zweite: gesammelte Werke

Nachbarn sehen sich immer wieder im Fokus von Videoüberwachungskameras. Die geringen Kosten für Anschaffung, Installation und Betrieb hochleistungsfähiger Überwachungsanlagen führen zu einer massenhaften Verbreitung und entsprechenden Gefährdungen für das Persönlichkeitsrecht.

Das ULD wird häufig gebeten, in durch Kameraüberwachung ausartende **Nachbarstreitigkeiten** vermittelnd einzugreifen. Regelmäßig erfassen die Kameras nicht nur das eigene Grundstück, sondern auch das Eigentum oder den Zugangsbereich Dritter oder allgemein zugängliche Flächen. Teilweise werden sogar Kameras mit Tonaufzeichnung eingesetzt, um außer den Bewegungen zudem die Äußerungen der Nachbarn und deren Gäste zu erfassen.

Zulässig ist die Videoüberwachung des eigenen Grundstücks und Eigentums, soweit nicht der öffentliche Raum oder fremde Grundstücke erfasst werden. Nicht zu rechtfertigen ist die auch nur teilweise Überwachung des Grundstücks von Nachbarn. Vergleichbares gilt innerhalb von Mehrfamilienhäusern. Besonders extrem ist es, wenn die Betroffenen nicht mehr **unbeobachtet ihre Wohnung**

oder ihr Haus **betreten und verlassen** können. Nicht nur ordnungswidrig, sondern strafbar kann die Überwachung werden, wenn neben der optischen Aufzeichnung das gesprochene Wort erfasst wird.

Was ist zu tun?
Vor Inbetriebnahme jeder Video- oder Webkamera müssen die Betreiber sich über die Grenzen der Zulässigkeit solcher Anlagen informieren. Nachbarn und deren Besucher müssen in der Lage sein, unbeobachtet Wohnungen zu betreten oder zu verlassen.

6 Systemdatenschutz

6.1 IT-Konzept: Grundlage für das Datenschutzmanagement

Jede Daten verarbeitende Stelle muss nachweisen, dass die automatisierte Verarbeitung personenbezogener Daten sicher und kontrolliert erfolgt. Ein Sicherheitskonzept dokumentiert die tatsächlich getroffenen technischen und organisatorischen Sicherheitsmaßnahmen. Ebenso wichtig ist es, in einem informationstechnischen Konzept die technischen und organisatorischen Vorgaben, den Verfahrenszweck und die erzielbaren Ergebnisse zu beschreiben.

In der Kürze liegt die Würze: In nur einem Satz fasst die Datenschutzverordnung (DSVO) die Erfolgskriterien einer Datenverarbeitung personenbezogener Daten zusammen. Die Datenverarbeitung muss vorab geregelt werden. Hierzu sind **technische und organisatorische Vorgaben** zu entwickeln.

Organisatorische Vorgaben zu entwickeln bedeutet vor allem festzulegen, wer für welche Teilaspekte eines Verfahrens verantwortlich und zuständig ist. Zusätzlich legt die Daten verarbeitende Stelle in einem IT-Konzept fest, wer bei einzelnen Schritten in einem Verfahren zu beteiligen und zu informieren ist. Mit den organisatorischen Vorgaben wird quasi der **Grundstein einer datenschutzkonformen Datenverarbeitung** gelegt.

Im Wortlaut:
§ 4 DSVO, Verfahrenszweck

Zum Nachweis der Zweckbestimmung des automatisierten Verfahrens § 7 Abs. 1 Satz 3 Nr. 2 LDSG sind die technischen und organisatorischen Vorgaben für die Verarbeitung sowie die erzielbaren Ergebnisse in einem informationstechnischen Konzept zu beschreiben.

Am Beispiel Datensicherung erkennt man den Nutzen organisatorischer Vorgaben: **Verantwortlich** für die korrekte Sicherung der personenbezogenen Daten auf geeignete Medien ist der IT-Leiter. **Zuständig** für die Sicherung ist der Administrator des betreffenden Systems. IT-Leiter und Administrator können jedoch nicht abschließend entscheiden, wie die Aufbewahrungsdauer der gesicherten Daten und die Häufigkeit der Datensicherungen zu wählen sind. Für diese Entscheidungen muss der jeweilige Fachbereich **beteiligt** werden. Der oder die behördliche Datenschutzbeauftragte muss bei der Einführung eines solchen Verfahrens beteiligt und bei einer wesentlichen Änderung zumindest **informiert** werden. Dieses Beispiel macht bereits klar: Gute organisatorische Vorgaben vermeiden so manche Panne im späteren Betrieb.

Die **Entwicklung technischer Vorgaben** bedeutet vor allem festzulegen, mit welchen technischen Mitteln – also Rechnern, Netzwerken, Diensten und Programmen – eine Verarbeitung personenbezogener Daten entsprechend dem aktuellen Stand der Technik stattzufinden hat. Das IT-Konzept bietet der Leitung einer Daten verarbeitenden Stelle das **Steuerungsinstrument**, mit dem ein geordneter, wirtschaftlicher und rechts- bzw. datenschutzkonformer IT-Betrieb erreicht werden kann. Ein IT-Konzept gemäß DSVO regelt damit die Dinge, die häufig mit

dem Schlagwort „IT-Controlling“ oder „IT-Steuerung“ erfasst werden. Planen Fachabteilungen den Einsatz neuer Verfahren, so kann mit Bezug zu einem bestehenden IT-Konzept einfach und schnell geprüft werden, ob das geplante Fachverfahren in die IT-Landschaft passt. Fehlinvestitionen und unliebsame Überraschungen in fortgeschrittenen Phasen eines Einführungsprojekts können so effektiv verhindert werden.

Mit einem guten IT-Konzept steuert der IT-Leiter, in enger Abstimmung mit der Leitung des Hauses, die **Technikentwicklung seiner Dienststelle**. Der Wildwuchs bei der IT-Austattung kann durch die Konzentration auf einzelne Modelllinien im IT-Konzept bekämpft werden. Ein hoher Personalaufwand bei der Unterstützung der Endanwender „in der Fläche“ kann beispielsweise dadurch verhindert werden, dass bereits im IT-Konzept verfahrensübergreifend die Regelungen für eine zentrale Softwareverteilung, ein datenschutzkonformes „Aufschalten“ auf die Endgeräte sowie eine gemeinsame, einheitliche Dokumentation aller verwendeten Geräte geregelt ist.

Das informationstechnische Konzept bildet die Grundlage für ein **erfolgreiches Datenschutzmanagement** (29. TB, Tz. 6.1). Es dient als „verlängerter Arm“ des Verfahrensverzeichnisses, indem es die **Zweckbestimmung** der automatisierten Verarbeitung personenbezogener Daten aufgreift. Die erzielbaren Ergebnisse der automatisierten Datenverarbeitung sind zu beschreiben. Es muss darin der Nachweis geführt werden, dass die eingesetzte Informations- und Kommunikationstechnologie den funktionalen, genauer gesagt den fachlichen Anforderungen des Verfahrens genügt. Dies bildet nicht nur die Grundlage für den Nachweis der Wirtschaftlichkeit eines Verfahrens, sondern ermöglicht vor allem einen besseren Einstieg in die Erstellung des Sicherheitskonzepts. Bereits hier können viele Fragen nach Vertraulichkeit, Integrität und Verfügbarkeit der Datenverarbeitung abschließend beantwortet werden. Dieser Nachweis bildet die Arbeitsgrundlage für den Datenschutzbeauftragten. Erst wenn klar ist, was gemacht werden soll, kann entschieden werden, wie es sicher umgesetzt werden soll. Und erst dann kann auch geprüft werden, ob es ausreichend sicher gemacht wurde.

Was ist zu tun?
IT-Leiter müssen über informationstechnische Konzepte die Grundlage für einen erfolgreichen IT-Betrieb legen. Erfolgreich bedeutet hier: geplant, wirtschaftlich, kontrollierbar und vor allem datenschutzkonform. Datenschutzbeauftragte müssen bei Kontrollen stets auch die Angemessenheit des IT-Konzeptes hinterfragen.

6.2 IT-Kooperation der Kreise Nordfriesland und Schleswig-Flensburg

Die Landkreise Schleswig-Flensburg und Nordfriesland werden ihre Informationstechnik modernisieren und in einem IT-Betrieb zusammenfassen. Auf Wunsch der Beteiligten berät und unterstützt das ULD dieses Vorhaben, damit die Daten der Einwohner dieser Landkreise von Beginn an datenschutzkonform und sicher nach dem Stand der Technik verarbeitet werden.

Die Kreise Nordfriesland und Schleswig-Flensburg haben mithilfe einer Wirtschaftlichkeitsanalyse festgestellt, dass sie ihre Informationstechnik (IT) in einem **gemeinsamen IT-Servicebetrieb** wirtschaftlicher betreiben können. Daher ist geplant, die IT-Abteilungen der beiden Kreise zusammenzulegen und die Ressourcen Personal, Technik und Fachverfahren gemeinsam über diesen Servicebetrieb zu nutzen.

Der IT-Servicebetrieb wird datenschutzrechtlich als **Auftragnehmer** die Datenverarbeitung der beiden Landkreise übernehmen sowie Dienstleistungen für die kreisangehörigen Kommunen erbringen. Planung und Umsetzung der datenschutz- und sicherheitsrechtlichen Voraussetzungen unterstützt das ULD beratend. Das Projekt lässt wirtschaftliche, qualitativ hochwertige und innovative Ergebnisse erwarten.

Was ist zu tun?
Bei der Errichtung des IT-Servicebetriebs sind die datenschutzrechtlichen Regelungen der Auftragsdatenverarbeitung zwischen dem IT-Betrieb als Auftragnehmer und beider Kreise als Auftraggeber zu berücksichtigen.

6.3 NSI – neue Steuerung

Die Landesregierung hat dauerhaft eine Kommission zur Entwicklung und zum Einsatz neuer Steuerungsinstrumente für Verwaltungen (NSI-Kommission) eingerichtet. Eine wesentliche Aktivität dieser Kommission besteht darin, ein Kennzahlen- und Indikatorensystem zur Kontrolle und Steuerung (Controlling) von Planung und Bewirtschaftung in Abstimmung mit allen Ministerien zu entwickeln.

Das ULD nimmt in beratender Funktion an der NSI-Kommission teil. Die Kommission will hiermit sicherstellen, dass von vornherein die Belange des Datenschutzes in Bezug auf neue Steuerungsinstrumente Beachtung finden. Controller und Datenschützer haben ein gemeinsames Ziel: eine **bessere Transparenz in Prozessen und Verfahren** in öffentlichen Verwaltungen.

Das Interesse an Transparenz ergibt sich aus verschiedenen Perspektiven: Die **Steuerbarkeit** von Verwaltungsorganisationen soll generell effektiviert, deren **Wirtschaftlichkeit** gesteigert und der Nachweis der **Rechtmäßigkeit** des Verwaltungshandelns gegenüber der bisherigen Situation verbessert werden. Dies alles ist mit Risiken für Bürger, aber vor allem für Mitarbeiterinnen und Mitarbeiter der Verwaltungen verbunden.

Die aktuelle Entwicklung im E-Government – vor allem die **EU-Dienstleistungsrichtlinie** – führt in Bezug auf die Verarbeitung personenbezogener Daten dazu, dass die bisherigen Lösungen zur Verhinderung der gesetzlich verbotenen Leistungs- und Verhaltenskontrollen bei Verwaltungsmitarbeitern erneut durchdacht und geregelt werden müssen. Diese Kontrollen fanden bislang größtenteils nicht statt, weil diese flächenübergreifend einzurichten zu aufwendig und die erzielten Ergebnisse methodisch oftmals zweifelhaft gewesen wären.

Im Zuge der anstehenden Elektronisierung eines jeden Verwaltungsarbeitsplatzes ändert sich diese Situation. Die Protokollierung von Mitarbeitertätigkeiten wird flächendeckend möglich. Die Protokollierungsfunktionen müssen deshalb mit Nachdruck gesichtet und auf ihre Rechtmäßigkeit hin bewertet werden. Die **Auswertung der Protokolle** muss dann durch technische und organisatorische Vorgaben unter arbeitsrechtliche und datenschutzkonforme Bedingungen gestellt werden. Hierbei ist die Situation der automatisierten Erfassung von Mitarbeitertätigkeiten aus datenschutzrechtlicher Sicht differenziert zu betrachten: Das Landesdatenschutzgesetz schreibt vor, dass Zugriffe von Personen, die Änderungen an automatisierten Verfahren bewirken, zu protokollieren und zu kontrollieren sind. Dies betrifft vornehmlich die Systemadministratoren. Von quantitativ größerer Bedeutung ist aber eine weitere Regelung, wonach zu protokollieren ist, wann, durch wen und in welcher Weise personenbezogene Daten gespeichert wurden, wenn diese Daten ausschließlich automatisiert gespeichert, verändert und übermittelt wurden. Genau dieser Umbau auf eine ausschließlich automatisierte Verarbeitung personenbezogener Daten einschließlich einer sehr viel genauer als bislang möglichen automatisierten Beobachtung von Mitarbeitertätigkeiten steht in den kommenden Jahren bis 2010 an. Hier fordert das Datenschutzrecht, dass eine Auswertung zwecks **Verhaltens- und Leistungskontrolle** nicht erfolgt.

Bei den anstehenden Aktivitäten gilt als dritte Anforderung, den **Datenschutz** für die von den Umstellungen betroffenen Bürger möglichst zu **verbessern**. Hierfür stehen die Chancen gut, weil in elektronischen Verfahren eine wohldurchdachte automatisierte Protokollierung dazu führen wird, die Rechtmäßigkeit eines Verfahrens bzw. der einzelnen Verfahrensschritte belegen und überprüfen zu können. Allerdings gilt es darauf hinzuwirken, dass sich mit der Umstellung auf digitale Verfahren keine neuen Begehrlichkeiten nach mehr Daten Bahn brechen oder ein bestehend schlechtes Sicherheitsniveau digital fortgesetzt wird, obwohl es sicherheits- und datenschutztechnisch bessere Verfahren gibt. Gemeinsam mit den technisch Verantwortlichen müssen rechtzeitig Fehler identifiziert werden, mit denen bei Einführung neuer Prozesse und Verfahren realistischerweise immer zu rechnen ist.

Was ist zu tun?
Das ULD wird in der NSI-Kommission darauf hinwirken, dass ausschließlich datenschutzkonforme Steuerungsinstrumente in den Behörden mit dem Ziel eingeführt werden, die Transparenz des Verwaltungshandelns zu steigern und die Anforderungen des Datenschutzes in Bezug auf die betroffenen Arbeitnehmer und Bürger einzuhalten.

6.4 SOA (Serviceorientierte Architekturen)

SOA steht für ein Konzept zur Abbildung von Verwaltungsverfahren bzw. Geschäftsprozessen auf IT-Prozesse. Das Besondere an einer SOA ist, dass die IT-Techniken heterogen und die Prozesse organisationsübergreifend eingerichtet sein können.

Die Flexibilität einer SOA erzwingt eine Standardisierung der Geschäfts- und IT-Prozesse. Über SOA können sich virtuelle Organisationen ausbilden; dadurch geraten die gesamten **organisationsübergreifenden Prozessketten** in den Blick. Aus Datenschutzsicht bieten die mit SOA einhergehende Standardisierung und die zweckmäßig zugeschnittenen, grundlegenden IT-Services die Chance, die Prüffähigkeit und Nachweisbarkeit einer ordnungsgemäßen Datenverarbeitung durch verbesserte Transparenz von Datenbeständen, Datenflüssen und der Datenverarbeitung wesentlich zu steigern.

Diese Chance zur Verbesserung der Transparenz des Umgangs mit personenbezogenen Daten in Organisationen entsteht über die notwendige Beteiligung der unterschiedlichen Akteure, die zwangsläufig zu einer offenen und transparenten Kommunikation und Dokumentation über Formate und Adressen führen muss. Kann nach erfolgter Standardisierung auf bislang separierte Datenbestände systemübergreifend und effektiv zugegriffen werden, so steigert dies jedoch das **Risiko einer Zweckänderung der Daten**. Durch das Zusammenführen und das Auswerten verschiedener Datenbestände lassen sich komfortabel Profile bilden. Allerdings bietet SOA die Chance der Datenkapselung in „Containern“. In solchen Datencontainern können sich, neben den eigentlichen Nutzdaten, auch automatisierbar zugängliche Regeln („Policies“) befinden, wie diese Nutzdaten verarbeitet werden dürfen, sowie die Protokollierungsdaten, die – wiederum automatisiert – darüber Auskunft geben können, welche Verarbeitung tatsächlich erfolgte. Das heißt: Mit SOA kann man bei der Automatisierung des Erzeugens und Umgangs mit Protokolldaten einen effektiven Schritt vorankommen.

Wenn in einer SOA derartige Policies zur Verfügung stehen, kann sich der Absender von Daten vergewissern, dass seine Daten in einer Umgebung mit angemessenem Datenschutzniveau und nur für den vorgesehenen Zweck verarbeitet werden. Der Empfänger von Daten muss vor der eigenen weiteren Verarbeitung prüfen, ob diese Verarbeitung wirklich machbar und zulässig ist. Dieser Ansatz ermöglicht es, den Nutzdaten die erlaubten und vertraglich vereinbarten **Datenverarbeitungsvorschriften** mitzugeben. Solche Container bieten eine neue, qualitativ gute Möglichkeit, die Flüsse der Daten sowie deren beabsichtigte Verwendung durch Policies und deren erfolgte Verwendung anhand von Protokolldaten automatisiert zu kontrollieren und beweisfest zu belegen.

SOA wird zumeist in einen Zusammenhang mit **Web Services** gebracht. Web Services sind Standards, mit denen Daten in die Sprache XML definiert, beschrieben, weltweit eindeutig identifiziert und über internetbasierte Protokolle wie beispielsweise HTTPS ausgetauscht werden. Derartige Datenweitergaben über Web Services sind wie alle Datenübermittlungen zwischen unabhängigen Organi-

sationen an enge gesetzliche Rahmen gebunden. Es ist absehbar, dass Organisationen sich darum bemühen werden, innerhalb dieses Rahmens ihre Workflows stärker aufeinander abzustimmen. Das ergibt nicht nur in der auf SOA setzenden Zulieferindustrie von Automobilherstellern ökonomischen Sinn, sondern ebenso zwischen unterschiedlichen Verwaltungen – unter Beibehalt der jeweiligen Organisationshoheit und Zuständigkeit.

Das bedeutet aber auch, dass trotz zunehmender gegenseitiger Abhängigkeit die Organisationen sich darum kümmern müssen, ihrer **Verantwortung für die Datenverarbeitung** gerecht zu werden. Alle Beteiligten sollten ein Interesse daran haben, dass eventuell auftretende Fehler korrekt zugerechnet werden können. Es entsteht dadurch ein unausweichlicher Bedarf für die Organisationen, die Korrektheit der eigenen Funktionalwahrnehmung gegenüber den anderen Beteiligten in der Prozesskette zweifelsfreier als bislang nachweisen zu können. Dieser Nachweis des rechtmäßigen Umgangs mit Daten, der funktionalen Effektivität und der ökonomischen Effizienz lässt eine Win-win-Situation für alle, auch der mit Kontrollaufgaben befassten Stellen, entstehen.

In **Schleswig-Holstein** sind auf Landes- als auch auf Kreisebene erste Ansätze von serviceorientierten Architekturen auszumachen. Das ULD ist in mehreren Beratungsprojekten aktiv beteiligt. Richtig gestaltet sind SOAs für den Datenschutz ein Gewinn. Das ULD bietet öffentlichen und privaten Stellen seine rechtliche und sicherheitstechnische Beratung an.

Was ist zu tun?
Bei der Entwicklung von SOA-Konzepten auf Web-Service-Basis müssen die Verantwortlichen darauf achten, dass die im Rahmen von WS-Security und WS-Policy angebotenen Mechanismen adäquat umgesetzt werden. Ein besonderes Augenmerk ist auf die Protokollierung von Transaktionen und auf datenschutzgerechte Verträge mit externen Partnern, die einen Service für das Verfahren anbieten, zu legen.

6.5 Datenschutz bei der Softwareentwicklung

In der öffentlichen Verwaltung wird inzwischen zumeist Standardsoftware eingesetzt. Wird spezielle Software entwickelt, dann sind schon zu diesem Zeitpunkt Datenschutzanforderungen zu beachten. Besonderer Wert ist auf die Dokumentation des Quellcodes und die spätere Nachvollziehbarkeit der Operationen der Software im laufenden Betrieb zu legen.

Die Datenschutzverordnung für Schleswig-Holstein (DSVO) stellt spezifische Anforderungen an die Dokumentation bei der Softwareentwicklung. Die Dokumentation des Programmcodes soll es ermöglichen, den Programmcode aus Datenschutzsicht zu überprüfen, sodass das Programm nicht intransparent und unkontrollierbar Daten verarbeitet. Zu dieser Dokumentation zählen auch solche „Texte“, die während des Betriebes als Protokollierungsdaten anfallen. Auf diese **Selbstauskunft von Programmen** muss künftig stärker als bisher geachtet werden,

weil zunehmend damit zu rechnen sein wird, dass an derartige Protokolltexte arbeitsrechtliche Folgen geknüpft werden.

Nicht nur die Dokumentation des Programms und dessen Betrieb, bereits die Entwicklung der Software muss revisionssicher erfolgen. Die Zugriffe auf die Quelltexte durch die Programmierer müssen geregelt sein. Während der Entwicklung muss es eine **qualitätssichernde Testinstanz** geben, welche die Änderungen am Programm tatsächlich nachvollzieht und freigibt. Für die Tests von Programmen empfiehlt das ULD den Einsatz dedizierter Test-Suiten mit prototypischen, generierten Testdaten. Wenn für ein neues Verfahren in der Pilotphase bereits ein aussagekräftiges IT- und Sicherheitskonzept in einer hinreichenden Qualität vorliegen, kann es für einen begrenzten Zeitraum und in begrenztem Umfang auch mit Realdaten getestet werden. Auch hier gilt: Sämtliche Tests sind zu dokumentieren.

Im Wortlaut: § 5 Abs. 2 DSVO

Die Programme sind grundsätzlich in der Ausgangsprogrammiersprache (Quellcode) zu dokumentieren. Soweit nur Nutzungsrechte an Programmen bestehen (Fremdsoftware), kann die Programmdokumentation auf die Herstellerangaben (Lizenzgeber), die Programmbezeichnung und die Versionsnummer sowie die genutzten Programmsteuerungsbefehle (Parameter) begrenzt werden.

Ist eine Software im Einsatz, so muss jederzeit sofort geklärt werden können, **welche Version in welcher Konfiguration** betrieben wird (Release- bzw. Configuration-Management). Handelt es sich um eine Spezialsoftware, an der auch die Besitzrechte bestehen, so muss es eine zweifelsfreie Verbindung zwischen dem Quelltext und der im Betrieb befindlichen Version geben. Das ULD empfiehlt hierfür den Einsatz von Versionsmanagementsystemen.

Findet die Software dann Anwendung bei Daten verarbeitenden Stellen, so bedeutet eine datenschutzfreundliche Softwareentwicklung die **Einrichtung fester Zyklen** zur Produktentwicklung und eine Dokumentation der durchgeführten Änderungen. Durch feste Zyklen für neue Programmversionen wird die Planbarkeit für Test- und Freigabeverfahren bei den Daten verarbeitenden Stellen verbessert. Mithilfe einer genauen Dokumentation der durchgeführten Änderungen kann eine Daten verarbeitende Stelle ihre eigenen Tests und die notwendige Freigabe besser auf die neuen oder verbesserten Funktionen zuschneiden.

Was ist zu tun?
Bei der Softwareentwicklung gelten dieselben Transparenzanforderungen wie im Verfahrensbetrieb. Unklare Zuständigkeiten, nicht dokumentiertes Vorgehen und schlechte Planbarkeit sind hier genauso wenig angebracht wie beim späteren Einsatz der Software beim Kunden.

6.6 Sicherheitslücken im FHH-Net: Auswirkungen auf Schleswig-Holstein

Der Hamburgische Datenschutzbeauftragte hat eklatante Sicherheitslücken im Behördennetz der Freien und Hansestadt Hamburg aufgezeigt. Das ULD hat die Auswirkungen auf die Datenverarbeitung schleswig-holsteinischer Behörden geprüft. Ein akuter Datenmissbrauch konnte nicht festgestellt werden, doch sind bei Dataport erhebliche Änderungen in der IT-Infrastruktur nötig.

Unsere hamburgischen Kollegen haben im Rahmen einer Prüfung des von den Behörden in Hamburg genutzten Netzwerkes (kurz: FHH-Net) eine Reihe von **gravierenden Schwachstellen** festgestellt, die es einem internen Angreifer mit Zugang zum FHH-Net ermöglichten, unbefugt auf personenbezogene Daten von schleswig-holsteinischen Kunden bei Dataport zuzugreifen. Ursache ist zum einen eine mangelhafte Durch- und Umsetzung datenschutzrechtlicher Vorgaben im Bereich der Administration bei Dataport. Zum anderen beruhen die festgestellten Mängel – soweit sie Dataport und Schleswig-Holstein betreffen – auf dem Umstand, dass das interne Datennetz von Dataport auf dem FHH-Net aufsetzt und von diesem sicherheitstechnisch nicht ausreichend separiert ist. Derart „erbt“ das interne Datennetz von Dataport konzeptionelle Schwächen des FHH-Net.

Wir haben die Ergebnisse und Bewertungen des Prüfberichts nachvollzogen und durch **eigene Untersuchungen vor Ort** ergänzt. Das ULD teilt die Einschätzung unserer Hamburger Kollegen über die offensichtlichen Fehler bei der Administration sowie über die konzeptionellen Schwachstellen des internen Hausnetzes von Dataport.

Ein direkter Zugriff aus dem FHH-Net auf schleswig-holsteinische Fachverfahren und die dort verarbeiteten personenbezogenen Daten ist nicht erfolgt. Ein solcher Zugriff hätte über das **Landesnetz Schleswig-Holstein** passieren müssen, welches – anders als das FHH-Net – strikt aufgeteilt und damit stärker kontrolliert ist. Die Aufteilung des Landesnetzes Schleswig-Holstein begrenzt die Auswirkungen eines Sicherheitsvorfalles deutlich. Die Kontrollmechanismen stellen hier sicher, dass nur Verbindungen möglich sind, die von den jeweiligen Kommunikationspartnern beantragt und genehmigt wurden. Die an das Landesnetz angeschlossenen Teilnehmer können jederzeit eigenständig die sie betreffenden Einstellungen kontrollieren (29. TB, Tz. 9.1).

Aus dem FHH-Net konnte jedoch auf die **Bürokommunikationsumgebung bei Dataport** zugegriffen werden. Aufgrund einer zu offenen Berechtigungsvergabe war ein Zugriff auf die Dataport-interne Dateiablage möglich. Dort waren sicherheitskritische Dokumente und personenbezogene Daten in großer Menge einsehbar. Sicherheitsmaßnahmen wie eine Verschlüsselung von Dateiablagen oder eine minimalisierte Vergabe von Rechten für den Zugriff auf diese Ablagen waren nicht getroffen worden.

Das ULD hat die von Dataport getroffenen Sofortmaßnahmen geprüft und eigene Kontrollen durchgeführt. Im Ergebnis und gemäß dem Dataport-eigenen Sicher-

heitsmanagement ist es nach dem Stand der Technik unumgänglich, dass das interne **Datennetz des Dienstleisters Dataport** aus dem FHH-Net herausgelöst wird. Das ULD wird den Prozess der Trennung des Dataport-Netzes aus dem FHH-Net beratend begleiten. Dataport muss zudem seine **interne Dateiablage** stärker absichern. Für Daten mit hohem Schutzbedarf ist eine Verschlüsselung einzuführen, um diese dem systembedingten Zugriff von Administratoren bei Dataport zu entziehen. Für alle Datenablagen sind die vergebenen Zugriffsrechte zu überarbeiten und auf die zwingend notwendigen Zugriffsmöglichkeiten zu beschränken.

Was ist zu tun?
Dataport muss sein Verwaltungsnetz von dem FHH-Net und jedem anderen Kundennetz netzwerktechnisch trennen und seine Bürokommunikationsumgebung stärker absichern. Die Behebung der aktuellen Sicherheitsprobleme ist im Rahmen des eigenen Sicherheitsmanagements zu dokumentieren; die Änderungen sind seinen Kunden durch einen Abschlussbericht transparent zu machen.

6.7 Datenschutz und Datensicherheit an den Hochschulen

Die Lage des Datenschutzes an den Hochschulen Schleswig-Holsteins ist schlecht. Dies wurde im Jahr 2007 anhand von Prüfungen, einer zunächst schleppend verlaufenden Auditierung und mehreren Beratungsterminen vor Ort erneut sichtbar.

Die Feststellung ist nicht überspitzt formuliert, dass sich die Hochschulen unter dem Label „Freiheit für Forschung und Lehre“ um die Schaffung vom Datenschutz unbeobachtbarer Räume bemühen, und zwar selbst dort, wo ambitioniert Mechanismen des Finanz-Controllings installiert sind (Tz. 6.8.4). Unser Fazit: Hochschulen haben generell ein **Steuerungsproblem**.

Das ULD wird langsam auch von Hochschulen nicht nur als **Aufsichtsbehörde**, sondern auch als **Beratungsinstitution** wahrgenommen. So erkundigte man sich bei Beratungsterminen an Hochschulen vor Ort u. a. nach den Auffassungen des ULD zu Service Oriented Architectures (SOA, Tz. 6.4), Überlegungen zum Risk-Management gemäß der „IT Infrastructure Library“ sowie zu einzelnen Maßnahmen, die im Rahmen von BSI-Grundschutz anzuwenden sind. Wohl standen praxisorientierte Erläuterungen der rechtlichen Anforderungen im Vordergrund. Nach solchen Beratungen erwarten wir, dass gemeinsam gefundene und festgelegte Lösungen dann auch tatsächlich umgesetzt werden und der Dialog mit dem ULD fortgesetzt sowie an Datenschutzschulungen teilgenommen wird.

Häufig begegnen wir in Gesprächen mit Hochschulvertretern einem glaubwürdigen Bekunden von Sensibilität für Datensicherheit und Datenschutz. Die Systemadministratoren an Hochschulen erweisen sich überwiegend als technisch kompetent; sie haben ihre IT-Systeme weitgehend im Griff. Festzustellen ist allerdings, dass kein einziger der auf IT gestützten Kernprozesse bei unseren Überprüfungen **hinreichend dokumentiert** war. Nur die Dokumente zum Thema „Anweisungen

der EDV-Nutzung für Studierende“ waren bei allen Hochschulen in einer passablen Verfassung. Schon bei den Dienstanweisungen für die Sachbearbeiterinnen und Sachbearbeiter hörte es dann auf. Es konnten keine aktuellen Organigramme der Hochschulorganisation, keine gültigen Geschäftsverteilungspläne sowie keine Tätigkeitsbeschreibungen – insbesondere für Systemadministratoren – vorgelegt werden. Als „Verfahrensverzeichnis“ betitelte Dokumente waren durchweg auf einem rudimentären Stand. Es fehlten ferner durchgängig IT- und Verfahrensbeschreibungen sowie Sicherheitskonzepte. Netzwerkpläne, ohne die eine Administration eines Computernetzes undenkbar ist, waren zwar teilweise vorhanden, aber methodisch unzureichend gestaltet und nie aktuell.

Rechnersysteme zum Testen von Software waren teilweise vorhanden, aber es konnten keine Dokumentationen erfolgter Tests und deren Ergebnisse vorgelegt werden. Die Zugriffsrechte der Hochschulleitungen, des Verwaltungspersonals oder des akademischen Lehrapparats auf Dateiserver oder Datenbanken mit personenbezogenen Daten von Studierenden konnten in keinem Fall dokumentiert oder zumindest rasch aus den Systemen selbst erzeugt werden. Auch wurden keine Dokumente zur Freigabe von Programmen vorgelegt, die den Akt der Verantwortungsübernahme durch einen Fachverantwortlichen und die Entlastung des IT-Verantwortlichen signalisierten. **Verträge mit externen Dienstleistern**, insbesondere den IT-Dienstleistungen der „Hochschul-Informations-System GmbH“ (HIS), fehlten entweder ganz oder waren unzureichend. Nicht zuletzt herrschten durchgängig weitgehende Unkenntnisse über die geltenden Rechtsvorschriften, insbesondere auf der Ebene der Fakultäten, Institute und Fachbereiche.

Die Datenschutzbeauftragten waren in der Regel mit zu **geringen Zeitkontingenten** ausgestattet (5 % bis 50 %), verfügten durch die Bank nur über geringe technische Kenntnisse und konnten keine auf Nachhaltigkeit zielende Strategien mit Gestaltungsanspruch vorweisen. Es blieb einzig bei anlassbezogenen Aktivitäten im Modus einer akuten Brandbekämpfung. Sie wussten aber von keinen Sicherheitsvorfällen zu berichten. Entsprechend war ihnen der Gedanke fremd, im Rahmen eines Sicherheitsmanagements bei Sicherheitsvorfällen bestimmter Qualität zwangsläufig beteiligt zu werden.

Es gibt keine einfache Lösung für die oben aufgeführten Mängel und Probleme. Die Bereitstellung von einfach mehr Ressourcen für den Datenschutzbeauftragten wäre wenig zielführend. Mehr Ressourcen gibt es erfahrungsgemäß nur, wenn die oder der Datenschutzbeauftragte etwas sichtbar Funktionales zu bieten hat. Sie oder er sollte zumindest als ein **aktiver Wächter** der Rechtmäßigkeit im Umgang mit personenbezogenen Daten auftreten. Dafür gilt es, Bündnispartner mit Interessenüberschneidungen zu finden, also mit dem Personalrat bezüglich Mitarbeiterdatenschutz ins Gespräch zu kommen, mit Studierendenvertretern zu sprechen und den Kontakt zum Sicherheitsbeauftragten des Rechenzentrums zu suchen. Mit der IT muss eine Dokumentationsstrategie vereinbart werden. Ein Anfang könnte in einer Dokumentation liegen, welche Datenverarbeitungen in welcher Form und wo zugänglich protokolliert werden und wer unter welchen Umständen diese Daten wie auswerten muss. Dabei ist dann festzulegen, wie mit möglicherweise festgestellten Sicherheitsvorfällen und Datenschutzverstößen umzugehen ist, um

Kopflosigkeit und ungeregelte Prozesse zu vermeiden. Dies wäre ein Einstieg in den Aufbau eines Datenschutzmanagementsystems (DSMS).

Im Herbst 2007 wurde aufgrund einer Prüfung des ULD eine erste Initiative seitens einiger Hochschuldatenschutzbeauftragter gestartet, um die Dokumentationssituation in einer **gemeinsamen Anstrengung** zu verbessern. Datenschutz zu betreiben heißt heute: konstruktive Beteiligung am gesamten Kommunikationsmanagement nach innen und außen, mit entsprechenden Anforderungen an den Datenschutzbeauftragten.

Was ist zu tun?
Viel: Die Verantwortlichen müssen mit dem Dokumentieren ihrer Verwaltungsprozesse beginnen. Die HIS ist stärker bezüglich Transparenz der von ihr betriebenen IT und den angebotenen Verfahren in die Pflicht zu nehmen. Den Hochschulleitungen muss dargelegt werden, dass Datenschutz ein konstruktiver Aspekt des Qualitäts- bzw. Risk-Managements einer jeden Organisation sein kann.

6.8 Kontrollen vor Ort – ausgewählte Ergebnisse

6.8.1 Querschnittsprüfung „Landesnetz“

Im Rahmen einer Querschnittsprüfung des vom ULD auditierten Landesnetzes wurde überprüft, wie die Landesnetznutzer ihren vertraglichen Pflichten nachkommen und welche Praxisprobleme bei der Nutzung, der Dokumentation und der Überprüfung der Landesnetzanschlüsse bestehen.

Im August 2006 wurde das Landesnetz durch das ULD auditiert. Zum Jahresbeginn 2007 waren nahezu alle Verwaltungen in Schleswig-Holstein an das Landesnetz angeschlossen. Darauf folgend wurden vom ULD die Landesnetzanschlüsse (LN-Anschlüsse) von elf Ämtern und Gemeinden überprüft. Im Interesse der Einheitlichkeit und Vergleichbarkeit wurden **prüfungsspezifische Checklisten** für folgende Bereiche erstellt und eingesetzt: Vertragssituation, Dokumentation der Kommunikationsaufträge und -beziehungen, Freischaltung und Einsatz der Tools LNRC und LNWebView sowie Rolle des Kommunikationskoordinators.

Folgende **datenschutzrechtliche Aspekte** standen im Vordergrund:

- Beachtung von Rechtsvorschriften zur Datensicherheit und zur Ordnungsmäßigkeit der Datenverarbeitung,
- konzeptionelle Festlegung und Umsetzung von technischen und organisatorischen Datensicherheitsmaßnahmen,
- Vollständigkeit der Verträge bei einer Auftragsdatenverarbeitung.

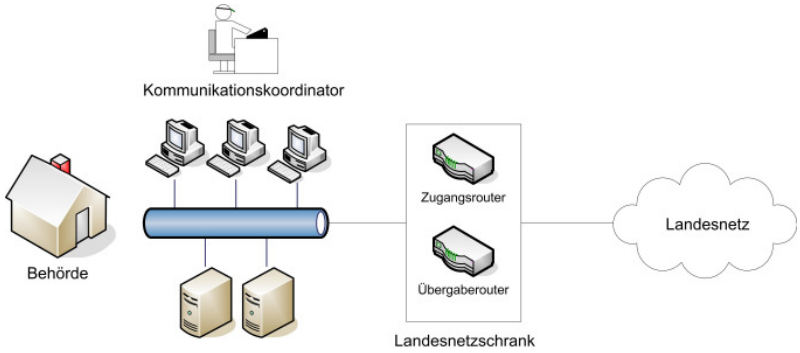
Weiterhin wurden die ablaufspezifischen Vorgänge bei

- der Beantragung des Landesnetzanschlusses,
- der Beantragung von Kommunikationsbeziehungen und
- der Beantragung der Kommunikationsbeziehungen (Routen) für die Tools LNWebView und LNRC

in Verbindung mit den notwendigen Anträgen, Bestätigungen und Dokumentationen berücksichtigt.

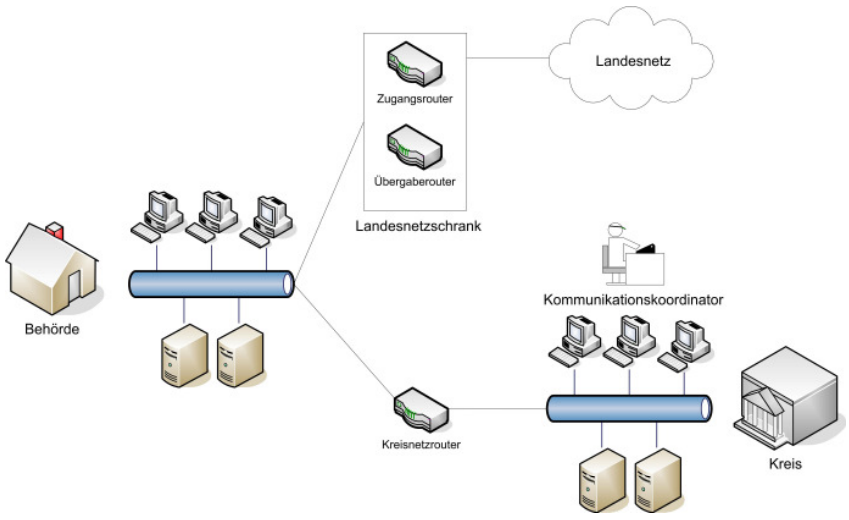
Der Anschluss der Behörden an das Landesnetz konnte im Verlauf der Prüfung in drei unterschiedliche Typen klassifiziert werden, die sich besonders in Bezug auf Verantwortlichkeiten, Auskunftsfähigkeit und Dokumentationsverhalten unterscheiden.

Typ 1:



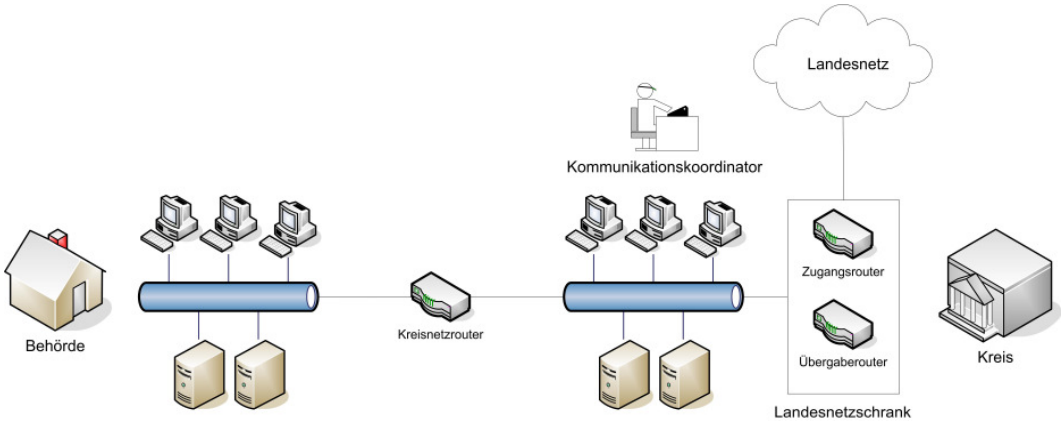
Die Behörde hat einen **eigenen** LN-Anschluss, d. h., der Zugangs- und der Übergaberouter sind in den eigenen Räumlichkeiten installiert. Die Behörde hat einen **eigenen** Kommunikationskoordinator benannt. Er leitet alle Schritte bis zum voll funktionsfähigen Landesnetzanschluss in Verantwortung der eigenen Behörde in die Wege.

Typ 2:



Die Behörde hat einen **eigenen** LN-Anschluss, d. h., der Zugangs- und der Übergaberouter sind in den eigenen Räumlichkeiten installiert. Der Kommunikationskoordinator ist **beim Kreis** benannt. Er leitet alle Schritte bis zum funktionsfähigen Landesnetzanschluss in Vertretungsfunktion der Behörde in die Wege.

Typ 3:



Die Behörde hat **keinen eigenen** LN-Anschluss, sondern ist über das Kreisnetz an das Landesnetz angeschlossen. Der Kommunikationskoordinator ist **beim Kreis** benannt. Er leitet alle Schritte bis zum funktionsfähigen Landesnetzanschluss in Verantwortung des Kreises in die Wege.

Die Prüfungsergebnisse waren unterschiedlich: Der **Landesnetzanschluss Typ 1** ist dadurch gekennzeichnet, dass sowohl die Verträge als auch die Funktion des Kommunikationskoordinators in dem Verantwortungsbereich der entsprechenden Behörde liegen. Zusammenfassend: Die Behörden, die ihre Datenverarbeitung im Allgemeinen datenschutzkonform organisieren und dokumentieren, haben bei der Landesnetzprüfung mit wenigen oder ohne Mängel abgeschnitten. Die Sorgfalt, die bei dem Umgang und der Dokumentation des Landesnetzes angesetzt wurde, kann als Spiegel der allgemeinen Datenverarbeitung innerhalb der Behörde gesehen werden.

Der **Landesnetzanschluss Typ 2** zeichnet sich dadurch aus, dass die Verträge in dem Verantwortungsbereich der entsprechenden Behörde liegen und die Funktion des Kommunikationskoordinators beim Kreis in Vertretung der Behörde wahrgenommen wird. Die Prüfung fiel umso besser aus, je besser der Kommunikationskoordinator beim Kreis mit der Behörde kommunizierte. So funktionierte z. B. die Weiterleitung der Vertragsbestandteile bzw. der Kommunikationsberichte oder die Freischaltung von den Routen, die für den Einsatz von den Überwachungstools notwendig sind, nicht immer reibungslos.

Der **Landesnetzanschluss Typ 3** ist dadurch gekennzeichnet, dass sowohl die Verträge als auch die Funktion des Kommunikationskoordinators nicht in dem Verantwortungsbereich der entsprechenden Behörde, sondern in der des entsprechenden Kreises liegen. Die Prüfungsergebnisse waren nur bei den Behörden positiv, die vom Kreis entsprechend informiert waren bzw. selbst die Initiative ergriffen haben. Einige Behörden waren gar nicht über die Funktionalitäten des

Landesnetzes und/oder des Kreisnetzes informiert. Beim Landesnetzanschluss Typ 3 konnte keine vollständige Prüfung durchgeführt werden, da weder die Vertragslage noch der Einsatz der Überwachungstools beim Kreis beurteilt werden konnten. Der Kommunikationskoordinator beim Kreis übernimmt die Aufgabe, die Landesnetzparameter für die angeschlossenen Behörden zu verwalten und zu überprüfen sowie die Behörden über Änderungen beim Landesnetzanschluss oder über Änderungen in der Routerkonfiguration zu informieren. Auch die Erfüllung dieser Aufgaben wurde nicht überprüft.

Die allgemeinen und speziellen Problemstellungen und Unsicherheiten, die sich in Bezug auf den Landesnetzanschluss bei allen elf Prüfungen ergeben haben, lassen sich folgendermaßen **zusammenfassen**:

- Das Tool LNRC wurde von einigen Administratoren installiert. Die erzeugten LNRC-Routerausdrucke konnten allerdings von keinem Administrator interpretiert werden. Hier muss auf externe Hilfe zurückgegriffen werden.
- Die Rolle des Kommunikationskoordinators ist vor allem bei den Behörden mit dem Landesnetzanschluss Typ 2 und 3 häufig nicht klar. Aus diesem Grund sind während der Prüfung Missverständnisse bei der Kommunikation zwischen Behörde, Kreis und Dataport sowie bei der Frage nach den Verantwortlichkeiten aufgetreten.
- Die Anfragen der Kommunikationskoordinatoren der Kreise beim ULD und die Erfahrungsberichte aus den Ämtern und Gemeinden lassen darauf schließen, dass der Aufgabenumfang eines Kreiskommunikationskoordinators nicht eindeutig definiert ist.
- Häufig wurden innerhalb einer Behörde die relevanten Informationen, die sich aus dem Nutzervertrag und der Generaldokumentation für den Administrator und den Kommunikationskoordinator ergeben (Installation und Freischaltung des Tools LNRC, Benutzung und Freischaltung von LNWebView usw.), nicht weitergegeben.

Daraus ergeben sich folgende **Anforderungen**: Die Aufgabenbereiche eines Kommunikationskoordinators müssen je nach Einsatzbereich (Landesnetzanschluss Typ 1 bis 3) detailliert definiert werden. In diesem Zusammenhang sollten bei den Gemeinden und Ämtern die Kommunikation mit dem Systemadministrator und Dataport sowie die Dokumentationspflichten beachtet werden. Bei den Kreiskommunikationskoordinatoren hingegen müssen zusätzlich die Aufgaben bei der Verwaltung und Überprüfung der Landesnetzparameter sowie die angemessene Information der angeschlossenen Behörden berücksichtigt werden.

Das ULD hat für die Behörden in Schleswig-Holstein eine **Arbeitsanleitung** erstellt, die die Aufgaben von Kommunikationskoordinatoren und Administratoren in den Kommunen und Kreisen sowie von angeschlossenen Behörden bei Kreislandesnetzanschlüssen strukturiert. Gewählt wurde eine je nach Einsatzbereich differenzierte Darstellung sowohl als Checkliste als auch als Prozesskette.

Was ist zu tun?
Die Aufgabenbereiche der Kommunikationskoordinatoren in kleineren Verwaltungen als auch bei den Kreisen müssen klar definiert werden.

Eine Hilfestellung kann die vom ULD bereitgestellte Arbeitsanleitung darstellen, die beim ULD angefordert oder im Internet heruntergeladen werden kann unter


https://www.datenschutzzentrum.de/landesnetz/

6.8.2 Vorbildliches Bad Bramstedt

Die meisten Beanstandungen bei unseren routinemäßigen Prüfungen betreffen eine fehlende oder unvollständige Dokumentation. Umso erfreulicher war es, dass die Stadtverwaltung Bad Bramstedt eine (fast) perfekte Dokumentation vorlegen konnte.

Wir hatten die Stadtverwaltung Bad Bramstedt auf dem falschen Fuß erwischt; sie befand sich gerade mitten in einer Telefonanlagen- und Serverumstellung. Die Stadt konnte dennoch das Prüfungsergebnis als Erfolg verbuchen. Ein Großteil dieses Erfolgs ist auf die sorgfältige und vom Systemadministrator vorgelegte (fast) **lückenlose Dokumentation** zurückzuführen:

- Sicherheitskonzept mit Risikoanalyse,
- Verfahrensverzeichnis mit Verweisen zu Verfahrensakten, Test und Freigabe,
- kombiniertes Geräte- und Patchverzeichnis,
- Netzwerkplan,
- Dokumentation der eingesetzten Benutzerkonten und -gruppen,
- Verträge aller externen Dienstleistungen und
- Dienstanweisungen für die Mitarbeiter.

Insgesamt wirkte die gesamte Dokumentation gut durchdacht und strukturiert. Es fehlen nur noch **Kleinigkeiten**, um eine perfekte Dokumentation zu haben:

- Die Bestandteile, die den IT-Einsatz in der Stadtverwaltung beschreiben, sind aus dem Sicherheitskonzept herauszuziehen und in einem IT-Konzept zusammenzufassen.
- Die Berechtigungen, die die unterschiedlichen Benutzer und Systemadministratoren im System haben, sind in einem Administrations- und Berechtigungskonzept festzuhalten.

Auch wenn die Stadtverwaltung Bad Bramstedt nicht ohne Beanstandungen aus dieser Prüfung herausgegangen ist, so hat sie bei uns doch den **positiven Eindruck** hinterlassen, dass sie sich mit der Problematik Datenschutz beschäftigt hat, die einzelnen Bereiche in Bezug auf organisatorische oder technische Sicher-

heitsmaßnahmen sorgfältig durchdacht und dokumentiert sowie die Maßnahmen für die Mitarbeiter in Form von Dienstanweisungen aufbereitet hat.

Eine **datenschutzkonforme Dokumentation** nach LDSG und DSVO ist eine Grundlage für die ordnungsgemäße Datenverarbeitung von öffentlichen Stellen. Aus diesem Grund nimmt sie einen hohen Stellenwert bei Prüfungen ein und sollte mindestens einen ebenso großen Wert bei den Verwaltungen selbst haben. Das ULD bietet allen öffentlichen Stellen ein umfassendes Beratungsangebot, angefangen bei Kursen der DATENSCHUTZAKADEMIE (Praxisforum, Tz. 13) bis hin zu Einzelberatungen.

Was ist zu tun?
Weiter so bzw. Bad Bramstedt zum Vorbild nehmen.

6.8.3 Stadtverwaltung Tönning

Die Prüfung der allgemeinen Datenverarbeitung und des Internetanschlusses ergab, dass sich die Stadtverwaltung Tönning auf dem richtigen Weg befindet; sie hat den Nutzen einer guten Dokumentation und einer sicheren Datenverarbeitung erkannt und arbeitet an der Defizitbehebung.

Die Bestellung einer **behördlichen Datenschutzbeauftragten** kann zu einer deutlichen Erhöhung des Datenschutzes in der Verwaltung führen. Dies war dem büroleitenden Beamten wohl erst nach der Prüfungsankündigung bewusst. Zwei Wochen vor dem Prüfungstermin wurde eine Mitarbeiterin schriftlich bestellt. Es stellte sich sehr schnell positiv heraus, dass der Verwaltungschef diese Position nicht als „Feigenblatt“ sieht, sondern als deutliches Signal, die personenbezogenen Daten der Bürger vor unbefugter Kenntnisnahme Dritter zu schützen und als zentraler Ansprechpartner in Datenschutzfragen für die Führungsebene und die Mitarbeiter tätig zu sein.

Folgende **Mängel** wurden vorgefunden:

- Die Verfahrensdokumentation gemäß DSVO war unvollständig, Tests und Freigaben fehlten vollständig.
- Die Zugriffsberechtigungen waren nur systemseitig nachvollziehbar, ein Berechtigungskonzept fehlte.
- Eine revisionsfähige Protokollierung der administrativen Tätigkeiten fand nicht statt.
- Das Sicherheitskonzept war nur ansatzweise vorhanden. Die Risikoanalyse fehlte vollständig.
- Es existierten keine schriftlichen organisatorischen Regelungen bezüglich des Umgangs mit der IT.

Was ist zu tun?
Die Stadtverwaltung Tönning muss die datenschutzrechtlichen und sicherheitstechnischen Mängel zügig beheben.

6.8.4 Universität Flensburg

Das ULD hatte Anlass, die allgemeine Datenverarbeitung der Universität Flensburg zu prüfen. Wir waren darauf aufmerksam gemacht worden, dass sensible personenbezogene Daten auf einem der gesamten Hochschulverwaltung zugänglichen Laufwerk gespeichert waren.

Die Prüfung führte zur **Beanstandung der Dokumentationslage**. Nicht ein einziges Verfahren war auch nur in seiner Funktionalität ausreichend beschrieben. Das IT-Konzept befand sich in den Anfängen, das Sicherheitskonzept fehlte.

Wir stellten Mängel in der **technischen Konfiguration** universitätsweit eingesetzter PCs und Server sowie des Netzwerks fest. So zeigte sich, dass alte Mailbestände abrufbar waren, die als längst gelöscht galten. Das Management der IT geschieht nicht nach einer einheitlichen Methode. Durch den Rückgriff auf inzwischen übliche IT-Paradigmen wie etwa ITIL, COBIT oder BSI-Grundschutz könnte die Universität Flensburg eine Vielzahl der fehlenden Konzepte und Dokumente in einem geordneten Prozess erstellen und den Betrieb der Informations- und Kommunikationstechnologie durch technische und organisatorische Maßnahmen absichern.

Die Universität Flensburg verfügt über **kein funktionierendes Datenschutzmanagementsystem** (DSMS, 29. TB, Tz. 6.1), das sämtliche datenschutz- und datensicherheitsrelevanten Prozesse im Blick behält. Es gibt bisher weder eine Strategie, geschweige denn eine gelebte Praxis, die an der Hochschule eingesetzten Verfahren anlassbezogen und regelmäßig auf ihre Ordnungsmäßigkeit hin zu kontrollieren. Gleichwohl funktioniert der alltägliche operative Betrieb; die Systemadministration verfügte über erwartbare Kompetenzen beim Betreiben der Server. Die Verarbeitung der Daten der Studierenden durch die Verwaltung war rechtlich betrachtet im Grundsatz in Ordnung. Allerdings stellte sich die Frage, ob die für Schleswig-Holstein geltenden gesetzlichen Regelungen der Studierendenverordnung vom Dienstleister Hochschul-Informations-System (HIS), dessen Leistungen zur StudentInnenverwaltung beansprucht werden, vollständig umgesetzt werden. Dies wurde im Rahmen der Prüfung nicht näher geklärt. Die Universität sagte die Prüfung zu.

Die Leitung der Universität signalisierte Einsicht, dass der Datenschutz bislang vernachlässigt wurde. Die Folgen sind weitgehende **Intransparenz der Verfahren** und Zweifel an der Nachweisbarkeit eines ordnungsgemäßen Verwaltungsbetriebs an der Hochschule. Ärgerlich ist, dass sich die Papierlage selbst bei Produkten, die beim HIS „von der Stange“ genutzt werden, als nicht ausreichend erwies.

Was ist zu tun?
Universität und ULD haben ein gemeinsames Vorgehen vereinbart, in dem in Zusammenarbeit vor allem mit der Universität Lübeck landesweit geltende Standards für IT-Sicherheit und IT-Management an den Hochschulen erarbeitet werden sollen.

7 Neue Medien

7.1 Vorratsdatenspeicherung

Trotz erheblicher verfassungsrechtlicher Bedenken hat der Bundesgesetzgeber die Anbieter von Telekommunikationsdiensten verpflichtet, die Verkehrsdaten aller Teilnehmerinnen und Teilnehmer sechs Monate „auf Vorrat“ und „für den Fall der Fälle“ einer möglichen Fahndung zu speichern. Gespeichert werden u. a. Informationen, wer mit wem wann und womit und von wo kommuniziert hat.

Der Gesetzesbeschluss bedeutet einen **Paradigmenwechsel** (Tz. 4.3.1 und 29. TB, Tz. 7.1): Zum ersten Mal in der deutschen Geschichte werden alle Bürgerinnen und Bürger in ihren Kommunikationsfreiheiten ohne Ausnahme und ohne einen konkreten Anlass gegeben zu haben beschränkt. Die Dimensionen sind erheblich: Es geht um mehrere Millionen Datensätze zu Kommunikationsbeziehungen, die von den Diensteanbietern für Zwecke der sicherheitsbehördlichen Tätigkeiten einschließlich der Nachrichtendienste täglich neu bereitgestellt werden müssen. Tausende von Betroffenen haben mittlerweile Verfassungsbeschwerde beim Bundesverfassungsgericht eingelegt.

Von der Vorratsdatenspeicherung ist jeder Kommunikationsteilnehmer betroffen, der einen öffentlich zugänglichen Dienst der Telekommunikation – ob **Telefon** über Festnetz, Mobilfunk, **E-Mail** oder den **Zugang zum Internet** – nutzt. Ausgenommen sind lediglich die Zugriffe auf Internetseiten, für die nach wie vor restriktive Löschungspflichten gelten.

Erfasst werden auch die Anschlüsse von Teilnehmern, deren Kommunikationen regelmäßig besonderen Vertraulichkeitsverpflichtungen unterliegen, z. B. **Ärzten, Strafverteidigern** oder **Geistlichen**. Erfasst werden die Kommunikationen der Bürgerinnen und Bürgern mit ihren Abgeordneten des Land- oder Bundestages. Selbst die Telekommunikationsbeziehungen der **Abgeordneten** untereinander sind in die staatlich veranlasste Kommunikationserfassung einbezogen, obwohl die demokratisch legitimierten Kontrolleure unabhängig von einer staatlich veranlassten Kommunikationsüberwachung sein sollten. Die Regelung ist für die Diensteanbieter öffentlich zugänglicher Telekommunikationsdienste zum Jahresbeginn 2008 in Kraft getreten. Lediglich die Anbieter von Internetzugangsdiensten, elektronischer Post und Internettelefonie haben noch bis zum Jahresbeginn 2009 Zeit zur Umsetzung.

Ausgenommen von der Verpflichtung zur Vorratsdatenspeicherung sind die Telekommunikationsanbieter für **geschlossene Benutzergruppen**. Darunter sind Dienste zu verstehen, deren Anschlüsse nicht öffentlich zugänglich sind, sondern die nur einem definierten Teilnehmerkreis – z. B. den Beschäftigten einer Behörde oder eines Unternehmens – als Arbeitsmittel zur Verfügung gestellt werden. Die Gesetzesbegründung nennt ausdrücklich unternehmensinterne Netze, Nebenstellenanlagen oder E-Mail-Server, die ausschließlich den dort immatrikulierten Studierenden zum Arbeiten bereitgestellt werden.

Das ULD hat die Gesetzgebung mit einer ausführlichen Stellungnahme begleitet:


www.datenschutzzentrum.de/presse/20070628-vorratsdatenspeicherung.htm

Was ist zu tun?
Die Zukunft der Vorratsdatenspeicherung liegt nun in der Hand des Verfassungsgerichts.

7.2 Datenschutzgestaltung von Webseiten

Die Landesregierung hat ein neues Content Management System eingeführt (CMS II), über das sich Regierung und Behörden der Öffentlichkeit im Internet präsentieren. Bei der Gestaltung der Datenschutzerklärung hat das ULD das Finanzministerium beraten und unterstützt.

Wie bei zahlreichen anderen Vorhaben des E-Governments bemüht sich das ULD nach Kräften, die Verwaltungen aus Land und Kommunen mit **Hinweisen zur Datenschutzgestaltung** zu unterstützen, so auch beim neuen CMS II der Landesregierung und beim Online-Beteiligungsverfahren zur Landesentwicklungsplanung des Innenministeriums (LEP-Online). Auch die Polizei sowie das Ministerium für Justiz, Europa und Arbeit beraten wir hinsichtlich einer gemeinsamen Internetpräsentation der Bundesländer.

Was gehört in eine Datenschutzerklärung?

- Informationen über den Betreiber mit Namen und Adresse („Impressum“),
- Informationen über den Dienstleister, der den Internetauftritt hostet,
- Informationen über den Zweck der Datenerhebung auf dem Webserver,
- Informationen über Cookies und andere automatisierte Erhebungsinstrumente,
- Informationen über die Erhebung über besondere Dienste (z. B. Bestellungen über Webformular, E-Mail usw.).

Die datenschutzrechtliche Grundregel für die Verarbeitung von Daten in Logfiles ist einfach: Personenbezogene Nutzungsdaten sind unmittelbar nach dem Ende der Nutzung zu **löschen**. So steht es im Telemediengesetz. Dieser Grundsatz gilt auch für die IP-Adresse, denn sie ist zumeist ein „personenbeziehbares“ Datum. Der Gesetzgeber wollte ausdrücklich unterbinden, dass die Nutzung einzelner Webseiten konkreten Personen zugeordnet wird: So wie man einzelne Artikel in seiner Tageszeitung am Frühstückstisch ohne Kontrolle durch den Verlag lesen kann, so soll es nach dem Willen des Gesetzgebers auch online sein.

Dieser Grundsatz gilt im Übrigen auch für die Webseiten, die von der Polizei im Rahmen ihrer Öffentlichkeitsarbeit in das Internet gestellt werden. Demgegenüber hat das Bundeskriminalamt offensichtlich über einen längeren Zeitraum die

IP-Adressen der Besucher der Webseiten mit den Informationen zur **Öffentlichkeitsfahndung** ausgewertet. Diese Praxis steht im Widerspruch zum Telemediengesetz, ist also rechtswidrig. In Schleswig-Holstein wurde diesem schlechten Vorbild nicht gefolgt; die Webseiten – auch des Landeskriminalamtes – sind datenschutzkonform gestaltet.

Die Verpflichtung zur unmittelbaren Löschung von IP-Adressen wirft Fragen im Umgang mit sogenannten **Statistikprogrammen** auf, die automatisiert Informationen über die Nutzung der Webseiten eines Anbieters zusammenfassen. Hierbei werden insbesondere auch die IP-Adressen ausgewertet. Die Erstellung einer Nutzungsstatistik ist ein legitimes Interesse des Anbieters. In der Praxis zeigt sich, dass aussagekräftige Statistiken mit den marktgängigen Programmen erstellt werden können, ohne dass der Datenschutz verletzt wird. Hier setzt die Beratung des ULD an.

Wer über seine Webseite automatisiert Daten bei seinen Nutzerinnen und Nutzern erhebt wie z. B. über das Setzen von **Cookies**, der sollte unbedingt die Erforderlichkeit und in jedem Fall die Voreinstellungen bei dieser Praxis überprüfen. Die Grundregel lautet: Cookies sollten nur eine Gültigkeit für den Zeitraum der aktuellen Nutzung haben (Session). Die Nutzer sind zwingend über das Setzen solcher Programme wie Cookies zu informieren. Mehr zum Thema Cookies ist zu finden unter

www.datenschutzzentrum.de/selbstdatenschutz/internet/cookies/cookies.htm

Werden **Bestelldienste** oder eine **Kontaktadresse** per E-Mail bereitgestellt, so sollten die Nutzerinnen und Nutzer unmittelbar auf dieser Angebotseite über den verantwortlichen Empfänger, den Verwendungszweck sowie etwaige Übermittlungen seiner Daten informiert werden. Auch derartige Informationen sind Pflicht.

Völlig **unbrauchbar sind Leerformeln** wie „Unsere Datenverarbeitung erfolgt im Rahmen der Datenschutzgesetze." Derartige Formulierungen haben keinerlei Informationsgehalt. Bei Nachfragen mussten wir regelmäßig feststellen, dass die Verantwortlichen des Anbieters die gesetzlichen Regelungen nicht kannten. Solche Leerformeln sind ein Hinweis auf fehlende Kenntnisse des Anbieters über seine Pflichten und damit zugleich ein Indiz dafür, dass das Gegenteil des Behaupteten zutrifft.

Noch ein genereller Hinweis: Gut überlegt sein sollte die **Freizeichnung von einer Haftung** hinsichtlich der Inhalte auf einer Webseite. Wer – als Unternehmen oder als Verwaltung – in seine Datenschutzerklärung den Passus aufnimmt, er hafte für die Inhalte seiner Webseite nicht und sei auch für die von ihm gesetzten Links nicht verantwortlich, hinterlässt einen mehr als nur zwiespältigen Eindruck bei seinen Nutzern. Die Erklärung, ich bin für mich nicht verantwortlich, ist falsch und nützt im Rechtsverkehr wenig, wenn es konkret um eine Haftungsfrage geht. Die Grundregel der Haftung bei Webseiten lautet: Jeder Anbieter haftet für die Inhalte seiner Webseite. Wer zitiert, muss das Zitat überprüfen. Das gilt auch für die **von einem Anbieter gesetzten Links**. Das Gesetz

hat die Haftung für die Inhalte auf der Webseite, auf die verlinkt wird, begrenzt. Mit Kenntnis des Inhalts der Webseite, auf die verlinkt wird, haftet der Anbieter einer Webseite immer. Sorgfalt sollte daher insbesondere auf die Formulierung des Linktextes verwendet werden, mit dem der Anbieter auf eine andere Webseite verweist, weil aus diesem Text erkennbar wird, mit welchem Kenntnisstand er den Link gesetzt hat.

Was ist zu tun?
Verwaltungen und Unternehmen sollten ihre Datenschutzerklärungen nach den oben genannten Grundsätzen auf ihre Datenschutzkonformität hin überprüfen.

7.3 Fiktion oder Realität? „Gesucht wird ..."

Das Internet bietet eine Fülle an Informationen aus öffentlichen Webforen, Blogs und Gästebüchern, deren Wahrheitsgehalt häufig nicht bewertet werden kann.

Ein Petent hat das ULD auf eine Textzeile im Internet aufmerksam gemacht, in der eine mit Namen und Geburtsdatum bezeichnete Person **als „Mörder" gesucht** wird. Die Person selbst war dem Petenten nicht bekannt. Sie konnte auch nicht von uns mit den verfügbaren Mitteln identifiziert werden. Nur in einigen wenigen Suchmaschinen war die Suchmeldung ausgewiesen und wurde dort mit „seriösen" Anbietern in Verbindung gebracht. Eine Nachprüfung dieser Verweise durch uns brachte kein Ergebnis. Ein verantwortlicher Anbieter mit Sitz in Kiel hatte sein Gästebuch mittlerweile geschlossen, „weil es nur Ärger gemacht hat". In einem anderen Fall – bei einem Sportverein – wird das Webforum mittlerweile von einem anderen Betreiber gepflegt. Das in der Suchmaschine ausgewiesene Forum wird aktuell nicht mehr angeboten und ist nur noch als Rest in der Suchmaschine verfügbar.

Nur in einem Fall konnte das Zitat nach aufwendiger Recherche in einem Blog nachgewiesen werden, dem eine E-Mail-Adresse zugeordnet werden konnte. Letztlich kam es zu keinem aufsichtsbehördlichen Einschreiten, da ohne Kenntnis weiterer Daten, z. B. der Wohnanschrift, nicht aufzuklären war, ob es die gesuchte **Person tatsächlich gibt** oder ob es sich um eine Fiktion handelt. Die Ergebnisse unserer Nachprüfung sprechen für eine Fiktion.

Der Petent hat sich auch an andere Stellen gewandt, u. a. an den Petitionsausschuss. Dabei zeigte der Petent persönlich seine Sensibilität für den **Schutz seiner Identität**: Man konnte nur postlagernd oder über eine pseudonyme E-Mail mit ihm kommunizieren. Er rief an, nutzte die Rufnummernunterdrückung und hinterließ keine Rückrufnummer. Postlagernde Briefe wurden allerdings nach Ablauf einer Woche „als nicht abgeholt" wieder zurückgesandt.

Was ist zu tun?
Die Moderation öffentlich zugänglicher Gästebücher und Webforen ist zeit- und unter Umständen nervenaufwendig. Wer als Anbieter Zeit und Nerven nicht aufbringen will oder kann, sollte auf derartige Angebote lieber verzichten.

7.4 Internetsuchmaschinen

Suchmaschinen sind eine der meistgenutzten Internetangebote, weil mit ihnen gewaltige Informationsmengen erschlossen werden können. Zugleich sind sie wegen der im Internet verfügbaren personenbezogenen Daten wie auch wegen der dabei anfallenden Nutzungsdaten zunehmend ein Datenschutzproblem.

Die Datenverarbeitung mit Internetsuchmaschinen beschäftigt das ULD zunehmend (29. TB, Tz. 10.5). Im Rahmen eines laufenden **Wettbewerbsverfahrens** äußerten wir gegenüber der EU-Kommission unsere Besorgnis darüber, dass es bei der Fusion des Suchmaschinenbetreibers Google mit dem Online-Werbevermarkter DoubleClick zu einer massiven Verletzung der Datenschutzrechte der Konsumentinnen und Konsumenten in Europa kommen könnte, wenn, was von den beteiligten Unternehmen bisher nicht ausgeschlossen werden konnte, die jeweiligen Datenbestände der Firmen zusammengeführt würden.

Suchmaschinen ermöglichen das Auffinden von Inhalten im Internet. Ein Nutzer oder eine Nutzerin gibt Stichwörter ein, nach denen der Suchmaschinenbetreiber das Internet durchsucht und die Internetseiten, die die jeweiligen Stichworte enthalten, anzeigt. Beim Betrieb von Suchmaschinen fallen in großer Zahl personenbezogene Daten an, die je nach Nutzung einen teilweise hochsensiblen Einblick in die Gewohnheiten und Interessen der Betroffenen ermöglichen. Die meisten der Suchmaschinenbetreiber können die Suchanfragen über die Auswertung der IP-Adressen einem anfragenden Computer oder gar der diesen verwendenden Person zuordnen. Eine Zusammenführung ermöglicht das Erstellen **aussagekräftiger Interessenprofile**.

Die DoubleClick Inc. ist der weltweit größte Vermarkter von Online-Werbung. Viele deutsche Online-Anbieter kooperieren mit DoubleClick und schalten von DoubleClick vertriebene Anzeigen auf ihren Webseiten. Ist Werbung von DoubleClick auf einer Webseite, kann ein mit DoubleClick kooperierendes Unternehmen über einen Cookie den Nutzer wiedererkennen und dessen **Surfverhalten nachvollziehen**. Durch die Fusion mit Google muss befürchtet werden, dass eine Verknüpfung der Interessenprofile Suchanfragen mit den Surfprofilen stattfindet und so ein noch sensiblerer Datenbestand entsteht, über den die Betroffenen faktisch keine Verfügungsmöglichkeit haben. Im Rahmen der Studie „Verkettung digitaler Identitäten“ (Tz. 8.8) sowie im Rahmen der Sommerakademie 2007 haben wir beispielhaft dargestellt, was für eine Informationssammlung durch die Zusammenführung der Datenbestände entstehen kann.

https://www.datenschutzzentrum.de/suchmaschinen/

Was ist zu tun?
Der Dialog zwischen Datenschützern und dem ULD auf der einen Seite und Google und weiteren Suchmaschinenbetreibern auf der anderen Seite muss fortgesetzt werden, um Lösungen für die aus Datenschutzsicht bisher unbefriedigende Situation zu entwickeln und zu implementieren.

8 Modellprojekte und Studien

Im letzten Jahrzehnt hat sich die Idee „Datenschutz durch Technikgestaltung“ mehr und mehr durchgesetzt. Alte und neue Partner beteiligen sich mit uns zusammen an Modellprojekten für Datenschutz, nicht nur auf nationaler Ebene. Im Mai 2007 veröffentlichte die Europäische Kommission die **Mitteilung über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre** (Privacy Enhancing Technologies). Der Tenor dieser Kommissionsmitteilung: Die Entwicklung datenschutzfördernder Technik soll ebenso gefördert werden wie ihr Einsatz bei Datenverarbeitern und Verbrauchern. Datenschutz-Gütesiegel (Tz. 9) werden explizit genannt. Besonders hat uns gefreut, dass die Projekte PRIME (Tz. 8.2) und FIDIS (Tz. 8.3), die wir maßgeblich mitgestalten, als Positivbeispiele hervorgehoben wurden. Wir werden uns weiter engagiert in diesem Bereich einbringen.

Unsere Kompetenz ist nicht nur in Konsortien für Technikentwicklungsprojekte nachgefragt, sondern auch bei der Ausarbeitung von **Studien** zu Themen, die mit Aspekten von Privatsphäre in Zusammenhang stehen. Sämtliche Aktivitäten werden vom Innovationszentrum Datenschutz & Datensicherheit (ULD-i) koordiniert, dessen Leistungen ebenfalls anderen Interessenten in Schleswig-Holstein zur Verfügung stehen (Tz. 8.1).

8.1 ULD-i – Nachfrage nach Datenschutz und Datensicherheit

Das Innovationszentrum Datenschutz & Datensicherheit (ULD-i) berät Interessenten bei allen Fragen rund um Datenschutz und Datensicherheit. Die Serviceleistungen des ULD-i werden insbesondere Unternehmen aus der Region angeboten, um die Wirtschaftskraft im Norden zu stärken.

Das ULD-i unterstützt Wirtschaft und Wissenschaft dabei, Datenschutz und Datensicherheit in Produkte und Prozesse zu integrieren. Dadurch soll das **Vertrauen der Verbraucher** in die Produkte und in deren Anbieter gestärkt werden. Das ULD-i stand im letzten Jahr in gewohnter Weise als kompetenter Ansprechpartner den Wirtschaftsunternehmen und Hochschulen zur Verfügung. Insbesondere im Rahmen des schleswig-holsteinischen Förderprogramms e-Region PLUS (Tz. 8.6) wurde das ULD-i von einer Reihe von Antragstellern kontaktiert. Die Zusammenarbeit reichte dabei von einfachen Informationsgesprächen bis zu einer engen projektbegleitenden Kooperation.

Die verschiedenen Anfragen aus Wirtschaft und Wissenschaft zeigen, dass unsere allgemeinen Ausführungen zu der Wirkung von Datenschutz und Datensicherheit auf die **wirtschaftlichen Unternehmensfaktoren** von Interesse sind. Daher hat das ULD-i auf seiner Webseite ein Tutorial zu diesen Fragen veröffentlicht. Es

unterstützt Unternehmen bei der Erarbeitung geeigneter Geschäftsmodelle und erläutert die Vorteile der Implementierung von Datenschutz und Datensicherheit.

Das ULD-i wurde durch eine **Kofinanzierung der Europäischen Union** und des ULD bis zum Ende des Jahres 2007 unterstützt. Die Koordination erfolgte durch das Wirtschaftsministerium des Landes über das Regionalprogramm 2000 im Rahmen der Förderung der Technologieregion K.E.R.N. Die Arbeit geht auch nach dem Auslaufen der Förderung weiter, wobei sich das ULD-i langfristig auf die am stärksten nachgefragten Serviceleistungen konzentrieren wird.

Weitere Informationen zum ULD-i befinden sich im Internet unter


www.uld-i.de/

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

ULD-i
Holstenstraße 98, 24103 Kiel
Tel.: 0431/988-1399
E-Mail: kontakt@uld-i.de

8.2 Nutzergesteuertes Identitätsmanagement mit PRIME und PrimeLife

Das EU-Projekt PRIME – Privacy and Identity Management for Europe – konsolidierte seine Ergebnisse: Die entwickelten Konzepte für nutzergesteuertes Identitätsmanagement realisieren Datenschutzprinzipien sowohl auf Nutzer- als auch auf Anbieterseite. Ab 2008 startet das Folgeprojekt PrimeLife, das aufbauend auf den Resultaten von PRIME datenschutzfreundliches Identitätsmanagement breit verfügbar machen will.

Identitätsmanagementsysteme soll es den Nutzern erleichtern, ihre Daten in der digitalen Gesellschaft zu verwalten. Sie unterstützen beim Zugang zu geschützten Internetseiten, ersparen das Ausfüllen von Formularen und ermöglichen z. B. eine Altersverifikation. Allerdings ist nicht jedes Identitätsmanagementsystem datenschutzfreundlich. In dem von der Europäischen Kommission geförderten Projekt PRIME (29. TB, Tz. 8.4) arbeitet das ULD zusammen mit 19 Partnern seit 2004 an Lösungen, um **mit Identitätsmanagement effektiveren Datenschutz** zu gewährleisten, als dies bisher möglich ist. Die entwickelten Ideen werden in Prototypen für das Internet, für Mobiltelefonie und kollaboratives E-Learning getestet.

Die in PRIME erarbeiteten Lösungen stellen das Prinzip maximaler Datensparsamkeit in den Vordergrund. Personenbezogene Daten sollen grundsätzlich nur dann verarbeitet werden, wenn dies für das Funktionieren des jeweiligen Services unerlässlich ist. Hier kommen auch innovative Lösungen wie die „**privaten**

Credentials“ zum Einsatz, die Zurechenbarkeit und Datensparsamkeit kombinieren. Alle Nutzer sollen verstehen, wofür die Daten benötigt werden; hierzu wurden eigene **Benutzungsoberflächen** entwickelt. Ein Schwerpunkt der Forschung lag auf Methoden, die Nutzern mehr Transparenz über die Datenverarbeitung, aber auch über etwaige Risiken bieten. Die Verarbeitungsregeln aus der anbieterseitigen Datenschutzerklärung, z. B. für welchen Zweck die Daten erhoben wurden oder wie lange sie gespeichert bleiben dürfen, können an die von Nutzern herausgegebenen Daten gebunden werden (sogenannte „sticky Policies“). Bei der Verarbeitung der Daten werden diese Regeln einbezogen, sodass ihre Einhaltung überprüfbar bleibt.

Im Berichtsjahr lag ein Fokus unserer Arbeit darauf, die Resultate des PRIME-Projektes in die aktuelle **Standardisierung** von Identitätsmanagement durch die International Telecommunication Union (ITU) und die International Organization of Standardization (ISO) einzubringen. Daneben wurden die Ergebnisse auf einer Vielzahl von Konferenzen präsentiert, darunter auch auf dem Internet Governance Forum der Vereinten Nationen. Bereits jetzt setzen einige industrielle Produkte auf Technologie, die in PRIME entwickelt wurde. So sind datenschutzfreundliche PRIME-Komponenten Grundlage für einen kommerziellen Lokalisierungsdienst bei T-Mobile geworden.

Die Förderung von PRIME läuft 2008 aus, doch führen wir mit einem geänderten Konsortium die Arbeit im **Nachfolgeprojekt PrimeLife** fort, das im März 2008 startet. Was in klassischer Client-Server-Realisierung ausprobiert wurde, muss dann für soziale Netzwerke und andere Dienste, in denen Nutzer direkt miteinander interagieren, angepasst werden. PrimeLife wird außerdem einen Schwerpunkt auf Open Source legen, sodass die entwickelten Komponenten noch einfacher Eingang in andere Software finden können, die für Identitätsmanagement geeignet ist.

Weitere Informationen zum EU-Projekt PRIME, wie z. B. die sogenannten Tutorials (auch deutschsprachig) und das „White Paper“, befinden sich im Internet unter

www.prime-project.eu/

Was ist zu tun?
Es sollte geprüft werden, inwieweit PRIME-Konzepte auch für andere Verfahren, die mit personenbezogenen Daten arbeiten, zu gebrauchen sind. Hier sind insbesondere „private Credentials“, „sticky Policies“ und Überlegungen für mehr Transparenz für Nutzer zu nennen.

8.3 FIDIS – Identitätsmanagement der Zukunft

Das von der EU geförderte Exzellenznetzwerk FIDIS arbeitet seit 2004 am Thema „Identität". Wichtige Resultate gibt es zum Identitätsmanagement in öffentlichen Verwaltungen, zu elektronischen Identitätsdokumenten und zu Ubiquitous Computing, d. h. allgegenwärtiger Informationsverarbeitung.

Im Projekt „FIDIS – Future of Identity in the Information Society", einem sogenannten „**Network of Excellence**" (29. TB, Tz. 8.5), arbeiten wir mit weiteren 23 Partnern aus 12 Ländern zusammen. Ergebnisse des Projektes sind europäische Studien, Berichte und Artikel zu verschiedenen Aspekten von Identität, Identifizierung und Identitätsmanagement, die unter www.fidis.net, in Büchern oder Magazinen publiziert werden. Wir vertreten dabei aus unterschiedlichen fachlichen Perspektiven grundsätzliche und angewandte Aspekte des Datenschutzes.

Bildeten in den vergangenen beiden Jahren wirtschaftsnahe Aspekte des Identitätsmanagements den Schwerpunkt der Arbeit, wie z. B. RFID (Radio Frequency Identification) in Logistik und Vertrieb, Location Based Services oder Identitätsmanagement in Geschäftsprozessen, so verlagert sich der Schwerpunkt mittlerweile zu **verwaltungsnahen Aspekten**. Aus diesem Bereich stammen die beiden erstgenannten Ergebnisse:

- **ePass:** Die im Jahr 2006 rund um die „Budapest-Erklärung" begonnenen Aktivitäten wurden fortgesetzt, indem wir die Sicherheitslücken im elektronischen Reisepass (29. TB, Tz. 8.5) genauer unter die Lupe nahmen. Hierbei wurden die technischen Änderungen berücksichtigt, die sich mit der zweiten Stufe der Einführung des ePasses zum November 2007 ergeben haben. Leider konnten unsere Bedenken nicht ausgeräumt werden: Es ist technisch möglich, dass sich Unbefugte kontaktlos Zugriff auf Bürgerdaten und das biometrisch optimierte Gesichtsbild auf Reisepässen verschaffen. Ein höherer Schutz besteht lediglich für die nun zusätzlich gespeicherten Fingerabdruckdaten. Neben zahlreichen Publikationen haben wir in Zusammenarbeit mit der Meldebehörde Lübeck ein Merkblatt für Bürger erstellt und vertreiben dies zusammen mit einer Schutzhülle für den ePass (Tz. 4.1.3). Weitere Meldebehörden in Schleswig-Holstein und außerhalb bekundeten ihr Interesse an der Aktion.

- **Identitätsmanagement in der öffentlichen Verwaltung:** Gleich zwei Studien legen hierauf ihren Schwerpunkt: eine Studie zu Möglichkeiten und Grenzen von Anonymität im Umgang mit der Verwaltung, die zweite zu **Identitätskennzeichen** („ID Numbers") als wesentlichem Instrument des Identitätsmanagements im öffentlichen Bereich. Die letztgenannte Studie setzt sich auch mit den Möglichkeiten der Verkettbarkeit öffentlicher Identitätsinformationen und praktizierten Ansätzen zu deren Vermeidung im Vergleich von neun

europäischen Mitgliedstaaten auseinander. Die Ergebnisse flossen in das Projekt „Verkettung digitaler Identitäten“ (Tz. 8.8) ein. Weitere Studien zum Identitätsmanagement in der Verwaltung sind in Arbeit.

- **Umsetzung heutiger Rechtsprinzipien beim Ubiquitous Computing:** Eine weitere Studie setzt sich mit der Frage auseinander, wie in Zukunft das traditionelle Recht in der Welt allgegenwärtiger Datenverarbeitung, bei der jede Sache mit Sensoren und Transpondern ausgestattet sein kann, um- und durchgesetzt werden kann. Die so entstandene Vision eines „**Ambient Law**“ stützt sich auf eine technisch unterstützte Durchsetzung von Recht. In der Studie diskutieren wir technische Ansätze, die aus Nutzersicht die Transparenz in solchen Umgebungen erhöhen sollen (sogenannte „**Transparency Enhancing Technologies**“, TETs).

- **Datenspuren in technischen Kommunikationsprotokollen:** Computer kommunizieren miteinander gemäß spezifizierten Standards, sogenannten Protokollen. Den Nutzern ist meist nicht bewusst, was technisch im Hintergrund abläuft und wo sie in den Computernetzen Spuren hinterlassen. Dies haben wir in einer FIDIS-Studie genauer analysiert und beschrieben, wo welche Schutzmaßnahmen, z. B. Anonymisierungstechniken, greifen können, will man solche Datenspuren vermeiden. Ein wesentliches Ergebnis dieser Studie ist, dass bei heutigen und künftigen Entwicklungen im Bereich des Internets und der Computervernetzung weiterhin **unnötige Daten** entstehen, über die Nutzer **kaum eine Kontrolle** haben. Daher scheint eine Einbeziehung von Datenschutzexperten bei der Standardisierung von Kommunikationsprotokollen geboten. Diese Arbeit ist allerdings aufwendig.


www.fidis.net/

Was ist zu tun?
Die Ergebnisse der FIDIS-Studien sollen zukünftig verstärkt in praxisbezogene Konzeptions- und Beratungsprozesse eingebracht werden. Mögliche Adressaten sind hierbei die Art. 29-Datenschutzgruppe und zuständige Generaldirektionen der EU.

8.4 AN.ON – Anonymität online weiter wichtig

Der Abruf von Webseiten ist möglich ohne Datenspuren, mit deren Hilfe Nutzer identifiziert werden können. Unser Anonymisierungsdienst AN.ON bietet weiterhin eine Grundversorgung mit Anonymität beim Surfen im World Wide Web.

Seit 2001 beschreiben wir jährlich in unseren Tätigkeitsberichten (zuletzt 29. TB, Tz. 8.2) den Fortschritt bei „AN.ON – Anonymität online“, einem Anonymisierungsdienst für Webzugriffe. Nachdem die Förderung durch das Bundesministerium für Wirtschaft und Technologie im Jahr 2006 plangemäß ausgelaufen war,

stand der Anonymisierungsdienst auf eigenen Füßen. Ebenso wie die an der Entwicklung beteiligten Partner von der Technischen Universität Dresden und der Universität Regensburg betreiben wir unseren eigenen Anonymitätsserver (einen sogenannten Mix) innerhalb der AN.ON-Kaskaden weiter. Dessen Nutzung ist **kostenlos** und gewährleistet zurzeit zusammen mit den Mixen, die von anderen Organisationen betrieben werden, für Internetnutzer eine **Grundversorgung** mit anonymem Webzugriff. Unser Mix wird durchschnittlich von 1.000 Nutzern gleichzeitig angesprochen. Daneben haben ehemalige Entwickler von AN.ON die private Firma JonDos GmbH gegründet und vermarkten im Sinne der Projektziele das System seit Juni 2007 kommerziell. Das ULD ist hieran nicht unmittelbar beteiligt. Wir verfolgen aber interessiert die Entwicklung bei unseren ehemaligen Partnern.

Wie bisher werden wir von verschiedenen Institutionen und Privatpersonen insbesondere zu rechtlichen Fragen rund um Anonymität im Internet angefragt. Auch nach Auslaufen des AN.ON-Projektes werden wir weiterhin als **kompetente Ansprechpartner** für diesen Bereich angesehen. Vorträge zu AN.ON sind regelmäßig gut besucht, z. B. auf der CeBIT, bei der uns der Heise-Verlag auch 2007 ein Forum bot.

Der im letzten Tätigkeitsbericht (29. TB, Tz. 8.2) angesprochene **Widerspruch gegen die Beschlagnahme** des vom ULD betriebenen AN.ON-Servers wurde vom Landgericht Konstanz zurückgewiesen. In der Begründung des Beschlusses wurde ausgeführt, dass sich die Angelegenheit durch Rückgabe des Servers erledigt habe. Das Gericht behauptete, das Vorgehen sei verhältnismäßig gewesen. Die Ermittlungsbehörden hätten nicht gewusst, dass hinter dem ULD-Server der AN.ON-Dienst stehe. Allerdings wäre dies unserer Ansicht nach durch eine simple Eingabe der IP-Adresse bei Google oder durch die Nachfrage beim Provider über den Mieter des Servers in Erfahrung zu bringen gewesen. Eine weitere Beschwerde gegen den Beschluss des Landgerichts Konstanz war rechtlich nicht möglich.

Gravierende Auswirkungen auf den Betrieb von Anonymisierungsdiensten kann das im November 2007 beschlossene Gesetz zur **Vorratsdatenspeicherung** haben (ausführlich hierzu Tz. 7.1). Nach dem erklärten Willen des Gesetzgebers sollen auch Anonymisierungsdienste erfasst werden. Wie dieses jedoch bei verteilten Diensten wie AN.ON oder TOR umgesetzt werden soll, ist völlig offen. Es ist schon absehbar, dass künftig vermehrt Server im Ausland betrieben werden, auf die europäische Strafverfolgungsbehörden keinen Zugriff haben. Das ULD und AN.ON haben sich stets zu der Pflicht bekannt, bei Vorliegen eines richterlichen Beschlusses Daten im Rahmen der angeordneten Überwachung zu protokollieren. Ein **Ausweichen auf Anonymisierungsserver ins außereuropäische Ausland** führt dazu, dass die inländischen Strafverfolgungsbehörden dieser Möglichkeit beraubt werden. Zugleich garantieren viele ausländische Anonymisierungsdienste ihren Nutzern nicht das hohe Schutzniveau gegen unautorisierte Zugriffe, das AN.ON bietet. Wir werden die Entwicklungen kritisch beobachten und uns bemühen, auch künftig einen vertretbaren Ausgleich zwischen den Interessen der Bürger und denen der Strafverfolgungsbehörden zu erwirken.

Weitere Informationen zu AN.ON befinden sich im Internet unter

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

Was ist zu tun?
Die Möglichkeit, das World Wide Web anonym zu nutzen, muss gewahrt bleiben.

8.5 PRISE – Sicherheitstechnik mit eingebautem Datenschutz?

Im 7. Forschungsrahmenprogramm der EU ist Sicherheitsforschung seit 2007 ein eigener Themenschwerpunkt. In den nächsten sieben Jahren stehen dafür Fördermittel in Höhe von 1,4 Milliarden Euro zur Verfügung. Die Europäische Kommission will bei der Sicherheitsforschung und der Entwicklung neuer Sicherheitstechnik die Privatsphäre respektieren und die Bürgerrechte wahren.

Um die europäische Gesellschaft und ihre Bürgerinnen und Bürger vor Bedrohungen des Terrorismus oder der organisierten Kriminalität zu schützen, arbeiten viele Forscher und Entwickler an Sicherheitstechnologien. Neben Techniken zur Abschottung gegen unautorisierte Zugriffe wird vor allem an der Verbesserung von Überwachungssystemen gearbeitet. Solche Systeme ermöglichen mittlerweile ein automatisiertes Beobachten von Menschen und Sachen per Audio, Video oder andere **Sensorik** und können die Daten nach auffälligem oder unerwünschtem Verhalten auswerten.

Im Projekt PRISE (Privacy Enhancing Shaping of Security Research and Technology) erarbeiten wir seit 2006 produktbezogene Kriterien für die **Gestaltung von Sicherheitstechnologien**, anhand derer geprüft werden kann, inwieweit entwickelte Systeme mit deutschem und europäischem Datenschutzrecht konform sind und Eingriffe in die Privatsphäre von Menschen minimieren (29. TB, Tz. 8.6). Gleichzeitig kann der Kriterienkatalog herangezogen werden, um von Anfang an rechtskonforme Produkte zu entwickeln.

? Sensoren

Mithilfe von Sensoren können physikalische und chemische Eigenschaften von Räumen, Personen und Gegenständen erfasst werden. Es gibt optische, thermische, elektrische, mechanische sowie weitere spezielle Sensoren. Unterscheidbar sind nach Einflussgrößen beispielsweise:

- *Luftfeuchtigkeit,*
- *Dehnung,*
- *elektromagnetische Strahlung,*
- *magnetische Feldstärke,*
- *elektrische Spannung,*
- *Temperatur.*

Bei der Überwachung von Räumen und Personen können durch Sensoren detaillierte Angaben über Bewegungen von Personen, bei sich getragene Gegenstände und körperliche Eigenschaften erfasst werden. Mithilfe von Analysetools lassen sich die Messwerte zusammenführen und auf Auffälligkeiten hin automatisch untersuchen, ohne dass dies für den Betroffenen erkennbar ist.

Im Rahmen von PRISE wurden zufällig ausgewählte Bürger in sechs europäischen Staaten zu ihren Erwartungen und Befürchtungen im Hinblick auf Sicherheitstechnologien und deren Auswirkung auf die Privatsphäre befragt. Mit verschiedenen Szenarien zu Sicherheitstechnologien konfrontiert, zeigten sich die Teilnehmer überwiegend sensibilisiert, wobei nationale Unterschiede sichtbar wurden. Bei den deutschen Befragten dominierte eine eher kritische Grundhaltung in Bezug auf Überwachungssysteme. Techniken wie „Naked Machine“, bei denen Menschen durch **Terahertzstrahlung** ohne Kleidung – **buchstäblich nackt** – dargestellt werden und so mitgeführte Gegenstände ebenso wie körperliche Details leicht erkennbar werden, wurden von der deutschen Gruppe als zu invasiv abgelehnt. Für andere Überwachungsmethoden forderten die Teilnehmer wirksame Kontrollmethoden, um einen Missbrauch zu verhindern.

Im April 2008 wird das PRISE-Projekt die entwickelten Konzepte auf einer großen **Konferenz in Wien** Verantwortlichen aus Politik, Forschung und Wirtschaft präsentieren.

Weitere Informationen zum EU-Projekt PRISE finden sich unter

@ www.prise.oeaw.ac.at/

Was ist zu tun?
Im Rahmen der Sicherheitsforschung muss schon zum frühestmöglichen Zeitpunkt, also schon bei der Funktionsfestlegung, ein Hauptaugenmerk auf die privatsphärenfreundliche Technikgestaltung gelegt werden.

8.6 e-Region PLUS

Das Förderprogramm e-Region PLUS wird von der Europäischen Union kofinanziert und unterstützt mehr als 40 Projekte aus den Programmsäulen „Informationsgesellschaft“ und „Wissenstransfer“. Ziel ist es, innovative Projekte zu fördern, die die Nutzung moderner Informations- und Kommunikationstechnologien verbessern.

Das Ministerium für Wissenschaft, Wirtschaft und Verkehr des Landes Schleswig-Holstein als Förderer und durchführende Stelle legte auf die Beleuchtung der **datenschutzrechtlichen und sicherheitstechnischen Aspekte** der e-Region-PLUS-Projekte Wert und teilte dies den Projektverantwortlichen mit. Vor allem Vertreter von Projekten in der Programmsäule „Informationsgesellschaft“, die sich an kleine und mittlere Unternehmen richtete, nahmen daraufhin Kontakt zu uns auf. Teilweise ging es um punktuelle, schnell beantwortbare Einzelfragen; bei komplexeren Konstellationen empfahl sich eine detaillierte Ausarbeitung der datenschutzrechtlichen Aspekte, die manchmal sogar zu einer projektbegleitenden Zusammenarbeit wurde.

Projekte, die sich mit einer Vielzahl von datenschutzrechtlichen und sicherheitstechnischen Fragen an das ULD gewandt haben, waren neben den Projekten SpIT-AL (Tz. 8.6.1) und BoatSecure (Tz. 8.6.2) Vorhaben wie „DMS Stadt Kiel“ und „e-Gewerbe“ mit einem hohen Einfluss auf den öffentlichen Bereich. Das Projekt „DMS Stadt Kiel“ zielt auf die Einführung eines Dokumentenmanagementsystems im Gesundheitsamt der Stadt Kiel (29. TB, Tz. 4.6.2) ab. Im Projekt „e-Gewerbe“ sollen Gewerbeanzeigen wie An-, Um- und Abmeldungen elektronisch erfasst und bearbeitet werden. Wir haben die Projekte **beratend** bei Fragen zu Datenschutz und Datensicherheit unterstützt.

8.6.1 SpIT-AL – Werbeanruf? Und tschüs!

Unerwünschte Werbeanrufe rauben manchem den letzten Nerv – mal sollen Lotterielose, mal Telefontarife aufgeschwatzt werden. Diesen Werbeterror hat die Kieler Telefongesellschaft TNG aufs Korn genommen und mit uns zusammen im Projekt SpIT-AL eine Abwehrlösung entwickelt, die den Telefonkunden nun zur Verfügung gestellt wird.

Voice-over-IP (VoIP) heißt eine Form der Internetnutzung, die zunehmend als „hip“ gilt. Die Rede ist von Sprachtelefonie, die nicht leitungsgebunden, sondern durch die Weiten des internationalen Datennetzes vermittelt wird. Insbesondere Auslandstelefonate lassen sich so kostengünstiger abwickeln. Einfacher wird auf diesem Wege auch die Kundenakquise per Telefon, weshalb bei zunehmender Verbreitung von VoIP von einer Zunahme von **telefonischem Werbemüll** ausgegangen werden muss. Dies wird in Fachkreisen SpIT, Spam over Internet Telephony, genannt.

Damit niemand vor Verzweiflung wegen des ständig klingelnden Telefons einen Nervenzusammenbruch erleidet, hat das Kieler Unternehmen TNG (The Net Generation) unter öffentlicher Förderung im Rahmen des schleswig-holsteinischen Förderprogramms e-Region PLUS eine Software entwickelt, die es den Kundinnen und Kunden erlaubt, selbst zu entscheiden, für wen sie wann erreichbar sein wollen. SpIT-AL, **SpIT-Abwehrlösung**, lautet der Name des Projektes. Das ULD hat die datenschutzrechtliche und -technische Begleitung der TNG-Entwicklung vorgenommen.

Diese **Innovation aus Schleswig-Holstein** findet internationale Aufmerksamkeit: auf der CeBIT, nationalen und internationalen Forschungskongressen, der Internationalen Funkausstellung – überall war das SpIT-AL-Team eingeladen, das Projekt und dessen Konzept vorzustellen. Damit sich diese Innovation weiterentwickeln und verbreiten kann, wurde die Entwicklung der Software in ein **Open-Source-Projekt** vorangetrieben und steht so der Allgemeinheit zur Verfügung.

Eine Weiterentwicklung ist bereits vollzogen: Obwohl zunächst nur im Hinblick auf VoIP konzipiert und vorangetrieben, bietet TNG den Service inzwischen auch für das **Festnetz** an.

Weitere Informationen zu SpIT-AL und dem entwickelten SpIT-Filter befinden sich im Internet unter


www.spit-abwehr.de/

Was ist zu tun?
Verbraucher müssen die Möglichkeit erhalten, sich mit einfachen Mitteln vor lästigen Anrufen zu schützen. Verbote von Spam und SpIT sollten besser, auch mit technischer Hilfe, durchgesetzt werden.

8.6.2 BoatSecure – Sensorik auf Schiffen

Die Gefahr des Diebstahls wertvoller Jachten aus häufig wenig gesicherten Jachthäfen ist groß. Um das Wiederauffinden im Falle eines Diebstahls zu ermöglichen, besteht ein Interesse an der Ortung von Jachten. Die Überwachung verschiedener Messwerte mithilfe von Sensoren aus der Ferne kann dem Bootseigentümer überdies Hinweise über einen Wassereinbruch im Boot oder einen niedrigen Batteriestand geben.

Im Rahmen des Förderprogramms e-Region PLUS hat das ULD die datenschutzrechtliche Begleitung des Projektes BoatSecure übernommen. Ziel ist die Entwicklung eines GSM-Moduls und eines Webportals, mit deren Hilfe verschiedene **durch Sensoren erfasste Messwerte** über ein Webportal online abrufbar sind und grafisch bearbeitet dargestellt werden. Bootseigentümer können sich mit dem Service aus der Ferne z. B. die Funktion der Lenzpumpe (Wassereinbruch), die Batteriespannung oder die GPS-Positionsdaten über das Webportal anzeigen lassen.

> ***? Global Positioning System (GPS)***
>
> *Beim Global Positioning System handelt es sich um ein satellitengestütztes Positionsbestimmungssystem. Ein GPS-Empfänger berechnet seine auf wenige Meter genaue Position mithilfe der Signallaufzeit zu mindestens drei Satelliten.*
>
> *Europa plant ein eigenes Satellitennavigationssystem: Galileo. Dieses soll ab 2011 eingesetzt werden.*
>
> *Mithilfe von Satelliten sind wesentlich präzisere Positionsbestimmungen möglich, als dies z. B. durch die Einbuchung eines Handys in einer Mobilfunkzelle der Fall ist. So lassen sich präzise Bewegungsprofile erstellen.*

Nutzt ein Bootseigentümer sein Boot selbst und aktiviert die GPS-Ortung, wohl wissend, dass beim Betreiber des Systems Daten über die Position anfallen, ist dies datenschutzrechtlich unproblematisch. Komplizierter ist die Konstellation bei Charterbooten, wenn Nutzern nicht bewusst ist, dass die **Position ihres Schiffes** stets im Blick des Vercharterers ist. Hier ist eine informative und verständliche Ausgestaltung der Dokumentation und der Einwilligungserklärung vonnöten. Zudem bestehen besondere Anforderungen an die Sicherheit der Datenübermittlung und -verarbeitung, die Speicherdauer, das Zugriffs- und Berechtigungskonzept sowie die Transparenz und die Kontrollmöglichkeiten für den Betroffenen. Die Forderung nach Datensparsamkeit steht dabei im Vordergrund.

Was ist zu tun?
Bei der Entwicklung von privatsphärenrelevanten Technologien wie bei BoatSecure sind Fragen des Datenschutzes und der Datensicherheit bereits frühzeitig systematisch zu prüfen und entwickelte Lösungen praktisch umzusetzen.

8.7 Datenschutz für Bürgerportale

Bürgerportale, betrieben von unterschiedlichen Anbietern, sollen künftig sichere und verbindliche elektronische Kommunikation im Internet ermöglichen. Das Bundesministerium des Innern koordiniert die Spezifikation von Diensten in Bürgerportalen als Teil der Hightechstrategie der Bundesregierung sowie des Programms „E-Government 2.0". Das ULD definiert Anforderungen aus Datenschutzsicht.

Bürgerportale sollen als vertrauenswürdige Dritte die Identität von Partnern in der elektronischen Kommunikation bestätigen bzw. überprüfbar machen (**Identitätsprovider**), persönliche Postfächer und zuverlässige Versand- und Zustelldienste für elektronische Dokumente bieten (**Kommunikationsgateway**) und als sicherer Speicher für elektronische Dokumente dienen (**Datensafe**). Bürgerinnen und Bürgern, aber auch der Wirtschaft und Verwaltung soll mithilfe der Bürgerportale eine vertrauliche sowie verbindliche Kommunikation über das Internet ermöglicht werden.

Bürgerportale sollen von unterschiedlichen Anbietern bereitgestellt werden, die im Wettbewerb zueinander stehen und sich durch unterschiedliche Mehrwerte, die über die Bürgerportaldienste hinausgehen, voneinander abgrenzen können. Es ist geplant, dass alle Anbieter eines Bürgerportals gegenüber einer unabhängigen Stelle die Zuverlässigkeit der Verfahren und Prozesse **nachweisen** müssen. Auch alle relevanten Datenschutzaspekte sollen in die Prüfung einfließen.

Die Spezifikation der einzelnen Dienste ist noch nicht abgeschlossen. Viele wichtige **Datenschutzanforderungen** konnten wir aber schon herausarbeiten und in die Diskussion bei Entwicklern und potenziellen Betreibern einbringen. Wir haben Vorschläge zu Anforderungen an die Betreiber von Bürgerportalen und zu den notwendigen und angemessenen Vorgehensweisen bei der Überprüfung dieser Anforderungen im Rahmen eines Zertifizierungsverfahrens unterbreitet.

Besonders relevant ist die **Information der Nutzenden** über die sie betreffende Datenverarbeitung und daraus resultierende Pflichten, die sich aus dem angestrebten hohen Grad an Verbindlichkeit ergeben. Beispielsweise könnte gefordert sein, dass man in sein Bürgerportalpostfach ebenso regelmäßig hineinschaut wie in den Postbriefkasten. Wir begrüßen die Möglichkeit, verschiedene **Pseudonyme** statt nur einer einzigen „offiziellen" Kommunikationsadresse zu verwenden. Vielleicht kann hier später ein funktionierendes nutzergesteuertes Identitätsmanagement aufgesetzt werden, wie es beispielsweise im PRIME-Projekt konzipiert wird (Tz. 8.2). Gut ist auch, dass nicht sämtliche Datenverarbeitung über einen zentralen Server abgewickelt wird, dessen Betreiber dann Zugriff auf alle Daten hätte.

Doch auch bei einer Vielzahl von Anbietern müssen unautorisierte Zugriffe durch geeignete technische und organisatorische Maßnahmen verhindert werden. Schließlich wird zu erörtern sein, wie die Umsetzung der Europäischen Richtlinie zur Vorratsdatenspeicherung (Tz. 7.1) die Bürgerportale konkret betrifft.

Weitere Informationen zu Bürgerportalen befinden sich im Internet unter

www.buergerportale.de/

Was ist zu tun?
Bürgerportale müssen Datenschutz- und Datensicherheitsanforderungen vorbildlich umsetzen, damit Nutzer in den verbindlichen Internetgeschäftsverkehr Vertrauen fassen können.

8.8 „Verkettung digitaler Identitäten" – elementare Zutaten für die Privatsphäre

Das zusammen mit dem Lehrstuhl „Datenschutz und Datensicherheit" der Technischen Universität Dresden durchgeführte Projekt „Verkettung digitaler Identitäten" nimmt in seinem Abschlussreport die wesentlichen Bausteine für Privatsphäre unter die Lupe.

Hinter dem sperrigen Titel „Verkettung digitaler Identitäten" stecken ganz konkrete praktische Themen, die Menschen in ihrer Rolle z. B. als Bürger, Kunde, Arbeitnehmer oder Internetnutzer bewegen: „Wo werden welche Daten über mich erhoben? Wer kann sie miteinander verknüpfen, wo werden **Profile** über mich erstellt? Wie lassen sich diese verketteten Daten auswerten?" All dies veranschaulicht unser 2007 erschienener Report, der im Auftrag und unter Förderung des Bundesministeriums für Bildung und Forschung im Rahmen der Innovations- und Technikanalyse erstellt wurde. An dem Vorhaben arbeiteten neben Juristen und Informatikern auch Betriebswirte, Soziologen und Historiker mit, die das Thema aus ihrer jeweiligen Perspektive diskutieren.

Die Frage, inwieweit persönliche Informationen verkettet werden können und sollen, betrifft die **Basis des Konzeptes „Datenschutz"** – oder genauer: des Schutzes der Privatsphäre der Menschen. In unserer Informationsgesellschaft geschieht dies vor allem über sogenannte „digitale Identitäten". Diese finden sich beispielsweise in Nutzerkonten bei Anbietern im Internet, in Kundendatenbanken von Unternehmen oder auch in staatlichen Datenbeständen. Zu digitalen Identitäten gehören auch Ordnungsnummern der Verwaltung, biometrisch aufgenommene Merkmale wie beispielsweise Fingerabdrücke oder selbst flüchtige Daten, z. B. die einem Gast eines Internetcafés zugeordnete IP-Adresse. Mit ihnen lassen sich einzelne Datenspuren verketten und zu umfassenden Persönlichkeitsprofilen oder persönlichen Historien verknüpfen.

Ein wesentlicher Inhalt des 230 Seiten langen Berichts ist eine Bestandsaufnahme von Datensammlungen und Verkettungsmöglichkeiten in Verwaltung, Wirtschaft und Internet-Communities. Im technischen Teil werden Mechanismen zur Verkettung vorgestellt sowie Maßnahmen, mit denen diese verhindert oder eingeschränkt werden kann. Die Problematik des nachträglichen „Entkettens“ wird aufgezeigt, das aus technischer Sicht kaum verlässlich zu realisieren ist. Vier **Szenarien** aus den Bereichen „Überwachung mithilfe von Alltagsgegenständen“, „Internetsuchmaschinen“, „Arbeitnehmer und ortsbezogene Dienste“ sowie aus dem noch visionären „Ambient Assisted Living“, in dem Menschen in einer Welt voller Sensoren in ihrem Tun unterstützt werden, kombinieren die vorherigen Einzelbeobachtungen zu lebendigen und leicht nachvollziehbaren Praxisfällen.

Darauf aufbauend benennt der Report **Handlungsempfehlungen und Bedingungen** für die Verkettung digitaler Identitäten. Die Bedingungen sollen im gesellschaftlichen Diskurs ausgehandelt werden und zur Verbesserung der technischen Standards, Rechtsnormen sowie Best Practices von Datenverarbeitern führen. Vorgeschlagen werden Maßnahmen zur Erhöhung der Transparenz und des Verständnisses der Betroffenen, zum Aufbau eines nutzergesteuerten Identitätsmanagements sowie zur Qualitätssicherung. Diese Maßnahmen sollen hinsichtlich der Nutzung von Informationstechnik vertrauensbildend wirken und für mehr Gerechtigkeit und Grundrechtsschutz in der Informationsgesellschaft sorgen.

Der Bericht zeigt auf, wie die Verkettung selbst von nicht personenbezogenen Daten und die Erstellung anonymer Profile zu unerwünschten Folgen, z. B. zu **Diskriminierungen von Betroffenen**, führen können. Er geht dabei über das aktuelle europaweit harmonisierte Datenschutzrecht hinaus. Diesen Punkt diskutiert das ULD zurzeit in der Arbeitsgruppe der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) „Privacy & Technology“ mit internationalen Datenschutzexperten. Der Report wird über den Buchhandel zur Verfügung gestellt. Er ist auch kostenlos abrufbar über unsere Website unter

www.datenschutzzentrum.de/projekte/verkettung/

Was ist zu tun?
Bei jedem Entwurf technischer Systeme und organisatorischer Prozesse sollten im Vorfeld die Bedingungen für Verkettung überdacht werden: Wann soll eine Verkettung möglich oder sogar notwendig sein? Wann darf dies nicht geschehen? Systeme in unserer Informationsgesellschaft bedürfen der Transparenz über Daten und ihre Verkettungen, damit die Bürgerinnen und Bürger die Risiken für ihre Privatsphäre abschätzen können. Gestalter von Technik, Recht und Politik sind aufgefordert, für eine Verbesserung im Sinne der Handlungsempfehlungen, die im Report aufgeführt sind, zu sorgen.

8.9 Gestaltungsvorschläge für datenschutzkonforme serviceorientierte Architekturen

Im Rahmen des Projektes SOAinVO wurden Gestaltungsvorschläge für eine beherrschbare serviceorientierte Architektur entwickelt und zum Gegenstand einer umfangreichen Analyse gemacht.

Das Projekt SOAinVO – **Serviceorientierte Architekturen in virtuellen Organisationen** lief von Dezember 2006 bis September 2007 und wurde vom Bundesministerium für Bildung und Forschung im Rahmen der Innovations- und Technikanalyse gefördert. Projektpartner waren das ULD und die Universität Koblenz-Landau mit dem Institut für Informatik und dem Institut für Wirtschafts- und Verwaltungsinformatik.

> ***? Virtuelle Organisation***
>
> *Eine virtuelle Organisation ist ein virtueller Zusammenschluss rechtlich unabhängiger Organisationen, die zur Erreichung bestimmter Ziele über einen gewissen Zeitraum hinweg zusammenarbeiten.*

Der Begriff „serviceorientierte Architektur“ (SOA) bezeichnet ein Gestaltungsprinzip für die Orchestrierung lose gekoppelter Dienste, welches sich an Geschäftsprozessen orientiert und mit dem verschiedene Systeme und Datenbestände mithilfe standardisierter Formate und Schnittstellen verbunden werden können (Tz. 6.4). Eine SOA erleichtert die Zusammenarbeit von bestehenden Softwarelösungen **über organisatorische Grenzen hinweg**, wie sie insbesondere auch in sogenannten „virtuellen Organisationen“ praktiziert wird.

Im Rahmen des Projektes wurden die Faktoren **Unterrichtung, Auskunft, Zusicherung und Protokollierung** als datenschutzrelevante Aspekte, mit denen die Beherrschbarkeit von SOA gewährleistet werden kann, identifiziert. Anhand dieser vier Faktoren sowie spezifischer rechtlicher und technischer Kriterien wurden in der SOAinVO-Analyse verschiedene Anwendungsszenarien analysiert und hierauf aufbauend detaillierte Gestaltungsvorschläge und Lösungsansätze für das Design datenschutzkonformer serviceorientierter Architekturen unterbreitet. Die SOAinVO-Analyse ist abrufbar unter

https://www.datenschutzzentrum.de/soa/

Was ist zu tun?
Die Ergebnisse der SOAinVO-Analyse zeigen, dass bei serviceorientierten Architekturen in virtuellen Organisationen insbesondere in Bezug auf die Entwicklung von Beschreibungssprachen für Zusicherungen und Protokollierung weiterer Forschungsbedarf besteht.

8.10 Datenschutz in Online-Spielen

Online-Spiele bestimmen mehr und mehr den Markt der Computer- und Videospiele. Hierbei dürfen Daten-, Jugend- und Verbraucherschutz nicht auf der Strecke bleiben. Die Sammlung von Spielerprofilen, die Online-Einbindung von Werbung oder auch der Einsatz von Kameras und Mikrofonen bergen Risiken, die schon bei der Entwicklung von Online-Spielen beachtet werden sollten.

Seit September 2007 führen wir ein Projekt zu „**Datenschutz in Online-Spielen**“ **(DOS)** durch, das vom Bundesministerium für Bildung und Forschung über zwei Jahre gefördert wird. Die meisten Spiele auf Konsolen, Handhelds und PCs – so auch Online-Rollenspiele wie „World of Warcraft“ oder „Herr der Ringe Online“ – ermöglichen inzwischen das Spielen über das Internet. Dies wird durch Systeme wie „Xbox Live“ oder „Playstation Home“ mit zusätzlichen Funktionen wie z. B. Chatrooms und öffentlichen Bewertungsprofilen unterstützt. „Second Life“ verlässt sogar die reine Spielebene und entwickelt sich zu einer virtuellen Welt mit weit mehr Möglichkeiten als dem Austausch von Spielergebnissen.

Im Projekt DOS wird erstmalig genauer der Datenschutz bei Online-Spielen wissenschaftlich untersucht. Verwandte Aspekte aus Jugendschutz und Verbraucherschutz werden dabei einbezogen. Mit Blick auf kommende neue Entwicklungen ist es wichtig, den Herstellern und Betreibern aufzuzeigen, welche gesetzlichen Regelungen für sie gelten und wie diese von ihnen umgesetzt werden können. Die Umsetzung ist umso leichter, je früher diese Kriterien im Entwicklungsprozess beachtet werden. **Unklarheiten und Unwissenheit** führen zu Produkten, die **rechtswidrig** sind und massive Risiken für die Privatsphäre der Spieler in sich bergen.

Viele Nutzerinnen und Nutzer sind sich dieser Risiken nicht bewusst. Aufklärung durch klare Darstellung der Pflichten der **Betreiber** und Hinweise auf die Rechte der Nutzer sind notwendig. Für Unternehmen in Deutschland bietet sich die Möglichkeit, bei Online-Spielen eine **Vorreiterrolle im Bereich Datenschutz** einzunehmen. Anbieter, die sich an die im Projekt entwickelten Grundsätze halten, zeigen, dass sie verantwortungsvoll mit den Daten ihrer Kunden umgehen. Ein so erzielter hoher Qualitätsstandard kann sich positiv auf die Nutzerzahlen und das Image der Anbieter auswirken. Dies gilt für Anbieter von Online-Spielen wie für Zulieferer von entsprechender Technik und Zertifikaten. Letztlich kann damit eine Erhöhung der Investitionssicherheit der beteiligten Unternehmen erreicht werden.

Die während der Projektlaufzeit erarbeiteten **Anforderungskataloge, Vorlagen und Leitfäden** ermöglichen es den **Herstellern** von Online-Spielen, früh in der Entwicklung die Vorgaben des Datenschutzes zu beachten und in ihre Produkte zu integrieren. So entfallen die Kosten für spätere Nachbesserungen am Produkt, wenn sich erst im Nachhinein Mängel zeigen. Die Anforderungskataloge und Leitfäden können mit leichten Modifikationen auch für andere Bereiche internetbasierter Kommunikationsdienste genutzt werden.

Die **Entwicklung praxisnaher Ergebnisse** wird durch die Kooperation mit Projektpartnern wie IBM oder Pixelpark sowie mit den Spielerinnen und Spielern sichergestellt.

Weitere Informationen zum Projekt DOS befinden sich im Internet unter

www.datenschutzzentrum.de/dos/

Was ist zu tun?
Auch in Online-Spielen müssen Datenschutzstandards eingehalten werden. Hersteller und Betreiber von Online-Spielern sind eingeladen, sich in das Projekt einzubringen und von den Ergebnissen in ihrer praktischen Arbeit zu profitieren.

8.11 bdc\Audit – unterwegs zur auditierten Biobankforschung

Im Projekt bdc\Audit werden Methoden und Kriterien für eine praxisgerechte und zugleich datenschutzfachlich korrekte Biobankforschung entwickelt. Erste Ergebnisse stoßen in der Fachwelt auf großes Interesse und Zustimmung.

Das Projekt wird vom ULD gemeinsam mit dem Forschungsschwerpunkt Biotechnik, Gesellschaft und Umwelt der Universität Hamburg (BIOGUM) und dem Institut für Informatik der Christian-Albrechts-Universität zu Kiel ausgeführt, wobei jede beteiligte Stelle ein separates Teilprojekt verantwortet (29. TB, Tz. 8.1). Das Teilprojekt des ULD befasst sich damit, wie Biobanken dem Grundsatz der informierten Spendereinwilligung Rechnung tragen und wie systemseitig die datenschutzrechtlichen Vorgaben beachtet werden können. Es untersucht, wie der **Spenderdatenschutz** bei den Biobanken bereits von Anfang an als Bestandteil der Aufbau- und Ablauforganisation umgesetzt werden kann, sodass eine spätere kostenträchtige Nachrüstung betrieblicher Prozesse entbehrlich wird.

Das ULD hat eine Befragung von Biobanken begleitet und deren Antworten ausgewertet. Neben guten Lösungen stießen wir auf Verbesserungsbedarfe.

? Biobank

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 meist zusammen mit soziodemografischen und medizinischen Daten der Spenderinnen und Spender aufbewahrt. Proben und Daten stammen teilweise von 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 genutzt werden.

Biobankforschung erfordert über Zeiträume von zehn und mehr Jahren den Zugriff auf die Proben und Daten der Spenderinnen und Spender. Ein wesentlicher Fokus liegt auf genetischen Untersuchungen. Hierbei ist das Recht der Spender, ihre Proben aus der Forschung zurückzuziehen, vielfach nicht ausreichend gesichert. Diesbezüglich können allgemein zugängliche **Biobankenregister** weiterhelfen. Diesen sollten die Spender dauerhaft entnehmen können, in welchen Forschungsprojekten mit ihren Proben geforscht wurde, geforscht wird und künftig geforscht werden soll. Oft bleibt die eigentumsrechtliche Zuordnung der gespendeten Proben im Unklaren. Dies beeinträchtigt nicht nur die Spenderrechte, sondern verursacht für die betroffenen Biobanken gravierende Risiken im Wettbewerb: Wenn Proben dauerhaft an andere Biobanken im In- und Ausland weitergegeben werden, ist die Klärung der Rechte hieran unverzichtbar. Es erweist sich schon jetzt als ein Mangel des deutschen Rechts, dass es nach wie vor kein **Forschungsgeheimnis** gibt.

Auf der Grundlage der gefundenen Erhebungsergebnisse entwickelt das ULD einen **Leitfaden zur Auditierung der betrieblichen Prozesse bei Biobanken**. Die Gestaltung von Anfang an zuverlässiger, rechtssicherer und datenschutzfördernder Prozesse dient sowohl den Interessen der Spender, der Biobanken als auch allgemein der Qualitätssicherung in der Biobankforschung.

Die Kosten, die jemand einsetzen muss, um die genetischen Daten einer Person zu ermitteln, werden immer niedriger. Das Interesse an ihrer Nutzung breitet sich entsprechend aus. In dieser Situation werden unzureichend geschützte oder schlecht organisierte Biobanken zunehmend ein lohnendes Ziel für sachfremde oder kriminelle Zugriffe. Zum Schutz hiervor wird bdc\Audit durch seine Vorgaben zu Auditierung und Zertifizierung einen Beitrag leisten, der Biobanken mit hohem Datenschutzniveau einen **bedeutenden Wettbewerbsvorteil** verschafft.

Was ist zu tun?
Die Politik sollte, dem Schweizer Beispiel folgend, ein Biobankenregister auf den Weg bringen, das u. a. die einzelnen durchgeführten Forschungsprojekte erfasst. Regelungsbedürftig ist auch, welche Wahlalternativen ein Spender mindestens haben muss und welche Rechte ihm nicht genommen werden dürfen.

8.12 RISER (Registry Information Service on European Residents)

Die europäische Melderegisterauskunft RISER, der erste E-Government-Dienst für grenzüberschreitende Meldeauskünfte in Europa, ist auch in der Markteinführungsphase erfolgreich.

Das seit März 2004 laufende Projekt RISER (Registry Information Service on European Residents) wird weiter erfolgreich im Markt eingeführt. Das vom ULD begleitete und bisher von der Berliner PSI AG geleitete Projekt ist an die eigenständige RISER ID Services GmbH übertragen worden. Die nach erfolgreicher Marktevaluierung im September 2006 gestartete Markteinführungsphase wird **weitere Melderegister** über den Dienst verfügbar machen. Zurzeit bietet RISER

Anfragemöglichkeiten nach Österreich, Deutschland, Estland, Ungarn, Irland, Schweden und in die Schweiz. Auch 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 unübersichtlichen Melderegisterlandschaft in Europa. Über das Serviceportal können Meldeanfragen als Datei- oder Einzelanfrage über das Internet an die zuständige Meldebehörde weitergeleitet werden. RISER übernimmt dabei die **Funktion eines Zustellers**.

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?

Einen Höhepunkt bei RISERid bildete die Organisation der **3. Internationalen Konferenz zum Europäischen Meldewesen** in Budapest, Ungarn, an der Delegierte der öffentlichen Verwaltungen aus vielen EU-Ländern teilnahmen. Auf der Konferenz wurden unter aktiver Beteiligung des ULD die Rolle und Bedeutung des Meldewesens in Europa und die Möglichkeiten der praktischen Zusammenarbeit zwischen den nationalen Datenschutzbehörden diskutiert.

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

8.13 IM Enabled

Instant-Messaging-Dienste liegen im Trend. Will auch eine Behörde online und in Echtzeit mit den Bürgern kommunizieren, sind besondere Anforderungen an den Providerdienst zu stellen. Im Projekt IM Enabled E-Government Services werden die Anforderungen vom Unabhängigen Landeszentrum erarbeitet.

An dem September 2006 gestarteten Projekt Instant Messaging (IM) Enabled sind neben dem ULD Partner aus Irland, Frankreich, Italien und Deutschland beteiligt. Welche Behördeninformationen können datenschutzgerecht über Instant Messaging zur Verfügung gestellt werden? Welche Anforderungen sind an Anbieter von Instant-Messaging-Diensten zu stellen, damit der Bürger sicher mit seiner Behörde kommunizieren kann? Das Marktevaluierungsprojekt unter Führung des Waterford Institutes of Technology aus Irland wird im Rahmen des eTEN-Programms von der Europäischen Union gefördert. Der Instant Messaging Information Service (IMIS) ermöglicht es, **E-Government-Dienste über Instant Messaging** für Bürger und Unternehmen bereitzustellen. Da bei den meisten Anbietern solcher Dienste sichere Übertragungsmöglichkeiten fehlen, ist diese Methode zur Kommunikation mit Behörden derzeit nur begrenzt geeignet.

Was ist zu tun?
Den Bürgerinnen und Bürgern dürfen behördliche Informationen über Instant Messaging nur zur Verfügung gestellt werden, wenn deren datenschutzgerechte Übertragung und Abrufbarkeit gewährleistet werden kann.

8.14 Gutachten zu Geodaten

Geodaten, also vor allem digitale Informationen mit Bezug zu einer über die Erdoberfläche definierten räumlichen Lage, sind in zunehmendem Maß Gegenstand der Verarbeitung in Verwaltung und Wirtschaft.

Auftakt eines umfassenderen Engagements des ULD zum Thema war die Erstellung eines Gutachtens im Auftrag des Bundesministeriums für Wirtschaft und Technologie. Hintergrund des gesteigerten, vor allem wirtschaftlich motivierten Interesses an staatlicherseits vorgehaltenen Geoinformationen ist die inzwischen problemlos mögliche örtliche Referenzierung von Daten durch Satellitennavigation und andere Techniken und deren komfortable Präsentation in auch über Internet teilweise erschlossenen **Geoinformationssystemen** (GIS), die von Bund, Ländern und Kommunen bereitgestellt werden. Unterstützt wird diese Entwicklung in der Europäischen Union, die z. B. in Form der sogenannten INSPIRE-Richtlinie die Errichtung einer einheitlichen europaweiten Geodateninfrastruktur anstrebt.

Geoinformationen können einen **Personenbezug** haben. Klärungsbedürftig bleibt die Frage, unter welchen Bedingungen Geobasisdaten, z. B. topografische Informationen, und Geofachdaten, z. B. Angaben über Raumnutzung, Aussagen über die persönlichen und sachlichen Verhältnisse einer natürlichen Person beinhalten. Diskussionsbedarf besteht zudem zur Frage, in welchem Verhältnis Offenbarungs- und Geheimhaltungsinteressen bezüglich der jeweiligen Fachdaten stehen. Das ULD zielt darauf ab, eine Sensibilisierung sämtlicher Akteure im Hinblick auf den Datenschutz und eine Annäherung der bestehenden inhaltlichen Differenzen bei deren Bewertung zu erreichen. Den berechtigten Wünschen der Wirtschaft und des Staates an einer wirtschaftlichen Verwertung von Geoinformationen sollte nachgekommen werden, wobei die schutzwürdigen Belange der Betroffenen aber ausreichend und umfassend geschützt werden müssen.


www.datenschutzzentrum.de/download/Datenschutz-und-Geoinformationen.pdf

Die frühzeitige Einbindung datenschutzrechtlicher Anforderungen in die Maßnahmen zur wirtschaftlichen Nutzung von Geoinformationen sichert nicht nur die Gesetzeskonformität, sondern fördert zugleich die gesellschaftliche Akzeptanz. Das ULD hat die Federführung für einen von den Datenschutzbehörden des Bundes und der Länder eingerichteten Arbeitskreis übernommen. Außerdem wird das ULD als ständiger beratender Gast im Arbeitskreis Geodaten des Landes Schleswig-Holstein, dessen Ziel die Errichtung einer Geodateninfrastruktur ist (GDI-SH), mitwirken. Über Kontakte zu den Akteuren in der Wirtschaft verfolgen wir einen **ganzheitlichen Ansatz**.

Im Rahmen einer parlamentarischen Anhörung nahm das ULD gegenüber dem Bundestag zum Entwurf eines Satellitendatensicherheitsgesetzes Stellung. Zielsetzung dieses Gesetzes ist die Schaffung eines rechtlichen Rahmens für die Bereitstellung von über Satelliten erhobenen Fernerkundungsdaten für den globalen Markt. Der Entwurf beschränkte sich auf die Sicherung der außen- und sicherheitspolitischen Interessen Deutschlands. Er löste aber eine umfassendere Diskussion über die Regulierung von Satellitendaten aus, die inzwischen in einer hohen Auflösung selbst für den Internet-Nutzer auf dem Home-PC abrufbar sind: Derartige Daten können z. B. für kriminelle oder gar terroristische Aktivitäten genutzt werden. Sie sind unter Umständen auch geeignet, das Persönlichkeitsrecht von Betroffenen zu verletzen. Wir haben gerne die Möglichkeit genutzt, das inzwischen verabschiedete Gesetz zu nutzen, um diesbezüglich eine Sensibilisierung zu erreichen.


www.datenschutzzentrum.de/geodaten/20070831-stellungnahme-satdsig.pdf

Der Personenbezug von Geodaten bildet auch einen Faktor bei der Entscheidung über einen Zugangsanspruch nach dem Umweltinformationsgesetz Schleswig-Holstein (UIG-SH). Geodaten sind oft **Umweltinformationen** im Sinne des UIG-SH. Ein Antrag auf Informationszugang ist allerdings abzulehnen, wenn personenbezogene Daten offenbart würden, deren Vertraulichkeit durch eine Rechtsvorschrift vorgesehen ist.

Was ist zu tun?
Bei der Etablierung neuer Geoinformationssysteme ist von Anfang an darauf zu achten, dass die Datenschutzbelange von Grundstückseigentümern und Bewohnern sowie von sonstigen Betroffenen beachtet werden.

9 Audit und Gütesiegel

Selbst die **optimistischsten Prognosen** vor sieben Jahren (23. TB, S. 9, 78; 24. TB, Tz. 10) wurden **übertroffen**. Die Gründe sind einfach und plausibel: Die vom ULD entwickelten und durchgeführten Auditierungs- und Gütesiegelverfahren sind für die Behörden und Unternehmen „werthaltig". Sie verbessern den Datenschutz in Verwaltung und Wirtschaft qualitativ und belohnen die Investitionen in den Datenschutz und die Sicherheit der Datenverarbeitung werbe- und wettbewerbswirksam. Auch für den Datenschutz hat sich die Investition gelohnt: Die Verfahren reduzieren die Verletzlichkeit der Informationsverarbeitung im Interesse der Betroffenen und sind darüber hinaus für den Steuerzahler kostendeckend. Kein Wunder, dass die Erfolge aus Schleswig-Holstein bundesweite und internationale Anerkennung, Nachahmung und Unterstützung finden.

Sechs Jahre nachdem der Gesetzgeber im Bundesdatenschutzgesetz eine allgemeine Regelung zum Datenschutz-Audit aufgenommen hat, wurde nun vom Bundesinnenministerium der Entwurf eines **Bundesdatenschutzauditgesetzes** der Öffentlichkeit vorgelegt. Es ist sehr zu begrüßen, dass nunmehr das zuständige Bundesministerium auch offiziell den Datenschutz als Wettbewerbsfaktor anerkennt und hierzu einen konkreten Vorschlag vorgelegt hat. Dieser sieht aber bisher noch ein recht kompliziertes und konfliktträchtiges Verfahren vor. Zugleich leidet der Entwurf daran, dass die Qualität von verliehenen Datenschutzzertifikaten nicht in einem festgelegten Verfahren gewährleistet wird. Es wird daher nun darum gehen, in der weiteren Erörterung die bestmögliche Lösung zu finden, die die Freiwilligkeit des Verfahrens herausstreicht, eine hohe Akzeptanz bei den Beteiligten und Betroffenen findet und zugleich einen Beitrag zur Verbesserung des präventiven Datenschutzes leistet. Das ULD hat zu dem Entwurf eine erste Stellungnahme abgegeben.


www.datenschutzzentrum.de/bdsgauditg/20070928-stellungnahme.html

9.1 Datenschutz-Audits

9.1.1 ZIAF-Audit

Mit dem beim Landwirtschaftsministerium (MLUR) durchgeführten ZIAF-Audit wurde ein neues Kapitel der Zertifizierung aufgeschlagen: Das ULD zertifizierte auf Wunsch des Ministeriums die sicherheitstechnische Seite auch nach dem nationalen Sicherheitsstandard des Bundesamtes für die Sicherheit in der Informationstechnik (BSI), dem sogenannten IT-Grundschutz.

Mit dem ZIAF-Verfahren zur Agrarförderung werden in Schleswig-Holstein vom MLUR auf ca. 350 Arbeitsplätzen von neun verschiedenen Organisationseinheiten an zwölf Standorten Fördermaßnahmen für die Landwirtschaft verwaltet. Von 2002 bis 2007 wurden über das Verfahren ca. 535.000 Zahlvorgänge mit einem Auszahlungsvolumen von rund 2.160 Millionen Euro durchgeführt. Ein solches

Verfahren muss nach den europarechtlichen Vorgaben **besonderen Sicherheitsanforderungen** genügen: Die Informationstechnik darf nicht ausfallen, die Antragsdaten sollen ihren Empfänger erreichen und dürfen nicht in die Hände Unbefugter gelangen. Die Bundesländer haben sich für das Verfahren auf den Sicherheitsstandard IT-Grundschutz des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) verständigt.

Die Überprüfung nach den Anforderungen des Datenschutzes und der IT-Sicherheit „auf Herz und Nieren“ (29. TB, Tz. 9.1.7) erfolgte in einer ersten Stufe bis Herbst 2007 hinsichtlich der **Sicherheitskonzeption** beim Ministerium sowie beim Dienstleister Dataport. Das Konzeptaudit bestätigt, dass die Zahlstelle des MLUR über eine rechts- und normenkonforme Konzeption (Generaldokumentation) verfügt, die die Festlegung und Umsetzung der Sicherheitsanforderungen der EU- und der Landesdatenschutzvorschriften beschreibt. Dazu zählen insbesondere auch wirkungsvolle IT-Sicherheitsprozesse und -maßnahmen auf der Grundlage der Sicherheitsstandards 100-1 bis 100-3 des BSI. Bereits im Rahmen des Konzeptaudits konnte stichprobenartig die Umsetzung von einzelnen Maßnahmen festgestellt werden.

Die Konzeption zeichnet sich durch folgende **datenschutzfreundliche Aspekte** aus:

- Die Datenverarbeitung wird nach den Sicherheitszielen der Verfügbarkeit, Vertraulichkeit, Integrität sowie der Ordnungsmäßigkeit in einer geregelten Aufbau- und Ablauforganisation betrieben.
- Die Generaldokumentation beschreibt umfassend den Einsatz und den Betrieb der in der Zahlstelle eingesetzten Informationssysteme mit einem vorbildlich nachvollziehbaren Sicherheitskonzept.
- Der Dienstleister Dataport verpflichtet sich über einen Betreibervertrag zu den erforderlichen Leistungen für Datenschutz und Datensicherheit einschließlich der von der EU geforderten Grundschutzkonformität.
- Die Zahlstelle verfügt über ein funktionierendes Sicherheitsmanagement, das aufbau- und ablauforganisatorisch in der Lage ist, die in der IT-Sicherheitsleitlinie festgelegten Ziele zu erreichen und dauerhaft aufrechtzuerhalten.

Zwecks Erfüllung der EU-Anforderungen arbeitet das MLUR nun gemeinsam mit Dataport am Nachweis der **Umsetzung der Sicherheitskonzeption**.

Das ULD hat zwei Mitarbeiter zu vom **BSI lizenzierten Grundschutzauditoren** qualifizieren lassen. Weitere Mitarbeiter werden 2008 folgen. So gewährleistet das ULD die Kompatibilität der sicherheitstechnischen Anforderungen nach der Datenschutzverordnung (DSVO) und des Standards IT-Grundschutz: Wer die Anforderungen des IT-Grundschutzes nachweist, garantiert zugleich den nach den Datenschutzgesetzen geforderten Stand der Technik.

Was ist zu tun?
MLUR und Dataport müssen die Festlegungen ihrer datenschutz- und grundschutzkonformen Generaldokumentation vollständig umsetzen, um sich auch die Implementierung der Anforderungen vom ULD bestätigen lassen zu können.

9.1.2 KITS.system

Das ULD hat in einem Audit bestätigt, dass das in den Kommunen in Schleswig-Holstein eingesetzte Standardsystemkonzept für die Bürokommunikation (KITS.system) im kommunalen Bereich datenschutzfreundlich umgesetzt worden ist und betrieben wird.

„KITS.system ist ausgezeichnet!“ – so lautet die gemeinsame Meldung der Auditpartner. Ausgezeichnet wurde KITS.system durch ein erfolgreiches Datenschutz-Audit. Für KITS.system hat das Finanzministerium die folgenden **Datenschutzziele** festgelegt:

- Umsetzung der gesetzlichen und vertraglichen Vorgaben,
- Gewährleistung der Ordnungsmäßigkeit der Datenverarbeitung,
- Gewährleistung der Integrität und Verfügbarkeit der zentralen Systeme,
- Schutz vertraulicher Informationen,
- Minimierung der Gefährdung der Systeme der KITS-Nutzer durch die zentralen Systeme,
- Minimierung der Gefährdung der zentralen Systeme durch KITS-Nutzer.

Zur Erreichung dieser Datenschutzziele mussten das Kommunale Forum für Informationstechnik der Kommunalen Landesverbände in Schleswig Holstein (KomFIT), das Finanzministerium, Dataport und das ULD einige Hürden nehmen (29. TB, Tz. 9.1.9). KITS.system basiert auf dem **zentralen Verzeichnisdienst** Active Directory der Firma Microsoft. Dieses Active Directory besitzt keine aussagekräftige revisionssichere und manipulationssichere Protokollierung administrativer Tätigkeiten (29. TB, Tz. 6.3). Die kommunalen Nutzer von KITS.system müssen aber sicherstellen, dass die gemeinsamen genutzten Komponenten korrekt und vor allem nach ihren Weisungen verwaltet werden.

Zur Erfüllung dieser Anforderungen wurde während des Audits für das Active Directory eine **Lösung eines Drittherstellers** implementiert. Diese bietet den kommunalen Nutzern ein detailliertes Berichtswesen zu den wichtigen sicherheitskritischen Parametern von KITS.system. Alle Änderungen am Verzeichnisdienst und an den zentralen Komponenten von KITS.system werden aussagekräftig protokolliert. Die Protokollierung kann von den Systemadministratoren nicht umgangen werden.

Alle KITS-Kunden sind in einer sogenannten Domäne – einer Gliederungseinheit des Active Directory – zusammengefasst. Diese Designentscheidung führt dazu, dass die **Authentifizierungs- und Autorisierungsdaten** aller kommunalen Nutzer in einer Datenbank vorgehalten werden. Um die Arbeitsfähigkeit bei den kommunalen Kunden bei einer Netzwerkstörung aufrechtzuerhalten, muss diese Datenbank bei allen Kunden in Kopie vorgehalten werden. Eine Kompromittierung dieser lokalen Kopien durch eine unberechtigte Einsichtnahme oder Veränderung würde nach Aussagen Microsofts dazu führen, dass der komplette Verzeichnisdienst überprüft und in wesentlichen Teilen neu aufgebaut werden muss.

Um diesen nicht unerheblichen Aufwand und den damit verbundenen zeitweisen Ausfall der Systeme zu vermeiden, müssen die Domänencontroller – so heißen die Server bei den Kunden, die die Kopie der Datenbank vorhalten – gut gesichert werden, um ungerechtfertigte Zutritte und Zugriffe auszuschließen. Eine lediglich vertragliche Vereinbarung mit den Nutzern über die notwendigen Sicherheitsmaßnahmen genügt nicht. Aus diesem Grund führen das Finanzministerium und KomFIT bei den KITS-Nutzern gesondert gesicherte **Schutzschränke** ein. In einem Schlüsselkonzept ist über einen Mechanismus von versiegelten Umschlägen und regelmäßigen Kontrollen sichergestellt, dass ein unberechtigter Zugriff auf diese sicherheitskritischen Server erkannt und der Sicherheitsvorfall in einem geordneten Vorgehen bearbeitet werden kann.

Ein geordnetes Vorgehen bei Sicherheitsvorfällen bildet einen weiteren wichtigen Baustein zur Umsetzung der Datenschutzziele. KomFIT, Dataport und das Finanzministerium haben hierzu ein **integriertes Datenschutz- und Sicherheitsmanagementsystem** (DSMS) sowie ein Vorgehen zum Durchführen von Änderungen an der zentralen Infrastruktur (Change-Management) eingeführt.

Im DSMS werden Werkzeuge, Maßnahmen und Verantwortlichkeiten zusammengefasst, die ein dauerhaft hohes und nachhaltiges Datenschutz- und Datensicherheitsniveau umsetzen und gewährleisten sollen. Hierunter fallen regelmäßige und anlassbezogene Kontrollen, das Erstellen eines jährlichen Sicherheitsberichts und ein geordnetes Vorgehen bei Sicherheitsvorfällen. Beim Finanzministerium, bei KomFIT und bei Dataport wurden Verantwortliche für Sicherheitsfragen benannt. Die KITS-Nutzer entsenden jeweils einen entscheidungsbefugten Vertreter in ein **Sicherheitsgremium**, welches Sicherheitsvorgaben erarbeitet und an der Weiterentwicklung des Sicherheitskonzeptes beteiligt ist.

Im Wortlaut: § 17 Abs. 2 LDSG

Die Daten verarbeitende Stelle hat dafür Sorge zu tragen, dass personenbezogene Daten nur im Rahmen ihrer Weisungen verarbeitet werden. Sie hat die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um dies sicherzustellen. Sie hat Auftragnehmende unter besonderer Berücksichtigung ihrer Eignung für die Gewährleistung der nach den §§ 5 und 6 notwendigen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Aufträge, ergänzende Weisungen zu technischen und organisatorischen Maßnahmen und die etwaige Zulässigkeit von Unterauftragsverhältnissen sind schriftlich festzulegen.

Das **Change-Management** legt ein Vorgehen fest, wie Änderungen an der zentralen Infrastruktur den Beteiligten mitgeteilt und wie diese ausgeführt werden. Hiermit ist sichergestellt, dass die zentrale Infrastruktur nur in Übereinstimmung mit den Regelungen zur **Auftragsdatenverarbeitung** umgesetzt wird (siehe Kasten). Darüber hinaus wird gewährleistet, dass die zentrale Infrastruktur nur mit dem Einverständnis und nach den Vorgaben der Kunden als Auftraggeber weiterentwickelt wird.

Das Auditverfahren zeigt: Große Infrastrukturen können durch gezielte Sicherheitsmaßnahmen, eine aussagekräftige Protokollierung und eine umfangreiche Dokumentation datenschutzfreundlich gestaltet werden und sind gleichzeitig **wirtschaftlich und effizient**.

Was ist zu tun?
Die KITS-Nutzer müssen die zentral angebotenen Sicherheitsmaßnahmen nutzen, insbesondere die zentrale Protokollierung und das Berichtswesen. Die Wahrung des hohen Sicherheitsniveaus setzt die Kooperation aller Beteiligten am Sicherheitsgremium und am Change-Management voraus.

9.1.3 ISMS Dataport

Dataport hat ein Informationssicherheitsmanagementsystem (ISMS) installiert, das im Einklang mit den Vorgaben des IT-Grundschutzes des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) steht. Es legt die Aufgaben und Prozesse fest, in denen Dataport für einen sicheren Betrieb seiner Kundendaten Sorge trägt.

Dataport als IT-Dienstleister des Landes Schleswig-Holstein hat sich **IT-Grundschutz** des BSI als unternehmensweiten Sicherheitsstandard auf die Fahnen geschrieben. Ein Kernelement ist der Aufbau eines operativen Sicherheitsmanagements mit Schnittstellen zu einem proaktiven und kontrollierenden Datenschutzmanagement. Das ULD unterstützt diesen Kurs, weil eine einheitliche Aufbau- und Ablauforganisation mit Schnittstellen zu den Auftraggebern nicht nur das Sicherheitsniveau qualitativ absichert, sondern auch die Verantwortlichkeit der Auftraggeber für die Sicherheit ihrer Daten stärkt.

Mit der Konzeption des Informationssicherheitsmanagementsystems definiert Dataport Vorgaben für die Festlegung der **Verantwortlichkeit für die IT-Sicherheit im Unternehmen** „von oben bis in die Linie“. Über das IT-Sicherheitsvorfallmanagement können sicherheitsrelevante Ereignisse rechtzeitig erkannt und die erforderlichen Maßnahmen eingeleitet werden. In einem Handbuch werden die erforderlichen technischen und organisatorischen Abläufe des ISMS beschrieben. Die Prozessbeschreibungen orientieren sich an dem internationalen Standard ITIL, den Dataport für andere unternehmensinterne Prozesse bereits verwendet.

Die Praxistauglichkeit des Konzepts wird durch seine **Implementierung** für einzelne Fachverfahren von Kunden bestätigt. Hierzu zählen ZIAF, das Landes-

netz sowie KITS.system. Eine allmähliche Ausweitung des ISMS-Konzepts ist von Dataport vorgesehen.

Was ist zu tun?
Dataport muss das auditierte ISMS Schritt für Schritt unternehmensweit implementieren, die im Auftrag der Kunden betriebenen Fachverfahren in das Managementsystem einbeziehen und die Schnittstellen zu den jeweiligen Kunden definieren.

9.1.4 Gemeinde Stockelsdorf

Stockelsdorf hat seine interne Datenverarbeitung und seinen Internetanschluss so ausgestaltet, dass eine datensparsame und datenschutzfreundliche Datenverarbeitung nach den Anforderungen des LDSG und der DSVO erfüllt wird.

Der Aufwand hat sich für die Gemeinde Stockelsdorf gelohnt (29. TB, Tz. 9.1.11). Das Auditverfahren wurde erfolgreich abgeschlossen. Die Erstellung und die weitere Pflege der Dokumentation erleichtern der Gemeindeverwaltung, die erreichten technischen und organisatorischen Sicherheitsmaßnahmen für zukünftige Planungen zu sichern. Der behördliche Datenschutzbeauftragte orientiert sich hierbei an einem allgemeinen **Strukturierungsvorschlag des ULD** (29. TB, Tz. 6.5).

Bei der Umsetzung der Sicherheitsmaßnahmen in ihrer internen Datenverarbeitung setzt die Gemeindeverwaltung auf **Zentralisierung** und einen **hohen Grad an Automatisierung**. Das Audit zeigt anschaulich, dass eine sicherheitstechnische Konzeption nach den Vorgaben des ULD gleichzeitig auch die Wirtschaftlichkeit des IT-Betriebes sichert. Hierzu zählen unter anderen

- die Inventarisierung und Verteilung von Sicherheitsupdates,
- die Verteilung und Kontrolle von Antivirensoftware,
- die Installation von Standardsoftware,
- das Sperren und selektive Freigeben sämtlicher Schnittstellen (z. B. USB-Anschlüsse und DVD-Laufwerke),
- die Nutzung eines Verzeichnisdienstes zur Authentisierung und Autorisierung,
- die Beschränkung der an den Endgeräten angebotenen Funktionen (in diesem Fall durch Gruppenrichtlinien),
- die Beschränkung des zur Verfügung stehenden Festplattenspeichers pro Benutzer,
- die Filterung sämtlichen Datenverkehrs mit externen Netzwerken sowohl auf Inhalts- als auch auf Transportebene.

Die Erfahrungen der Gemeindeverwaltung Stockelsdorf zeigen, dass mit der Konzentration der IT-Ressourcen der Rücken frei wird, um anspruchsvolle IT-Projekte besser planen zu können.

9.1.5 Rezertifizierung Bad Schwartau

Bad Schwartau ist die erste Kommune, die ihre Datenverarbeitung nach Ablauf der Gültigkeit des Datenschutz-Audits erfolgreich einer Rezertifizierung unterzogen und mit Bravour bestanden hat.

Im Sommer 2004 hatte Bad Schwartau seine interne Datenverarbeitung als eine der ersten Kommunen zertifizieren lassen (27. TB, Tz. 9.2.3). Nach Ablauf der Gültigkeit des Zertifikats von drei Jahren hat sich Bad Schwartau erneut zertifizieren lassen. Da sich die IT-Konzeption nicht wesentlich geändert hatte, konnte die Rezertifizierung zügig und kostengünstig durchgeführt werden. Die Stadt hat bei dem Auditgegenstand sein hohes Datenschutzniveau gehalten. Hervorzuheben ist nicht nur unter wirtschaftlichen, sondern auch unter sicherheitstechnischen Aspekten das Terminal-Server-Konzept der Stadt sowie die restriktiv abgesicherte Nutzung der Internetdienste.

Was ist zu tun?
Zur Bestätigung der Nachhaltigkeit der Datensicherheit sollte das Datenschutz-Audit nach Ablauf seiner Gültigkeit von drei Jahren erneut angestrebt werden. Die Rezertifizierung erfolgt in einem verkürzten und kostengünstigen Verfahren.

9.1.6 Kreis Plön

Der Landkreis Plön hat für die elektronische Zusammenarbeit mit den Kommunen ein sicheres und kreisgebietbezogenes Kommunikationsnetz geschaffen, das erfolgreich auditiert wurde.

Der Kreis Plön hat mit Bravour das Auditverfahren für sein Kreisnetz durchlaufen und hierfür im November 2007 das Auditzeichen erhalten (29. TB, Tz. 9.1.5). Nach der Konzeption des Kreisnetzes Plön wird der **Datentransport zwischen definierten Anschlüssen** und zwischen genehmigten Teilnehmern (Nutzern) erbracht. Das Kreisnetz Plön dient dem Zweck,

- eine flächendeckende und einheitliche Kommunikationsinfrastruktur für die öffentlichen Verwaltungen im Kreis Plön herzustellen,
- Daten zwischen den angeschlossenen Verwaltungen elektronisch in einem einheitlichen Verfahren sicher und datenschutzkonform zu übermitteln,
- durch die einheitliche Anschlusstechnik und flächendeckende Verfügbarkeit übergreifende Verwaltungsprozesse im Kreis Plön sicherzustellen und
- eine Kommunikationslösung und die damit verbundenen Prozesse einfach, beherrschbar und wirtschaftlich anzubieten.

Alle kreisangehörigen Kommunen sind an dieses Kreisnetz angeschlossen. Zurzeit gibt es zwischen der Kreisverwaltung und den Kommunen über 150 Dienstleistungsvereinbarungen über die Nutzung von Services, die das Kreisnetz Plön als Netzinfrastruktur voraussetzen. Dazu zählt die Möglichkeit, dass jede Kommune über das Kreisnetz Plön zentral installierte Anwenderprogramme des Kreises nutzen kann.

Im Auditverfahren wurde die Umsetzung der im Sicherheitskonzept festgelegten **Sicherheitsmaßnahmen** festgestellt. Die Praxistauglichkeit der für das Kreisnetz Plön erstellten Dokumentation wird durch den ordnungsgemäßen Betrieb des Netzes bestätigt. Die Leitungsebene ist sensibilisiert und übernimmt Aufgaben und Pflichten für die Informationssicherheit im Rahmen des von ihr eingerichteten Sicherheitsmanagements.

Das Kreisnetz Plön zeichnet sich durch folgende **datenschutzfreundliche Aspekte** aus:

- Mit dem Einsatz von Sicherheitsfunktionen **(MPLS-Technologie**) und der Einrichtung **redundanter Netzkomponenten** von T-Systems werden während des Transports der Daten über das Kreisnetz die Verfügbarkeit, Vertraulichkeit und die Integrität sowie die Ordnungsmäßigkeit der Datenverarbeitung hinreichend gewährleistet.
- Die Kreisverwaltung stellt sicher, dass die im Kreisnetz Plön eingesetzten **Übergaberouter** nach den Kommunikationsparametern der Kommunen ordnungsgemäß administriert werden.
- Sicherheitsrelevante Ereignisse können über den Einsatz eines **Überwachungsservers** von den Administratoren der IT-Abteilung der Kreisverwaltung Plön und von den Administratoren der Kommunen rechtzeitig erkannt und ausgewertet werden.
- Die technischen und organisatorischen Abläufe im Kreisnetz werden in der **Kreisnetzdokumentation** vollständig beschrieben.

Was ist zu tun?
Die vom Kreis Plön für die Kreisnetznutzer entwickelten Netzkontrollinstrumente sind praxistauglich und sollten als Sicherheitsstandard festgelegt und für alle anderen Verwaltungs- und Behördennetze eingesetzt werden.

9.1.7 Kreise Nordfriesland und Schleswig-Flensburg

Die Kreise Nordfriesland und Schleswig-Flensburg beabsichtigen, ihre IT-Abteilungen in einem gemeinsamen Kommunalunternehmen in Gestalt einer Anstalt des öffentlichen Rechts zusammenzuführen. Der „neue" IT-Servicebetrieb hat das ULD beauftragt, in zwei Auditverfahren die Konzeption der Zusammenlegung der IT-Abteilungen und das von ihm betriebene Kommunikationsnetz Nord (KKN) zu auditieren.

Das gemeinsame Kommunalunternehmen soll einen umfassenden IT-Service für die beiden Kreise bereitstellen und bedarfsgerechte Dienstleistungen gegenüber dem kreisangehörigen Raum beider Kreise vorhalten (Tz. 6.2).

- **Audit „Konzeption gemeinsamer IT-Servicebetrieb"**

Wenn zwei IT-Abteilungen zusammengelegt werden sollen, dann stehen **konzeptionelle Fragestellungen** im Vordergrund; Personalressourcen müssen gebündelt und strategische Entscheidungen über die zukünftige Hard- und Sofwarearchitektur getroffen werden. Darunter fallen z. B.

- die Vereinheitlichung der in beiden Kreisverwaltungen eingesetzten **Verzeichnisdienste** (Microsoft Active Directory oder Novell eDirectory) als Basis für eine übergreifende Client-Server-Kommunikation,
- der **mandantenfähige Ausbau** der in den Abteilungen der Kreisverwaltungen genutzten Fachverfahren,
- die **Auslastung und Dimensionierung** von Servern und Netzen,
- der Einsatz eines einheitlichen **Dokumentenmanagements**,
- die einheitliche Anbindung an das **Internet und** an das **Landesnetz**,
- die flächendeckende Bereitstellung von **Services für die kreisangehörigen Kommunen** sowie
- der Betrieb eines flexiblen und sicheren **Kommunikationsnetzes** für die zu betreuenden Kommunen und sonstigen Stellen.

Um sicherzustellen, dass die Neugestaltung der Technik auch den datenschutzrechtlichen und sicherheitstechnischen Anforderungen nach dem Stand der Technik entspricht, will der IT-Servicebetrieb **sein Konzept durch das ULD auditieren** lassen. Das Verfahren soll 2008 abgeschlossen werden.

- **Audit „Kommunikationsnetz Nord (KKN)"**

Mit der Vereinheitlichung der IT-Infrastruktur durch die Bündelung von Hard- und Softwareressourcen sind die Kreisverwaltungen auf eine funktionierende und sichere Kommunikation angewiesen. Das **Kommunikationsnetz Nord** – so der Name dieses Netzes – soll über eine einheitliche Anschlusstechnik eine flächendeckende Verfügbarkeit übergreifender Verwaltungsprozesse sicherstellen. Ferner

soll es eine definierte Kommunikationslösung mit einfachen, beherrschbaren und wirtschaftlichen Prozessen anbieten. Folgende Rahmenbedingungen sind gegeben:

- Der IT-Servicebetrieb ist Betreiber des Kommunikationsnetzes Nord (KKN) und für alle Betriebs- und Datensicherheitsaspekte verantwortlich.
- Der IT-Servicebetrieb ist alleiniger Ansprechpartner für die an das KKN angeschlossenen Teilnehmer.
- Das KKN wird auf der Plattform des Kommunikationsnetzes Schleswig-Holstein der Firma T-Systems betrieben.
- Die Teilnehmer (Kreisverwaltungen, Kommunen und Sonstige) schließen für den Anschluss an das KKN mit dem IT-Servicebetrieb einen sogenannten Anschlussvertrag ab.
- Auf der Grundlage des Anschlussvertrages schließen die Teilnehmer Nutzungsvereinbarungen mit dem IT-Servicebetrieb über die bei ihm bezogenen Leistungen ab.

Für den IT-Servicebetrieb hat das KKN eine große Bedeutung. Es ist die Basis für die mit der Zusammenlegung der Rechenzentren beider Kreise entstehenden Kommunikationsprozesse. Das Audit soll sicherstellen, dass das KKN seinen Teilnehmern eine ausreichende **Verfügbarkeit und die Sicherheit der übertragenen Daten** gewährleisten kann. Der IT-Servicebetrieb wird hierfür die von der Kreisverwaltung Plön implementierten mustergültigen Netzkontrollinstrumente einsetzen (Tz. 9.1.6).

Was ist zu tun?
Die Zusammenlegung der Datenverarbeitung von zwei Kreisen erfordert eine gut vorbereitete Konzeption. Veränderungen in der Hard- und Softwarearchitektur sind unter Einbeziehung der fachbereichspezifischen und datenschutzrechtlichen Vorschriften durchzuführen.

9.1.8 Christian-Albrechts-Universität

Das ULD hat mit der rechtswissenschaftlichen Fakultät und dem Rektorat der Christian-Albrechts-Universität zu Kiel (CAU) ein Audit zur automatisierten Verarbeitung von Studierendendaten begonnen.

Nach einem erfolgreichen Start Anfang 2007 ist das Auditverfahren nach der Bestandsaufnahme in einen **Ressourcenengpass der CAU** gerutscht. Das Audit war kurz vor der Umstellung auf die Bachelor-Studiengänge des Fachbereiches gestartet. Die geringe Personaldecke zur Durchführung der Umstellung führte vor allem in der zentralen EDV-Verwaltung zu einer Verzögerung der Bearbeitung. Dennoch konnten erste Verbesserungen, deren Dringlichkeit die Bestandsaufnahme deutlich gemacht hatte, eingeleitet werden. Erklärter Wille der Beteiligten ist es, das Auditverfahren 2008 erfolgreich zu beenden. Die ersten Voraussetzungen sind von der CAU durch einen neuen **Ressourcenplan** geschaffen worden.

Was ist zu tun?
Die festgelegten Maßnahmen zur Mängelbehebung müssen von der CAU jetzt priorisiert umgesetzt werden.

9.1.9 Begutachtung des Online-Portals der IKK-Direkt

Die IKK-Direkt beauftragte uns, sie hinsichtlich des Login-Bereichs ihres Online-Portals zu beraten. Aus datenschutzrechtlicher Sicht konnten wir einige Verbesserungshinweise geben.

Obwohl die Gebäude der IKK-Direkt in Kiel in Sichtweite des ULD liegen, sind für die Datenschutzaufsicht nicht wir, sondern der Bundesbeauftragte für den Datenschutz und Informationsfreiheit (BfDI) in Bonn zuständig. Daher konnten wir auf die Anfrage nach einer Überprüfung des Login-Verfahrens des Online-Portals kein förmliches Datenschutz-Audit durchführen, wohl aber eine **beratende Begutachtung**. Als Ergebnis war somit kein werbewirksames Datenschutzauditzeichen, wohl aber die Mitteilung möglich, dass das Datenschutzkonzept der Registrierung aus unserer Sicht in Ordnung ist.

Die IKK-Direkt ist eine Krankenkasse ohne Filialnetz. Für ihre Kundinnen und Kunden ist die Kontaktaufnahme per Telefon oder Internet besonders wichtig. Auf ihrem Online-Portal stellt sie einen **persönlichen Bereich** zur Verfügung, in dem sich Versicherte nach Eingabe von Versichertennummer und Passwort vor allem Formulare herunterladen, Leistungsanträge abgeben oder Adressen ändern können. Auch Arbeitgeber können auf diese Weise mit der IKK-Direkt Kontakt aufnehmen und so Meldungen und Beitragsnachweise bearbeiten. Diese Funktionalitäten waren nicht Gegenstand der Begutachtung, sondern lediglich das Konzept des Registrierungsverfahrens, mit dem sich Nutzer per Webformular einen Zugang für den persönlichen Bereich freischalten lassen können. Hierzu ist die Eingabe von Adressdaten und Versichertennummer erforderlich, die mit der versicherungsinternen Datenbank abgeglichen werden. Danach wird dem Nutzer postalisch ein Passwort übermittelt – oder bei fehlgeschlagener Registrierung eine E-Mail zugesandt. Im Rahmen unserer Begutachtung konnten wir feststellen, dass es aus Datenschutzsicht nach Umsetzung einiger kleiner Verbesserungsvorschläge **keine Einwände** gegen das Identifizierungsverfahren gibt.

Was ist zu tun?
Auch wenn aus formalen Gründen eine Auditierung nach dem LDSG nicht infrage kommt, können wir im Rahmen von kostenpflichtigen Beratungen Konzepte und Verfahren begutachten.

9.1.10 Wirtschaftsförderung Lübeck

Die Wirtschaftsförderung Lübeck GmbH entwickelt eine neue Software zur Förderung von Wirtschaftsbetrieben. Da in den Datenbanken auch sensible Geschäftsdaten gespeichert werden sollen, wurden wir mit einer Begutachtung des Softwarekonzeptes beauftragt.

Das neue **Informations- und Managementsystem** der Wirtschaftsförderung Lübeck GmbH verfügt über Funktionen zur Unterstützung der Wirtschaftsförderung in der Hansestadt. Dazu gehören neben Datenbeständen über Firmen, Umsatzzahlen, Mitarbeiter usw. auch eine Börse für Gewerbeimmobilien, Werkzeuge für die Bestimmung und Visualisierung von Branchenbeziehungen und Clustern sowie ein Ticketsystem, mit dem Anfragen und Beratungen verwaltet und dokumentiert werden können. Das Projekt wird durch das Land Schleswig-Holstein im Rahmen des Ziel-2-Programmes mit Mitteln der EU gefördert. Der Wunsch des Förderers war es, schon in der Konzeptphase sicherzustellen, dass die Software datenschutzgerecht erstellt wird.

Inhaltlich scheinen die Firmendaten nicht besonders brisant – sind sie doch gegen Bezahlung von Wirtschaftsauskunfteien relativ einfach zu erlangen. Spannend wird aber die Gesamtsicht aller Funktionalitäten: Die Adressdaten werden mit **Geokoordinaten** (Tz. 8.14) versehen, die eine geografische Analyse, z. B. zur räumlichen Branchenverteilung, erleichtern. Die Zulieferbeziehungen können auf diese Weise erfasst werden. Anfragen und Beratungen betreffen nicht nur die Förderung gesunder Unternehmen, sondern auch die Hilfe für Not leidende Firmen. Solche Informationen müssen selbstverständlich vertraulich behandelt werden.

> **? *Geokoordinaten***
>
> *Jeder Ort auf der Erde lässt sich über Geokoordinaten eindeutig beschreiben. Dazu werden verschiedene Koordinatensysteme verwendet, z. B. Längen und Breitenangaben in der Schifffahrt (Grad, Minuten, Sekunden) oder Gauß-Krüger-Koordinaten in der Landvermessung. Mithilfe von Geokoordinaten lassen sich räumliche Analysen, Abstände, Nachbarschaftsbeziehungen usw. leichter analysieren als über Adressdaten wie Straßennamen und Hausnummern.*

Die Software wurde **mandantenfähig** entwickelt und kann nach Fertigstellung auch anderen Wirtschaftsförderungsorganisationen zur Verfügung gestellt werden, sodass nicht nur der Raum Lübeck hiervon profitiert. In einigen wenigen Teilbereichen konnten wir Verbesserungen vorschlagen, die z. B. die Archivierung von Altfällen, die Mandantenadministration und die Protokollierung von Zugriffen betrafen. Derzeit befindet sich die Software in der Umsetzungsphase.

Was ist zu tun?
Unternehmen, die komplexe Softwareprodukte planen, und Förderer, die solche Entwicklungen unterstützen, sollten sich schon frühzeitig datenschutzrechtlich beraten lassen bzw. für eine solche Beratung sorgen, um Fehlentwicklungen rechtzeitig kosten- und zeitsparend zu vermeiden.

9.2 Datenschutz-Gütesiegel

9.2.1 EuroPriSe (European Privacy Seal)

Das erfolgreiche schleswig-holsteinische Datenschutz-Gütesiegel wird europäisch. Erstmalig führt das ULD ein Konsortium mit namhaften Partnern aus acht europäischen Ländern zur Einführung eines europäischen Datenschutz-Gütesiegels unter dem Namen EuroPriSe (European Privacy Seal).

Das vom ULD geleitete Projekt zur Marktevaluierung und zur Vorbereitung der **Markteinführung eines europäischen Datenschutz-Gütesiegels** wird im Rahmen des eTEN-Programms von der EU über eine Laufzeit von 18 Monaten mit 1,3 Millionen Euro gefördert. Neben dem ULD als Konsortialführer sind an dem Projekt die spanische Datenschutzbehörde APDCM von Madrid, die nationale französische Datenschutzbehörde CNIL, das Institut für Technikfolgenabschätzung der Österreichischen Akademie der Wissenschaften, das Institut für Menschenrechte der Metropolitan Universität in London, der TÜViT aus Deutschland, VaF aus der Slowakei, Borking Consultancy aus den Niederlanden und Ernst & Young, Schweden, beteiligt.

Ziel des im Juni 2007 gestarteten Projektes ist die Anpassung des schleswig-holsteinischen Gütesiegels an die faktischen und rechtlichen Rahmenbedingungen in der Europäischen Union (EU). Das europäische Datenschutz-Gütesiegel (European Privacy Seal) basiert auf dem in Schleswig-Holstein durchgeführten und bewährten Verfahren, in dem das ULD die zentrale Aufgabe der Qualitätssicherung wahrnimmt. In einem ersten Arbeitspaket wurden das schleswig-holsteinische Gütesiegelverfahren und seine Prüfkriterien an die europäischen Anforderungen angepasst. Die Anerkennungskriterien wurden im Rahmen des Projektes um eine europäische Komponente erweitert. Grundlage ist die **Europäische Datenschutzrichtlinie** mit deren Umsetzung in den nationalen Datenschutzgesetzen.

Fachkundige internationale Gutachter prüfen in einem Assessment IT-Produkte und IT-Dienstleistungen auf ihre Vereinbarkeit mit den EuroPriSe-Kriterien und erstellen Gutachten. **Unabhängige Behörden** prüfen die Gutachten nach dem Vieraugenprinzip auf Vollständigkeit und Plausibilität und verleihen das EuroPriSe-Zertifikat. Während des Projektlaufes werden das ULD und die spanischen Kollegen aus Madrid das europäische Datenschutz-Gütesiegel verleihen.

Ein zweites Arbeitspaket sieht die internationale **Anerkennung von Sachverständigen** vor. Voraussetzungen für die Anerkennung sind der Nachweis der Fachkunde und Zuverlässigkeit sowie das Verfassen eines Trainingsgutachtens für ein fiktives Produkt. Der erste EuroPriSe-Expertenworkshop fand mit über 80 Teilnehmern aus 13 EU-Ländern im November 2007 in Wien statt.

EuroPriSe eröffnet Herstellern und Anbietern von IT-Produkten und -Dienstleistungen die Möglichkeit, ihre Produkte in **Pilotverfahren** zertifizieren zu lassen. Interessierte Hersteller konnten sich in einer ersten Runde bis Ende Februar 2008 um die Teilnahme im Pilotverfahren bewerben.

Das Projekt findet seit seinem Start hohe **internationale Beachtung** und wurde auf der 29. Internationalen Konferenz der Datenschutz- und Informationsfreiheitsbeauftragten in Montreal, Kanada, dem European Privacy Officers Forum in Brüssel sowie auf einem Symposium über Internationale Datenschutzgütezeichen in Tokio, Japan, vorgestellt. Eine Delegation der polnischen Datenschutzbehörde informierte sich in Kiel umfassend über das schleswig-holsteinische und das europäische Gütesiegel. Eine Delegation des Ungarischen Datenschutzbeauftragten nahm am Expertenworkshop in Wien teil.

Für interessierte Hersteller wurde eine Informationsbroschüre in englischer Sprache erstellt, die beim ULD erhältlich ist. **Informationen zum Projekt** für Bürger, Sachverständige und Hersteller befinden sich auch im Internet in deutscher und englischer Sprache unter

www.datenschutzzentrum.de/europrise.htm
www.european-privacy-seal.eu

Was ist zu tun?
Hersteller und Anbieter von IT-Produkten und -Dienstleistungen sind auf die Möglichkeit des europäischen Datenschutz-Gütesiegels hinzuweisen. Die Verbreitung des Siegels auf einem hohen einheitlichen europäischen Niveau ist fortzuführen. Hierfür ist die Kooperation mit den europäischen Partnern aus dem Bereich Datenschutz, insbesondere mit der Art. 29-Datenschutzgruppe, zu intensivieren.

9.2.2 Internationale Entwicklungen im Gütesiegelbereich

Die Umsetzung von Gütesiegelverfahren schreitet auch im Ausland voran.

Mit der **polnischen Datenschutzaufsicht** gab es intensive Gespräche über unsere Zertifizierungsverfahren. Die Kontakte mit der staatlichen Universität Tsukuba in Tokio und dem japanischen System „Privacy Mark“ (29. TB, Tz. 9.2.5) wurden im Rahmen des EuroPriSe-Projektes (Tz. 9.2.1) intensiviert.

In der **Schweiz** wurde im September 2007 mit einer Verordnung das Verfahren der Datenschutzzertifizierung konkretisiert. Der Eidgenössische Datenschutzbeauftragte wird darin beauftragt, inhaltliche Kriterien für eine Zertifizierung von Datenschutzmanagementsystemen und von IT-Produkten vorzulegen. Diese Prüfungen lassen sich mit den Ansätzen aus Schleswig-Holstein vergleichen.

Derzeit befindet sich ein Vorschlag für Prüfkriterien für Datenschutzmanagementsysteme in der Anhörung, danach folgen Kriterien für IT-Produkte. In der Verordnungsbegründung wird explizit darauf hingewiesen, dass eine Orientierung an den **Kriterien aus Schleswig-Holstein** möglich ist. Dies wäre sinnvoll; die im Verordnungstext genannten Produktanforderungen Datensicherheit, Datenvermeidung, Transparenz und technische Unterstützung der Anwender bei der Einhaltung weiterer Datenschutzgrundsätze sind genau diejenigen, die auch die schleswig-

holsteinische Datenschutzauditverordnung (DSAVO) nennt. Es erfolgt diesbezüglich ein Austausch mit den Schweizer Kollegen.

Was ist zu tun?
Die grenzüberschreitende Koordination von Gütesiegelverfahren muss ausgebaut werden, damit Inhaber des schleswig-holsteinischen Gütesiegels mit ihren Produkten Erleichterungen bei der Zertifizierung in anderen Staaten haben.

9.2.3 Abgeschlossene Gütesiegelverfahren

Das ULD konnte 2007 wieder zahlreichen Produkten ein Datenschutz-Gütesiegel verleihen. Die Zahl der Neuzertifizierungen wie der Rezertifizierungen hat deutlich zugenommen. Es wurden elf Produkte erstmalig zertifiziert. Neun weitere Produkte wurden nach Fristablauf der ersten Zertifizierung in einem vereinfachten Verfahren rezertifiziert.

Das **gestiegene Interesse** der Hersteller an Rezertifizierungen zeigt, dass das Gütesiegel den Herstellern einen echten Wettbewerbsvorteil bietet, der gesichert werden soll. Für 2008 haben sich schon einige namhafte Hersteller für Zertifizierungen angekündigt.

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

- Microsoft Update Service (Version 6.0) und Windows Server Update Service (Version 2.0): Bereitstellung und Abruf von Updates und Upgrades für Microsoft-Produkte,
- Easypark (Stand: 28. Februar 2007): Bezahlung von Parkgebühren über das Mobiltelefon,
- Vernichtung von Akten und Datenträgern im Vor-Ort-Verfahren durch die Shred-it GmbH (Stand: 15. Januar 2007),
- DIBIKO mit Fotokabine VC 100 und DIBIKO Small Business (Stand: Juli 2007): digitale Bildintegration für Kommunen mit und ohne Fotokabine,
- Altersüberprüfung durch Einlesen des Personalausweises oder des Führerscheins (Stand: 2. Juli 2007),
- OPEN/PROSOZ (Version 3.1, Release 2): Dialogsystem für den Einsatz im Bereich der sozialen Sicherung,
- ePharm (Version 1.0): Realisierung einer telematischen Kommunikationslösung für das Gesundheitswesen,
- Windows Genuine Advantage – WGA (Version 1.7): Service zur Feststellung, ob eine Windows XP-Installation genuin ist,
- Predictive Targeting Networking durch die nugg.ad AG (Version 2.0): Generierung von statistischen Annahmen aus Nutzungsinformationen,

- Elefant Profi (Version 8.01): Verwaltungsprogramm für psychotherapeutische und ärztliche Praxen,
- KOMBOSS – verschiedene Module (Version 2.8.3.5): Unterstützung von Kommunen und öffentlichen Stellen in den Bereichen Personalwesen, zentrale Verwaltung und Organisation.

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

- LN-Card (Stand: 21. November 2006): Bonuskarte für Abonnenten der Lübecker Nachrichten,
- VISOR (Version 2.0): Software zur Online-Prüfung von PCs im Hinblick auf Sicherheitslücken,
- PROSOZ/S für Windows: Dialogverfahren zur Erfassung von Sozialhilfedaten, Berechnung rechtlicher Ansprüche, Fallmanagement und Ausgabe entsprechender Bescheide direkt am Arbeitsplatz,
- PrimeSharing TeamDrive (Version 1.3): Kollaborationstool für den Zugriff mehrerer Benutzer auf einen verschlüsselten Datenbestand zur gemeinsamen Bearbeitung von Dokumenten,
- e-pacs Speicherdienst (Version 3.0): elektronische externe Archivierung von Röntgenbildern und anderen patientenbezogenen medizinischen Daten,
- ALLRIS (Version 3.8): Ratsinformationssystem für den kommunalen Sitzungsdienst, mit dem Sitzungen vor- und nachbereitet sowie Informationen hierüber entsprechend abgestuft Amtsangehörigen, Ratsangehörigen und Bürgern zugänglich gemacht werden können,
- MBS-easy (Version 3.6.0.0): Softwareapplikation für die Aufnahme, weitere Verarbeitung und Verwaltung von digitalen ärztlichen Diktaten,
- Verfahren zur Vernichtung von Akten und Datenträgern durch die Lutz von Wildenradt GmbH im Auftrag für öffentliche und nicht öffentliche Stellen (Stand: Oktober 2007),
- Vernichtung von Akten und Mikroformen gem. DIN 32 757 Sicherheitsstufe V aus von der Akten- und Datenträgervernichtung Zentrale Nord GmbH (AVZ) Kunden zur Verfügung gestellten verschlossenen Containern.

Insbesondere in Folge der Zertifizierung der beiden Microsoft-Produkte war eine merkliche Zunahme von Anfragen zum Gütesiegel zu verzeichnen, was sich voraussichtlich auf die Zertifizierungen 2008 auswirken wird. Der Start des Projekts EuroPriSe (Tz. 9.2.1) verstärkte die Nachfrage von Interessenten. Die weite Streuung der zertifizierten Produkte aus den unterschiedlichsten Bereichen der Datenverarbeitung – vom Parken mit Handybezahlfunktion über Fotokabinen bis hin zu Online-Werbung – zeigt, dass Datenschutz ein Thema ist, das überall relevant werden kann. Der vertrauenswürdige Umgang mit Daten wird nicht mehr als notwendiges Übel, sondern als eine Möglichkeit gesehen, bei den Nutzern eine Marktbindung zu erreichen. Die **auf Qualität ausgerichtete Ausgestaltung** des

Gütesiegelverfahrens, bei dem die Gutachten der Sachverständigen durch das ULD als unabhängige staatliche Stelle auf ihre Richtigkeit hin geprüft und zertifiziert werden, wird von den Herstellern, mit denen wir im Gespräch sind, als sehr wichtig angesehen.

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. Wir werden generell und speziell im Projekt EuroPriSe mit anderen Stellen zusammenarbeiten, um Synergien zu nutzen und interessierte Hersteller umfassend zu beraten.

9.2.4 Gütesiegel für Microsoft und deren Auswirkungen

2007 wurden vom ULD zwei Gütesiegel an die Firma Microsoft verliehen. Diese betrafen zum einen den Microsoft Updateservice (MU) und Windows Server Update Service (WSUS) und zum anderen Windows Genuine Advantage (WGA). Beide Gütesiegel haben weitreichendes Echo in der Presse gefunden und das Interesse der Industrie am Gütesiegel merklich gesteigert.

Die Übergabe des Gütesiegels für MU 6.0 und WSUS 2.0 erfolgte im Februar 2007 in der Landesvertretung von Schleswig-Holstein in Berlin durch Ministerpräsident Peter Harry Carstensen (29. TB, Tz. 9.2.2). Das Gütesiegel für WGA Version 1.7 folgte im September 2007 bei einer Zeremonie in Unterschleißheim bei München. Mit diesem Produkt wird die Gültigkeit einer **Lizenz von Windows XP überprüft**, indem u. a. die Lizenznummer mit den bei Microsoft gespeicherten freigegebenen Nummern abgeglichen wird. Stellt sich hierbei heraus, dass keine gültige Lizenz vorliegt, bietet WGA dem Nutzer verschiedene Wege an, eine entsprechende Lizenz zu erwerben. Die Installation von WGA ist unter Windows XP freiwillig. Sie wird aber notwendig, wenn nicht sicherheitsrelevante Updates eingespielt werden sollen. Sicherheitskritische Updates werden auch ohne WGA-Prüfung bereitgestellt. Mit WGA soll – in datenschutzkonformer Weise – die Verbreitung von Raubkopien eingedämmt und dem Nutzer die Möglichkeit eröffnet werden, die Gültigkeit seiner Lizenz zu überprüfen.

Die Gutachter der Prüfstellen haben untersucht, welche Daten im Rahmen von WGA vom Rechner des Nutzers an Microsoft übermittelt werden und wie diese bei Microsoft verarbeitet werden. Dabei wurde festgestellt, dass zwar Daten zur Identifizierung des Rechners übertragen werden, deren Personenbeziehbarkeit aber durch den Einsatz unterschiedlicher Hash-Verfahren und durch organisatorische Festlegungen innerhalb der Microsoft Corporation unterbunden wird, sodass auch im Nachhinein **keine Identifizierung von Nutzern** durch Microsoft möglich ist.

Im Rahmen beider Microsoft-Zertifizierungen konnten für die Produkte Verbesserungen hinsichtlich des Datenschutzes erreicht werden. Nach der Verleihung beobachten wir natürlich die Entwicklung und **Diskussion** um die mit dem Gütesiegel ausgezeichneten Produkte kritisch weiter. Dabei stießen die Verfahren in der Öffentlichkeit nicht nur auf Zustimmung. Ein Großteil der Kritik beruhte auf Missverständnissen hinsichtlich der konkreten Verfahren. Wir nehmen aber jede Kritik ernst und überprüfen die entsprechenden Aussagen. Unser Zertifizierungsverfahren beruht auf der Idee der Transparenz, was sich insbesondere in der Notwendigkeit der Veröffentlichung eines aussagekräftigen Kurzgutachtens zeigt.

Die Microsoft-Gütesiegelverfahren haben das **Interesse zahlreicher Hersteller** von IT-Produkten aus dem In- und Ausland geweckt mit der Folge einer zunehmenden Zahl von Anfragen. Dies ändert nichts daran, dass sich das Gütesiegel auch in Zukunft an mittelständische Hersteller richtet. Das breite Angebot zur Auswahl der Sachverständigen und moderate Zertifizierungskosten des ULD gewährleisten, dass ein Gütesiegelverfahren für die meisten Unternehmen realisierbar ist. Das Gütesiegel bietet gerade auf umstrittenen Märkten die Chance, sich von der Konkurrenz positiv abzugrenzen. Aber auch für große Unternehmen wird die Bedeutung des Datenschutzes und das Interesse an einer Profilierung durch qualifizierte Zertifikate zunehmen.

Die Kurzgutachten zu den Gütesiegeln befinden sich im Internet unter

www.datenschutzzentrum.de/guetesiegel/register.htm

Was ist zu tun?
Weiterhin zielt das ULD darauf ab, neben den Großkonzernen vor allem auch innovative kleine und mittelständische Unternehmen anzusprechen.

9.2.5 Sachverständige

Das Verfahren zur Anerkennung von Sachverständigen und Prüfstellen für das Gütesiegelverfahren brachte viele neue Akkreditierungen.

Beim Gütesiegelverfahren erfolgt die Begutachtung der zu zertifizierenden Produkte durch beim ULD anerkannte Datenschutzsachverständige. Anerkennungen erfolgen für den Bereich Recht oder den Bereich Technik. Bei entsprechender **Qualifikation** ist eine Doppelzulassung möglich. Auch ganze Prüfstellen können zugelassen werden. Voraussetzungen einer Anerkennung sind stets neben Zuverlässigkeit und Unabhängigkeit der Nachweis der erforderlichen Fachkunde, insbesondere in Bezug auf den Datenschutz.

2007 wurden folgende Sachverständige akkreditiert:

- Sachverständiger Jörg Deusinger (Technik),
- Sachverständiger Dipl.-Inf. Michael Westermann (Technik),

- Sachverständiger Dipl. Ing. (FH) Wolfgang Neudörffer (Technik),
- Sachverständiger Rechtsanwalt Dr. Fritjof Börner (Recht).

Inzwischen sind beim ULD 29 Einzelsachverständige **registriert**, 13 Sachverständige für Recht, 11 für Technik, fünf für beide Bereiche. Hinzu kommen sieben Prüfstellen, zwei für Recht, drei für Technik und zwei für Technik und Recht.

Die Sachverständigen sind verpflichtet, im Abstand von jeweils drei Jahren nach dem Datum der Anerkennung **Nachweise** über die Wahrnehmung von Fortbildungen und zum Erfahrungsaustausch beizubringen. Zahlreiche Sachverständige sind bereits seit mehr als drei Jahren anerkannt und haben die entsprechenden Nachweise vorgelegt.

Ende August 2007 fand der jährliche **Gutachterworkshop** in Kiel statt. Diese Möglichkeit des Erfahrungsaustausches nutzten 14 Sachverständige. Diskutiert wurden Erfahrungen mit Neu- und Rezertifizierungen, Fragen des Marketings des Gütesiegels wie auch Möglichkeiten der Internationalisierung. Ein Schwerpunkt war die Vorstellung des Europäischen Gütesiegels „EuroPriSe“ und die Diskussion über die Einbindung der Gutachter in das Projekt (Tz. 9.2.1).

Weitere Informationen für Sachverständige finden sich im Internet unter

www.datenschutzzentrum.de/guetesiegel/akkreditierungsunterlagen.htm

Was ist zu tun?
Die Sachverständigen sind ein wichtiger Faktor für den Erfolg des Gütesiegels. Daher unterstützen wir sie bei ihrem Ziel, neue Produkte für das Gütesiegelverfahren zu gewinnen.

9.2.6 Zulassung von Prüfstellen

Die Voraussetzungen zur Zulassung von Sachverständigen und Prüfstellen wurden überarbeitet. Dies war notwendig, um den geänderten Interessen der Gutachter gerecht zu werden.

Neben kleineren formalen Änderungen, z. B. müssen künftig keine Gesichtsfotos beigelegt werden, betraf die Überarbeitung insbesondere die Zulassungsvoraussetzungen von Prüfstellen. Bisher konnte nur ein **Leiter der Prüfstelle** vom Antragsteller benannt werden. Dieser musste die notwendige Fachkunde der Prüfstelle in sich vereinigen. War der Leiter nur in einem der Bereiche Recht oder Technik fachkundig, so konnte die gesamte Prüfstelle nur hinsichtlich dieser Fachkunde zugelassen werden. Nach Überarbeitung ist es nunmehr möglich, zwei Leiter mit unterschiedlicher Fachkunde zu benennen, die jeweils für ihren Bereich verantwortlich sind. Dies erleichtert in fachlich sinnvoller Weise den Zugang zum Markt. Diese Änderung geht auf Wünsche anerkannter Sachverständiger zurück. Erste Anträge mit Doppelleitung liegen bereits vor.

Die Antragsunterlagen für Sachverständige befinden sich im Internet unter

www.datenschutzzentrum.de/guetesiegel/akkreditierung.htm

Was ist zu tun?
Das ULD ist für Verbesserungsvorschläge bezüglich Gütesiegelverfahren und Gutachteranerkennung offen. Sofern damit die Qualität des Siegels bewahrt oder sogar verbessert werden kann, werden diese gerne berücksichtigt.

9.2.7 Präsentation des Gütesiegels auf Veranstaltungen

Das Gütesiegel stieß auf ein großes öffentliches Interesse und durchgehend auf positive Resonanz.

Viele der Gütesiegelverleihungen fanden im Rahmen öffentlicher Veranstaltungen statt (29. TB, Tz. 9.2.4), z. B. auf der IT-Messe CeBIT 2007 in Hannover bei dem schleswig-holsteinischen Gemeinschaftsstand oder bei der Sommerakademie 2007 in Kiel. Auf diesen Veranstaltungen präsentierten wir dieses proaktive Datenschutzinstrument generell und warben gezielt weitere Interessenten. Bei ihren **Vorträgen und Beratungsgesprächen** wird von ULD-Mitarbeitern und -Mitarbeiterinnen regelmäßig auf das Datenschutz-Gütesiegel hingewiesen. Vor allem im Rahmen des Projektes EuroPriSe (Tz. 9.2.1) wurde das Gütesiegel auch ausländischen Herstellern und Gutachtern nähergebracht.

10 Aus dem IT-Labor

10.1 Patch-Management – eine Selbstverständlichkeit

Die Praxis des Einspielens von Sicherheitsupdates für die Microsoft-Betriebssysteme zeigt vielerorts essenzielle Sicherheitsmängel.

Vor zwei Jahren hat das ULD zur automatisierten Installation von Sicherheitsupdates Ratschläge gegeben (28. TB, Tz. 10.5). Mit dem kostenlos erhältlichen Windows Server Update Service (WSUS) lassen sich nicht nur die Betriebssysteme auf dem aktuellen Stand halten, sondern auch weitere Microsoft-Produkte wie beispielsweise Office oder Visio. Im Mai 2007 hat der Hersteller die aktuelle Version 3.0 freigegeben. Administratoren des Vorgängers WSUS 2.0 können ihre Server einfach aktualisieren, um die Vorteile der neuen Version zu nutzen. Ältere Versionen, wie der Service Update Server (SUS), werden seit Juli 2007 weder unterstützt noch mit Updates beliefert. Zu den Neuerungen gegenüber WSUS 2.0 zählen die bequeme Verwaltung über die Microsoft **Update Management Console**, die E-Mail-Benachrichtigung bei Updates und Fehlern oder neue Statusberichte. Administratoren sollten sich mit der Vielzahl an neuen Möglichkeiten vertraut machen, um effektiver Microsoft-Updates zu verwalten.

Praxisbeispiel eines typischen Einsatzes: Alle Einstellungen für die Microsoft-Updates werden über die **Gruppenrichtlinien** gesteuert. Für einen geordneten Test- und Freigabeprozess ist es entscheidend, die Kontrolle zu behalten, welches System wann welche Updates installiert. Diese Freigaben können über die Managementkonsole leicht erfolgen. Um nicht für jeden Computer einzeln Freigaben erteilen zu müssen, werden Computer zu Gruppen zusammengefasst. Als Beispiel könnte das eine Gruppierung nach Abteilungen sein. Neue Updates sollten zuerst automatisiert auf einer dafür vorgesehenen Testgruppe installiert und getestet werden. In der Praxis hat es sich bewährt, dass die Administratoren die Testgruppe sofort mit allen sicherheitsrelevanten Updates ausstatten. Nicht selten kommt es vor, dass Updates Fehler enthalten und Schaden anrichten oder bestimmte Anwendungen nicht mehr funktionieren. Entsprechende Meldungen werden häufig in der einschlägigen Fachpresse kurz nach Erscheinen eines Updates gemeldet. Daher sollte kurz nach dem sogenannten **Microsoft Patchday** – jeweils der zweite Dienstag oder manchmal auch Mittwoch im Monat – nach entsprechenden Berichten Ausschau gehalten werden.

In der Regel stellen sich auch nach ein paar Tagen Wartezeit keine Probleme ein, sodass die Updates auf die weiteren Computergruppen verteilt werden können. Es hat sich bewährt, die Patches abteilungsweise freizugeben. Dieser Prozess ist mit Angaben zu den Patchnamen und zum Testzeitraum zu dokumentieren, um jederzeit bei Fehlern die Freigabe nachvollziehen zu können. Nebenbei werden über einen solchen gestuften Freigabeprozess auch die **Anforderungen an Test und Freigabe** der Datenschutzverordnung erfüllt.

Was ist zu tun?
In einer vernetzten IT-Umgebung ist die automatisierte Installation von Microsoft-Updates eine notwendige Sicherheitsmaßnahme. Patches sind in speziellen Gruppen zu testen und danach freizugeben. Regelmäßige Berichte zum aktuellen Patchstand aller Server und Clients im Netzwerk vervollständigen das Patch-Management und gewährleisten einen datenschutzkonformen Betrieb.

10.2 Antivirenmanagement

Der Schlüssel für ein erfolgreiches Antivirenmanagement liegt nicht allein in hohen Erkennungsraten der eingesetzten Lösung. Ebenso wichtig ist der nachgewiesene lückenlose Einsatz und die Aktualität der eingesetzten Software.

Das ULD wird regelmäßig um Beratung beim Einsatz und bei der Planung von Antivirenlösungen gebeten. Während die Erkennungsraten bei vielen am Markt erhältlichen Produkten hinreichend gut sind, ist gerade die **zentrale Administration und Konfiguration** für eine Vielzahl von Clients immer noch ein Schwachpunkt. Das ULD hat hierfür die folgenden Erfolgsfaktoren herausgearbeitet:

- Alle relevanten Einstellungen und Berichte müssen an einer zentralen Stelle getätigt werden können; eine Bearbeitung von Einstellungen auf einzelnen Rechnern ist fehlerträchtig und nicht mehr zeitgemäß.
- Alarmierungen müssen an dieser zentralen Stelle auflaufen und dürfen nicht nur dem Endbenutzer angezeigt werden.
- Nicht nur der Status aller mit Antivirensoftware versorgten Geräte muss zentral abrufbar sein, es muss auch zentral festgestellt werden können, welche Geräte im Verwaltungsnetz nicht mit einem aktuellen Virenscanner versehen sind.
- Das Installieren der Antivirensoftware und die Verteilung der üblicherweise tagesaktuellen Updates muss automatisiert erfolgen.

Wegen der aktuellen Bedrohung durch Viren, Würmer und Trojaner ist eine ordnungsgemäße Datenverarbeitung ohne zentrales Antivirenmanagement nur in wenigen untypischen Ausnahmefällen möglich.

Was ist zu tun?
IT-Verantwortliche müssen prüfen, ob sie eine hinreichende zentrale Verwaltung und Kontrolle ihrer Antivirenlösung implementiert haben.

10.3 Sicherheit im lokalen Netz

Die Sicherheit der lokalen, also organisationsinternen Netzwerke entwickelt sich mehr und mehr zum Schwachpunkt von organisationsübergreifenden IT-Verfahren. Im IT-Labor hat das ULD mehrere technische Maßnahmen zur Absicherung getestet. Häufig sind die Bausteine schon vorhanden, man muss sie nur geeignet zusammensetzen.

Die in aktuellen Kommunikationsnetzen verwendeten Protokolle sind im Vertrauen darauf erstellt, dass nur vertrauenswürdige Personen direkten Zugang zum internen Netzwerk einer Organisation haben. Während gegen Angriffe aus anderen Netzwerken, z. B. dem Internet, häufig angemessene Sicherheitsmaßnahmen wie der Einsatz von Firewallsystemen getroffen werden, sind die internen Netze häufig ungeschützt. Das Innentäterszenario, also ein **Angriff von innen**, wird häufig in der Sicherheitskonzeption und Risikoanalyse nicht ausreichend betrachtet.

Durch Designschwächen in den verwendeten Netzwerkprotokollen ist es mit handelsüblichen Rechnern und frei verfügbarer Software oft möglich, ein organisationsinternes Netzwerk mit schon seit Jahren bekannten **Angriffsmethoden** zu kompromittieren. Das hierfür notwendige technische Wissen ist eher gering; den meisten Programmen liegen detaillierte Anleitungen bei. Ein Angreifer kann sowohl Daten passiv mitlesen (Verlust der Vertraulichkeit der Daten) als auch Daten aktiv verändern (Verlust der Integrität der Daten). Selbst wenn diese Angriffe nicht erfolgreich sind, so kann das Netzwerk so stark gestört werden, dass keine Daten mehr abgerufen werden können (Verlust der Verfügbarkeit).

Die beste Wahl zur Absicherung ist die Nutzung von Fachverfahren, die z. B. durch Verschlüsselung eine **Ende-zu-Ende-Sicherheit** aufbauen. Sobald nur die berechtigten Kommunikationspartner, nicht aber der „Mann in der Mitte“ die Daten verarbeiten können, laufen viele Angriffe ins Leere. Ist dies nicht möglich, muss die Sicherheit der lokalen Netzwerke durch technische Maßnahmen erhöht werden.

Durch sogenannte Port-Security und MAC-Filter können die Netzwerkzugänge so abgesichert werden, dass zumindest einfache Manipulationen und der Anschluss von fremden Geräten erschwert werden. Gänzlich verhindern lässt sich der unberechtigte Zugriff hiermit nicht, da die hierfür verwendeten Kennungen (MAC-Adressen) sich einfach und vielfach über direkt im Betriebssystem aufrufbare Methoden verändern lassen (sogenanntes MAC-Spoofing).

Nahezu jedes Netzwerk ist heutzutage unzureichend gegen Angriffe gesichert, die die lokale Zuordnung von Rechneradressen zu Netzwerkanschlüssen am Gerät verändern (sogenannte **ARP-Attacken**). Hiermit ist es möglich, selektiv den Datenfluss zwischen zwei Geräten einzusehen. Dieser Angriff lässt sich nicht

verhindern, jedoch zuverlässig erkennen und sollte sofort als Sicherheitsvorfall behandelt werden. Hierzu ist sowohl freie als auch kommerzielle Software erhältlich, die diese Angriffe erkennt und den IT-Sicherheitsbeauftragten oder Datenschutzbeauftragten benachrichtigt.

Eine wirksame Absicherung des lokalen Netzes gegenüber unerlaubt eingebrachte Fremdgeräte ist eine Geräteauthentifizierung mittels **802.1x**. In einem Verzeichnisdienst sind sämtliche verwendeten und von der Systemadministration freigegebenen Geräte verzeichnet. Beim Anschluss eines Gerätes wird abgefragt, ob das Gerät bekannt und zugelassen ist. Nicht freigegebene Geräte werden zurückgewiesen. Gerade in Verbindung mit dem weitverbreiteten Active Directory und aktueller Netzwerkinfrastuktur kann dies einfach und schnell realisiert werden.

Mehrere uns vorgetragene Anfragen und von uns im Auftrag durchgeführte Penetrationstests zeigen, dass dieses Thema aktueller denn je ist. Bei vielen lokalen Netzen sind immer noch **zusätzliche Sicherheitsmaßnahmen** dringend nötig.

Was ist zu tun?
IT-Leiter müssen prüfen, ob sie z. B. 802.1x in Verbindung mit einem Active Directory einsetzen können. Bei Neubeschaffungen muss darauf geachtet werden, dass die Geräte aktuelle Authentifizierungsmechanismen oder einen verschlüsselten Transport der Daten übers Netzwerk unterstützen.

10.4 Sicherheit bei Netzwerkgeräten

Die Zugänge zu sämtlichen aktiven Komponenten im Netzwerk müssen mit Benutzername und Passwort gesichert werden. Die Sicherheit eines Netzwerkes ist abhängig von der Verwaltung dieser Zugänge. Eine einfache Möglichkeit für eine sichere zentrale Verwaltung bietet sich mit sogenannten AAA-Servern.

Schon in einem kleineren Netzwerk befinden sich Dutzende aktiver Komponenten, z. B. Switches, Router und Firewalls. Diese werden meist einfach per Benutzername und Passwort abgesichert. Häufig stellen wir fest, dass für alle Geräte nur ein **globales Administrationspasswort** eingerichtet wurde, welches zudem noch nie geändert wurde. Gerade bei Geräten wie Firewalls und Switches, die für die Sicherheit im Netzwerk wichtig sind, ist dieses Vorgehen nicht akzeptabel.

Für dieses Problem existiert schon seit längerer Zeit eine sichere, bisher wenig genutzte Alternative. Mithilfe sogenannter AAA-Server (Authentifizierung, Autorisierung und Accounting, auch Triple-A-Systeme genannt) können Benutzer und Berechtigungen an einer **zentralen Stelle für das gesamte Netzwerk** festgelegt werden. In vielen Bereichen leicht zu implementieren ist der Microsoft IAS, der die Benutzerdaten mit dem Active Directory abgleichen kann. Der Aufwand, dedizierte Passwörter und Benutzerdaten zu pflegen, entfällt somit vollständig.

Ein weiterer großer Vorteil von AAA ist die Möglichkeit, administrative Tätigkeiten an der Infrastruktur **vollständig zu protokollieren**. Somit lässt sich jederzeit nachvollziehen, wer sich wann auf welchen Geräten eingeloggt und welche sicherheitskritischen Änderungen durchgeführt hat.

Was ist zu tun?
Über AAA-Server können aktive Komponenten im Netzwerk einfach und sicher verwaltet werden. Auch günstige Geräte unterstützen die Protokolle hierfür seit Langem; teilweise sind AAA-Server kostenlos verfügbar. IT-Verantwortliche sollten diese zusätzlichen Sicherheitsfunktionen nutzen.

10.5 Softwarevirtualisierung

Sicherheit gewinnen und dabei die Effizienz steigern? Diese verlockende Versprechung wird mit der Virtualisierung von Programmen oder ganzen Servern wahr. Software wird dabei in virtuelle Kapseln geschlossen, damit Schädlinge kein allzu großes Unheil anrichten können. Nebenbei kann die Technologie die Arbeit für Administratoren erheblich erleichtern.

Unter Virtualisierung von Software versteht man die logische Trennung eines Programms vom zugrunde liegenden Betriebssystem. Dabei wird das Programm nicht direkt im Betriebssystem ausgeführt, sondern es werden mithilfe einer Abstraktionsschicht alle Zugriffe abgefangen, die das Programm auf das Betriebssystem vornimmt. Eine auf diese Weise virtualisierte Software hat also keinen direkten Zugriff auf die Ressourcen des Computers. Wird dieses Verfahren für ein einzelnes Programm angewandt, spricht man von einer Sandbox. Es lassen sich ganze Betriebssysteme virtualisieren, sodass auf einem einzelnen Rechner mehrere sogenannte „**virtuelle Maschinen**“ laufen können, die allesamt unter der Ägide der Virtualisierungssoftware stehen. Der Vorteil liegt nicht nur in einer erhöhten Sicherheit, sondern auch in der deutlich effizienteren Hardwarenutzung, da auf einem einzigen Computer virtuell mehrere Maschinen laufen können und so die Anschaffung weiterer Hardware vermieden werden kann.

Jüngst hat sich der Markt für Virtualisierungslösungen stark verändert. Sowohl Software für virtuelle Maschinen als auch Sandbox-Programme sind in verschiedensten Ausführungen verfügbar, professionelle Lösungen sind teilweise kostenlos erhältlich. Dabei sind zum Erreichen eines höheren Sicherheitsniveaus vor allem Lösungen zur **Applikationsvirtualisierung** interessant. So kann der Internetbrowser in eine Sandbox eingeschlossen werden. Da sämtliche Zugriffe des Browsers auf das System von der Virtualisierungssoftware abgefangen werden, kann dem Browser eine definierte Rechnerumgebung vorgegaukelt werden. Dabei unterscheidet sich dieser Ansatz grundlegend vom klassischen Berechtigungskonzept, denn dort ist eine verbotene Ressource immerhin sichtbar. In einer virtuellen Umgebung „sieht“ die darin befindliche Applikation hingegen nur genau die Bereiche, auf die sie zugreifen darf – alles andere existiert innerhalb der Sandbox nicht.

In einer idealen Umgebung wären alle Applikationen voneinander abgekapselt, sodass ein Angreifer, der beispielsweise den Browser unter seine Kontrolle bringt, weder Daten noch andere Programme erreichen kann. Angriffe wie auch Softwarefehler würden so stets ausschließlich das jeweilige Programm sowie den dazugehörigen Datenbestand betreffen. In der Praxis ist jedoch eine vollständige Kapselung nicht möglich, z. B. wenn Dokumente sowohl mit der Textverarbeitung bearbeitet als auch mit dem Browser über einen Webmailer verschickt werden sollen. Daher erhalten die gekapselten Programme in der Regel Zugriff auf den gesamten Datenbestand des Rechners. Ein Datenabfluss kann durch Virtualisierung also in der Regel nicht verhindert werden. Trotzdem hebt die Softwarekapselung das allgemeine Sicherheitsniveau; eine komplette Übernahme eines Rechners wird deutlich erschwert. Ein Angreifer, dem es gelingt, eine Applikation zu übernehmen, hat damit lediglich die Kontrolle über die jeweilige Sandbox. Dies ist vor allem im Hinblick auf **Webbrowser** relevant, die ein Hauptangriffspunkt bei vernetzten Computern sind. Werden aktive Inhalte wie JavaScript zugelassen, ist eine Kapselung des Browsers dringend geboten, um das Risiko einer Ausnutzung von Sicherheitslücken zu begrenzen.

Interessant sind auch Virtualisierungslösungen, die Softwarepakete verwalten können. Neben dem Sicherheitsgewinn steht hier der Vorteil einer deutlich **erleichterten Auslieferung und Wartung von Applikationen**. Virtualisierte Anwendungen lassen sich als Paket auf andere Rechner übertragen, auf denen die gleiche Virtualisierungssoftware läuft. Da die virtuellen Umgebungen jeweils immer identisch sind, kann ein Softwarepaket direkt auf Einzel-PCs übertragen werden, ohne dass auf die spezifische Hard- und Software vor Ort Rücksicht genommen werden muss. Eine aufwendige Installation und Konfiguration entfällt, was den Ausrollprozess einfacher und effizienter macht. Änderungen an der Konfiguration oder umfassende Softwareupdates lassen sich so zentral vorbereiten und bei Bedarf auf die einzelnen Rechner übertragen.

Was ist zu tun?
Unter den Aspekten Sicherheit und Effizienz stellt Virtualisierung von Servern und einzelnen Applikationen eine interessante Lösung dar. Internetanwendungen sollten nach Möglichkeit in einer Sandbox gekapselt werden, vor allem wenn aktive Inhalte zugelassen werden.

10.6 Google Text und Tabellen

Internetdienste bieten neuerdings Online-Anwendungen, die den heimischen PC beinahe überflüssig machen. Dokumente lassen sich direkt im Browser auf Servern im Internet bearbeiten. Keine Software muss installiert werden, und die Dokumente sind an jedem Internetanschluss verfügbar.

Eine relativ neue Spielart des viel beschworenen „Web 2.0“ stellen klassische Anwendungsprogramme dar, deren Arbeit nun auf das Internet übertragen wird. Unter dem Begriff „**Software-as-a-Service**“ werden solche Dienste vermarktet. Anwendungen laufen nicht mehr auf dem lokalen PC des Nutzers, sondern werden

vom Serviceanbieter in Form einer leistungsfähigen Webseite bereitgestellt und beim Nutzer im Internetbrowser angezeigt. Office-Anwendungen wie Textverarbeitung und Tabellenkalkulation sind die prominentesten Beispiele, aber auch umfangreiche Bildbearbeitung ist so möglich. Dokumente online zu bearbeiten und zu speichern, um jederzeit von jedem Rechner darauf zugreifen zu können, klingt für viele Nutzer verlockend.

Auch Google fand die Idee reizvoll und erwarb Anfang 2006 die **Online-Textverarbeitung** Writely. Inzwischen ist der Dienst unter dem Namen „Google Docs“ bzw. „Google Text und Tabellen“ ins umfangreiche Portfolio des Unternehmens integriert und wird sogar von IT-Beratern empfohlen. Die Vorteile von derlei Software-as-a-Service-Produkten sind offensichtlich: Dokumente immer im Zugriff zu haben und dabei nicht auf teure Hardware oder Anwendungsprogramme zurückgreifen zu müssen, ist nicht nur für Unternehmen ökonomisch einleuchtend. Kollaboration wird massiv vereinfacht; die Arbeit wird flexibler; kurz: die Kosten sinken. Die Schattenseiten dieser Dienste sind hingegen nicht ganz so augenfällig. Sie verstecken sich in technischem und juristischem Gestrüpp.

Wer Google Text und Tabellen benutzt, speichert seine erstellten und bearbeiteten Dokumente nicht auf seinem eigenen Computer; dort wären sie nicht universell verfügbar. Stattdessen werden die **Dokumente auf Google-Servern** abgelegt. Diese gespeicherten Daten sind zunächst nicht öffentlich verfügbar, sondern liegen nur im Zugriffsbereich des eigenen Nutzerkontos. Aus technischer Sicht hat jedoch Google freien Zugriff auf so gespeicherte Dokumente.

Im September 2007 gab es einige Aufregung um Google Text und Tabellen, als bekannt wurde, dass das Unternehmen sich selbst Rechte zur Nutzung und Weiterverarbeitung der eingestellten Dokumente einräumte. Es stellte sich jedoch heraus, dass es sich bei den zitierten Fundstellen schlicht um Übersetzungsfehler handelte. Die Google eingeräumten Rechte beziehen sich auf die notwendige Datenverarbeitung, um dem Nutzer seine Dokumente überhaupt anzeigen zu können. Das Urheberrecht und die Verantwortlichkeit verbleiben vollständig bei den Nutzern. Trotzdem waren diese verunsichert; tatsächlich macht sich kaum jemand Gedanken, welche Konsequenzen die Nutzung von Online-Applikationen hat. Ähnlich wie bei Googles E-Mail-Dienst (27. TB, Tz. 10.6; 29. TB, Tz. 10.9) müssen sich Nutzer bewusst sein, dass ihre persönlichen Dokumente technisch gesehen vollständig in der **Verfügungsgewalt von Google** sind. Die Analyse der Dokumente, die Google bei seinem Maildienst praktiziert, wird im Fall von Google Text und Tabellen offensichtlich nicht angewandt, technisch möglich wäre sie.

Das Nutzerverhalten wird von Google schon jetzt umfangreich analysiert, wie die allgemeine Datenschutzerklärung darlegt, die auch für Google Text und Tabellen gilt: „Google records information such as account activity (e.g. storage usage, number of log-ins, actions taken), data displayed or clicked on (e.g. UI elements, links), and other log information (e.g. browser type, IP address, date and time of access, cookie ID, referrer URL).“

www.google.com/google-d-s/privacy.html

Auch wenn Google bislang die gespeicherten Dokumente nicht auswertet: Die genannten **persönlichen Nutzungsdaten** werden auch im Kontext von Googles „Text und Tabellen“ gesammelt, also wer wie lange und von welchem Rechner aus an einem Dokument gearbeitet hat. So lassen sich Arbeitsgruppen und soziale Netzwerke der Nutzer erkennen. Ein Zugriff von US-Sicherheitsbehörden, auch Geheimdiensten, auf die online gespeicherten Dokumente ist denkbar.

Dies gilt nicht nur für Google, sondern für **alle Online-Dienste**. Die Nutzungsdaten fallen neben den eigentlichen Dokumenten immer an, sodass eine entsprechende Auswertung leicht möglich ist. Bei Google kommt jedoch die leichte Verknüpfbarkeit dieser Informationen mit Daten hinzu, die Google aus seinen anderen Diensten gewinnt. Die größte Skepsis sollte jedoch dem Zugriff auf die Klartextdokumente gelten: Will man wirklich Briefe, Berichte und Kalkulationen in die Hände eines Dienstleisters geben? Eine wirkliche Kontrolle hat man über online gespeicherte Dokumente nicht mehr. Man ist vielmehr abhängig von der Qualität der Dienstleistung und der Sorgfalt des Anbieters. Dieser Umstand konkretisiert sich bei Google Text und Tabellen z. B. darin: Wer eine online gespeicherte Datei löscht, sollte wissen, dass Kopien seines Dokuments bis zu drei Wochen in den Google-Systemen verbleiben – auf Cache- und Backup-Systemen.

Eine derartige Verarbeitung ist im Grundsatz rechtlich als Auftragsdatenverarbeitung einzustufen. Vor allem für **sensible Personendaten** und Unternehmensdaten sollte das Gebot gelten, die Bearbeitung mit Online-Anwendungen zu meiden.

Was ist zu tun?
Wer Online-Anwendungen nutzen möchte, muss kritisch abwägen, ob er seine persönlichen oder firmeninternen Dokumente in die Obhut des Dienstleisters abgeben möchte und darf. Sobald personenbezogene Daten Dritter verarbeitet werden, kommen die aktuell verfügbaren Online-Dienste nicht infrage.

11 Europa und Internationales

11.1 PNR – der Sicherheitswahn greift in den Himmel

Nach der gesetzlich beschlossenen Vorratsdatenspeicherung der Telekommunikationsverkehrsdaten droht nun die der Flugverkehrsdaten.

Die terroristischen Anschläge des 11. September 2001 inspirierten zu vielen Datensammlungen. Da das Anschlagsmittel Flugzeuge waren, lag es für die US-Regierung scheinbar nahe, in einem „Aviation and Transportation Act“ von Flugunternehmen Daten, sogenannte **Passenger Name Records** (PNR), über sämtliche Fluggäste zu verlangen, auch von europäischen Gesellschaften, die die USA anfliegen. Ein Abkommen zwischen den USA und der Europäischen Union (EU), das diese einseitige Praxis zu regulieren versuchte, war aus Datenschutzsicht viel zu weitgehend und wurde im Jahr 2006 vom Europäischen Gerichtshof wegen mangelnder Zuständigkeit der EU-Kommission aufgehoben. Inzwischen wurde ein neues Abkommen vom EU-Rat geschlossen, das US-Behörden berechtigt, 38 Datenfelder sämtlicher Flugreisender abzugreifen und diese Daten 15 Jahre zu speichern und zu nutzen. Vom Beginn des Jahres 2008 an sollte statt des Zugriffs auf die Datenbanken (Pull-Verfahren) eine aktive Übermittlung (Push-Verfahren) treten.

Trotz aller Kritik fanden sich in der EU immer mehr Freunde dieser Maßnahme. 2004 verpflichtete der Rat der EU die Beförderungsunternehmen unter dem Kürzel API (**Advanced Passenger Information**), Angaben über die beförderten Personen zu übermitteln, wobei die Verbesserung der Grenzkontrollen und die Bekämpfung illegaler Einwanderung im Vordergrund standen. Die nationale gesetzliche Umsetzung dieses Beschlusses erfolgte Ende 2007.

Obwohl bisher noch keine Auswertungen mit den Erfahrungen der bisher praktizierten Maßnahmen vorlagen, startete die EU im November 2007 eine weiter gehende Initiative für einen Rahmenbeschluss zur Speicherung von Fluggastdatensätzen zu Strafverfolgungszwecken. Ganz nach dem US-Vorbild sollen danach sämtliche Flugunternehmen, die die EU anfliegen, die PNR-Fluggastdatensätze übermitteln; diese Daten würden dann **13 Jahre lang** für Sicherheitszwecke gespeichert werden.

Damit würden die Flugverkehrsdaten von sämtlichen die EU-Grenzen überquerenden Personen in einer Sicherheitsdatei ohne jeden konkreten Anlass und ohne jeglichen Sicherheitsbezug bevorratet und genutzt. Der Versuch des ULD und anderer Datenschutzkollegen, die Länder im Rahmen des Bundesratsverfahrens zu einer kritischen Stellungnahme zu veranlassen, waren erfolglos. Diese neue Maßnahme **ins Blaue hinein** wäre verfassungswidrig. Sie knüpft an den unbestimmten Begriffen des Terrorismus und der organisierten Kriminalität an. Die Daten sollen schon zur Verhütung von Straftaten im Vorfeld einer Gefahr ausgewertet und in komplexen Verfahren analysiert werden. Selbst Ansätze von datenschutzrechtlichen Sicherungen wurden nicht vorgelegt.

Damit wird die EU Vorbild für viele Staaten, die Reisebewegungen minutiös erfassen wollen. Tatsächlich dauerte es nur wenige Wochen, bis Korea von europäischen Fluglinien genau die Forderung aufstellte, die die EU aufzuerlegen sich anschickt. Auch andere Staaten folgen dem schlechten Beispiel der USA und nun der EU. Wenn die EU den Rahmenbeschluss fasst, so wird sich die Speicherung von Fluggastdaten voraussichtlich **weltweit etablieren**; vom Datenschutz bleibt keine Spur. Betroffen sein werden von der langjährigen Beobachtung nicht nur Touristinnen und Touristen, sondern ebenso Geschäftsreisende. Welchen wirtschaftlichen Schaden dies für die betroffenen Personen, Unternehmen und Geschäftszweige anrichten wird, ist noch nicht abschätzbar. Die ULD-Stellungnahme ist abrufbar unter

www.datenschutzzentrum.de/flugdaten/20071204-rahmenbeschluss.htm

Was ist zu tun?
Die Pläne eines EU-Rahmenbeschlusses zur Speicherung von Fluggastdatensätzen sollten schleunigst und unwiderbringlich von der politischen Agenda verschwinden.

11.2 Datenschutz in der 3. Säule

Die Normierung des Datenschutzes in der 3. Säule der Europäischen Union – also in den Bereichen Polizei und Justiz – kommt nur langsam voran. Das absehbare Ergebnis ist wenig ermutigend.

Der Vorschlag eines **Rahmenbeschlusses des Rates** über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, hat eine lange Geschichte ohne bisher absehbares Ende. Nach mehrjährigen Vorbereitungen hatte die Kommission dem Rat der Europäischen Union (EU) im Oktober 2005 einen ersten Entwurf übermittelt. Die deutsche EU-Präsidentschaft schaffte es auch bis Mitte 2007 nicht, hierüber Einigkeit herzustellen. Derweil gibt es weniger Einigungsprobleme bei der Verabredung der informationellen Zusammenarbeit, etwa jüngst zur Fluggastdatenspeicherung (Tz. 11.1). Inzwischen liegt ein Text vor, der eigentlich noch im Jahr 2007 hätte beschlossen werden sollen, woraus aber nichts wurde. Dennoch ist schon eindeutig zu erkennen, dass der Entwurf über einen Minimalkonsens nur wenig hinausgeht. Mit deutschem Datenschutzverständnis wäre eine solche Minimallösung nicht in Einklang zu bringen.

Der Rahmenbeschluss wird künftig weniger den Bund, sondern vor allem die **Länder** betreffen, da dort fast vollständig die Zuständigkeit für die Gefahrenabwehr und die Strafverfolgung liegt. Umso unverständlicher ist es, dass die Einbindung der Länder in die Diskussion des geplanten Beschlusses zu wünschen übrig ließ. Die Datenschutzbeauftragten der Länder wurden teilweise gezielt über die aktuellen Texte im Unklaren gelassen.

Anstatt sich auf einen einheitlichen Mindeststandard beim Datenschutz im Sicherheitsbereich zu verständigen, soll der Rahmenbeschluss nur für den **grenzüberschreitenden Datenverkehr** gelten. Dies mag angesichts des teilweise sehr niedrigen Datenschutzniveaus in manchen EU-Staaten erklärlich sein, hinsichtlich des Umstandes, dass künftig alle Staaten durch ein Grundrecht auf Datenschutz gebunden sein sollen, ist dies aber nicht ausreichend. Durch die Beschränkung des Datenschutzregimes auf grenzüberschreitend ausgetauschte Daten entsteht ein hoher bürokratischer Aufwand durch die Notwendigkeit der Datenkennzeichnung im Hinblick auf Datenqualität, Herkunft und Zweckbindung sowie die Notwendigkeit der separierten Verarbeitung und der Einholung der Zustimmung bei weiter gehenden Nutzungen.

Der **Nutzungsbereich der Daten** wird extensiv beschrieben, indem neben der Ermittlung, Feststellung oder Verfolgung von Straftaten auch deren Verhütung erfasst wird. Angesichts der auch in Deutschland bestehenden Tendenz, damit Lebensbereiche des sogenannten Vorfeldes und der Gefahrenermittlung mit zu erfassen, in denen also weder eine Straftat noch eine konkrete Gefahr vorliegen, wird der Rahmen für die Verarbeitung praktisch nicht mehr greifbar. Von der nach dem deutschen Recht bewährten Trennung zwischen Gefahrenabwehr und Strafverfolgung ist nirgends die Rede. Damit sind auch diese weiten Zwecke keine normative Grenze für die Datenverwendung. Vielmehr wird die Zweckänderung generell erlaubt, vorausgesetzt sie ist verhältnismäßig und nicht mit dem ursprünglichen Verarbeitungszweck unvereinbar. Selbst an die Übermittlung der Daten in Drittstaaten werden kaum strengere Anforderungen geknüpft. Die wesentlichen nationalen Sicherheitsinteressen und insbesondere die Tätigkeit der Geheimdienste sollen durch den Rahmenbeschluss unberührt bleiben. Dies muss wohl so verstanden werden, dass von einem anderen EU-Staat übermittelte Daten von den Geheimdiensten nach nationalem Recht genutzt werden dürfen.

Überarbeitungsbedürftig sind auch die **Transparenzregeln**. Bei der Benachrichtigung der Betroffenen hat man es sich einfach gemacht: Statt den Versuch zu starten, gemeinsame Regeln zu definieren, wird jeweils auf das nationale Recht verwiesen. Selbst dieses Niveau kann unterschritten werden, wenn der übermittelnde Mitgliedstaat darum ersucht. Geradezu beängstigend ist die Regelung zum Auskunftsrecht, die tatsächlich keine Auskunft über die Daten gewährleistet, sondern im schlechtesten Fall die Bestätigung von der nationalen Kontrollstelle, dass alle erforderlichen Überprüfungen durchgeführt wurden; und selbst dieses Recht kann aus Sicherheitsgründen weiter beschränkt werden.

Man hätte nun erwarten können, dass eine einheitliche Instanz zumindest für die **Datenschutzkontrolle** zuständig erklärt würde, aber wieder Fehlanzeige: Bisheriger Stand ist der Entwurf einer Ratserklärung, wonach geprüft werden soll, ob die bisher von unterschiedlichen kollektiven Kontrollgremien wahrgenommenen Aufgaben zusammengefasst werden können. Dass dies nicht nur möglich, sondern eine Zusammenfassung beim Europäischen Datenschutzbeauftragten nötig ist, hat sich bei den Ratserörterungen den Beteiligten offensichtlich bisher nicht erschlossen. Angesichts dessen ist es nur noch ein minder schwerer Mangel, dass das Regelungskonzept für die technisch-organisatorische Datensicherheit dem Stand

der Neunzigerjahre des letzten Jahrhunderts entspricht. Bei allem Verständnis für die Nowendigkeit eines intensiveren Datenaustausches bleibt die Notwendigkeit des Grundrechtsschutzes bestehen. Der aktuelle Text des Rahmenbeschlusses wird kaum noch änderbar sein: eine dürftige Basis für den Start eines gemeinsamen Datenschutzes im Sicherheitsbereich der EU.

Was ist zu tun?
Der Text des Rahmenbeschlusses muss umgehend einer gründlichen Revision unterworfen werden.

11.3 Das Binnenmarktinformationssystem auf dem Prüfstand

Im Rahmen der Umsetzung der EG-Richtlinie 2005/36/EG über die Anerkennung von Berufsqualifikationen soll künftig im Wege der Amtshilfe zwischen den einzelnen Mitgliedstaaten ein grenzüberschreitender Austausch sensibler personenbezogener Daten von Angehörigen freier Berufe erfolgen. Dabei müssen die Vorschriften der EG-Datenschutzrichtlinie beachtet werden.

Worum geht es beim Binnenmarktinformationssystem (IMI – Internal Market Information System)? Ein Beispiel: Ein in Deutschland niedergelassener Arzt möchte in Frankreich eine Dienstleistung erbringen. Nach dem national umgesetzten europäischen Recht soll die in Frankreich **für die Zulassung zuständige Behörde** im Wege der Amtshilfe von der in Deutschland für den Arzt zuständigen Behörde alle Informationen über die Rechtmäßigkeit seiner Niederlassung und seiner „guten Führung“ anfordern können. Sie soll sich u. a. darüber informieren können, dass gegenüber dem Arzt keine berufsbezogenen disziplinarischen oder strafrechtlichen Sanktionen verhängt worden sind.

Den Betrieb des Systems will die EU-Kommission auf eine „Entscheidung“ über den Schutz personenbezogener Daten bei der Umsetzung des Binnenmarktinformationssystems vom Dezember 2007 stützen, in der die Kommission von einer **gemeinsamen datenschutzrechtlichen Verantwortung** der so genannten IMI-Akteure ausgeht. IMI-Akteure sind demgemäß die zuständigen Behörden der Mitgliedstaaten, die Koordinatoren sowie die EU-Kommission. Die Kommission ist Betreiber des Rechenzentrums, in dem das IMI-System gehostet ist. Sie hat die Aufgaben der Verfügbarkeit und Wartung der IT-Infrastruktur sowie der Bereitstellung eines mehrsprachigen Systems und eines zentralen Helpdesks. Sie nimmt also gegenüber den mitgliedstaatlichen Behörden im Datenschutzsinne die Rolle eines Auftragnehmers wahr. Dies bedeutet, dass die Kommission nach den Vorschriften der EG-Datenschutzrichtlinie gegenüber den für die Verarbeitung verantwortlichen Behörden der Mitgliedstaaten insbesondere den Nachweis einer ausreichenden technischen und organisatorischen Sicherheit zu führen hat. Sie kann in ihrer Eigenschaft als Betreiberin des Rechenzentrums nicht gleichzeitig für die Datenverarbeitung verantwortlich sein. Die datenschutzrechtliche Verantwortung liegt bei den Stellen, die über Inhalte, Zwecke und Mittel der Datenverarbeitung entscheiden. Diese Festlegungen liegen aber im Kompetenzbereich der mitgliedstaatlichen Behörden.

Die sogenannten **Koordinatoren** haben die Aufgabe, die zuständigen Behörden zu registrieren bzw. deren Registrierung zu authentifizieren. Damit sind auch diese nicht für die Datenverarbeitung verantwortlich, da hierbei keine Entscheidungen über die Inhalte und Zwecke der personenbezogenen Datenverarbeitung getroffen werden.

Was ist zu tun?
Bei der Realisierung des Binnenmarktinformationssystems muss die EU-Kommission die Vorgaben der EG-Datenschutzrichtlinie beachten. Die Entscheidung der Kommission gemäß dem aktuellen Stand bildet keine tragfähige Grundlage zur Regelung der datenschutzrechtlichen Verantwortlichkeit.

12 Informationsfreiheit

International, national als auch auf Landesebene gab es bei der Informationsfreiheit neue **Bestrebungen und Entwicklungen**. Die Kommission der Europäischen Union hat eine Initiative gestartet, den Zugang zu Informationen über Agrarsubventionen für die Öffentlichkeit zu verbessern. In diesem Zusammenhang ist die Frage diskutiert worden, ob die Empfänger von Agrarsubventionen namentlich veröffentlicht werden sollen. Auf Bundesebene ist das lang und breit diskutierte Verbraucherinformationsgesetz verabschiedet worden, das hinter vielen Erwartungen zurückblieb, aber einen Schritt in die richtige Richtung darstellt. Auf Landesebene musste ein Umweltinformationsgesetz erlassen werden. Letztlich wurde ein Konsens darüber erzielt, dass das bisher geltende Informationsfreiheitsgesetz (IFG-SH) nicht verändert werden soll (29. TB, Tz. 12.1).

12.1 Transparenzinitiative: Zugang zu Daten über EU-Agrarsubventionen

Die Transparenzinitiative der Europäischen Kommission zielt auf die Veröffentlichung der begünstigten Subventionsempfänger ab. Dabei muss ein ausgewogenes Verhältnis zwischen Informationszugang und Datenschutz gefunden werden.

Die Konferenz der Informationsfreiheitsbeauftragten hatte sich im August 2006 für die Offenlegung der Empfänger von Agrarsubventionen ausgesprochen und die Nennung von finanziell begünstigten Vorhaben, die Höhe des Förderungsbetrages und des konkreten Förderungszwecks gefordert (29. TB, Tz. 11.1). Die Europäische Kommission plant indes, den Umfang der zugänglichen Informationen auf die Mitteilung des **Gesamtbetrages der öffentlichen Mittel je Begünstigten** zu beschränken. So würde insbesondere der Verwendungszweck für die bereitgestellten finanziellen Mittel verborgen bleiben. Es bestünden für eine kritische Öffentlichkeit keine effektiven Möglichkeiten zu kontrollieren, ob die verausgabten Steuergelder zweckmäßig verwendet wurden. Das ULD sieht in den Bestrebungen der Kommission einen Rückschritt in den Bemühungen um mehr Transparenz bei der Verwendung öffentlicher Mittel.

Im Fortgang der Debatte sollte zum Schutz von Kleinunternehmen eine **Bagatellgrenze** vorgesehen werden, über die ein ausgewogenes Verhältnis zwischen mehr Transparenz und Datenschutz hergestellt wird. Die unbeschränkte Offenlegung von Informationen über die Subventionierung von Einpersonenbetrieben könnte zu Diskriminierungen führen und damit unter Umständen letztlich zum Verzicht auf öffentliche Fördermittel. Durch eine Aggregierung der Daten bei geringen Beträgen kann dennoch eine hinreichende Kontrolle ermöglicht werden.

Was ist zu tun?
Die Umsetzung der Europäischen Transparenzinitiative in nationales Recht muss die Offenlegung der Vorhaben, der Förderungshöhe und des jeweiligen Verwendungszwecks beinhalten, zugleich aber die Diskriminierung von Kleinunternehmen vermeiden.

12.2 Verbraucherinformationsgesetz in Kraft

Nachdem der Bundesrat gegen das neue Verbraucherinformationsgesetz keinen Einspruch einlegte, ist der Weg für mehr Transparenz im Bereich der Informationen über den Verkauf von verdorbenen Lebensmitteln und über dadurch entstehende Gesundheitsgefahren frei.

Die wesentlichen Errungenschaften des Gesetzes bestehen in der Schaffung eines **individuellen Informationsanspruches** der Verbraucher gegenüber den Behörden und in der Eröffnung des freien Zugangs zu Daten aus dem Bereich der Lebens- und Futtermittelüberwachung. Der Informationsanspruch umfasst Daten über Verstöße gegen das Lebens- und Futtermittelgesetzbuch, über von Erzeugnissen ausgehenden Gefahren oder Risiken für die Gesundheit und Sicherheit für die Verbraucher, über Ausgangsstoffe und die eingesetzten Verfahren sowie ergriffene Überwachungsmaßnahmen.

Bei diesem Gesetz verweigerte der Bundespräsident zunächst seine Unterschrift, weil er dessen Regelungen mit dem Grundgesetz für nicht vereinbar hielt. Den Gemeinden und Gemeindeverbänden dürfen durch ein Bundesgesetz keine Aufgaben übertragen werden. Nachdem eine Klarstellung bezüglich der Verpflichtung der kommunalen Behörden, Anträge auf Informationszugang nach dem Verbraucherinformationsgesetz zu bearbeiten, vorgenommen wurde, sah der Bundespräsident den kompetenzrechtlichen Konflikt bereinigt, sodass das Gesetz nun in Kraft treten konnte.

Was ist zu tun?
Das Verbraucherinformationsgesetz schafft in einem engen Kundensegment einen verbesserten Zugang zu wichtigen Informationen. Hierbei sollte der Gesetzgeber nicht stehen bleiben. Andere Bereiche, z. B. die aus Datenschutzsicht besonders relevanten IT-Angebote, bedürfen einer massiv verbesserten Durchschaubarkeit.

12.3 Landesumweltinformationsgesetz

Zweck des Gesetzes ist es, den Zugang zu Umweltinformationen bei informationspflichtigen Stellen des Landes und der Kommunen sowie den Weg für die Verbreitung dieser Umweltinformationen frei zu machen.

Das Umweltinformationsgesetz für das Land Schleswig-Holstein (UIG-SH) trat im März 2007 in Kraft. Es orientiert sich an dem Wortlaut der Europäischen

Umweltinformationsrichtlinie und an deren Umsetzung auf Bundesebene. Wesentliche Unterschiede zum IFG-SH bestehen in einem weiteren Anwendungsbereich sowie bei der Offenbarung von personenbezogenen Daten. Das UIG-SH erfasst auch **Personen des Privatrechts**, die im Zusammenhang mit der Umwelt öffentliche Zuständigkeiten haben, öffentliche Aufgaben wahrnehmen oder öffentliche Dienstleistungen erbringen und dabei der Kontrolle einer juristischen Person des öffentlichen Rechts unterliegen. Sind von einem Antrag auf Informationszugang **personenbezogene Daten** betroffen, können diese bei überwiegendem Interesse der Allgemeinheit offenbart werden. In jedem Einzelfall wird das öffentliche Interesse an der Bekanntgabe gegen das Interesse an der Geheimhaltung der Informationen abgewogen. Eine entsprechende Abwägungsklausel ist im IFG-SH nur bei der Offenbarung von Betriebs- und Geschäftsgeheimnissen vorgesehen.

Im Anschluss an das UIG-SH ist die **Landesverordnung über Kosten** nach dem Umweltinformationsgesetz für das Land Schleswig-Holstein (UIG-SH-KostenVO) verabschiedet worden. Diese begrenzt die Gebühr auf maximal 500 Euro und legt die Höhe der zu erhebenden Auslagen für die Herstellung von Duplikaten fest. Für die Erstellung einer DIN-A4-Kopie sind 10 Cent (schwarz-weiß) bzw. 25 Cent (farbig) zu erheben. Insoweit bietet die Kostenverordnung einen guten Maßstab auch für Anträge nach dem IFG-SH. Hier fehlt es bisher an einer einheitlichen Regelung.

Was ist zu tun?
Da für den Zugang zu Informationen über die Umwelt das neue UIG-SH eine Grundlage schafft, die über das IFG-SH hinausgeht, sollten Personen, die Zugang zu Umweltinformationen haben wollen, sich vorrangig auf das UIG-SH berufen.

12.4 Interessante Einzelfälle

12.4.1 Wie viel Wärme brauchen Sie?

Für die Ausstellung von Energiepässen benötigen Hauseigentümer und damit Vermieter von ihren Energieunternehmen Verbrauchsdaten. Können Vermieter diese Daten von kommunalen Versorgern nach dem IFG-SH erhalten?

Ein Vermieter erbat unter Berufung auf das IFG-SH von seinen Stadtwerken die Übersendung von Informationen zum Energieverbrauch einzelner Mieter. Diese benötigte er zur Eintragung in den sogenannten Energieausweis. Wird ein Gebäude errichtet, hat der Bauherr sicherzustellen, dass der Eigentümer des Gebäudes einen Energieausweis erhält. Soll ein mit einem Gebäude bebautes Grundstück verkauft werden, hat der Verkäufer dem Kaufinteressenten einen Energieausweis zugänglich zu machen. Eine entsprechende Verpflichtung gilt für den Eigentümer als Vermieter oder Verpächter eines Grundstückes. Der Energieausweis dient zur Feststellung der **Energieeffizienz eines Gebäudes**.

Die Ausstellung von Energieausweisen nach dem Energiebedarf ist gesetzlich vorgeschrieben, sofern

- ein Gebäude errichtet wird oder
- ab dem 1. Januar 2008 ein mit einem Gebäude bebautes Grundstück verkauft, vermietet oder verpachtet wird, das Wohngebäude weniger als fünf Wohnungen hat und der Bauantrag für das Wohngebäude vor dem 1. November 1977 gestellt wurde.

Der Aussteller des Energieausweises hat nun die Möglichkeit, die gesetzlich geforderten Angaben auf Basis des **Energiebedarfs** oder des tatsächlichen Energieverbrauchs zu berechnen. Der Energiebedarf wird dabei auf der Grundlage der Bauunterlagen bzw. gebäudebezogenen Daten und unter Annahme standardisierter Raumbedingungen (z. B. standardisierte Klimadaten, definiertes Nutzerverhalten, standardisierte Innentemperatur und innere Wärmegewinne) berechnet. Da aus standardisierten Raumbedingungen kein Rückschluss auf den tatsächlichen Verbrauch gezogen werden kann, handelt es sich bei den Energiebedarfswerten nicht um personenbezogene Daten.

Zur Ermittlung des **Energieverbrauchs** sind Verbrauchsdaten aus Abrechnungen von Heizkosten nach der Heizkostenverordnung für das gesamte Gebäude oder andere geeignete Verbrauchsdaten, insbesondere Abrechnungen von Energielieferanten oder sachgerecht durchgeführte Verbrauchserfassungen, zu verwenden. In diesen Unterlagen können personenbezogene Daten enthalten sein. Verbrauchsdaten lassen dabei aber nur Rückschlüsse auf eine bestimmte oder bestimmbare Person zu, wenn individuelle Merkmale erkennbar sind. Werden die Verbrauchsdaten mehrerer Wohnungen zusammengefasst, sodass Rückschlüsse auf einzelne Mieter nicht mehr möglich sind, so besteht bei diesen aggregierten Daten bei hinreichender **Anonymisierung** kein Personenbezug mehr. Davon kann ausgegangen werden, wenn mindestens drei Wohnungen zusammengefasst werden.

Begehrt der Vermieter oder Verpächter hingegen Verbrauchsdaten einer einzigen Wohnung oder zusammengefasst von zwei Wohnungen, so besteht ein **konkreter Personenbezug**. Nach den Vorschriften des IFG-SH kommt es darauf an, ob der Antragsteller ein rechtliches Interesse an der Kenntnis der begehrten Informationen hat und überwiegende schutzwürdige Belange des betroffenen Mieters der Offenbarung der personenbezogenen Verbrauchsdaten entgegenstehen. Ein rechtliches Interesse des Antragstellers besteht beim Verkauf, der Vermietung oder Verpachtung aufgrund der vertraglichen Beziehungen zum Mieter. Dieses rechtliche Interesse entfällt nicht durch den Umstand, dass die Berechnung nach Energieverbrauchswerten als gleichwertige Alternative neben der Berechnung nach Energiebedarfswerten besteht, soweit die Berechnung nach dem Energiebedarf nicht zwingend gesetzlich vorgeschrieben ist. Der Antragsteller ist gesetzlich verpflichtet, einen Energieausweis zu erstellen. Ein Verstoß ist eine Ordnungswidrigkeit, welche mit einer Geldbuße mit bis zu 15.000 Euro geahndet werden kann.

Der Mieter kann schutzwürdige Belange geltend machen, z. B. dass die Preisgabe seiner Verbrauchsdaten Rückschlüsse auf ein individuelles Verbraucherverhalten

ermöglichen. Diese Belange müssen allerdings überwiegen. Die Stadtwerke müssen dem Mieter Gelegenheit zur Stellungnahme geben; dieser muss objektiv nachvollziehbare Gründe benennen, die einer Offenbarung der Verbrauchsdaten entgegenstehen. In jedem Fall muss dann eine Einzelfallprüfung stattfinden. Kann der **Mieter besondere Belange** darlegen, so kann im Ausnahmefall der Zugang zu den Verbrauchsdaten nach dem IFG-SH verweigert werden.

Was ist zu tun?
Bei der Auskunft über Verbrauchsdaten sind die oben gegebenen Hinweise zu beachten. Soweit möglich, ist mit aggregierten Daten zu arbeiten.

12.4.2 Herausgabe eines Wirtschaftlichkeitsgutachtens

Externe Gutachten, die von öffentlichen Stellen in Auftrag gegeben werden, müssen auf Anfrage grundsätzlich herausgegeben werden. Eine interne Vereinbarung, das Gutachten geheim zu halten, reicht als Geheimhaltungsgrund nicht aus.

Eine Stadt bzw. ihre Stadtverordnetenversammlung hatte eine externe Beratungsfirma mit einer **Organisationsuntersuchung und Stellenbewertung der Kernverwaltung** beauftragt. Nach Fertigstellung des Gutachtens verweigerte die Stadt einem Bürger die Einsichtnahme mit der Begründung, das Einvernehmen bestünde, diese nicht öffentlich zu behandeln. Das Gutachten sei zudem Bestandteil von nicht öffentlichen Sitzungen gewesen und damit nicht der Öffentlichkeit zugänglich.

Immer wieder muss daran erinnert werden: Eine Geheimhaltung von Unterlagen der Verwaltung bzw. eine Ablehnung ihrer Offenbarung ist nur aus den im IFG-SH genannten Gründen möglich. Eine interne **Geheimhaltungsabsprache** ist nicht vorgesehen. Nicht zu offenbaren sind nach dem IFG-SH Protokolle vertraulicher Beratungen; geschützt wird hierdurch der freie Meinungsaustausch innerhalb und zwischen den Behörden. Besprechungen, Entscheidungsvorschläge, Bewertungen und Entscheidungsdiskussionen müssen folgerichtig nicht offenbart werden. **Beratungsgegenstände und Beratungsergebnisse** selbst sind dagegen nicht vom Informationszugang ausgeschlossen. Diese wurden im Gesetzgebungsverfahren bewusst aus dem Schutzbereich der Vorschrift herausgenommen. Damit korrespondiert auch die gesetzliche Konkretisierung, dass insbesondere Beweiserhebungen und Stellungnahmen nicht der unmittelbaren Vorbereitung von Entscheidungen dienen und damit offenbart werden dürfen.

Die Vorschriften der Gemeindeordnung ergeben nichts Gegenteiliges. Dort ist lediglich festgeschrieben, dass die **in nicht öffentlichen Sitzungen gefassten Beschlüsse** bekannt zu geben sind, wenn nicht ausnahmsweise Gemeinwohlinteressen bzw. berechtigte Interessen Dritter entgegenstehen. Zur Geheimhaltung von einzelnen Beratungsgegenständen ist damit nichts ausgesagt. Die Stadt hat schließlich das Gutachten dem Petenten zur Verfügung gestellt.

Was ist zu tun?
Bei Anträgen auf Zugang zu externen Gutachten liegen nur selten Geheimhaltungsgründe im Sinne des IFG-SH vor.

12.4.3 Gibt es für Eigenbetriebe Geschäftsgeheimnisse?

Der Zugang zu Informationen nach dem Informationsfreiheitsgesetz kann bei Betriebs- und Geschäftsgeheimnissen Dritter beschränkt sein. Bei kommunalen Eigenbetrieben ist das aber kein Argument.

Ein Bürger erbat Zugang zu Bilanzen und Gutachten zum **Unternehmenswert eines städtischen Eigenbetriebes**. Zum Zeitpunkt der Antragstellung hatte die Gemeinde den Eigenbetrieb bereits in eine GmbH überführt und 49,9 % der Anteile an ein privates Energiedienstleistungsunternehmen verkauft. Der Petent begehrte dabei Informationen, welche sich auf den Zeitpunkt vor der Umwandlung des städtischen Eigenbetriebes bezogen.

Der Antrag nach dem IFG-SH kann abgelehnt werden, soweit durch die Übermittlung der Informationen ein schutzwürdiges Betriebs- oder Geschäftsgeheimnis offenbart würde. Als Inhaber von Betriebs- und Geschäftsgeheimnissen kommen nach der Gesetzessystematik jedoch nur solche Personen in Betracht, die nicht selbst nach dem Informationsfreiheitsgesetz als Auskunftspflichtige in Anspruch genommen werden können. Dies ist der Fall bei Behörden und auch bei Privatpersonen, soweit eine Behörde sich dieser zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben bedient oder diesen die Erfüllung öffentlich-rechtlicher Aufgaben übertragen wird. Bei einem städtischen Eigenbetrieb bedient sich die Behörde einer besonderen Organisationsform und erbringt dabei selbst regelmäßig öffentlich-rechtliche Leistungen der Daseinsvorsorge. Dies hat zur Folge, dass der städtische Eigenbetrieb nach dem IFG-SH auf Informationszugang in Anspruch genommen werden kann. Der städtische Eigenbetrieb mit seiner 100%igen **Bindung an die Gemeinde** tritt nicht als privater Dienstleister auf und kann sich daher nicht auf Betriebs- und Geschäftsgeheimnisse berufen.

Da der Bürger nur Informationen begehrte, die sich auf einen Zeitraum **vor der Umwandlung** des städtischen Eigenbetriebes in eine GmbH bezogen, war der Informationszugang nicht wegen entgegenstehender Betriebs- und Geschäftsgeheimnisse beschränkt. Insoweit konnte sich das private Energiedienstleistungsunternehmen auch nicht auf eigene Betriebs- und Geschäftsgeheimnisse berufen, die eine Abwägung mit dem Offenbarungsinteresse der Allgemeinheit erforderlich gemacht hätten.

Was ist zu tun?
Der Schutz von Betriebs- und Geschäftsgeheimnissen dient der Sicherung privatwirtschaftlicher Positionen und unterfällt dem grundrechtlich gewährleisteten Schutz des Unternehmers an seinem eingerichteten und ausgeübten Gewerbebetrieb. Städtischen Eigenbetrieben steht dieser verfassungsrechtliche Schutz nicht zu.

12.4.4 Gebühren bei Einsichtnahme in Protokolle der Gemeindevertretung

Möchte ein Bürger in Protokolle einer Ratsversammlung einsehen, dürfen ihm nicht unverhältnismäßig hohe Kosten auferlegt werden.

Ein Bürger erhielt nach dem IFG-SH Kopien aus Protokollen verschiedener öffentlicher Sitzungen seiner Gemeindevertretung. Die Gemeinde stellte dem Bürger den Zeitaufwand für die Zusammenstellung der gewünschten Protokolle in Rechnung und verlangte zusätzlich pro erstellte Kopie 75 Cent. Für Amtshandlungen nach dem IFG-SH können Verwaltungsgebühren erhoben werden. Nicht zulässig ist jedoch die Abwälzung von allgemeinen Personal- oder Sachkosten, die der Behörde bei der Beschaffung und Pflege ihres Informationsbestandes entstehen; diese Tätigkeiten sind im Katalog des IFG-SH nicht aufgeführt. Die Gemeinden müssen bereits nach der Gemeindeordnung Protokolle ihrer öffentlichen Sitzungen für ihre Einwohner zur Einsichtnahme bereithalten. **Aufbereitung und Vorhaltung der Protokolle** sind damit kein Aufwand anlässlich eines Informationsbegehrens nach dem IFG-SH, sondern eine originäre Pflicht nach der Gemeindeordnung, der nicht in Rechnung gestellt werden darf.

Möglich ist die Auferlegung der Kosten für die Erstellung und Versendung von Kopien. Diese Kosten dürfen aber nicht unverhältnismäßig sein. Der Preis für die Herstellung von Kopien bewegt sich heutzutage im Bereich um die 5 Cent pro Seite (29. TB, Tz. 12.4.5). Dementsprechend legt die UIG-SH-KostenVO als Auslagenersatz für eine Schwarz-Weiß-Kopie 10 Cent fest. Ein **pauschaler Preis von 75 Cent pro Kopie** ist nicht zu rechtfertigen.

In dem vorliegenden Fall wollte der Antragsteller ursprünglich vor Ort Einsicht nehmen, was ihm nicht gestattet wurde. Nur die Zusendung von Kopien wurde bewilligt. Nach den Vorschriften des IFG-SH hat der Antragsteller grundsätzlich die **freie Wahl**, ob er eine Auskunft wünscht, ob er Einsicht in die Informationsträger erhalten möchte und/oder Kopien übersandt werden sollen. Ist die kostenlose Einsichtnahme vor Ort aus Gründen, die die Behörde zu vertreten hat, nicht möglich, dürfen dem Antragsteller aus diesem Umstand keine gesonderten Kosten entstehen. Daher war bereits jede Erhebung von Auslagen unzulässig.

Was ist zu tun?
Der Zeitaufwand für die Aufbereitung und Vorhaltung von Protokollen von öffentlichen Sitzungen von Gemeindevertreterversammlungen darf für den Informationszugang nach dem IFG-SH nicht in Rechnung gestellt werden.

12.4.5 Tonträgeraufzeichnungen von Ratsversammlungen

Tonträgeraufzeichnungen, die bei Sitzungen von Rats- oder Gemeindevertreterversammlungen erstellt werden, sind Informationen, die interessierten Bürgern grundsätzlich zugänglich gemacht werden müssen. Über einen Antrag auf Informationszugang entscheidet im Regelfall der Bürgermeister.

Anträge auf Zugang zu Tonträgeraufzeichnungen können abgelehnt werden, wenn es sich um Vorentwürfe und Notizen handelt, die **nicht Bestandteil des Vorgangs** werden sollen und alsbald vernichtet werden. Sind die Tonträgeraufzeichnungen nicht dazu bestimmt, langfristig archiviert zu werden, sondern helfen diese lediglich bei der Abfassung des Protokolls, liegt es im Ermessen der Behörde, diese Informationen zu offenbaren. Ist eine langfristige Aufbewahrung vorgesehen, so liegt die Offenbarung nicht im Ermessen der Behörde; sie kann nur abgelehnt werden, wenn ein Ablehnungsgrund im Sinne des IFG-SH vorliegt.

Grundsätzlich hat der Bürgermeister über einen solchen Antrag zu entscheiden, denn ihm obliegt nach der Gemeindeordnung die Führung der **Geschäfte der laufenden Verwaltung**, wozu die Bereitstellung der Niederschriften und die Einsichtnahme in die Tonträgeraufzeichnungen gehört. Die Niederschrift muss dem Vorsitzenden **und** dem Bürgermeister unverzüglich zugeleitet werden wegen deren Aufgaben der Beschlussausführung und Rechtsprüfung. Die Protokolle werden damit Bestandteil der Verwaltungsunterlagen der Gemeinde und sind damit im Sinne des IFG-SH vorhanden.

Was ist zu tun?
Tonträgeraufzeichnungen gehören neben den Unterlagen in Papierform zu den Informationen, zu denen im Rahmen des IFG-SH Zugang zu gewähren ist.

13 DATENSCHUTZAKADEMIE – Kompetenz für alle

Die kontinuierliche Nachfrage nach Weiterbildungskursen der DATENSCHUTZAKADEMIE Schleswig-Holstein zeigt wachsendes Interesse an maßgeschneiderten Datenverarbeitungsprozessen wie an qualifiziertem Datenschutzmanagement in Verwaltung und Betrieben, in sozialen, schulischen und medizinischen Einrichtungen.

Datenschutz ist schon lange kein esoterisches Nischenthema mehr. Professionelle Verarbeitung und Sicherung personenbezogener Daten hilft bei der Optimierung der Organisationsstrukturen, der Planung von Arbeitsabläufen, der Gestaltung des IT-Einsatzes, der Entwicklung des Produktangebots und der Außendarstellung des Unternehmens bzw. der Behörde. Über qualifizierte Kurse der DATENSCHUTZAKADEMIE bietet das ULD in diesem Bereich sinnvollen Support für Firmen und Verwaltungen in Schleswig-Holstein.

- **Schulungsbetrieb 2007**

Der Ausbau im technischen Angebot der DATENSCHUTZAKADEMIE konnte fortgeführt werden:

- Mit dem Kurs **„Datenschutz und Datensicherheit für SystemadministratorInnen (DS)“** wurde für Einsteiger eine gelungene Mischung aus der Vermittlung theoretischer Grundlagen und Bearbeitung aktueller, praxisrelevanter Sicherheitsproblematiken am Rechner realisiert.
- Der Kurs **„Windows Terminal Server mit Citrix Metaframe 4.0“ (WIN-TS)** machte erfahrene Systemadministratoren mit den unterschiedlichen Terminalservertechnologien der Firmen Citrix und Microsoft vertraut. Diese Techniken ermöglichen eine erhebliche Konsolidierung des administrativen Aufwands in Verwaltungen – eine Tatsache, die von zunehmendem Interesse im Rahmen der anstehenden Reformen im kommunalen Bereich ist.
- Nach intensiven Vorarbeiten in diesem Jahr wird 2008 der Kurs **„IT-Sicherheitsmanagement“ (ITS)** durch den Kurs **„Sicherheitsmanagement auf Basis von IT-Grundschutz“ (ITS II)“** ergänzt.
- Das ebenfalls neu erarbeitete Schulungskonzept **„Mit dem BSI-Grundschutztool zum IT-Sicherheitskonzept“ (BSI-GST)** vermittelt, wie IT-Verbünde von Organisationen mithilfe des Grundschutztools verwaltet werden.

Praxisforum

*Das neue Angebot der DATENSCHUTZAKADEMIE als **Diskussionsrunde aus der Praxis für die Praxis** hat sich bewährt und wird fortgeführt.*

Neben dem diesjährigen Thema „Wie strukturiere ich meine Dokumentation nach LDSG und DSVO?“ wird im kommenden Jahr zusätzlich das Thema „Test und Freigabe“ behandelt.

Nächste Termine erfahren Sie über: akademie@datenschutzzentrum.de

- Nach Absolvierung des Kurses **„Von der Bedrohung zum Restrisiko“ (RISK)** sollen die Teilnehmer selbstständig Risiko- und Restrisikoanalysen im Rahmen von IT-Sicherheitskonzepten durchführen können.
- Wie Testumgebungen auf der Basis von Virtualisierungstechniken aufgebaut und betrieben werden, lehrt der Kurs **„Test und Freigabe“ (TEST)**.
- Aufgrund aktuellen Bedarfs wird in Zukunft auf Nachfrage die Inhouse-Veranstaltung **„Interner IT-Auditor“ (ITA-Inhouse)** angeboten: Durch einen lizenzierten ISO 27001-BSI-Auditor werden die Teilnehmer dazu befähigt, IT-Sicherheitschecks bzw. interne Sicherheitsaudits eigenständig durchzuführen.
- Als krönender Abschluss kann das **„DatenschutzzertifikatfürSystemadministratorInnen“ (SDZ)** erworben werden.

Das Unabhängige Landeszentrum für Datenschutz (ULD) hat in der DATENSCHUTZAKADEMIE in diesem Jahr zum fünften Mal in Folge Systemadministratoren zertifiziert. Die Systemadministratoren der Gemeinde Stockelsdorf, des Amtes Landschaft Sylt, der Generalstaatsanwaltschaft des Landes Schleswig-Holstein und der Firma Atos Origin GmbH unterzogen sich im November 2007 einer mehrstündigen theoretischen und praktischen Prüfung mit Erfolg und erhielten den Titel „Systemadministrator mit Datenschutzzertifikat“.

Mit diesem Abschluss können folgende Kompetenzen nachgewiesen werden:

- fundierte Kenntnisse im Bereich Datenschutzrecht, Systemdatenschutz und Datensicherheit,
- methodische Vorgehensweise beim IT-Sicherheitsmanagement, beim Aufbau und bei der Begutachtung von IT- und Sicherheitskonzepten,
- sichere Verwaltung von Sicherheitsfunktionalitäten der Betriebssysteme Windows Server 2003 und XP,
- Entwicklung und Einsatz von datenschutz- und datensicherheitskonformen Strategien bei der Anbindung an externe Netze.

Mit dem Erwerb des Datenschutzzertifikats können die Systemadministratoren ihre persönliche und berufliche Qualifikation verbessern und geben ihren Arbeitgebern die Sicherheit, dass die vorgeschriebenen technischen, organisatorischen und datenschutzrechtlichen Vorschriften bei der Systemadministration berücksichtigt werden. Für die Prüfungsvorbereitung bietet das ULD im Rahmen der DATENSCHUTZAKADEMIE Schleswig-Holstein Kurse an, mit denen die geforderten Kenntnisse im Bereich Datenschutzrecht, IT-Revision und Sicherheitsfunktionen der Betriebssysteme vermittelt werden.

Die Grundlagenkurse der DATENSCHUTZAKADEMIE werden weiterhin gut angenommen. Dies sind **„Datenschutzrecht/Datensicherheitsrecht für behördliche Datenschutzbeauftragte“ (DR/DT)**, **„Einführung Datenschutz im Schulsekretariat“ (ES)** und **„Führung von Personalakten“ (PA)**.

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 eine 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

Weitere Schwerpunkte der Akademiearbeit bilden traditionell die Kurse zum betrieblichen Datenschutz. Im **„Grundkurs Bundesdatenschutzgesetz" (BDSG-I)** werden die Grundzüge des für die Wirtschaft geltenden Datenschutzrechts den betrieblichen Datenschutzbeauftragten in handlungsoptimierter und praxisbezogener Form vermittelt. Die Teilnehmer erhalten mit den „Sieben Goldenen Regeln des Datenschutzrechts" Wegweiser durch die Fülle gesetzlicher Regelungen: Rechtmäßigkeit, Einwilligung, Zweckbindung, Erforderlichkeit, Transparenz, Datensicherheit und Kontrolle.

- Die Kurse „Betriebliches Datenschutzmanagement nach dem Bundesdatenschutzgesetz" (BDSG-II), „Technischer Datenschutz/ Systemdatenschutz nach dem BDSG" (SIB) und „IT-Sicherheitsmanagement" (ITS) rundeten die Angebote im Bereich des betrieblichen Datenschutzes ab.
- 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 viele Unklarheiten im Zusammenhang mit der geplanten Einführung der elektroni-

schen Gesundheitskarte führten ebenso bei den Kursen „Datenschutz im Krankenhaus“ (DK) und „Datenschutz in der Arztpraxis“ (AR) zu reger Nachfrage.

- Steigender Schulungsbedarf ist auch im Anwendungsbereich des Sozialgesetzbuches (SGB) zu verzeichnen. Arbeitsgemeinschaften der Bundesanstalt für Arbeit (ARGE), soziale Dienstleister, Wohlfahrtsverbände, Werkstätten für Menschen mit Behinderungen suchten in zahlreichen Inhouse-Veranstaltungen um Schulungen ihrer MitarbeiterInnen zum „Datenschutz im Sozialhilfebereich“ nach. Der besonderen Bedeutung dieser Problematik trägt die DSA auch im kommenden Jahr Rechnung durch das Angebot von Sonderkursen zu folgenden Themen: „SGB II – Hartz IV/Arbeitslosengeld II“, „SGB V/XI – Das Datenschutzrecht der Kranken- und Pflegekassen“, „SGB VIII – Kinder- und Jugendhilferecht“.

Im Jahr 2007 fanden 53 Schulungsveranstaltungen statt, in denen insgesamt 766 Personen (2006: 616) teilnahmen. Dabei verdoppelte sich die Anzahl der Sonderkurse von 11 auf 22. Dies deutet darauf hin, dass der Bedarf an kundenorientiert maßgeschneiderten Schulungsprogrammen ansteigt. Zu den Kunden zählten dabei Landesministerien ebenso wie ARGEn, Kommunalverwaltungen, Betriebsräte oder Einrichtungen für behinderte Menschen.

Über 400 Personen besuchten den alljährlichen Höhepunkt der DATENSCHUTZAKADEMIE, die **Sommerakademie** am 27. August 2007 im Maritim Hotel Bellevue in Kiel zum Thema **„Offene Informationsgsellschaft und Terrorbekämpfung – ein Widerspruch?“**.

- **Jahresprogramm 2008 der DATENSCHUTZAKADEMIE**

März	03.03.	ES	Datenschutz im Schulsekretariat	
	04.03.	BDSG-I	Grundkurs Bundesdatenschutzgesetz	
	05.03.	BDSG-II	Betriebliches Datenschutzmanagement	
	05.03. - 07.03.	ITS	IT-Sicherheitsmanagement	
	06.03.	SIB	Technischer Datenschutz/ Systemdatenschutz nach BDSG	
	07.03.	PD	Datenschutzgerechtes Produktdesign	
	10.03. - 12.03.	ITS-II	Sicherheitsmanagement auf Basis von IT-Grundschutz	*NEU*
April	07.04. - 09.04.	WIN-I	Windows 2003 Sicherheit I	
	09.04. - 11.04.	BSI-GST	Mit dem BSI-Grundschutztool zum IT-Sicherheitskonzept	*NEU*
	21.04. - 22.04.	DR	Datenschutzrecht für behördliche Datenschutzbeauftragte	
	22.04. - 23.04.	SIKO	Sicherheitskonzepte erstellen	
	23.04. - 25.04.	DT	Datensicherheitsrecht für behördliche Datenschutzbeauftragte	

Mai	05.05.	DWBT	Workshop für betriebliche Datenschutzbeauftragte	
	06.05.	IFG	Informationsfreiheitsgesetz Schleswig-Holstein	
	07.05.	AR	Datenschutz in der Arztpraxis	
	08.05.	DK	Datenschutz im Krankenhaus	
	28.05. - 29.05.	RISK	Risikoanalyse und Risikomanagement	*NEU*
Juni	03.06. - 04.06.	TEST	Test und Freigabe	*NEU*
	18.06.	LDSG-R	Landesdatenschutzgesetz Schleswig-Holstein	
	18.06.	ES	Datenschutz im Schulsekretariat	
Juli	01.07.	BDSG-I	Grundkurs Bundesdatenschutzgesetz	
	02.07.	BDSG-II	Betriebliches Datenschutzmanagement	
	03.07.	SIB	Technischer Datenschutz/ Systemdatenschutz nach BDSG	
	07.07. - 09.07.	WIN-TS	Windows 2003 Terminal Server mit Citrix Metaframe 4.0	
September	01.09.		Sommerakademie „Internet 2008 – Alles möglich, nichts privat?“	
	08.09. - 09.09.	DR	Datenschutzrecht für behördliche Datenschutzbeauftragte	
	10.09. - 12.09.	DT	Datensicherheitsrecht für behördliche Datenschutzbeauftragte	
	15.09. - 17.09.	S	Sozialdatenschutzrecht	
	16.09.	ES	Datenschutz im Schulsekretariat	
	22.09. - 23.09.	PA	Führung von Personalakten	
	22.09. - 24.09.	WIN-II	Windows 2003 Sicherheit II	
	25.09. - 26.09.	DS	Datensicherheit und Datenschutz für SystemadministratorInnen	
Oktober	06.10.	BDSG-I	Grundkurs Bundesdatenschutzgesetz	
	07.10.	BDSG-II	Betriebliches Datenschutzmanagement	
	08.10.	SIB	Technischer Datenschutz/ Systemdatenschutz nach BDSG	
November	03.11. - 04.11.	FW	Firewalls: Theorie und Praxis	
	05.11. - 07.11.	ITS	IT-Sicherheitsmanagement	
	11.11. - 12.11.	WIN-NG	Vista und Longhorn für erfahrene AdministratorInnen	*NEU*
	17.11. - 19.11.	WIN-I	Windows 2003 Sicherheit I	
	26.11.	SDZ	Prüfung zum/zur Systemadministrator/in mit Datenschutzzertifikat	

Sommerakademie 2008 ∗ Sommerakademie 2008 ∗ Sommerakademie 2008

Internet 2008 – Alles möglich, nichts privat?

Die Sommerakademie 2008 nimmt das Internet – mit all seinen schillernden Eigenschaften – zum Schwerpunkt. Es erweist sich als Motor für Wirtschaft und Verwaltung, als nützlich, ja als unerlässlich für die Kommunikation, für demokratische Diskussion und für die Verbreitung und Beschaffung von Informationen, als Plattform für Freizeit und Unterhaltung.

Zugleich wird die Erstellung von Interessen-, Kommunikations-, Bewegungs-, Betätigungs- und Sozialprofilen erleichtert – mit gravierenden Konsequenzen für die Individualität der Menschen. Die Begehrlichkeiten bei Staat und Unternehmen werden offensiv vorgetragen. Sie reichen von Vorratsdatenspeicherung über Online-Überwachung bis hin zu Informationssammlungen für Werbe- und Geschäftszwecke. Damit stellt das Internet eine Gefahr für das dar, was in der realen Welt mit „Privatheit“ bezeichnet wird.

Der Datenschutz zeigt technisch, organisatorisch und rechtlich Wege auf, wie die Privatheit im Internet verteidigt werden kann. Die Konflikte und Lösungen werden auf der Sommerakademie präsentiert und zur Diskussion gestellt.

Montag, 1. September 2008,
Maritim Hotel Bellevue, Kiel

Die Teilnahme ist kostenlos. Bitte melden Sie sich an unter

www.datenschutzzentrum.de/sommerakademie

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstr. 98, 24103 Kiel
Tel.: 0431/988-1200
Fax: 0431/988-1223
E-Mail: akademie@datenschutzzentrum.de

Index

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z