Tätigkeitsbericht 2010

des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

Berichtszeitraum: 2009, Redaktionsschluss: 15.02.2010
Landtagsdrucksache 17/210

(32. 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: Schmidt & Klaunig, Kiel

Inhaltsverzeichnis

1 Datenschutz in Schleswig-Holstein

Das Land Schleswig-Holstein **kann sich glücklich schätzen**, dass ihm schon im Jahr 2000 der Landtag ein Informationsrecht, also ein Landesdatenschutzgesetz (LDSG) und ein Informationsfreiheitsgesetz (IFG), gab, das an Fortschrittlichkeit keinen Vergleich scheuen musste: die Verbindung der Zuständigkeit für Datenschutz und Informationsfreiheit in einem Zentrum, das Behörde und zugleich viel mehr ist, die gemeinsame Wahrnehmung der Datenschutzaufsicht im öffentlichen und im nicht öffentlichen Bereich, die Ergänzung des rechtlichen Datenschutzes um eine zweite, gleichberechtigte Säule „Technik“, die Erweiterung des klassischen Instrumentariums um präventive und marktorientierte Methoden und die Verbindung der Praxis mit der Wissenschaft. Dadurch blieben dem Land Konflikte und Probleme erspart, an denen andere Bundesländer bis heute laborieren. Dies war und ist durch die schleswig-holsteinische Tradition möglich, Datenschutzdebatten sach- und nicht ideologie- oder parteiorientiert zu führen und einvernehmliche Lösungen zu suchen. Statt sich in Grundsatzdebatten über Idee und Struktur des Informationsrechts zu verlieren, werden die praktischen Herausforderungen zielgerichtet angegangen.

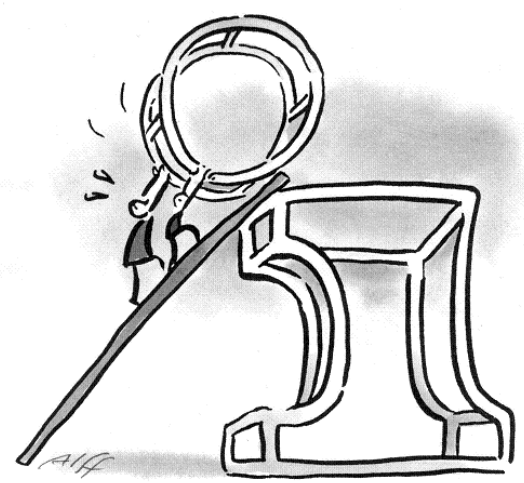
LDSG und IFG haben sich bewährt, ebenso die Konzentration der darin festgelegten staatlichen Aufgaben im Unabhängigen Landeszentrum für Datenschutz (ULD) als Anstalt des öffentlichen Rechts. Dies hatte zur Folge, dass das schleswig-holsteinische Konzept Vorbild für Regelungen in anderen Ländern wurde. Es bleiben immense Aufgaben für die Zukunft: Das Internet hat inzwischen beim E-Government die Verwaltung, aber auch die Wirtschaft des Landes und den Alltag der Menschen fest im Griff. Dies verlangt adäquate rechtliche, technische und organisatorische Antworten, die zugleich pragmatisch und zukunftsoffen sind. Der technische Fortschritt muss zum Zweck der Kosteneinsparung, der Rationalisierung und der Erhöhung der Arbeitseffektivität genutzt werden, ohne den Draht zu den Bürgerinnen und Bürgern zu verlieren. Ja, es geht nicht nur darum, die Kontakte zu den Menschen zu halten, sondern diese zu intensivieren und dadurch demokratische Teilhabe und die Wahrnehmung von deren Rechten zu verbessern.

1.1 Informationsrecht bleibt eine Baustelle

Zehn Jahre nach der letzten Generalrevision unseres Informationsrechts ist es bei allen bisherigen Erfolgen angebracht, dessen Zukunftsfähigkeit auf den Prüfstand zu stellen. Der Zeitpunkt hierfür ist geradezu ideal: Sowohl im Bund als auch im Land bestehen nach den Parlamentswahlen für mehrere Jahre politische Planungssicherheit und damit konstante **Gestaltungsbedingungen**.

Zugleich befindet sich die gesellschaftliche Debatte über die Informationsgesellschaft in einem Umbruch. Das Bewusstsein entwickelt sich, dass wir uns gerade technikbedingt an der Schwelle einer **neuen Phase** der gesellschaftlichen Entwicklung befinden: Nach dem Erwerb der Sprache als Kommunikationsmittel, der Schrift als Mittel zur Informations- und Ideenkonservierung und des Buchdrucks

als Instrument für deren Verbreitung haben wir mit dem Internet nun das Werkzeug, Informationen und Ideen weltweit und ohne Zeitverzug zu kommunizieren und hierüber auch einen globalen demokratischen Dialog zu ermöglichen. Diese technische Revolution ist für die Menschheit überlebensnotwendig, da ohne sie eine weltweite Verständigung über aktuelle, technisch bedingte Gefahren nicht möglich wäre: atomare Bedrohung, Umweltverschmutzung und Klimaerwärmung.



Der Umbruch hat gravierende Konsequenzen für das Informationsrecht generell (Tz. 2.1). Ein Land wie Schleswig-Holstein hat die Wahl, sich von diesem Umbruch treiben zu lassen oder ihn mitzugestalten. Mitgestaltung beinhaltet nicht nur die Chance zur politischen Selbstbestimmung beim Umgang mit digitalen Informationen, sondern auch zur **Ressourceneinsparung**. Während sinnvolle Investitionen im sozialen, im ökonomischen und im ökologischen Bereich oft eine Amortisation erst nach vielen Jahren bringen, kann die sinnvolle Gestaltung von Informationstechnik kurzfristig zu finanziellen Einsparungen beitragen. Dies ist zweifellos nicht die gesetzliche Aufgabe des ULD, aber wohl eine Rahmenbedingung, die Datenschutz nicht nur aus Grundrechtssicht notwendig, sondern auch ökonomisch sinnvoll sein lässt (Tz. 1.3).

Die Musik der Informationspolitik spielt auf Landesebene – anders als auf Bundesebene – perspektivisch weniger im allgemeinen Datenschutzrecht. Die Schwerpunkte liegen künftig bei der Gestaltung des **E-Government**, also der Digitalisierung der Verwaltungsabläufe unter Einbeziehung der Bürgerinnen und Bürger, sowie beim Ausbau der Informationsdienstleistungen. Dies wurde von den aktuellen Regierungsparteien im Koalitionsvertrag aufgegriffen, der eine „Prozessoptimierung und die konsequente Einführung der elektronischen Verwaltung (E-Government)“ und die Zusammenlegung von Umweltinformationsgesetz und Informationsfreiheitsgesetz (Tz. 12) vorsieht. Die Informations- und Kommunikationspotenziale des Internets sind von der Verwaltung noch nicht ausgeschöpft. Einen Schub wird es mittelfristig durch die effektive Etablierung „Einheitlicher Ansprechpartner“ (Tz. 6.4) sowie durch die rechtliche und dann praktische Umsetzung der INSPIRE-Richtlinie und ein noch zu verabschiedendes Geodateninfrastrukturgesetz (Tz. 12.1) geben.

Dies soll nicht bedeuten, dass das **Landesdatenschutzgesetz** (LDSG) unantastbar wäre. Dieses Gesetz kann von einigem Ballast – es gibt dort einige nicht mehr praktisch relevante Regelungen – befreit werden, etwa denjenigen zum „Fernmessen und Fernwirken“, zu „öffentlichen Auszeichnungen“ oder zur „besonderen Dokumentationsstelle für Sekten“. Neben diesen randständigen Themen gibt es Modernisierungsmöglichkeiten im LDSG. Dies gilt für den technischen Datenschutz. Die Diskussion auf Bundesebene über technische Schutzziele ist inzwi-

schen mit maßgeblicher Beteiligung des ULD weiter fortgeschritten und kann nicht nur im Bundesdatenschutzgesetz (BDSG), sondern auch im LDSG normativ umgesetzt werden (Tz. 6.9). Die Automatisierung der Verwaltung im Kontakt zur Bürgerin bzw. zum Bürger spiegelt sich noch nicht in dem Gesetz wider, z. B. durch Regelung der elektronischen Einwilligung oder sonstiger Online-Verfahren. Die Videoüberwachung lässt sich auf der Basis der vorliegenden Erfahrungen klarer normieren. Ein weiterer Aspekt einer Überarbeitung des LDSG kann es sein, bisher unentgeltliche Serviceleistungen des ULD mit einem finanziellen Mehrwert für die interessierten Unternehmen als Gebührentatbestände vorzusehen, etwa die Genehmigung von Datenschutzverträgen zur Datenübermittlung ins Ausland außerhalb Europas.

1.2 Die Dienststelle

Durch die Bestätigung von Thilo Weichert als Leiter des ULD ist in der Dienststelle für weitere fünf Jahre personelle Kontinuität gegeben und es besteht für die Fortführung der vielfältigen Projekte Planungssicherheit. Besonders erfreulich ist die einstimmige Wiederwahl durch den Landtag – ohne Gegenstimmen oder Enthaltungen. Dieses Votum versteht die gesamte Dienststelle als ein Signal des Vertrauens und zugleich als Auftrag und Verpflichtung.

Das ULD war trotz steigender Belastung und zusätzlichen Anforderungen in der Lage, die dem Land entstehenden Kosten für Datenschutz und Informationsfreiheit seit acht Jahren weitgehend konstant zu halten. Damit leistet das ULD einen Beitrag zur **Ausgabenbegrenzung** angesichts eines stark belasteten Landeshaushaltes. Dies war durch eine effektive Nutzung neuer Technologien, durch eine straffe Organisation und durch Synergieeffekte möglich. Letztere konnten insbesondere im Servicebereich genutzt werden, also bei Zertifizierungen, bei Beratungen, bei der Aus- und Fortbildung, der Durchführung von Projekten und dem Erstellen von Gutachten. Über die damit erzielten Einnahmen konnten sogar Entlastungen im Kerngeschäft bewirkt werden, wo insbesondere durch zahlenmäßig steigende Eingaben zur Datenverarbeitung bei Wirtschaftsunternehmen wie auch durch Reaktionsbedarf auf neue technische und rechtliche Entwicklungen die Arbeit zunimmt. Aus Sicht der Beschäftigten ist es problematisch, dass wegen der zeitlich begrenzten Finanzplanbarkeit nur befristete Arbeitsverträge geschlossen werden können. Ohne das außergewöhnliche Engagement der Mitarbeiterinnen und Mitarbeiter trotz teilweise widriger Rahmenbedingungen wäre die auf dem ULD liegende Last nicht zu bewältigen.

1.3 Datenschutz zur Steigerung der IT-Effizienz

Wer sparen will, muss den Datenschutz stärken. Auf diese einfache Formel lässt sich herunterrechnen, was erfolgreiche Datenschützer und IT-Planer wissen. Eine stärkere Konsolidierung und Zentralisierung sind nur wirtschaftlich durchführbar, wenn zugleich Datenschutz und Datensicherheit gefördert werden.

Während sich viele Bereiche der öffentlichen Verwaltung und der Privatwirtschaft sichtlich schwer damit tun, **Einsparungen zu erwirtschaften**, ist dies für den

Bereich der Informations- und Kommunikationstechnik sowohl konzeptionell als auch bei konkreten Maßnahmen eine zentrale Zielsetzung und oft „geübte Praxis". Will man die Effizienz von Informationstechnik steigern, so ist ein Weg das Zusammenfassen von vorher getrennten Verarbeitungsprozessen. Die Schlagworte „Konsolidierung", „Virtualisierung" oder „Integration" bedeuten schlichtweg, dass bestehende Informationstechnik besser genutzt wird und anfallende Personalkosten besser eingesetzt werden.

Wird bisher dezentralisierte Datenverarbeitung zusammengefasst, so steigen unweigerlich die damit verbundenen Risiken bezüglich der Vertraulichkeit, Integrität und Verfügbarkeit. Diese Risiken sind bei zusammengefassten Verfahren aufgrund der höheren Datendichte und der umfänglicheren Zahl an Datenverarbeitungsprozessen mit einem **größeren Schadenspotenzial** verbunden: Statt 20 Sachbearbeitern einer kleineren Verwaltungseinheit sind dann 2.000 nicht arbeitsfähig, statt 100 sind vielleicht 100.000 Datensätze von Bürgerinnen und Bürgern im Internet zugänglich.

Soll die Effizienz des Einsatzes von Informationstechnik gesteigert werden, so führt kein Weg daran vorbei, Datenschutz und Datensicherheit für die Verfahren auszubauen. Alles andere wäre wegen der erhöhten Risiken mit deutlich vergrößerten Schadensszenarien weder rechtlich noch wirtschaftlich vertretbar. Datenschutz und Datensicherheit sind also nicht Verhinderer oder Kostentreiber, sondern ermöglichen die Steigerung von IT-Effizienz. **Datenschutz bildet die Grundlage für Effizienz.** Diese Wirkungen werden in den auf Bundesebene bereits etablierten Modellen und Fachkonzepten zur Betrachtung und Bewertung der Wirtschaftlichkeit von Informationstechnik bereits seit Jahren berücksichtigt. Neben den sofort monetär fassbaren Wirtschaftlichkeitsüberlegungen müssen die qualitativen Aspekte eines funktionierenden, starken Datenschutzes betrachtet werden. Konkrete Vorgaben zur Dokumentation der Planung und Durchführung der Verarbeitung personenbezogener Daten ermöglichen Datenschützerinnen und Datenschützern ein hohes Maß an Transparenz bezüglich der IT-getriebenen Verfahren und Verfahrensschritte. Ohne Transparenz wären die Verfahren aus Datenschutzsicht nicht bewertbar. Diese Transparenz bildet zudem eine wesentliche Grundlage, um Optimierungspotenzial beim IT-Einsatz zu erkennen und die Effizienz zu steigern. Datenschutz und Datensicherheit liefern die entscheidenden Basisinformationen, um Effizienzsteigerungen umsetzen zu können.

Besonders bei **kooperativen Verfahren** ist eine Steigerung der IT-Effizienz nur möglich, wenn ein nachvollziehbar hohes Niveau an Datenschutz und Datensicherheit besteht. Bei vielen Akteuren, die jeweils eigenständige, im Sinne des Datenschutzes verantwortliche Stellen sind, kann in komplexeren und vernetzten Verfahren die jeweilige Verantwortung wahrgenommen werden, wenn ein transparenter, nachvollziehbarer und kontrollierbarer Betrieb von Informationstechnik vorliegt.

Am **Beispiel des Landesnetzes** Schleswig-Holstein ist dies leicht nachvollziehbar: Als vom ULD zertifizierter Baustein der E-Government-Strategie des Landes ermöglicht das Landesnetz die zentrale Nutzung von konsolidierten Verfahren über ein sicheres und datenschutzkonformes Transportnetz. Aufwendige Sonder-

lösungen zur Absicherung des Datentransports entfallen, und die Nutzung zentraler Verfahren wird ermöglicht: So einfach kann es in einer Gesamtkostenbetrachtung sein, Wirtschaftlichkeit zu erreichen. Man muss nur Datenschutz und Datensicherheit entsprechend hoch priorisieren.

Was ist zu tun?
Land und Kommunen müssen sparen. Wer Datenschutz und Datensicherheit stärkt, kann vermehrt IT einsetzen und die Effizienz des bisherigen IT-Einsatzes steigern. Jede Verwaltung muss über ein funktionierendes Datenschutzmanagement verfügen, um umfangreiche Effizienzsteigerungen rechtskonform realisieren zu können.

2 Datenschutz – national und global

Datenschutz in Schleswig-Holstein – ist im Grunde heute nicht mehr möglich. Die nationalen, europäischen und globalen Verbindungen und Vernetzungen machen es erforderlich, bei der **Datenschutzaufsicht vor Ort** zumindest die nationale und die europäische Ebene mit zu berücksichtigen und oft auch ausländisches staatliches Recht einzubeziehen.

Dies gilt für die **Europäische Union** (EU), über die immer mehr Festlegungen erfolgen, z. B. durch die Tätigkeit der Artikel-29-Datenschutzgruppe, den koordinierenden Erfahrungs- und Informationsaustausch zwischen den EU-Aufsichtsbehörden in Grundsatzangelegenheiten sowie bei der Bewältigung von Einzelfragen, die Zertifizierung im Rahmen von EuroPriSe (Tz. 9.3), die Erarbeitung wissenschaftlicher Erkenntnisse und das gemeinsame Durchführen von Projekten (Tz. 8.2 und Tz. 8.3, Tz. 8.7 bis Tz. 8.9) oder die gegenseitige personelle und logistische Unterstützung, wie dies etwa im Rahmen von Twinning-Projekten stattfindet (z. B. 31. TB, Tz. 8.9). Nach Verabschiedung des Lissabon-Vertrages (Tz. 11.1) wird es hinsichtlich der informationellen Kooperation der Sicherheitsbehörden weiter gehende Initiativen geben, die sich direkt auf die Stellen des Landes auswirken (Tz. 11.2 und Tz. 11.3). Auch im allgemeinen Datenschutzrecht gibt es in der EU Bewegung. Nach der Überarbeitung der europäischen ePrivacy-Richtlinie für die Bereiche Telekommunikation und Online-Medien steht eine Überarbeitung der Datenschutzrichtlinie aus dem Jahr 1995 zur Diskussion sowie möglicherweise eine neue Richtlinie zum Arbeitnehmerdatenschutz.

2.1 Codex digitalis

Datenschutz ist Grundrechtsschutz. Bisher wurde Grundrechtsschutz analog gedacht. Zwar legte das Bundesverfassungsgericht mit dem Recht auf informationelle Selbstbestimmung seit dem Jahr 1983 und nun mit dem Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme im Jahr 2008 einen verlässlichen verfassungsrechtlichen Rahmen fest. Doch wurde die technische sowie die verfassungsrechtliche Entwicklung weder im Bewusstsein von Verwaltung und Wirtschaft noch in der Politik befriedigend angenommen. Es ist schon erstaunlich, dass ein renommierter Journalist mit einem Buch, das die technologische **Überforderung des Menschen** durch die digitale Technik thematisiert, in Deutschlands Bestsellerlisten auf Platz 1 landen kann.

Es ist irritierend, dass die **digitale Dimension der Grundrechte** immer noch nicht zu einem zentralen Gesetzgebungsimpuls für die Politik geworden ist. Von der Informationstechnik betroffen ist dabei nicht nur das allgemeine Persönlichkeitsrecht, das durch adäquate gesetzliche Regelungen geschützt werden muss: In Wohnungen kann man auch mit Lausch- und Spähangriffen eindringen. Für das Plündern des Bankkontos sind nur einige Kontodaten nötig. Mit sogenannten elektronischen Fußfesseln können Menschen unsichtbar ihrer Freiheit beraubt werden. Für politische Verfolgung bedarf es keiner Folter, es genügt die Dateispeicherung als angeblicher Terrorist.

Der US-amerikanische Internetpionier Tim O'Reilly sagte: „Wir steuern auf einen **Krieg über die Kontrolle des Internets** zu." Tatsächlich findet dieser „Krieg" nicht militärisch, sondern ökonomisch schon lange statt. Diese Auseinandersetzung führt in Diktaturen zu einer massiven Überwachung und Regulierung, zu Zensur und Beschränkung des Netzzugangs sowie zur Verfolgung der Inanspruchnahme von Menschenrechten im Netz. Für die Bundesrepublik und Schleswig-Holstein und für die hier lebenden Menschen relevanter ist die Dominanz von global tätigen Wirtschaftsunternehmen über das Netz und hiermit deren Möglichkeit, die Inanspruchnahme von Freiheitsrechten der Netznutzenden zu manipulieren oder gar gezielt zu beeinträchtigen. Es ist unbestreitbar, dass Konzerne wie Google faktisch eine Machtstellung über das Internet erlangt haben, die allerhöchste Grundrechtsrelevanz für die Menschen hat, ohne dass vonseiten der Politik und der Verwaltung hierauf bisher angemessen reagiert wird.

Es ist eine zentrale Aufgabe des **Staates als Garant der Grundrechte**, derartigen Manipulationen und Beeinträchtigungen entgegenzuwirken. Hierbei sind Datenschutz und Informationsfreiheit zentrale Aspekte, aber beileibe nicht die einzigen. Es geht auch um den Schutz von Kindern und Jugendlichen, um Kriminalitätsbekämpfung im Netz, um den Schutz von Urheberrechten und um die Wahrung der Rechte der Menschen, die gewollt oder ungewollt auf einen Netzzugang verzichten oder verzichten müssen. Technikfolgenabschätzung im modernen Gewand bedeutet in unserer globalen Informationsgesellschaft heute auch digitaler Grundrechtsschutz. Während jedoch bei der Technologiefolgenabschätzung in den 80er-Jahren des letzten Jahrhunderts die optimistische Annahme bestand, Technikrisiken vor ihrem Entstehen vermeiden zu können, ist die Situation heute die, dass sämtliche Operationen des Grundrechtsschutzes „am lebenden Körper" des Internets „on-the-fly" erfolgen müssen.

Eine frühe und adäquate staatliche Reaktion auf die technischen und ökonomischen Gegebenheiten ist dabei wichtig. Eines der **Früherkennungssysteme** – neudeutsch „Watchdogs" genannt – sind die Datenschutzbeauftragten. Diese können diese Aufgabe nicht allein erfüllen. Gefragt sind insofern auch die Verbraucherschützer, die Arbeitnehmervertretungen, Menschenrechtseinrichtungen und eine freie Presse. Letztlich gefordert ist die Politik, die die „Beobachtungen" der Früherkennungssysteme in formalisierte Entscheidungsprozesse und schließlich zu gesetzgeberischen Entscheidungen, die administrativ umgesetzt werden, bringt.

„Codex digitalis universalis" ist der Titel der **Sommerakademie 2010** Ende August (Tz. 13). Dabei soll die Normierungsnotwendigkeit des Datenschutzes in einen größeren informationsrechtlichen Zusammenhang unter Einbeziehung aller unserer Freiheitsrechte thematisiert werden. Es wird dabei nicht nur um Aufträge an die Gesetzgeber im Land, im Bund und in Europa gehen, sondern auch um die Frage der Selbstregulierung und der Normierung, also die Festlegung von Kodizes zwischen den Tarifpartnern, zwischen Wirtschaft und Verbrauchern, durch Eigenverpflichtungen der Wirtschaft und nicht zuletzt durch Festlegungen der Bürgerinnen und Bürger im Rahmen des Selbstschutzes. In den 70er-Jahren des letzten Jahrhunderts meinte man fälschlicherweise, das Recht automatisieren zu können. Inzwischen wissen wir, dass Recht in der Informationsgesellschaft nicht nur

rechtlich, sondern auch durch Organisation, Technik und letztlich durch Kultur umgesetzt werden muss. Dies ist ein anspruchsvoller Auftrag für die Zukunft. Das Adjektiv „universalis“ soll signalisieren, dass wir uns nicht nur Gedanken über diesen Codex für uns selbst machen müssen, sondern dieser allgemeine, weltweite Relevanz hat.

2.2 Neuer Bundestag – neues Glück

Die Weiterentwicklung des analogen um einen digitalen Grundrechtsschutz ist nicht nur nötig. Sie findet auch statt. Die analoge Sicht des Datenschutzes war lange negativ geprägt, etwa als bürokratisches Hindernis für die Privatwirtschaft oder als Täterschutz für die Sicherheits-, Finanz- und Sozialbehörden. Diese Sicht, die lange Zeit das Regierungshandeln bestimmte, scheint immer mehr einer differenzierten Sicht zu weichen, die das nötige Verständnis für die Besonderheiten digitaler Vorgänge hat. Ausdruck dessen ist die **Koalitionsvereinbarung** für die 17. Legislaturperiode des Deutschen Bundestages vom Oktober 2009, in der sich ein umfangreiches Kapitel mit der Informations- und Mediengesellschaft allgemein und mit dem Datenschutz konkret beschäftigt. Das Internet wird als das „freiheitlichste und effizienteste Informations- und Kommunikationsforum der Welt“ dargestellt. Netzneutralität, IT-Kompetenz, Selbstdatenschutz und verbesserte Strafverfolgung – auch bei Persönlichkeitsrechtsverletzungen – werden als staatliche Aufgaben ausdrücklich hervorgehoben.

Konkret ergeben sich daraus für die Koalitionsparteien **politische Handlungsnotwendigkeiten**. Hierzu gehört die Regelung des Datenschutz-Audits (Tz. 9.1) und des Arbeitnehmerdatenschutzes, der bisher nur rudimentär und unbefriedigend normiert ist (Tz. 5.1.1). Ein weites Handlungsfeld eröffnet sich in der Schaffung einer grundrechts- und sicherheitsfreundlichen Internetinfrastruktur, bei welcher der elektronische Personalausweis, die sogenannten De-Mail-Angebote mit Funktionen zur Verschlüsselung und zur digitalen Signatur sowie die rechtliche Basis in Form eines Bürgerportalgesetzes eine Rolle spielen.

Von den Koalitionsparteien wird versprochen, „das **Bundesdatenschutzgesetz** unter Berücksichtigung der europäischen Rechtsentwicklung lesbarer und verständlicher (zu) machen sowie zukunftsfest und technikneutral aus(zu)gestalten“. Da sich diese Aufgabe mit den Novellierungen im Jahr 2009 (Tz. 5.1.1) nicht erledigt hat, wurde von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Herbst 2009 eine Arbeitsgruppe eingerichtet, die konsistente Vorschläge für eine derartige Novellierung auf der Basis der Kontroll- und Beratungserfahrungen erarbeiten soll. Dabei erweist sich die versprochene umfassende BDSG-Novellierung als eine Herkulesaufgabe; seit 1990 sind die Strukturen dieses Gesetzes unangetastet geblieben. Anders als in Schleswig-Holstein wurde im Bund um die Jahrtausendwende anlässlich der Anpassung an die europäische Datenschutzrichtlinie keine konsistente Modernisierung vorgenommen.

Schon die reine Aufzählung der **notwendigerweise neu zu bearbeitenden Themen** zeigt die Dimension des erforderlichen Gesetzgebungswerkes:

- Definition des personenbezogenen Datums,
- Definition der Verarbeitungsphasen (übergeordneter Begriff des „Verarbeitens“, Einführen des Begriffs des „Veröffentlichens“),
- Beseitigung der Differenzierung Akte – (automatisierte) Datei,
- Klärung der Verantwortlichkeit bei komplexer Verarbeitung,
- Angleichung öffentlicher – nicht öffentlicher Bereich,
- Klarstellung der Anwendbarkeit des Datenschutzrechts (private Veröffentlichung, Rechtsanwälte, Finanzverwaltung, Gerichte),
- Spezifizierung der Normen bei der Auftragsdatenverarbeitung,
- Justierung des Rechts auf informationelle Selbstbestimmung mit den Grundrechten aus Art. 5 Grundgesetz,
- Regeln zur Konzerndatenverarbeitung,
- Erhöhung der Transparenzanforderungen,
- Benennung von Standards für das Datenschutzmanagement,
- Umstellung der technisch-organisatorischen Maßnahmen auf Schutzziele,
- Spezialanforderungen zum Zweck der Datensicherheit (Datenkennzeichnung, Verarbeitungsprotokollierung),
- Überarbeitung der Regeln zum Einsatz bestimmter Technologie (Einsatz von Funkchips wie RFID, mobile Datenverarbeitung, Lokalisierungsdienste, Videoüberwachung, gemeinsame Verfahren),
- Spezialkapitel zur Internetdatenverarbeitung mit Regeln zur Transparenz, zur Suchbarkeit, zur anonymen Veröffentlichung, zur Konfliktbearbeitung und zur Löschung,
- separate Spezialregelungen zu bestimmten Zwecken (z. B. Bonitätsbewertung, Werbung),
- Spezialregelungen zum Beschäftigtendatenschutz,
- Sicherung des Rechts auf Selbstdatenschutz,
- Ausweitung und Vereinfachung der Auskunftsansprüche Betroffener,
- Einführung bzw. Ausbau zivilrechtlicher Instrumente (z. B. Haftung),
- Einführung eines Datenschutz-Audits bzw. eines Verfahrens zur Zertifizierung von IT-Produkten und -Dienstleistungen,
- Sicherung der Unabhängigkeit und der föderalen Arbeitsteilung bei den Datenschutzbehörden,
- Neujustierung der Ermittlungs- und Sanktionskompetenzen der Datenschutzaufsicht und Ausweitung der Sanktionsmöglichkeiten,
- Ausbau der Datenschutzbehörden zu Serviceeinrichtungen,
- Einführung von Verbandsklagen (Verbraucherschutz, Arbeitnehmerdatenschutz).

Angesichts der bestehenden Herausforderungen sollte sich der neue Bundestag gleich zu Beginn seiner Tätigkeit darüber verständigen, wie er diese zu bewältigen gedenkt. Die Leidensgeschichte der BDSG-Novellierungen der letzten 15 Jahre voll verpasster Gelegenheiten darf nicht fortgesetzt werden. Es ist wohl unrealistisch, das BDSG in einem Kraftakt insgesamt zu reformieren. Hierbei werden zu viele Interessen tangiert, die auf das Gesamtwerk Einfluss zu nehmen suchen. Daher scheint es angebracht, eine Novellierung vom Allgemeinen zum Konkreten **in Einzelschritten** vorzunehmen und allenfalls brandaktuelle Kapitel wie den Arbeitnehmerdatenschutz und das Audit vorzuziehen.

Wichtiger als eine Klärung des chronologischen Vorgehens ist die **Struktur des parlamentarischen Entscheidungsprozesses**. Es scheint, als bedürfe der Bundestag eines separaten Gremiums, das sich ausschließlich der Aufgabe widmet, den Anforderungen an das künftige „Lex digitalis“ gerecht zu werden. Der aktuelle Vorschlag zur Einrichtung einer Enquetekommission weist in die richtige Richtung. Eine Einbindung der Länder nicht nur über den Bundesrat, sondern über deren Aufsichtsbehörden als wichtige Datenschutzexperten „an der Front“ sollte selbstverständlich sein. Daran besteht ein inhaltliches Interesse; dies ist auch nötig, um die für eine Umsetzung des Gesetzes unabdingbare gesellschaftliche Akzeptanz sicherzustellen.

2.3 Handlungsfeld – die ganze Welt

Globale Informationsgesellschaft bedeutet, dass weltweit agierende Unternehmen die Nutzungsdaten von Hunderten von Millionen Internetnutzerinnen und -nutzern praktisch unbeschränkt speichern und auswerten können und dass diese Unternehmen mehr Wissen und Macht über Menschen haben als die meisten Staaten. Wirtschaftsunternehmen können mit Daten Menschen gefügig machen, ohne dass die Betroffenen dies überhaupt merken. Es sind heute für viele noch Fremdwörter: Tracking, Scoring, Profiling, Identity Theft. Derart werden nicht nur Daten verarbeitet, so werden Menschen überwacht, diskriminiert und manipuliert, so werden Menschen ihrer Freiheit beraubt.

Immer gravierendere Folgen auf das lokale Datenschutzniveau hat die Situation in den **Vereinigten Staaten von Amerika** (USA). Wegen der engen politischen, wirtschaftlichen, sozialen, kulturellen und menschlichen Beziehungen zwischen Europa und den USA gibt es nicht nur einen intensiven Datenaustausch, sondern auch eine gegenseitige Beeinflussung beim Datenschutz. Dabei kann leider nicht von einer gleichgewichtigen Beziehung gesprochen werden. Vielmehr setzten sich beim Zwang zu einer Einigung bisher regelmäßig die USA durch. Dies war und ist weiterhin gleichbedeutend mit einem niedrigen Niveau des Datenschutzes, tendenziell hin bis zur völligen Ausblendung desselben.

Bei Safe Harbor erfolgte zwar eine formale Anerkennung einiger grundlegender Datenschutzprinzipien durch die USA, doch sind bis heute nicht einmal Ansätze für deren Realisierung erkennbar (Tz. 11.4). Bei Internetangeboten aus den USA ist es manchmal reine Glückssache, wenn Persönlichkeitsbeeinträchtigungen beendet werden können (31. TB, Tz. 7.4). Insbesondere bei den Angeboten von

Google ist in Grundsatzfragen noch keine Bewegung zu erkennen. Dies ist gravierend, da dieses Unternehmen in vielen Bereichen, voran bei den Suchmaschinen, den deutschen und europäischen Markt dominiert (Tz. 7.1 und Tz. 7.2). Ist es der reinen Marktmacht Googles geschuldet, die zum **Unterschreiten eines akzeptablen Datenschutzniveaus** führt, so ist die Selbstaufgabe des Datenschutzes im Sicherheitsbereich durch europäische Stellen nicht rational erklärbar. So bestand nach dem Umzug eines SWIFT-Rechenzentrums von den USA in die Schweiz die Möglichkeit, der nach europäischem Recht illegalen Auswertung von Banktransaktionsdaten endgültig den Garaus zu machen. Stattdessen aber öffnete der Europäische Rat von sich aus den USA zu weitgehend unkontrolliertem Tun diese Datenbestände (Tz. 11.3). Dem vorausgegangen war die Bereitstellung von Flugpassagierdaten, der „Passenger Name Records“, ohne hinreichende Datenschutzgarantien.

Der **Wechsel der US-Administration** Anfang 2009 war mit der Hoffnung bei europäischen Datenschützern verbunden, dass eine Trendwende in der US-Datenschutzpolitik erfolgt. Diese Hoffnungen wurden durch eine äußerst agile außerinstitutionelle Präsenz des Privacy-Gedankens in den USA, bei Bürgerrechtsorganisationen, in der Wissenschaft und auch bei einigen Unternehmen genährt. Mit Kanada haben die USA einen Nachbarn, der ein dem europäischen entsprechendes Datenschutzniveau aufweisen kann. Doch sind diese modernisierungsfördernden Momente noch nicht bis zur nach außen sichtbaren Politik durchgedrungen. Dies ist bedauerlich. Auf dem globalen Markt der Informationstechnik drängen mit China und einigen anderen Schwellenländern Staaten nach vorne, bei denen ein freiheitliches Verständnis von Datenschutz nicht nur auf Unverständnis und Ablehnung, sondern sogar auf aktive Abwehr stößt.

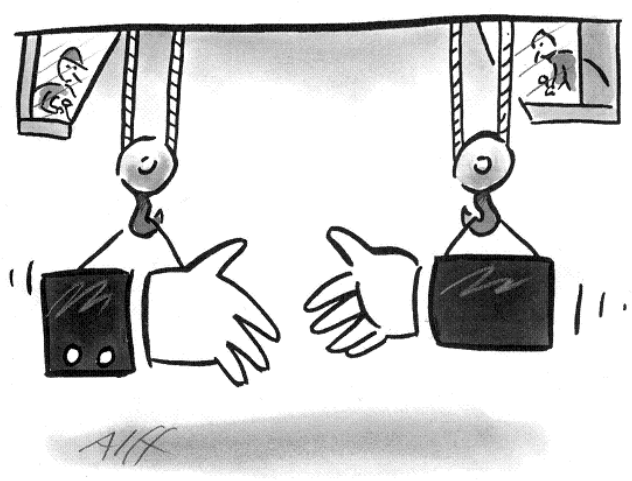
Globale Informationsgesellschaft bedeutet, dass Diktaturen mithilfe ihrer Internetüberwachung jede elektronische Kommunikation scannen, speichern, auswerten, kontrollieren und unterbinden können. Ein wesentliches Phänomen dabei ist, dass die Technik für die Überwachung und Zensur oft **aus westlichen Staaten importiert** wird – aus demokratischen Staaten wie Deutschland. Hiermit müssen wir uns in den freiheitlichen Gesellschaften ebenso auseinandersetzen wie mit dem Waffenexport in Krisengebiete.

2.3.1 Globale Harmonisierung

Nationales Recht, dessen Wirkung oder zumindest Durchsetzbarkeit zumeist an der Grenze endet, passt oft nicht mehr in der globalisierten und vernetzten Informationsgesellschaft. Eine Harmonisierung ist auch im Bereich Datenschutz nötig – im ersten Schritt auf der Ebene von Prinzipien.

Als die spanische Datenschutzbehörde dazu aufrief, gemeinsam einen Vorschlag für internationale Standards zum Datenschutz zu erarbeiten, haben wir – wie auch Kollegen aus vielen anderen Ländern – unsere Ideen eingebracht. Mit dem Fortschreiten internationaler Zusammenarbeit, globalem Handel und nicht zuletzt dem Internet werden personenbezogene Daten der Bürgerinnen und Bürger Schleswig-Holsteins immer öfter außerhalb Deutschlands und der Europäischen Union verar-

beitet. Bei einer internationalen Harmonisierung darf man es sich nicht dadurch einfach machen, dass der kleinste gemeinsame Nenner, also das schwächste Datenschutzniveau, zum Maßstab genommen wird. Darin waren sich alle Mitwirkenden aus dem Bereich der Datenschutzbehörden einig. Nach einiger Diskussion kristallisierten sich 25 Abschnitte heraus, in denen **Grundsätze zur Verarbeitung und zum Schutz personenbezogener Daten** beschrieben werden.



Das Resultat, die sogenannte „**Madrid-Resolution**“, wurde im November 2009 auf der 31. Internationalen Datenschutzkonferenz vorgestellt. Es haben bei Weitem noch nicht alle Länder der Welt diese Resolution mitgezeichnet, und sicherlich besteht weiterer Verbesserungsbedarf. Doch ist dies ein bemerkenswerter Schritt in Richtung Harmonisierung, die über den europäischen Rechtsraum hinausgeht. Nun gilt es, die Prinzipien weiter fortzuschreiben und auf internationaler Ebene in das Recht einzubringen. Mittelfristiges Ziel könnte eine völkerrechtlich verbindliche Konvention zu Datenschutzprinzipien sein.

2.3.2 Internationale Standardisierung

Wer sich mit Gestaltung oder Betrieb von Technik beschäftigt, kommt auf irgendeine Art mit den Spezifikationen der Standardisierungsorganisationen ISO und IEC in Berührung. Nun sollen deren Arbeiten im Bereich der Datensicherheit um eigene Datenschutzstandards ergänzt werden.

Neben rechtlichen Standards kommt für einen effektiven Datenschutz der technischen Standardisierung ein hoher Stellenwert zu, denn eine Vielzahl **technischer Standards** tangieren Datenschutzbelange in nicht unerheblichem Maße. Einige Standards sehen z. B. die Verwendung von bestimmten Daten vor, die bei einer alternativen Konzeption gemäß dem Datensparsamkeitsgrundsatz weggelassen werden könnten. Durch datenschutzfreundliche Gestaltung dieser Standards können frühzeitig mögliche Risiken reduziert oder ganz ausgeschlossen werden. Leider ist es den Datenschutzbehörden mit ihrer derzeitigen Ausstattung aufgrund der Vielzahl technischen Standardisierungs-

> **?** ***ISO und IEC***
>
> *ISO (engl.: International Organization for Standardization), die Internationale Organisation für Normung, erarbeitet internationale Normen in vielen Bereichen, die für das tägliche Leben notwendig sind. In Bezug auf Technikstandards kooperieren ISO und IEC, die Internationale elektrotechnische Kommission, die für Standards im Bereich Elektrik und Elektronik zuständig ist.*

aktivitäten nur selten möglich, ihre Expertise in den entsprechenden Gremien einzubringen.

Unter Nutzung von Projektmitteln der Europäischen Union beteiligt sich das ULD bereits seit 2007 an der gemeinsamen Arbeitsgruppe „**Identitätsmanagement und Datenschutztechnik**“ von ISO und IEC. Zentrale Standards, an denen das ULD hier mitwirkt, sind „ISO 29100 – Privacy Framework“, ein Rahmenstandard, der Grundbegriffe und Prinzipien zum Datenschutz und zum Schutz der Privatsphäre definiert, sowie „ISO 29101 – Privacy Reference Architecture“, in dem Eckpunkte für datenschutzfreundliche technische Architekturen beschrieben werden. Mit einer Veröffentlichung dieser Standards ist in Zukunft zu rechnen. Neben der Beteiligung an der Entwicklung dieser Standards bindet das ULD andere Datenschutzbehörden auf nationaler und europäischer Ebene in die Arbeit ein.

http://www.iso.org/iso/iso_technical_committee.html?commid=45306

3 Landtag

Der Landtag Schleswig-Holstein ist nicht nur das vom Volk gewählte oberste Organ der politischen Willensbildung. Das Parlament des Landes ist auch eine Organisationseinheit mit dem Landtagspräsidenten an der Spitze, in der unterschiedlichste **personenbezogene Daten verarbeitet** werden. Dies gilt für die oft äußerst sensiblen Eingaben, die im Petitionsausschuss und in dessen Geschäftsstelle verarbeitet werden, für den Internetauftritt des Parlaments und die elektronische Kommunikation, für den Betrieb der Telefonanlage (31. TB, Tz. 3), für die Verumdruckung des Schriftwechsels zwischen Bürgerinnen und Bürgern, Verbänden und Organisationen mit der Landtagsverwaltung, den Abgeordneten und den Ausschüssen (30. TB, Tz. 3.1) oder für die allgemeinen Verwaltungsvorgänge.

Der Landtag ist die Legislative, also die gesetzgebende Gewalt in Schleswig-Holstein. Das ULD wird zwar haushaltstechnisch beim Landtag geführt und hat eine gesetzlich definierte, von der Landesregierung weitgehend unabhängige Stellung. Doch sind dessen Tätigkeiten trotz der damit verbundenen Kontrollfunktionen unbestreitbar der exekutiven Gewalt zuzurechnen. Die **Gewaltenteilung** lässt es nicht zu, dass eine Stelle der Exekutive eine Kontrolle der Legislative vornimmt. Es ist umgekehrt Aufgabe des Parlaments, die Verwaltung zu kontrollieren. Daher kann es auch dem ULD – trotz aller gesetzlich gewährleisteten Unabhängigkeit – nicht zustehen, die personenbezogene Datenverarbeitung im Landtag zu kontrollieren.

Auch das Landesdatenschutzgesetz passt nicht auf die Wahrung des Persönlichkeitsschutzes im parlamentarischen Betrieb: Einerseits ist größtmögliche Transparenz des Parlamentsbetriebes geboten, da die getroffenen Entscheidungen und die Daten dazu – im wahrsten Sinne des Wortes – alle angehen und Persönlichkeitsrechte im Interesse demokratischer Transparenz oft zurückstehen müssen. Andererseits muss die **Vertraulichkeit von politischen Verhandlungen** und des Kontaktes zwischen Bevölkerung und Abgeordneten gesichert werden. Dies gilt – was für andere Stellen eher untypisch ist – auch innerhalb des Hauses: Die Fraktionen und die Abgeordneten wollen sich selbstverständlich nicht gegenseitig in die Karten schauen lassen.

Der Landtag hat hieraus die rechtlichen und organisatorischen Konsequenzen gezogen und sich selbst 1998 eine **Datenschutzordnung** gegeben. Darin ist vorgesehen, dass bei Datenschutzbeschwerden gegen den Landtag, die es selbstverständlich auch gibt und die in Unabhängigkeit bearbeitet werden müssen, sowie für die Datenschutzkontrolle ein Datenschutzgremium eingerichtet wird, dem jeweils ein Mitglied jeder Fraktion angehört.

Von Beginn an war vorgesehen und ist es seitdem bewährte Praxis, dass das ULD das **Datenschutzgremium berät**. Bei der Beratung geht es insbesondere darum, die technischen Kompetenzen des ULD zur Verfügung zu stellen. Diese kann aber auch weitergehen, indem das ULD unter Einbeziehung des Datenschutzgremiums bestimmte sensible Verfahren begutachtet und sogar in einem förmlichen Verfah-

ren deren Datenschutzkonformität bestätigt. So war der Landtag Vorreiter in mehreren Auditierungsverfahren, in denen die Datenschutzkonformität des Petitionsverfahrens und des Internetauftritts (25. TB, Tz. 3.2), des Zutrittsberechtigungssystems, der Videoüberwachung (27. TB, Tz. 3.1; 29. TB, Tz. 3.1) bzw. generell des Sicherheitskonzeptes geprüft und bestätigt wurde.

Was ist zu tun?
Das ULD wird weiterhin vertrauensvoll mit dem nach der Landtagswahl im September 2009 neu konstituierten Datenschutzgremium zusammenarbeiten.

4 Datenschutz in der Verwaltung

Die Automation in der Verwaltung geht rasant voran, auch wenn sich dies nicht in dicken Schlagzeilen in der Presse niederschlägt. Es geht nicht mehr um das „Ob“ des IT-Einsatzes, sondern um das weniger spektakuläre „Wie“. Beim „Wie“ ist der Datenschutz besonders gefordert. Dass dies nicht nur das ULD, sondern – mit wenigen Ausnahmen – inzwischen die gesamte Landes- und Kommunalverwaltung so sieht, erleichtert unseren Job gewaltig. Bei Projektplanungen wird das ULD frühzeitig eingebunden; unsere Vorschläge zu Strukturen wie zur konkreten Umsetzung werden regelmäßig berücksichtigt.

Die bedeutet jedoch nicht, dass im Land alles gut wäre beim Datenschutz. Dies zeigen die vielen Verstöße, die uns immer noch mitgeteilt werden und die wir beanstanden müssen. Doch scheint zumindest die nachträgliche Einsicht um sich zu greifen, nicht zuletzt weil inzwischen Datenschutzfragen oft und gerne von Medien aufgegriffen werden und Verstöße **Negativschlagzeilen** produzieren können. Wir stellen fest, dass die positive Resonanz auf eine unbeschönigte Sprache des Datenschutzes im Land schneller ankommt als auf Bundesebene, z. B. bei der Bundesanstalt für Arbeit. Dies hat sicher damit zu tun, dass öffentliche Diskussion vor Ort nachhaltiger wirkt als bei weit entfernten Zentraleinrichtungen. Dies muss sich – auch im Interesse des Landes – ändern, da nicht nur die Bundesgesetzgebung, sondern auch der Vollzug von Bundesbehörden einen zunehmenden Einfluss auf die personenbezogene Datenverarbeitung bei Stellen des Landes hat.

4.1 Allgemeine Verwaltung

4.1.1 Gesundheitsuntersuchung bei Bewerbern für Angestelltenpositionen

Die gesundheitliche Untersuchung von Tarifbeschäftigten vor der Einstellung ist in begrenztem Umfang zulässig: Es darf nur festgestellt werden, ob die Bewerber gegenwärtig gesundheitlich zur Ausübung der jeweils angestrebten Tätigkeit in der Lage sind.

Im Mai 2009 wurde das ULD durch Medienberichte auf die Praxis bei der Einstellung von Tarifbeschäftigten in einem Kreis aufmerksam. Die daraufhin durchgeführte datenschutzrechtliche Prüfung ergab Folgendes: Wenn eine Bewerberin oder ein Bewerber für eine zu besetzende Angestelltenposition ausgewählt worden war, wurde sie oder er durch das Gesundheitsamt des Kreises einer Gesundheitsuntersuchung unterzogen. Es wurde den Betroffenen zunächst ein **umfangreicher Fragebogen** zugesandt. Dieser enthielt eine Vielzahl von sehr intimen Fragen, wie z. B. danach, ob jemals eine ärztliche oder psychologische Behandlung stattgefunden habe, nach dem Alkohol- und Drogenkonsum, nach belastenden Erlebnissen in der Vergangenheit, nach der allgemeinen Stimmung und nach dem Bestehen oder der Möglichkeit einer Schwangerschaft. Zwar enthielt der Bogen den Hinweis, die Beantwortung sei freiwillig. Im von der Presse aufgegriffenen Fall hatte die Bewerberin es allerdings abgelehnt, den Bogen auszufüllen, mit der Folge, dass sie den Job, für den sie schon ausgewählt war, nicht erhielt.

Mit dem ausgefüllten Bogen hatten sich die Bewerbenden in der Regel zu zwei Terminen beim Gesundheitsamt einzufinden. Beim ersten Termin wurde **Blut abgenommen** und an ein Labor zur Untersuchung geschickt; analysiert wurden im Wesentlichen der Stoffwechsel sowie einige allgemeine Blutwerte. Eine diesbezügliche Aufklärung der Bewerber einschließlich der Frage, welche Erkenntnisse sich für ihre Eignung aus der Untersuchung ergeben würden, erfolgte nicht. Weiterhin wurden beim ersten Termin ein EKG, ein Hörtest und ein Sehtest vorgenommen.

Beim zweiten Termin wurde von den untersuchenden Ärzten eine **ausführliche ärztliche Anamnese** aufgenommen. Erhoben wurden teilweise sehr persönliche Daten; es finden sich Aussagen wie „grübelt viel wegen Arbeitslosigkeit“, Angaben zu „Wasserlassen“ und „Stuhlgang“, zu Fehlgeburten, zur Familienanamnese – Krankheiten und Todesursache der Eltern – und zur sozialen Anamnese – Kinder, Schulabschluss, Ausbildung.

Auf der Grundlage aller erhobenen Daten beurteilten die Ärzte im Gesundheitsamt die **Eignung des Bewerbers** für die zu besetzende Stelle; das Ergebnis wurde dem Personalamt übermittelt. Bei unauffälligen Befunden wurde lediglich mitgeteilt, dass entsprechende Untersuchungen stattgefunden hätten und dass aus ärztlicher Sicht keine Bedenken gegen eine Beschäftigung bestünden. Bei etwa der Hälfte der geprüften Akten wurden jedoch zusätzlich zu der Unbedenklichkeitsbescheinigung auch Einzelheiten aus der Untersuchung an das Personalamt gemeldet. Dabei finden sich Bemerkungen wie „leicht depressive Persönlichkeitsstruktur“ oder „Fettleibigkeit … es besteht ein erhebliches Risiko für die weitere Entwicklung einer Arteriosklerose“.

Der Landkreis hat sofort nach Bekanntwerden der Angelegenheit die Verwendung des vorab versendeten Fragebogens gestoppt und sämtliche bis dahin erhobenen **Fragebögen vernichtet**.

Die vorgefundene Verfahrensweise verstieß in mancher Hinsicht gegen den Datenschutz. Es stellt sich die Frage, ob Gesundheitsuntersuchungen von Bewerbern für Angestelltenpositionen überhaupt verlangt werden dürfen. Der aktuelle Tarifvertrag für den öffentlichen Dienst, der TVöD, sieht keine entsprechende **Pflicht der Bewerber** vor, anders als noch der Vorläufer-Tarifvertrag, der BAT. Doch ist in der arbeitsgerichtlichen Rechtsprechung anerkannt, dass der Arbeitgeber vor dem Abschluss des Arbeitsvertrages verlangen kann, dass der Bewerber sich ärztlich untersuchen lässt. Der Bewerber ist jedoch nicht verpflichtet, die Untersuchung über sich ergehen zu

lassen. Verweigert er diese, so ist es nach der Rechtsprechung der Arbeitsgerichte nicht zu beanstanden, wenn der Arbeitgeber von der Einstellung des Bewerbers absieht.

Die ärztliche Untersuchung darf aber nur dazu dienen festzustellen, ob zum Zeitpunkt der Einstellung die **gesundheitliche Eignung des Bewerbers** für den zu besetzenden Arbeitsplatz gegeben ist. Der Arbeitgeber bzw. die in seinem Auftrag tätigen Ärzte dürfen keine Daten über eventuelle Krankheitsanlagen, die sich noch nicht realisiert haben, erheben. Das Risiko, dass der Arbeitnehmer während des in Vollzug befindlichen Arbeitsverhältnisses erkrankt, hat grundsätzlich der Arbeitgeber zu tragen. Nach Datenschutzrecht erforderlich sind nur die Daten, die für die Entscheidung über die Einstellung benötigt werden; lediglich diese dürfen erhoben werden.

Die gesundheitliche Untersuchung von Bewerbern für Angestelltenpositionen gehört nicht zu den gesetzlich vorgegebenen **Aufgaben des Gesundheitsamtes**. Vielmehr wird das Gesundheitsamt quasi als verlängerter Arm des Arbeitgebers tätig. Daher gelten die in der arbeitsrechtlichen Rechtsprechung entwickelten Grundsätze zum Fragerecht des Arbeitgebers auch für das Gesundheitsamt.

Nach diesen Grundsätzen ist die Durchführung eines Seh- und Hörtests und des EKGs nicht zu beanstanden. Diese erhobenen Daten können bei der Beurteilung der gegenwärtigen Eignung von Bedeutung sein. Dagegen waren die Erhebungen im vorab versendeten Fragebogen und im Rahmen der ärztlichen Anamnese unzulässig und wurden vom ULD beanstandet. Bemängelt wurde auch, dass die Erhebung der **Blutwerte ohne Aufklärung** erfolgte. Es fehlte an der Information der Bewerber darüber, welche Blutwerte untersucht wurden und welche Erkenntnisse sich daraus ergeben würden. Beanstandet wurden ferner nicht erforderliche Datenübermittlungen an das Personalamt. Das Gesundheitsamt hätte sich auf die positive Meldung „für die Stelle geeignet“ beschränken müssen.

Warum wurden derart umfangreiche nicht erforderliche Daten erhoben? Das Gesundheitsamt verwendete die hier eingesetzten Formulare in **allen Fällen von Begutachtungen**. Dies betraf neben der Einstellung von Tarifbeschäftigten die Übernahme ins Beamtenverhältnis, Frühpensionierungen, Untersuchungen im Hinblick auf die Arbeitsfähigkeit bei Beziehern von Sozialleistungen usw. In den letztgenannten Konstellationen greifen aber andere Untersuchungskriterien. Es besteht zudem für die Betroffenen eine gesetzliche Pflicht, sich untersuchen zu lassen; das Gesundheitsamt hat dazu korrespondierend eine gesetzliche Befugnis, solche Untersuchungen vorzunehmen.

Das ULD hat die Prüfung zum Anlass genommen, sich verstärkt mit der Thematik zu befassen. Es wird zusammen mit dem betroffenen Landkreis und der Arbeitsgemeinschaft der Gesundheitsämter auf Landesebene zu rechtmäßigen und **allgemein akzeptierten Lösungen** bei der Begutachtung von Bewerbern für Angestelltenpositionen beitragen.

Was ist zu tun?
Bei der Einstellung von Angestellten sind öffentliche Stellen an die durch die arbeitsgerichtliche Rechtsprechung aufgezeigten Grenzen gebunden. Die Fragen durch das Gesundheitsamt sind in jedem Fall dem Arbeitgeber zuzurechnen.

4.1.2 Vollständige Personalakten für das Finanzverwaltungsamt

Die Übermittlung vollständiger Personalakten an das Finanzverwaltungsamt ist zur Durchführung familienrechtlicher Versorgungsausgleichsverfahren nicht erforderlich. Personalverwaltende Stellen müssen im Einzelfall die notwendigen Daten aus der Personalakte herausfiltern und dem Finanzverwaltungsamt zur Verfügung stellen. Ausnahmen bedürfen der schriftlichen Einwilligung der Betroffenen.

Immer wieder wird das ULD gefragt, ob das Finanzverwaltungsamt für familienrechtliche Versorgungsausgleichsverfahren vollständige Personalakten der Betroffenen erhalten darf. Das Landesbeamtengesetz gilt aufgrund einer Verweisung im Landesdatenschutzgesetz für alle Beschäftigten des Landes. Danach ist von einer Vorlage der Personalakte abzusehen, soweit eine Auskunft ausreicht. Vorlage und Auskunft sind auf den **erforderlichen Umfang** zu beschränken.

In Personalakten befinden sich viele sensible Daten ohne Relevanz für familienrechtliche Versorgungsausgleichsverfahren. Eine Übersendung der gesamten Akte ist allenfalls zulässig, wenn der Betroffene zuvor schriftlich eingewilligt hat. In allen anderen Fällen sollte es ausreichen, wenn die personalverwaltenden Stellen die **Daten zum beruflichen Werdegang** übermitteln. Eine detaillierte Kenntnis des Versorgungsrechts ist dafür bei den personalverwaltenden Stellen nicht erforderlich, da sie den beruflichen Werdegang nicht bewerten müssen.

Soll im begründeten Einzelfall eine Einwilligung für die Übersendung der Personalakte eingeholt werden, ist dafür das Finanzverwaltungsamt formal zuständig. Gemäß dem Landesdatenschutzgesetz muss für Datenübermittlungen die **ersuchende Stelle** die erforderlichen Angaben machen, insbesondere die Rechtsgrundlage benennen. Dies schließt gegebenenfalls den Nachweis der Einwilligung durch das Finanzverwaltungsamt ein.

Was ist zu tun?
Das Finanzverwaltungsamt sollte bei einer klaren beruflichen Historie des Betroffenen sich mit einer verbindlichen Auskunft der personalverwaltenden Dienststellen begnügen und auf eine Vorlage der Personalakte verzichten. In Ausnahmefällen sollte der Betroffene selbst um Einwilligung zur Übermittlung der Personalakte bitten.

4.1.3 Meldedatenabrufe durch die Polizei – endlich gesetzlich geregelt

Die Polizei benötigt für Zwecke der Gefahrenabwehr und Strafverfolgung listenmäßige Auswertungen aus den Melderegistern. Die fachliche Notwendigkeit eines solchen Online-Abrufs ist oft nicht zu bestreiten, nötig ist aber eine ausreichende gesetzliche Grundlage.

Seit September 2009 erlaubt das geänderte Landesmeldegesetz der Polizei „eine Datenabfrage auch ohne Kenntnis konkreter Identifikationsmerkmale von Personen“. Im Jahr 2005 stellten wir anlässlich einer Prüfung fest, dass die Polizei **Listenauskünfte**, z. B. Abfragen nach Straße und Hausnummer, erhalten hatte, ohne die vorgeschriebenen Angaben zur Identität der angefragten Personen gemacht zu haben. Solche Auskünfte waren nach damaliger Rechtslage nur in Papierform und nach Einzelfallprüfung durch die zuständige Meldebehörde zulässig.

Als Reaktion auf unser Prüfergebnis wollte die Polizei nicht das praktizierte Verfahren ändern, sondern forderte eine Anpassung der Rechtslage. In Fällen der Strafverfolgung und Gefahrenabwehr sei häufig ein sofortiger automatisierter Informationszugang zu den Meldedaten unter **Verwendung allgemeiner Suchkriterien** erforderlich. Dieses Anliegen schien uns plausibel. Gemäß unserer Empfehlung beschränkte das Innenministerium im Gesetzentwurf die Zulässigkeit der Abrufe darauf, dass „dies zur Gefahrenabwehr oder Strafverfolgung im Einzelfall erforderlich ist“. Durch eine Neukonzeption des EDV-Verfahrens werden zudem nur vordefinierte Auswertemöglichkeiten zur Verfügung gestellt, was die Einhaltung des Erforderlichkeitsprinzips technisch sicherstellt. Es besteht Einvernehmen mit der Polizei, dass lediglich eine Suche unter Verzicht auf bestimmte Identifikationsmerkmale, und zwar Vorname, Nachname, Anschrift, Geburtsdatum, und unter Angabe von Straße und Hausnummer erfolgen soll. Eine Kennzeichnung und Protokollierung der Abrufe soll später eine Evaluierung der Abrufberechtigung ermöglichen.

4.1.4 Internet und E-Mail in Kommunen – Sensibilität noch rudimentär

Unzulässige Veröffentlichungen vertraulicher Daten in Sitzungsunterlagen kommunaler Gremien auf der gemeindlichen Homepage nehmen zu, weil die einzustellenden Dokumente unzureichend kontrolliert werden. Für die Veröffentlichung privater Anschriften und Telefonnummern von ehrenamtlich Tätigen fehlt häufig die Einwilligung.

Die **Recherche nach den eigenen Daten** in Internetsuchmaschinen ist äußerst beliebt. Wer sich dabei auf der Homepage seiner Gemeinde wiederfindet, ist nicht immer begeistert: Mehrfach fanden Betroffene ihre Daten, verbunden mit Details über ihre Einwendungen gegen die Bauleitplanung. In einem Fall wurden Einzelheiten über eine Bewerberin um eine Sachgebietsleiterstelle ungewollt bekannt gegeben. Mandatsträger und andere ehrenamtlich Tätige wurden mit ihrer privaten Anschrift und Telefonnummer aufgeführt, ohne ihre Einwilligung erteilt zu haben.

Die Probleme erklären sich mit der Neigung von Kommunen, die Protokolle von Gemeindevertreter- und Ausschusssitzungen sowie die dazugehörigen Beschlussvorlagen der Allgemeinheit über das Internet zugänglich zu machen. Bei öffentlichen Sitzungen, in denen keine vertraulichen personenbezogenen Daten verarbeitet werden, bestehen insofern keine Datenschutzbedenken. In den beanstandeten Fällen fand jedoch keine ausreichende Prüfung und Abtrennung vertraulicher Unterlagen statt. Bei Einstellung von Dokumenten ins Internet sollte in jedem Fall das sogenannte **Vieraugenprinzip** gelten. Bei Einwendungen gegen die Bauleitplanung hätte zumindest eine Pseudonymisierung der Vorgänge stattfinden müssen, z. B. durch Beratung der Einwendungen unter einer Nummer anstelle des Namens.

Bei Mandatsträgern und anderen ehrenamtlich Tätigen ist die Veröffentlichung von Angaben, die nicht unmittelbar mit ihrer **Funktion** zu tun haben, nur zulässig, wenn dafür deren schriftliche Einwilligung vorliegt. Dies gilt auch für private Anschriften und Telefonnummern. Die dienstliche Erreichbarkeit – insbesondere von Mandatsträgern – kann und muss gegebenenfalls über ein Postfach im Rathaus gewährleistet werden.

Ehrenamtliche Bürgermeister sollten für ihre offizielle Tätigkeit statt ihrer privaten E-Mail-Adresse eine dienstliche und damit **funktionsbezogene Adresse** erhalten und verwenden. So können sie ihre Privatpost eindeutig von dienstlichen Vorgängen trennen. Auch die Bürgerinnen und Bürger sind so in der Lage, bereits bei der Adressierung festzulegen, ob sie den Bürgermeister als Privatperson, als Politiker oder in seiner dienstlichen Eigenschaft ansprechen wollen. Im Falle eines Ämterwechsels kann eine Mailadresse vom neuen Amtsinhaber problemlos übernommen und fortgeführt werden.

Zwar haben die Kommunen die beanstandeten Seiten schnell von ihrer Homepage entfernt, im **Cache der Suchmaschinen** blieben sie jedoch erhalten und damit für jeden Nutzer weiter verfügbar. Die Löschung dieser Speicherinhalte ist möglich, erfordert aber im Einzelfall einen nicht unbeträchtlichen Aufwand. Dieser Aufwand konnte den betroffenen Kommunen in den geprüften Fällen nicht erspart werden.

Was ist zu tun?
Kommunen sollten vor der Veröffentlichung von Unterlagen im Internet in jedem Einzelfall sorgfältig prüfen, ob vertrauliche personenbezogene Daten enthalten sind. Sollen private Anschriften und Telefonnummern von ehrenamtlich Tätigen in die Homepage aufgenommen werden, ist deren Einwilligung erforderlich.

4.1.5 Datenschutzkonforme freiwillige Umfrageaktionen

Öffentliche Stellen können im Rahmen ihrer Organisationshoheit freiwillige Umfragen grundsätzlich eigenständig vornehmen und gestalten. Doch müssen die Teilnehmerinnen und Teilnehmer vor der Befragung schriftlich über die Datenverwendung aufgeklärt werden. Dies ist zwingende Voraussetzung für eine wirksame Einwilligung der Betroffenen.

Ob es um die Zufriedenheit von Mitarbeitern am Arbeitsplatz, um Windkraftanlagen, den Ausbau von DSL-Anschlüssen in ländlichen Gebieten oder Ähnliches geht – in vielen Fällen kommen Fragebögen zum Einsatz, mit denen öffentliche Stellen Meinungen und damit Daten von Betroffenen auf freiwilliger Grundlage erheben. Wir haben mehrfach solche Verfahren bei öffentlichen Stellen geprüft, bei denen es oft an der **ausreichenden Anonymität** der Teilnehmer mangelte.

Befragungsaktionen müssen nicht zwangsläufig anonym stattfinden. Die Daten verarbeitenden Stellen können Verfahren und Modalitäten selbst festlegen, soweit dadurch nicht gegen Rechtsvorschriften verstoßen wird. Mit der Einwilligung der Betroffenen, die schon durch die **Teilnahme an der Befragung** zum Ausdruck kommt, kann eine personenbezogene Erhebung gerechtfertigt sein. Die befragende Stelle muss dann aber die Rahmenbedingungen der Befragung schriftlich, wenn möglich auf dem Fragebogen selbst, darlegen. Nur so sind die Betroffenen in der Lage abzuschätzen, was anschließend mit ihren Daten geschieht und in was sie mit der Teilnahme an der Befragung einwilligen.

Zu **folgenden Fragen** müssen die Betroffenen im Einzelnen aufgeklärt werden:

- Welchem Zweck dient die Befragung?
- Wer ist verantwortlich, wie erfolgt die Durchführung der Umfrage?
- Ist die Befragung anonym oder personenbeziehbar?
- Wie wird gegebenenfalls die Anonymität gewährleistet?
- Wer erhält gegebenenfalls Kenntnis bzw. Zugang zu personenbezogenen Daten?
- Werden Daten an Dritte übermittelt?
- Wann werden die Daten gelöscht?

Bei den von uns geprüften Fällen bestanden insbesondere Mängel bei der Aufklärung der Betroffenen über die Modalitäten der Befragung. Dies stellte die Wirksamkeit der Einwilligungen infrage, war aber auch schädlich für die Akzeptanz bei

den Betroffenen und wirkte sich so auf die Teilnehmerzahl aus. Transparenz ist also nicht nur eine Frage des Datenschutzes, sondern oft **Bedingung für den Erfolg** der Umfrage.

Was ist zu tun?
Daten verarbeitende Stellen sollten sich vor freiwilligen Umfragen sorgfältig mit der Beantwortung der vorstehenden Fragestellungen auseinandersetzen und die Modalitäten der Umfrage den Teilnehmenden schriftlich bekannt geben.

4.1.6 Grenzen der Privatisierung bei der Kurverwaltung

Der Trend zur Übertragung kommunaler Aufgaben auf private Dienstleister, die im überwiegenden Eigentum der Kommune stehen, hält weiter an. Die Grenzen der Auftragsdatenverarbeitung werden nicht immer ausreichend beachtet. Die gesetzlich vorgeschriebenen abschließenden Festlegungen für das Auftragsverhältnis fehlen häufig.

Wir hatten die Frage zu prüfen, ob es zulässig ist, einer Tourismusservice GmbH als privater Stelle im Sinne des Datenschutzrechts die Verarbeitung personenbezogener Daten für die Erhebung der Kurabgabe zu übertragen. Dies zählt nicht zum Kernbereich hoheitlicher Tätigkeit, sodass eine Beteiligung Dritter am Erhebungsverfahren auf der Grundlage der Auftragsdatenverarbeitung im Grundsatz möglich war. Allerdings müssen die Grenzen der Auftragsdatenverarbeitung sorgfältig beachtet werden. Insbesondere ist das Auftragsverhältnis so zu gestalten, dass dem Auftragnehmer keine Aufgaben zur eigenverantwortlichen Wahrnehmung übertragen werden, sondern er **nur weisungsgebunden** tätig wird.

Gegen eine Auftragsdatenverarbeitung sprach im konkreten Fall die **Kurabgabesatzung**, wonach die Tourismusservice GmbH beauftragt wurde, die Kurabgabe gemäß Satzung zu berechnen, diese entgegenzunehmen und anschließend mit der Kommune abzurechnen. Die Beauftragung durch eine Rechtsnorm erweckte den Eindruck, dass hier Aufgaben der öffentlichen Verwaltung, die in der Handlungsform des öffentlichen Rechts zu erledigen sind, an eine juristische Person des Privatrechts zur selbstständigen Wahrnehmung übertragen werden. Dies ist nach dem Landesverwaltungsgesetz nur durch oder aufgrund eines Gesetzes zulässig. Wir haben deshalb der Kommune empfohlen, diese Vorschrift aus ihrer Satzung zu entfernen.

Auftragsdatenverarbeitung bedingt den Abschluss eines Vertrages zwischen Auftraggeber und Auftragnehmer. Darin hat die Daten verarbeitende Stelle sicherzustellen, dass personenbezogene Daten **nur nach Weisung** verarbeitet werden. Die erforderlichen technischen und organisatorischen Maßnahmen sind festzulegen. Die Durchführung und Abwicklung des Auftrages sowie die Wahrnehmung der Kontrollrechte ist klar zu regeln, um den Handlungsspielraum des Auftragnehmers klar zu begrenzen. Nur hinreichend spezifizierte Weisungen können verhindern, dass es faktisch zu einer unzulässigen Funktionsübertragung kommt.

Wir empfahlen der Kommune, für die Kurabgabeerhebung und -kontrolle in einem Vertrag mit der Tourismusservice GmbH folgende Punkte präzise zu regeln, was sich übrigens auf andere Auftragsverhältnisse übertragen lässt:

- Beschreibung des Verwaltungsverfahrens der Kurabgabeerhebung und -überwachung,
- abschließende Festlegung der vom Auftragnehmer wahrzunehmenden Aufgaben,
- Benennung der verantwortlichen Personen bezüglich konkreter Aufgaben beim Auftraggeber wie beim Auftragnehmer,
- Sicherstellung einer ausreichenden Information der Kurgäste über die Auftragsdatenverarbeitung,
- Festlegung der erforderlichen Datensicherheitsmaßnahmen,
- Darlegung, wie der Auftraggeber die Einhaltung seiner Weisungen kontrollieren will.

Was ist zu tun?
Kommunen müssen beim Aufgabenoutsourcing durch Auftragsdatenverarbeitung sorgfältig darauf achten, dass die Grenzen nicht durch eigenverantwortliche Aufgabenwahrnehmung durch den Auftragnehmer überschritten werden. Die Verträge sollten zumindest die dargestellten Details regeln.

4.1.7 Unterrichtung der Handwerkskammer über Reisegewerbekarte

Die Unterrichtung anderer Behörden über ausgestellte Reisegewerbekarten ist bereichsspezifisch abschließend geregelt. Eine Beteiligung der Handwerkskammern ist nicht vorgesehen. Die Verwaltungsvorschriften zum Vollzug der Gewerbeordnung sehen nur eine Weitergabe an das Finanzamt, die Berufsgenossenschaft und gegebenenfalls die Ausländerbehörde vor.

Über Eingaben erfuhren wird, dass die Gewerbeämter der Kommunen häufig Daten über die Ausstellung einer Reisegewerbekarte an die jeweilige Handwerkskammer übermitteln. Die Kommunen verwiesen auf ein **Merkblatt der Handwerkskammer**, worin um Übersendung der entsprechenden Gewerbeanmeldung gebeten wurde. Hinweise auf Rechtsvorschriften zur Datenübermittlung waren dem Merkblatt nicht zu entnehmen.

Die Übermittlung personenbezogener Daten ist in der **Gewerbeordnung bereichsspezifisch** geregelt. Danach können öffentliche Stellen, die an gewerberechtlichen Verfahren beteiligt waren, über das Ergebnis informiert werden, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Öffentliche Stellen sind zudem zu informieren, wenn eine Entscheidung Rechtsfolgen hat und die Kenntnis der Daten aus Sicht der übermittelnden Stelle für die Verwirklichung dieser Rechtsfolgen erforderlich ist. Für weitere Zwecke sind Übermittlungen nur zulässig, soweit diese zur Verfolgung von Straftaten erforderlich sind oder eine besondere Rechtsvorschrift dies vorsieht.

In den geprüften Fällen bestand allenfalls die Besorgnis, dass die im Reisegewerbe zulässigen Grenzen bei den Tätigkeiten der Betroffenen überschritten werden könnten. Konkrete Anhaltspunkte dafür lagen nicht vor, zumal mit der Tätigkeit erst noch begonnen werden sollte. Es gab also keinen konkreten Anlass für die Übermittlungen. Es handelte sich um **regelmäßige Datenübermittlungen**, für die es an einer ausdrücklichen Rechtsvorschrift fehlte.

Was ist zu tun?
Kommunen dürfen nach Ausstellung einer Reisegewerbekarte davon nur die Behörden unterrichten, die in den Verwaltungsvorschriften zum Vollzug der Gewerbeordnung aufgezählt sind.

4.1.8 Audioaufzeichnung im Kernkraftwerk Krümmel

Die Überwachung riskanter Technologien macht gelegentlich Eingriffe in die Datenschutzrechte der Mitarbeiter nötig. Ein plausibler Zweck heiligt aber nicht die Mittel. Eingriffe sind nur mit eindeutiger gesetzlicher Grundlage zulässig.

Zu Recht erwarten die Bürger, dass Risikotechnologien wie die Atomkraft von den zuständigen staatlichen Stellen sorgfältig überwacht werden und dass alles getan wird, um Risiken zu erkennen und zu minimieren. In anderen Bereichen, wie im Luft- und Seeverkehr, ist der Einsatz von Audioaufzeichnungen, also von **Voice Recordern**, mit denen die Kommunikation des Bedienpersonals festgehalten wird, vorgesehen. Die dadurch möglichen Rückschlüsse auf die Ursache von Störungen und Unfällen sollen helfen, ähnliche Probleme in der Zukunft zu vermeiden.

In der Sache nachvollziehbar war für uns daher, dass die Atomaufsicht des Landes nach Problemen im Atomkraftwerk Krümmel in der ersten Hälfte des Jahres 2009 einen Verwaltungsakt erließ, mit dem der Kernkraftwerkbetreiber zu einer kontinuierlichen Audioaufzeichnung in der Hauptwarte des Kraftwerkes verpflichtet wurde. Die Gespräche der Mitarbeiter in der Hauptwarte sollten vollständig erfasst werden, um die sich anschließenden Handlungsabläufe nachvollziehen zu können. Dies solle auch der Vermeidung künftiger Vorfälle dienen. Insbesondere bei **meldepflichtigen Ereignissen und Störfällen** sollten die Aufzeichnungen der Aufsichtsbehörde zur Verfügung gestellt werden. Als Rechtsgrundlage für die Anordnung wurden Vorschriften aus dem Atomgesetz angegeben, die ein Betretungs- und Prüfungsrecht für die atomrechtliche Aufsichtsbehörde vorschreiben.

Bei den vorgesehenen Sprachaufzeichnungen handelt es sich um die Verarbeitung personenbezogener Daten der Mitarbeiterinnen und Mitarbeiter. Die Anordnung zielte auf eine Rekonstruktion im Nachhinein, wer bei einem Störfall was gesagt hatte. Da eine automatisierte Verarbeitung durch den Arbeitgeber gefordert wurde, ist das Bundesdatenschutzgesetz (BDSG) anzuwenden. Trotz der Veranlassung der Aufzeichnung durch die Aufsichtsbehörde handelt es sich hierbei nicht um eine Datenverarbeitung im Auftrag der Behörde. Rechtlich verantwortlich im

Sinne des Bundesdatenschutzgesetzes bliebe der Betreiber der Anlage, der **per Verwaltungsakt verpflichtet** wurde und die Verfügungsgewalt über die aufgezeichneten Daten haben würde, die nur in genau definierten Fällen herauszugeben wären. Unsere Prüfung ergab allerdings, dass die bestehenden Befugnisnormen für eine derartige Datenverarbeitung nicht anwendbar sind. Diese stellen nämlich darauf ab, dass die Verarbeitung „als Mittel für die Erfüllung eigener Geschäftszwecke“ erfolgt, was hier gerade nicht der Fall ist. Denn die Verarbeitung wird von einer anderen Stelle, der Atomaufsicht, auferlegt und würde letztlich in deren Interesse vorgenommen werden.

Die Rechtsvorschriften über die Atomaufsicht begründen nicht die Befugnis zur Anordnung einer derartigen Maßnahme. Das Atomrecht erlaubt nur den Zugriff der Atomaufsicht auf **bereits vorhandene Unterlagen**. Die Anordnung zukünftiger Sprachaufzeichnungen für spätere Untersuchungen von eventuell auftretenden Störfällen hat eine andere Qualität. Vergleichbare Pflichten in bestimmten Bereichen, wie z. B. beim Flug- und Schiffsverkehr, beruhen auf ausdrücklichen gesetzlichen Regelungen.

Eine hoheitliche Anordnung der Überwachung der Sprachkommunikation ist in zweifacher Hinsicht ein **Grundrechtseingriff**. Betroffen sind die wirtschaftlichen Grundrechte der Anlagenbetreiber und – mittelbar, aber zwangsläufig – das informationelle Selbstbestimmungsrecht der betroffenen Arbeitnehmerinnen und Arbeitnehmer. Die Konstellation ist vergleichbar mit der der Vorratsdatenspeicherung in der Telekommunikation (31. TB, Tz. 4.3.1): Der Staat verpflichtet ausgewählte Unternehmen, bestimmte Daten im Rahmen ihres Betriebsablaufs zu erheben und zu speichern, um sich im Bedarfsfall den Zugriff auf diese Daten zu sichern. Erfüllt werden damit letztlich staatliche Zwecke, nicht solche der Unternehmen.

Für einen derartigen mittelbaren Eingriff in die Datenschutzgrundrechte der Betroffenen fehlt die **Rechtsgrundlage**. Eine Sprachaufzeichnung in sicherheitskritischen Bereichen ist zweifellos geeignet, Störfälle aufzuklären und zu deren Vermeidung beizutragen. Dies muss aber klar im jeweiligen Fachgesetz geregelt werden. Anderenfalls könnten staatliche Behörden in allen möglichen Bereichen unter Berufung auf mehr oder weniger nachvollziehbare Belange des Gemeinwohls private Stellen zur Zwangserhebung von personenbezogenen Daten Dritter verpflichten.

Von Bedeutung war im vorliegenden Fall auch, dass der Kernkraftwerksbetreiber zum Prüfungszeitpunkt von sich aus keine Audioaufzeichnung in der Hauptwarte vornehmen wollte. Jenseits einer behördlichen Verpflichtung kann eine durch den Betreiber als verantwortliche Stelle **selbst initiierte Aufzeichnung** zulässig sein. Das BDSG enthält grundsätzlich die Ermächtigung zur Aufzeichnung von Daten als Mittel für die Erfüllung eigener Geschäftszwecke. Bei der nötigen Abwägung der widerstreitenden Interessen ist relevant, welcher Sicherheitsgewinn zu erwarten ist und mit welchen Schutzmaßnahmen übermäßige Eingriffe in die Datenschutzrechte der Betroffenen vermieden werden können.

Was ist zu tun?
Die Atomaufsicht muss sich auf die rechtlich zur Verfügung stehenden Mittel beschränken. Eine aufsichtsrechtliche Verpflichtung zur Audioaufzeichnung bedürfte einer klaren gesetzlichen Grundlage.

4.1.9 Schöffenvorschlagslisten gehören nicht ins Internet

Von den Gemeinden aufgestellte Schöffenvorschlagslisten enthalten personenbezogene Informationen. Das Gerichtsverfassungsgesetz, das abschließend regelt, in welcher Form und in welchem Zeitraum die Listen genutzt werden, sieht eine Internetveröffentlichung nicht vor.

Eine Internetrecherche überraschte eine Bürgerin: Auf der Website einer Stadtverwaltung fand sie ihren Namen und Vornamen sowie **Anschrift, Geburtsdatum, Geburtsort und Beruf**. Der Hintergrund: Sie war im vorangegangenen Jahr als Kandidatin für die Schöffenwahl aufgestellt worden. Die Daten befanden sich zusammen mit den Angaben über die weiteren Kandidaten in einer Schöffenvorschlagsliste auf der Website der Stadt.

Die Schöffenwahl wird durch die Gemeinde vorbereitet. Dazu stellt die Gemeinde eine Schöffenvorschlagsliste auf und übersendet diese an das Amtsgericht. Vor Übersendung muss die Schöffenvorschlagsliste für eine Woche in der Gemeinde zu **jedermanns Einsicht** ausgelegt werden. Der Termin für die Auslegung ist öffentlich bekannt zu geben. Im konkreten Fall war Folgendes geschehen: Der Termin für die Auslegung wurde durch amtliche Bekanntmachung kundgetan, als Anlage war die Schöffenvorschlagsliste angefügt. Die amtliche Bekanntmachung wurde samt Anhang im Internet veröffentlicht und befand sich nach über einem Jahr immer noch dort.

Das Gerichtsverfassungsgesetz schreibt nur eine Veröffentlichung des Termins der Auslegung, nicht aber eine Listenveröffentlichung vor. Über die einwöchige Listenauslegung in der Gemeinde hinaus erlaubt das Gesetz keine weitere Veröffentlichung der Liste. Die Stadtverwaltung hat nach unserer Aufforderung umgehend die Liste aus ihrem **Internetauftritt gelöscht**.

Ein anderes Praxisbeispiel zeigt, wie eine Stadtverwaltung die gesetzlichen Vorgaben für die Auslegung der Listen zu ernst genommen hat. Dort wurde einem Bürger bei der Einsichtnahme in die Schöffenvorschlagsliste untersagt, sich **handschriftliche Notizen** anzufertigen. Begründet wurde dies damit, dass das Gesetz nur die Einsichtnahme vor Ort vorsieht. Ganz so streng muss die Behörde nicht mit den Listen umgehen. Zweck der Auslegung ist, dass jedermann die Daten zur Kenntnis nehmen, prüfen und gegebenenfalls anschließend Einwände erheben kann. Dafür kann die Anfertigung von Notizen erforderlich sein und sollte den Einsichtnehmenden erlaubt werden.

Was ist zu tun?
Bei der Auslegung von Schöffenvorschlagslisten ist darauf zu achten, dass diese ausschließlich für eine Woche in der Gemeinde zur Einsicht ausgelegt werden. Weitere Veröffentlichungen müssen unterbleiben.

4.2 Polizei und Verfassungsschutz

4.2.1 „@rtus“ – Vorgangsbearbeitungssystem und mehr

Das Vorgangsbearbeitungssystem „@rtus-VBS“ der Polizei Schleswig-Holstein ging mit Unzulänglichkeiten in Betrieb. Gravierend sind die fehlende technische Trennung der Datenbestände „Vorgangsbearbeitung“ und „Dokumentation“ sowie eine unzureichende Protokollierung der Abrufe. Demnächst soll „@rtus-Auswertung“ eingesetzt werden, obwohl die Mängel an dem Vorgangsbearbeitungssystem nicht beseitigt sind. Doch die Kooperation von Polizei und ULD entwickelt sich vielversprechend.

Die Polizei des Landes Schleswig-Holstein verwendet seit einigen Jahren in der täglichen Arbeit das Verfahren „@rtus-VBS“ (31. TB, Tz. 4.2.1). Damit werden tägliche Arbeitsabläufe technisch erfasst und gesteuert. Das Vorgangsbearbeitungssystem unterliegt den Bestimmungen des Landesverwaltungsgesetzes (LVwG). Das Gesetz erlaubt unter dem Stichwort „Vorgangsbearbeitung“ die Verarbeitung personenbezogener Daten durch die Landespolizei, soweit dies zur Erfüllung der jeweiligen ordnungsbehördlichen oder polizeilichen Aufgabe erforderlich ist. Außerdem dürfen unter dem Stichwort „Dokumentation“ Daten zur **Vorgangsverwaltung** oder zur befristeten Dokumentation des behördlichen Handelns gespeichert werden. Hierfür genügt ein reduzierter Datenbestand. Das Innenministerium hat in einem Erlass aus dem Jahre 1996 beispielhaft die Daten genannt, die für die Vorgangsverwaltung erforderlich sind.

Diese beiden unterschiedlichen Datenbestände müssen getrennt geführt werden. Das Verfahren „@rtus-VBS“ lässt bisher die **Trennung der Daten** für die „Vorgangsbearbeitung“ und für die „Dokumentation und Vorgangsverwaltung“ nicht zu. Die Polizei meint, die gesetzlich vorgeschriebene Trennung und Nutzung der Daten durch organisatorische Regelungen, vor allem aber durch Schulungsmaßnahmen, bis zur technischen Umstellung sicherstellen zu können.

Wir bezweifeln, dass dadurch die **zweckgemäße Verarbeitung der Daten** im Polizeialltag sichergestellt wird. Die Gefahr, Vorgangsverwaltungsdaten dennoch im Rahmen der laufenden Sachbearbeitung zu nutzen, ist groß. Eine technische Trennung und ein wirksamer Zugriffsschutz würden diese Gefahr ausschließen. Es fällt uns schwer, das Argument des verantwortlichen Landespolizeiamtes nachzuvollziehen, dass eine Änderung des Zustandes erst mit der Einführung der Erweiterung um eine Auswertungskomponente möglich sei.

Die Projektleitung von „**@rtus-Auswertung**“ hat erfreulicherweise frühzeitig das Beratungsangebot des ULD angenommen. Im vorgelegten Berechtigungskonzept fehlen u. a. noch detaillierte Informationen zu den Funktionalitäten dieses Verfah-

rens, zu den rechtlichen Rahmenbedingungen und zur technischen Umsetzung. Beim Berechtigungskonzept nahm die Projektgruppe erforderliche und sachgerechte Beschränkungen bei der Recherche und den Auswertungsergebnissen vor. Der Kreis der Nutzenden des Verfahrens ist eingeschränkt: Bearbeiter mit Ermittlungsaufgaben, Kriminalitätsphänomene bearbeitende Zentralstellen beim Landeskriminalamt und eine kleine Gruppe in der Zentralen Auswertung sollen Rechercherechte für „@rtus-Auswertung“ erhalten. Das Konzept sieht für jeden Nutzerkreis ein abgestuftes Anwenderprofil vor, das die Erforderlichkeit der Recherche im Rahmen der Aufgabenerfüllung widerspiegelt. Unser erster Eindruck von den bisher vorgelegten Konzeptunterlagen ist positiv.

Das ULD hat der Projektgruppe auch **in technisch-organisatorischer Hinsicht** Beratung und Unterstützung zugesagt. Es geht primär darum, konzeptionell und in Tests die Anforderungen des Landesdatenschutzgesetzes und der neu gefassten Datenschutzverordnung umzusetzen. Sicherheitsmanagement und Risikoanalysen werden auf dem Prüfstand stehen. Wir halten den eingeschlagenen Weg für richtig und effizient. Beide Seiten können vom offenen und konstruktiven Dialog profitieren.

Was ist zu tun?
Das Landespolizeiamt sollte die gesetzliche Forderung nach Trennung der Datenbestände in „@rtus-VBS“ zeitnah umsetzen. Die Erweiterung um die Auswertungskomponente sollte getrennt behandelt und vor ihrer Implementierung sorgfältig geprüft werden.

4.2.2 Nutzung der Daten von INPOL-SH

Die Daten aus den Bereichen Gefahrenabwehr und Strafverfolgung werden in INPOL-SH, einer Datei der Landespolizei, gespeichert. Nach Ansicht des ULD unterliegt die Nutzung der Daten aus dem Bereich der Strafverfolgung den Regeln des Landesverwaltungsgesetzes; die Polizei hält die Strafprozessordnung für anwendbar. Vor Übermittlung der dort gespeicherten Daten muss eine Rechtmäßigkeitsprüfung erfolgen.

Ein Petent beschwerte sich, weil Angaben aus **lange Zeit zurückliegenden Strafverfahren** durch eine Polizeidienststelle im Rahmen einer Anzeigenbearbeitung genutzt wurden. Diese Daten, die in einer Kriminalakte und in INPOL-SH gespeichert waren, bezogen sich auf Anzeigen wegen des Verdachts der Körperverletzung im Jahre 2004 und wegen des Verdachts einer falschen Verdächtigung im Jahre 2005.

Auch nach Ansicht des Datenschutzbeauftragten des Landespolizeiamtes rechtfertigten die Sachverhalte nicht die Anlegung einer Kriminalakte und die Speicherung in INPOL-SH, weshalb umgehend die Löschung der Daten in INPOL-SH veranlasst wurde. Vor der Nutzung der Daten hätten diese aber auch im Rahmen der Sachbearbeitung gemäß dem Landesverwaltungsgesetz (LVwG) auf ihre Rechtmäßigkeit hin überprüft werden müssen, zumal die turnusmäßige Prüfung

nach der vom Gesetz vorgesehenen Frist fast unmittelbar bevorstand. Auch vor Ablauf dieser Frist kann im Einzelfall eine **Prüfung und Aussonderung** wegen nicht mehr bestehender Erforderlichkeit der Speicherung geboten sein. Bei den Aussonderungsprüffristen nach der Errichtungsanordnung für die Datei handelt es sich um verallgemeinerte Fristen. Sie werden den Umständen des Einzelfalls nur bedingt gerecht. Stellt die Polizei bei der Bearbeitung fest, dass die Daten nicht mehr erforderlich sind, sind sie zu löschen. Sie dürfen vorher nicht übermittelt werden.

Die Beanstandung des ULD wegen unterbliebener Löschung und wegen Übermittlung der in INPOL-SH gespeicherten Daten wurde vom Innenministerium zurückgewiesen. Es sah sich nicht zur nachträglichen Bewertung des unstreitigen Sachverhalts imstande. Es vertrat zudem die Ansicht, dass überhaupt keine Übermittlung personenbezogener Daten aus INPOL-SH an die die Anzeige bearbeitende Polizeidienststelle stattgefunden habe. Der Kreis derer, die Kenntnis von den Daten erhält, sei nicht erweitert worden. Das Ministerium verkennt bei der Argumentation, dass es sich bei INPOL-SH um ein automatisiertes Abrufverfahren handelt. Es dreht sich bei dem Abruf nicht um eine interne Nutzung, sondern um eine Übermittlung. Die Daten abrufende Polizeidienststelle ist immer Dritter, wenn sie nicht selbst für die Datenspeicherung verantwortlich ist.

Im Wortlaut: § 196 Abs. 2 LVwG

*In Dateien gespeicherte personenbezogene Daten sind zu löschen und die dazugehörigen Unterlagen zu vernichten, wenn bei der nach bestimmten Fristen vorzunehmenden Überprüfung **oder aus Anlass einer Einzelfallbearbeitung** festgestellt wird, dass ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgabe nicht mehr erforderlich ist. Anderenfalls ist eine neue Prüffrist festzulegen. Die Gründe hierfür müssen sich aus den Unterlagen ergeben.*

Das ULD musste auch der Auffassung des Innenministeriums widersprechen, dass für die Verwendung der übermittelten Daten die Strafprozessordnung (StPO) gilt. Die in INPOL-SH bereitgehaltenen Daten gehen über die enumerativ in der StPO genannten Datenkategorien hinaus. Zudem handelt es sich bei den in INPOL-SH gespeicherten Sachverhalten um solche der Gefahrenabwehr, also auch aus Strafverfahren. Somit handelt es sich um eine sogenannte „**Mischdatei**“ der Polizei. Für solche Mischdateien ist nach der StPO das Polizeirecht des jeweiligen Landes anzuwenden, also das Landesverwaltungsgesetz mit seinen Regelungen zur Datenübermittlung und -nutzung.

Was ist zu tun?
Das Innenministerium des Landes sollte seine Rechtsauffassung in den vorgenannten Punkten korrigieren und der Polizei entsprechende allgemeingültige Handlungshinweise an die Hand geben.

4.2.3 Prüfung im Jahr 2005: Abteilung 3 des Landeskriminalamtes

Nach langem Warten, viel Schriftwechsel und einigen Gesprächen ist es dank der Intervention des Innenministeriums gelungen, die Kontrolle der Abteilung 3 des Landeskriminalamtes abzuschließen.

Alle Beteiligten sind inzwischen anscheinend nicht nur erleichert, sondern auch zufrieden (31. TB, Tz. 4.2.5). Die wichtigsten Ergebnisse sind folgende: Die **Errichtungsanordnungen** für die Dateien „Warndatei rechts“ und „Innere Sicherheit Schleswig-Holstein“ konnten präzisiert und den gesetzlichen Vorgaben angepasst werden, insbesondere hinsichtlich des zu erfassenden Personenkreises und der Speicherungsfristen.

Die Datenverarbeitung in der Abteilung 3 des Landeskriminalamtes, also des sogenannten Staatsschutzes, wurde strukturell der übrigen Verarbeitung der Landespolizei angeglichen. Die Entscheidungen für eine bedarfsgerechte Anpassung der Technik sind getroffen und sollen kurzfristig umgesetzt werden. Die Aktenvorgänge werden fortan in einem **geschützten Bestand in @rtus** geführt und unterliegen denselben Regelungen wie die übrigen Polizeiakten.

Was ist zu tun?
Endlich konkret nichts mehr! Die Feststellungen aus Datenschutzkontrollen sollten künftig zeitnah abgearbeitet werden. Verzögerungen machen nur Arbeit und Ärger.

4.2.4 Kooperative Leitstellen von Polizei und Kommunen gehen an den Start

Im September 2009 hat die Leitstelle Nord in Harrislee ihren Betrieb aufgenommen. Damit ist deutschlandweit die erste Leitstelle in Betrieb, in der Polizei, Rettungsdienste und Feuerwehr kooperativ unter einem Dach zusammenarbeiten.

Die **Zusammenarbeit** von Polizei und kommunalen Einsatzdiensten ist technisch eine gewaltige Herausforderung. Die Datenbestände der einzelnen Stellen sind streng voneinander zu trennen, denn jede Stelle erledigt ihre Aufgaben eigenständig und bleibt für ihre Daten verantwortlich. Andererseits sollen so weit wie möglich Synergien genutzt und die Zusammenarbeit untereinander unterstützt werden. Das ULD war von Beginn an in die Planungen der kooperativen Leitstelle beratend eingebunden.

Von Beginn an haben wir auf die nötige **Trennung der polizeilichen und der kommunalen Datenbestände** hingewiesen. Umgesetzt wurde eine konzeptionell als „schwach“ zu bezeichnende Mandantentrennung, die auf der Ebene der Zugriffsrechte, nicht hardwareseitig oder datenbanktechnisch durchgesetzt ist. Dieses Defizit muss durch eine konzeptionell stark ausgelegte Revisionsfähigkeit von System und konkreter Datenverarbeitung kompensiert werden. Die Möglichkeiten automatisierter Protokollierungen müssen stärker als bislang genutzt

werden. Noch fehlt es an einer Darlegung, wie die Nutzung der zentralen Sprachaufzeichnungsanlage und die Sprachaufzeichnung am Disponententisch protokolliert wird. Das Aufsetzen eines dedizierten Protokollservers wäre angemessen.

Auf polizeilicher Seite bestehen mehrere Möglichkeiten zur **Aufzeichnung von Telefonanrufen**. Die eingesetzte Software erlaubt nicht nur, die Notrufe unter 110 und 112 automatisch aufzuzeichnen. Auch auf anderen Anschlüssen eingehende Gespräche lassen sich bei Bedarf speichern. Hiervon macht nur die Polizei, nicht aber die kommunale Seite Gebrauch. Die Begründung: Ruft eine Hilfe suchende Person nicht unter der Nummer 110, sondern unter der Amtsnummer an, und ist das Gespräch inhaltlich ein Notruf, so soll es wie ein Notruf behandelt werden. Dazu gehört die unter 110 allgemein übliche Gesprächsaufzeichnung. Das Gesetz sieht dies nicht vor. Eine gesetzliche Grundlage wäre aber erforderlich, da durch die Aufzeichnungen in das Recht am gesprochenen Wort und damit in erheblichem Umfang in ein Grundrecht eingegriffen wird. Bei Aufzeichnungen im Bedarfsfall hätten die Polizeibeamten, anders als bei der automatischen Aufzeichnung von Anrufen unter 110, einen Entscheidungsspielraum. Im Interesse einer einheitlichen und verhältnismäßigen Vorgehensweise muss der Gesetzgeber der Polizei klare Entscheidungskriterien an die Hand geben.

Was ist zu tun?
Bevor weitere kooperative Leitstellen in Schleswig-Holstein in Betrieb genommen werden, sollten alle Mängel bei der Leitstelle Nord behoben sein, damit diese sich nicht bei den nächsten Leitstellen fortsetzen.

4.2.5 Protokollierung

Es müsste im selbstverständlichen Eigeninteresse der Verantwortlichen eines Datenverarbeitungssystems liegen, dass sämtliche Transaktionen zu Revisionszwecken festgehalten werden, um Missbräuche oder Fehler rekonstruieren zu können. Die Landespolizei versucht dagegen, Ausnahmen von der Protokollierungspflicht und somit Sicherheitslücken zu rechtfertigen.

Gesetze der Länder und des Bundes regeln in unterschiedlicher Weise die Protokollierungspflichten der Daten verarbeitenden Stellen. Umfang und Inhalt lassen sich durch die **Zwecke der Protokollierung** bestimmen: Es geht um die Datenschutzkontrolle, die Datensicherheit, die Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage und die Ausübung von Aufsichts- und Kontrollbefugnissen durch Dienst- und Fachvorgesetzte. Klärungsbedürftig ist außerdem, wo die Protokolldaten abgelegt werden und wer diese nutzen darf. Dies sind eigentlich einfach zu lösende Fragen, aber ...

In der **Praxis der Polizei** gibt es vielfältige Varianten von Protokollierungen. Bei Dateien, die sowohl von Behörden der Länder als auch des Bundes genutzt werden, den sogenannten Verbunddateien wie z. B. dem polizeilichen Informationsverbund INPOL, erfolgen lückenlose Protokollierungen.

Die Errichtungsanordnung für das **Verfahren @rtus** der Landespolizei Schleswig-Holstein benennt die Zwecke der Protokollierung, die Löschfrist für Protokolldaten, die Auswertungsmöglichkeiten und die Personen, die den Datenbestand nutzen dürfen. Danach werden bei Zugriffen der Zeitpunkt des Zugriffs, der Nutzer von @rtus, die Dienststelle, die Vorgangsnummer und die Dienststelle des geöffneten Vorgangs protokolliert. Ein Mangel besteht darin, dass nicht alle Zugriffe protokolliert werden. Das Landespolizeiamt meint, Dateizugriffe bestimmter Personengruppen, wie z. B. von Vorgesetzten der zuständigen Bearbeiterin bzw. des zuständigen Bearbeiters, müssten nicht aufgezeichnet werden, da ihre Zugriffe auf Datensätze von @rtus stets zulässig seien. Die Performance leide unter zu viel Protokollierung. Zudem seien die Kosten für die Protokollierung dieser Daten unverhältnismäßig hoch.

Im Wortlaut:
§ 194 Abs. 1 Satz 2 bis 4 LVwG

(2) Abrufe sind in überprüfbarer Form automatisiert zu protokollieren.

(3) Die protokollierten Daten dürfen nur zum Zwecke der Datenschutzkontrolle, der Datensicherheit, zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage sowie zur Ausübung von Aufsichts- und Kontrollbefugnissen durch Dienst- und Fachvorgesetzte verwendet werden.

(4) Satz 3 gilt nicht, wenn Anhaltspunkte dafür vorliegen, dass ohne ihre Verwendung die Verhinderung oder Verfolgung einer schwerwiegenden Straftat, insbesondere gerichtet gegen Leib, Leben oder Freiheit einer Person oder mehrerer Personen, aussichtslos oder wesentlich erschwert wäre.

Nach dem Fachkonzept Protokollierung ist auch keine **anlassunabhängige Auswertung** vorgesehen. Für die Auswertung werden auch keine gesonderten Masken und Anwendungsfälle bereitgestellt. Erstaunlich für uns ist zudem die Aussage, bei Lesezugriffen auf Vorgänge einer Fremddienststelle erfolge die Protokollierung nicht zu Auswertezwecken, sondern zum „Nachweis des Datenschutzes“. Die Regelungen des Fachkonzepts ermöglichen noch keine datenschutzgerechte und revisionssichere Protokollierung, die den gesetzlichen Anforderungen genügt, sie müssen daher nachgebessert werden.

Was ist zu tun?
Die Umsetzung der schon vor Jahren vom ULD gegebenen Anregung, bei den DV-Anwendungen der Polizei des Landes ein einheitliches Protokollierungsverfahren einzuführen, würde Kosten und Arbeitsaufwand reduzieren.

4.2.6 AG INPOL der Datenschutzbeauftragten des Bundes und der Länder

Eine Projektgruppe arbeitet seit Jahren an der Modernisierung und Weiterentwicklung des polizeilichen Informationssystems der Polizeien des Bundes und der Länder – INPOL. Die Datenschutzbeauftragten werden über wesentliche Schritte informiert. Sie legten Empfehlungen zur Speicherung personengebundener Hinweise vor.

Das Speichern von **personengebundenen Hinweisen in INPOL** ist seit dem Jahr 1988 ein Dauerbrenner in der Diskussion zwischen Polizei und Datenschutz: Unter welchen Voraussetzungen dürfen solche Hinweise gespeichert werden? Deren Inhalt kann leicht stigmatisierend wirken. Bei Merkmalen wie z. B. „gewalttätig", „Ansteckungsgefahr" oder „geisteskrank" geraten die betroffenen Personen leicht in Gefahr, „abgestempelt" zu werden.

Klärungsbedürftig ist, in welchen Dateien diese Merkmale zu welchem Zweck gespeichert werden, ob alle Polizeibeamte hierauf Zugriff haben müssen und wie lange eine Speicherung erlaubt sein soll. Einige personengebundene Hinweise verlieren im Laufe der Zeit an Aktualität und Wahrheitsgehalt. Die Polizei darf sich nicht „blind" auf die Richtigkeit verlassen. Bei Kontrollen können die Hinweise **Auslöser für nicht angemessenes Vorgehen** sein. Die Betroffenen haben von diesen Speicherungen in der Regel keine Kenntnis. Daher kann eine kurzfristige Löschung bzw. Aktualisierung geboten sein. Die Arbeitsgruppe der Datenschützer hat ihre Anforderungen bei der Verwendung von personengebundenen Hinweisen im polizeilichen Informationssystem INPOL festgehalten und der Projektgruppe INPOL beim Bundeskriminalamt übermittelt.

Was ist zu tun?
Die Anregungen der Datenschutzbeauftragten sollten von der Projektgruppe INPOL umgesetzt werden.

Im Wortlaut: AG INPOL der Datenschutzbeauftragten des Bundes und der Länder

Bonn, 20.05.2009
Datenschutzrechtliche Anforderungen bei der Verwendung von personengebundenen Hinweisen (PHW) im polizeilichen Informationssystem INPOL

...

2. Bestandsaufnahme zu personengebundenen Hinweisen

Personengebundene Hinweise (PHW) werden in INPOL in der W-Gruppe gespeichert. Voraussetzung für das Anlegen einer W-Gruppe ist das Bestehen einer P-Gruppe und einer anwendungsspezifischen Datengruppe aus den Bereichen Fahndung (F-Gruppe), Erkennungsdienst (E-Gruppe) oder Kriminalaktennachweis (U-Gruppe).

Die W-Gruppe enthält folgende Datenfelder:

- *personengebundener Hinweis,*
- *Besitzer,*
- *Laufzeit,*
- *Sondervermerk.*

Mit Beschluss vom 1./2.2.1988 hat der AK II den Umfang der zulässigen PHW (neu) festgelegt. Ab diesem Zeitpunkt wurde die Beschränkung einzelner PHW auf einzelne Anwendungen (Dateien) aufgegeben. (Ausnahmen gelten nur für PHW „Prostitution“ und „Häufig wechselnder Aufenthaltsort“). Dieser Beschluss enthält als Anlage Kriterien für die Vergabe der einzelnen PHW, die so für alle Anwender verbindlich sind. Als Laufzeit für die PHW wird die Aufbewahrungsdauer der Kriminalpolizeilichen Sammlung (KpS) festgelegt. Ausnahmen gelten für „Ansteckungsgefahr“ und „Freitodgefahr“ (2 Jahre) sowie „Prostitution“ (5 Jahre).

Übersicht über die derzeit vorhandenen PHW:

***§ 7 Abs. 3 BKAG**: BEWA, Bewaffnet; GEWA, Gewalttätig; AUSB, Ausbrecher; ANST, Ansteckungsgefahr; GEKR, Geisteskrank; BTMK, BtM-Konsument; FREI, Freitodgefahr; PROS, Prostitution; **§ 8 Abs. 2 BKAG**: VEMO, Straftäter verbotener militanter Organisation/Vereinigung/Partei/Gruppe; REMO, Straftäter rechtsmotiviert; LIMO, Straftäter linksmotiviert; AUMO, Straftäter politisch motivierter Ausländerkriminalität; EXPL, Explosivstoffgefahr; SEXT, Sexualtäter; HWAO, Häufig wechselnder Aufenthaltsort; **§ 7 oder § 8 BKAG, je nach Fallkonstellation**: BEWA, Bewaffnet; GEWA, Gewalttätig; AUSB, Ausbrecher; FREI, Freitodgefahr.*

3. Anforderungen zur Verwendung von personengebundenen Hinweisen (PHW) aus Sicht des Datenschutzes

- *Es dürfen nur solche PHW in INPOL-Z erfasst werden, die den gesetzlichen Voraussetzungen der §§ 7 Abs. 3 oder 8 Abs. 2 BKAG entsprechen. Bei der Einführung neuer PHW muss begründet werden, warum diese notwendig ist – auch in Abgrenzung zu vorhandenen PHW.*
- *Für alle PHW muss es eine verbindliche Festlegung zur Vergabe geben. Diese darf sich nicht nur auf eine Ausformulierung der Kurzbezeichnung beschränken. Dazu kann auch eine Abgrenzung zu anderen PHW notwendig sein. Aus der Definition muss klar die Schwelle ersichtlich sein, wann ein Sachverhalt/Verhalten zur Vergabe des PHW führt. Hierfür kann ein Eintrag im Datenfeld „Sondervermerk" vorgenommen werden. Nur dann kann der Anwender, der in einem Datensatz einen PHW sieht, sich das Gleiche darunter vorstellen wie derjenige, der den PHW im Einzelfall vergeben hat.*
- *Es ist jeweils darzulegen, ob der PHW zur Eigensicherung oder zum Schutz der Person dient, für die er gespeichert ist. Bei jedem PHW ist festzulegen, für welche INPOL-Anwendung er verwendet werden darf. Insoweit sind die betreffenden Errichtungsanordnungen gegebenenfalls zu ergänzen. Soweit bestimmte Phänomene zur Einführung neuer spezifischer Dateien führen, muss die gleichzeitige Notwendigkeit eines PHW gesondert begründet werden. Bei PHW zur Eigensicherung ist eine Darstellung der (neuen) Gefährdung durch das zu erlassende Phänomen notwendig.*
- *Die für die Erhebung, Verarbeitung und Aktualität von PHW verantwortliche Polizeidienststelle muss erkennbar sein. Ihr obliegen neben einer Dokumentation die gesetzlichen Verpflichtungen bei der Verarbeitung von Daten gemäß § 3 Abs. 9 BDSG.*
- *Für jeden PHW müssen die Dauer der Vergabe sowie die Gründe für eine eventuelle Verlängerung der Speicherdauer definiert sein. Die Übereinstimmung mit der Laufzeit der KpS muss dabei die Ausnahme sein. Vielmehr ist für jeden PHW eine angemessene Speicherdauer bzw. Prüffrist festzulegen.*
- *Die Gründe für die Vergabe eines PHW im einzelnen Fall müssen aus der KpS ersichtlich sein. Art und Umfang der Dokumentation können bei den verschiedenen PHW unterschiedlich ausgestaltet werden. Bei einzelnen PHW kann dazu eine Dokumentation zusätzlicher Unterlagen gehören, z. B. bei ANST und GEKR. Auch die Gründe für die Verlängerung der Laufzeit des PHW sind zu dokumentieren.*
- *Bei der Vergabe der personengebundenen Hinweise „Ansteckungsgefahr", „Geisteskrank", „Freitodgefahr" ist ein qualifizierter Nachweis eines Arztes, Psychologen usw. notwendig.*
- *Die in einer Datei einsetzbaren PHW sind in der Errichtungsanordnung (gegebenenfalls auch mit der abweichenden Laufzeit) zu dokumentieren.*
- *Die Kriterien für die Vergabe/Notwendigkeit einzelner PHW sind regelmäßig zu überprüfen, gegebenenfalls zu ändern.*

4.2.7 NADIS-neu

Das nachrichtendienstliche Informationssystem der Verfassungsschutzbehörden des Bundes und der Länder (NADIS) ist „in die Jahre gekommen". Das Projekt einer technischen Runderneuerung wird nach bisherigen Planungen mehr als 20 Millionen Euro kosten.

Die Verfassungsschutzbehörden des Bundes und der Länder arbeiten unter Federführung des Bundes in dem **Projekt NADIS-neu** an einer Neugestaltung. Angestrebt wird eine zukunftssichere technische Plattform, mit der auch flexibel auf sich ändernde gesetzliche Anforderungen reagiert werden kann. Multimediadaten, also auch Bilder und Töne, sollen verarbeitet werden können. Die informationelle Zusammenarbeit der Verfassungsschutzbehörden soll durch technische Vereinheitlichung optimiert werden, u. a. durch Integration der vorhandenen Amtsdateien der Länder.

Nach dem bestehenden Recht ist NADIS ein **Indexverfahren** zur Erfüllung der gegenseitigen Unterrichtungspflichten. Die zum Auffinden von Akten und zur Identifizierung von Personen erforderlichen Daten dürfen gespeichert werden. Weiter gehende Informationen dürfen den Verbundteilnehmern grundsätzlich nicht zum Abruf online zur Verfügung gestellt werden. Sie werden in spezifischen Dateien beim Bundesamt für Verfassungsschutz gespeichert. Alle weiteren Datenbestände sind nach den Regelungen der jeweiligen Landesverfassungsschutzgesetze oder in Amtsdateien des Bundesamtes für Verfassungsschutz zu verarbeiten.

Bei einer Erweiterung in NADIS-neu müssen natürlich die bestehenden **gesetzlichen Begrenzungen** beachtet werden. Dies gilt auch für die Einbeziehung von Multimediadaten. Das ULD hat der Verfassungsschutzbehörde des Landes angeboten, den weiteren Entwicklungsprozess zu begleiten.

Was ist zu tun?
Die Verarbeitung von Landesdaten in NADIS sollte von der Verfassungsschutzbehörde mit dem ULD abgestimmt werden.

4.2.8 ADOS – neu beim Verfassungsschutz

Bei der Verfassungsschutzbehörde des Landes wurde unter frühzeitiger Beteiligung des ULD eine neue „Arbeitsdatei operative Sachverhalte" (ADOS) eingerichtet.

Bei ADOS handelt es sich um ein Verfahren für einen sehr eingeschränkten Nutzerkreis zur Steuerung der Aufgabenerledigung innerhalb des zuständigen Referats sowie zur Koordination operativer Vorgänge mit anderen Nachrichtendiensten. Auf Anregung des ULD wurde die Dateianordnung verbessert. Angesichts der weitgehenden **Geheimhaltungsbedürftigkeit** der beim Verfassungsschutz erfolgenden Datenverarbeitung kommt der Beteiligung des ULD eine

wichtige Funktion bei der Gewährleistung der gesetzlichen Vorgaben und der Grundrechte der Bürgerinnen und Bürger zu. Bei der Festlegung der Vorgaben der Dateianordnung zu ADOS zeigte sich, dass trotz unterschiedlicher Blickwinkel eine erfolgreiche Zusammenarbeit zwischen Verfassungsschutz und Datenschutz möglich ist.

Was ist zu tun?
Die Zusammenarbeit zwischen Verfassungsschutzbehörde und ULD bei der Einführung neuer Verfahren hat sich bewährt und sollte im allseitigen Interesse weiterentwickelt werden.

4.2.9 Körperscanner – Sicherheitsgewinn oder unverschämte Schamlosigkeit?

Auf Flughäfen in den USA werden bereits Körperscanner zur Personenkontrolle eingesetzt. In Europa sind solche Geräte bislang nur vereinzelt und in Deutschland gar nicht im Einsatz. Eine flächendeckende verpflichtende Nutzung steht zur Diskussion.

Auslöser der Debatte war der vereitelte Attentatsversuch am 1. Weihnachtstag 2009. Körperscanner nutzen zumeist Terahertz-, teilweise auch Röntgenstrahlung, um ein dreidimensionales Bild von der Körperoberfläche des Menschen unterhalb seiner Kleidung zu erstellen. Gegenstände wie **Waffen oder feste und flüssige Sprengstoffe** können damit sichtbar gemacht werden. Genauso ist der Körperscanner aber auch in der Lage, Merkmale zu erkennen und abzubilden, die keine Sicherheits-, aber dafür eine umso höhere Persönlichkeitsrelevanz haben, wie etwa Genitalien, Implantate, Prothesen bis hin zum künstlichen Darmausgang.

In Deutschland wird die Technologie seit 2008 von der Bundespolizei in Labors getestet. Untersucht werden neben der Wirksamkeit der Geräte deren Auswirkungen auf die Gesundheit sowie Möglichkeiten zum **Schutz der Privatsphäre**. Erste Ergebnisse sind für 2010 angekündigt. In der Entwicklung zeichnet sich ab, dass ein Verzicht auf eine detailgetreue Abbildung des nackten Körpers, wie sie bei den Geräten der ersten Generation gezeigt wird, durchaus möglich ist. Viele Fragen, etwa der Umgang mit besonderen körperlichen Merkmalen oder nach der Speicherung und weiteren Verwendung der vom Gerät erzeugten Bilder, sind noch offen. Dies gilt auch für den Nutzen der Geräte. Bis heute ist nicht wissenschaftlich dargelegt, wie welche Sicherheitsgewinne mit dem Scanner erreicht werden können.

Die zentrale Frage ist, **welche Maßnahmen** geeignet und im Interesse der Wahrung des Persönlichkeitsrechts, des Schamgefühls, der religiösen Überzeugung nicht nur von uns, sondern auch von Menschen aus anderen Kulturen verhältnismäßig sind. Die gemäß unserem Grundgesetz unantastbare Menschenwürde kann durch technische Vorkehrungen bewahrt werden. Doch Schamgefühl, religiöses Empfinden und die Wahrnehmung von Nacktheit sind individuell unterschiedlich. Scanner sollen besser optional eingesetzt werden. Technische Maßnahmen sind oft keine intelligenten Sicherheitsmaßnahmen; mit durchdachtem personalen Vor-

gehen ist offensichtlich ein höherer Sicherheitsstandard erreichbar. Ungeklärt ist, weshalb wirklich ausnahmslos alle Fluggäste gescannt werden müssen, vom Baby bis zum Greis. Das Bundesverfassungsgericht hat anlässlich einer Entscheidung zur „Entkleidungsuntersuchung“ im Strafvollzug hohe rechtliche Hürden bei derartigen Maßnahmen festgestellt. Danach wäre der undifferenzierte Einsatz des Körperscanners bei Flughafenkontrollen schlicht unverhältnismäßig.

4.3 Justizverwaltung

4.3.1 Justiz im Fernsehen

Das Fernsehformat des Reality-TV mit Reportagen, in denen Behördenmitarbeiter im Außendienst bei ihren Einsätzen begleitet werden, erfreut sich immer größerer Beliebtheit – leider oft auf Kosten der Betroffenen.

Eine Bürgerin fiel aus allen Wolken, als Nachbarn und Bekannte sie auf eine Pfändung von Gegenständen in ihrer Wohnung ansprachen, die ein Gerichtsvollzieher einige Zeit zuvor vorgenommen hatte. Es stellte sich heraus, dass die **Zwangsvollstreckung in der Wohnung** der Bürgerin ohne ihre Anwesenheit, dafür aber in Begleitung eines Fernsehteams stattgefunden hatte. Die vom Fernsehteam gemachten Aufnahmen waren kurze Zeit später gesendet worden.

Zwangsvollstreckungen sind auch in Abwesenheit des jeweiligen Schuldners möglich. Das Filmen der Amtshandlung durch ein Fernsehteam verstieß jedoch gegen datenschutzrechtliche Vorschriften. Lassen sich Behördenmitarbeiter bei ihrer Arbeit durch Fernsehteams begleiten, so haben sie darauf zu achten, dass die Persönlichkeitsrechte der Bürgerinnen und Bürger geachtet werden. Fernsehaufnahmen sind zulässig, wenn die betroffene Person **vorher ausdrücklich eingewilligt** hat. Die Einwilligung muss durch den Behördenmitarbeiter eingeholt werden, bevor er das Fernsehteam über einen konkreten Einsatz und die Person des Betroffenen informiert. Schon diese Information ist eine Datenübermittlung, die schutzwürdige Interessen der Betroffenen berührt. Eine gesetzliche Ermächtigung für die TV-Begleitung gibt es nicht. Unsere Petentin hatte dem Gerichtsvollzieher keine Einwilligung erteilt, ein Kamerateam mit in ihre Wohnung zu nehmen; diese Begleitung war daher unzulässig.

Das Landgericht, in dessen Gerichtsbezirk sich der Vorfall ereignet hat, hat sich gegenüber den datenschutzrechtlichen Fragestellungen sehr aufgeschlossen gezeigt.

Um in Zukunft ähnliche Situationen zu vermeiden, die oftmals aus Unwissenheit und einer Überforderung der Behördenmitarbeiter in einer speziellen Situation entstehen, haben wir mit dem betroffenen Landgericht **Leitlinien für Mitarbeiter der Justiz** erarbeitet und dem Justizministerium generell zur Verfügung gestellt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung die öffentlichen Stellen aufgefordert, grundsätzlich von der Mitwirkung an Reality-TV-Produktionen Abstand zu nehmen.


http://www.bfdi.bund.de/cae/servlet/contentblob/752962/publicationFile/42027/78DSK_RealityTV.pdf

Der Deutsche Journalistenverband (DJV) hat die Konferenz aufgefordert, die Entschließung zurückzunehmen, da sie mit der Presse- und Rundfunkfreiheit nicht im Einklang stehe. Der DJV verkennt hierbei, dass die verfassungsrechtlich gewährleistete Presse- und Rundfunkfreiheit keinen Anspruch auf staatliche Mitwirkung an solchen Reportagen verleiht. Hierzu hat das ULD ein ausführliches Gutachten erstellt.

Das Gutachten sowie die Leitlinien für Mitarbeiter der Justiz sind veröffentlicht unter:


www.datenschutzzentrum.de/rundfunk/

Was ist zu tun?
Fernsehsender haben keinen Anspruch auf Aufnahmen für Reportagen von Behördenmitarbeitern bei ihrem Umgang mit Bürgerinnen und Bürgern im Stil des Reality-TV. Sofern sich Behörden hieran beteiligen wollen, müssen sie vorher die Einwilligung der Betroffenen einholen.

4.3.2 Ein Chip für alles: Zutrittskontrolle und Zeiterfassung im Gericht

In einem Gerichtsgebäude ist ein elektronisches Zutrittsberechtigungssystem installiert, das nicht allein der Kontrolle von Zutritten ins Gebäude, sondern auch der Zeiterfassung dient. Das kombinierte System ist datenschutzgerecht einsehbar.

Besonderes Augenmerk bei kombinierten Systemen ist auf eine **Trennung der Datenverarbeitung** nach den unterschiedlichen Einsatzzwecken zu legen. Zutrittskontrollen dienen anderen Zwecken als einer Zeiterfassung. Dies wirkt sich z. B. bei der Aufbewahrungsdauer der Daten aus. Zeiterfassungsdaten müssen für einen längeren Zeitraum verfügbar sein. Anderes gilt für Daten über Zutritte zum Gebäude. Wenn überhaupt, ist deren Speicherung nur kurzzeitig erforderlich, um bekannt gewordene sicherheitsrelevante Vorfälle aufzuklären. Bei dem Gericht werden die Zeiterfassungsdaten nach einem Jahr, die Zutrittsdaten nach einer Woche gelöscht. Nach anfänglichen Schwierigkeiten konnte für die Zutrittsdaten eine eigenständige automatische Löschroutine eingerichtet werden.

Das Gericht hat den Umgang mit den erfassten Daten in einer **Dienstvereinbarung** geregelt. Danach ist eine Auswertung der Zutrittsdaten nur bei bestimmten Anlässen durch bestimmte Personen unter Nutzung eines Kennworts zulässig. Sämtliche Zugriffe auf die Zutrittsdaten werden unter Angabe des Zugriffsgrundes elektronisch für ein Jahr protokolliert.

Was ist zu tun?
Bei kombinierten Zutrittsberechtigungs- und Zeiterfassungssystemen ist auf eine separate Verarbeitungsmöglichkeit bei unterschiedlichen Zwecksetzungen zu achten. Der Umgang mit personenbezogenen Daten ist in einer Dienstanweisung zu regeln, die zumindest Festlegungen zum Zweck der Datenverarbeitung, zu den Voraussetzungen und zum Verfahren des Zugriffs auf die gespeicherten Daten enthalten muss.

4.3.3 Die Entscheidung über die Kostentragungspflicht in Betreuungssachen

Gerichtskosten werden in Betreuungssachen nur erhoben, wenn das Vermögen des Betreuten nach Abzug der Verbindlichkeiten mehr als 25.000 Euro beträgt. Diese auf den ersten Blick für den Betreuten günstige Regelung kann im Einzelfall zu umfangreichen Datenerhebungen führen.

Der überwiegende Teil der Betreuungen wird zum Zweck der Vermögenssorge eingerichtet. In diesen Fällen muss der Betreuer ein Verzeichnis über das Vermögen des Betreuten erstellen, das bei der Anordnung der Betreuung vorhanden ist, und dem Gericht vorlegen. Hierauf kann das Gericht für die Entscheidung zurückgreifen. In wenigen Fällen wird bei der Einrichtung einer Betreuung **keine Vermögenssorge** angeordnet. Dann stehen aus dem Verfahren keine Daten über das Vermögen des Betreuten zur Verfügung und müssen eigens für die Entscheidung über die Kostentragungspflicht erhoben werden.

Ein Bürger wurde als Betreuer für seine Mutter bestellt. Die Vermögenssorge wurde nicht angeordnet. Nach Einrichtung der Betreuung erhielt er vom Gericht kommentarlos einen umfangreichen Fragebogen, in dem überaus detaillierte Angaben zum Vermögen seiner Mutter erfragt wurden. Bei diesem Fragebogen handelte es sich um den Vordruck, der für die Erstellung des **Vermögensverzeichnisses** verwendet wird. Zur Prüfung, ob das Vermögen des Betreuten mehr oder weniger als 25.000 Euro beträgt, ist dieser Fragebogen nur bedingt geeignet. Zweckgemäß enthält dieser Vordruck detaillierte Fragen zu allen Vermögensbereichen sowie zu Einkommen und Verbindlichkeiten. Für die Kostenentscheidung ist dies nicht unbedingt erforderlich. Übersteigt ein einzelner Vermögenswert bereits die Grenze von 25.000 Euro, so kann sich die Angabe weiterer Vermögenswerte erübrigen, wenn nicht Verbindlichkeiten abzuziehen sind. Die Angabe weiterer Vermögenswerte kann – allerdings begrenzt – allenfalls für die Bemessung der Gebührenhöhe erforderlich sein. Erreichen alle Vermögenswerte zusammen nicht die Grenze von 25.000 Euro, bedarf es keiner Angabe von Verbindlichkeiten. Dies ist bei der Gestaltung des Vordrucks naturgemäß nicht berücksichtigt.

Was ist zu tun?
In den seltenen Fällen, in denen bei einer Betreuung keine Vermögenssorge angeordnet wird und somit kein Vermögensverzeichnis vorliegt, sollte das Vermögen des Betreuten individuell beim Betreuer erfragt werden. Der Vordruck für die Erstellung des Vermögensverzeichnisses ist hierfür nicht geeignet und sollte nicht bzw. nur mit individueller Erläuterung verwendet werden.

4.3.4 Aufbewahrung von Schriftgut in der Justiz – endlich gesetzlich geregelt

Die Aufbewahrung von hochsensiblen Informationen aus Straf- oder anderen Prozessen greift in das informationelle Selbstbestimmungsrecht der Bürger ein, auch wenn sie „nur" in Akten erfolgt. Die hierfür erforderliche gesetzliche Grundlage ist im Berichtszeitraum endlich geschaffen worden.

Bislang war die Aufbewahrung des Schriftguts der Gerichte, der Staatsanwaltschaften und der Justizvollzugsbehörden nur in Verwaltungsvorschriften geregelt. Dies genügt nicht den Anforderungen des Volkszählungsurteils, wonach die Verarbeitung personenbezogener Daten im Wesentlichen einer klaren gesetzlichen Regelung bedarf. Mit dem Justizschriftgutaufbewahrungsgesetz hat der schleswig-holsteinische Gesetzgeber die erforderliche Regelung getroffen. Das Gesetz regelt den Rahmen für die einzelnen **Aufbewahrungsfristen**. Diese müssen auf das unbedingt erforderliche Maß beschränkt bleiben. Fristbeginn ist das Ende des Jahres, in dem das Verfahren beendet und die Weglegung der Akten angeordnet wird. Die Aufbewahrungsfristen selbst sollen, je nach Aktentyp, durch eine Verordnung festgelegt werden. Das Gesetz stellt klar, dass es sich hierbei nicht um Mindestfristen, sondern um Höchstfristen handeln wird, die unterschritten werden können.

Was ist zu tun?
Die noch ausstehende Verordnung sollte zügig erlassen werden. Darin sollten die maximalen Aufbewahrungsfristen streng an der Erforderlichkeit bemessen werden.

4.3.5 Telefonieren im Strafvollzug – Fortsetzung

Die Beseitigung der gravierenden Mängel des in Justizvollzugsanstalten eingesetzten Systems für Gefangenentelefonate dauert immer noch an, macht aber Fortschritte.

Wir berichteten über Mängel beim Telefonsystem im Justizvollzug (31. TB, Tz. 4.3.2). Inzwischen können erste Erfolge verzeichnet werden. Die von uns kritisierte Möglichkeit, Gespräche mitzuschneiden, wird nicht mehr genutzt. Das Justizministerium bestätigte unsere Feststellung, dass es für derartige **Aufzeichnungen** keine Rechtsgrundlage gibt. Geklärt wurde ebenfalls die Frage des Hinweises auf ein bevorstehendes Mithören von Telefongesprächen. Auf Anweisung

durch das Justizministerium erfolgt ein konkreter Hinweis nur noch, wenn tatsächlich beabsichtigt ist, das Gespräch mitzuhören. Auf einen abstrakten Hinweis der theoretischen Möglichkeit des Mithörens, der die Gefangenen und ihre Gesprächspartner im Ungewissen lässt, wird verzichtet.

Nicht verzichten möchte die Justizvollzugsanstalt auf die Möglichkeit zur **Auswertung der Verkehrsdaten** der durchgeführten Gespräche. So sollen bei gravierenden Ereignissen oder bevorstehenden Gefahren, wie etwa einem Ausbruch, die Personen ermittelt werden, die der Gefangene besonders häufig kontaktiert hat und die z. B. bei einem Ausbruch geholfen haben könnten. Der Bedarf für solche Auswertungen ist, jedenfalls in schwerwiegenden Fällen, nachvollziehbar begründet. Doch fehlt hierfür eine gesetzliche Befugnis; die Nutzung der Verkehrsdaten für Zwecke des Strafvollzugs ist daher nicht zulässig. Sollen künftig derartige Auswertungen möglich sein, so muss eine klare spezifische und verhältnismäßige Gesetzesregelung dies erlauben. Darin sind die Zwecke und die Eingriffsschwellen genau zu definieren. Das Verfahren ist im Einzelnen zu regeln, so z. B. die Anordnung der Maßnahme, die Protokollierung der Zugriffe und der Umgang mit den durch die Auswertung gewonnenen Daten.

Erfreulich entwickelt sich die **Aufteilung der Datenverarbeitung** zwischen der Justizvollzugsanstalt und dem privaten Anbieter. Alle Beteiligten sind sich einig, dass das bestehende System der Speicherung sämtlicher anfallender Daten beim privaten Anbieter geändert werden muss. Personenbezogene Daten dürfen nur bei der Justizvollzugsanstalt selbst oder einem der Justizverwaltung angehörigen Dienstleister vorgehalten werden. Beim privaten Anbieter dürfen grundsätzlich nur Daten ohne Personenbezug verbleiben. Ausnahmen sind allenfalls mit einer Einwilligung des Betroffenen möglich; diese muss aber freiwillig sein. Der private Anbieter stellte insofern eine Lösung vor, die den Anforderungen weitgehend entspricht; Details müssen allerdings noch geklärt werden.

Was ist zu tun?
Die Verlagerung der Datenspeicherung auf die Justizvollzugsanstalt sollte schleunigst vorgenommen werden. Die Auswertung der Verkehrsdaten der von den Gefangenen geführten Gespräche darf ohne gesetzliche Grundlage nicht erfolgen.

4.3.6 Untersuchungshaftvollzugsgesetz

Die Föderalismusreform I brachte den Ländern die Gesetzgebungszuständigkeit für den Strafvollzug. Ein Gesetzentwurf der Landesregierung über den Vollzug der Untersuchungshaft wurde vom Landtag vor Ablauf der Legislaturperiode nicht mehr beschlossen.

Der Jugendstrafvollzug ist in Schleswig-Holstein durch Landesgesetz bereits geregelt. Im nächsten Schritt ist die Regelung des Vollzugs der Untersuchungshaft an der Reihe. Dieses Vorhaben ist besonders wichtig, weil die Strafprozessordnung und das Strafvollzugsgesetz den Vollzug der Untersuchungshaft nur am

Rande regeln. Das meiste dieses hochsensiblen Bereichs ist bislang überhaupt nicht gesetzlich, sondern nur durch eine Verwaltungsvorschrift, die **Untersuchungshaftvollzugsordnung**, geregelt.

Der von der letzten Landesregierung vorgelegte, in vielen Einzelpunkten verbesserungsbedürftige Gesetzentwurf enthielt eine Reihe wichtiger vollzugsrechtlicher Neuerungen. Als Beispiel ist die **Videoüberwachung** zu nennen. Hierfür gibt es im Vollzugsrecht des Bundes keine Rechtsgrundlage, sodass mit Ausnahme des bereits geregelten Jugendstrafvollzugs eine Videoüberwachung innerhalb der Vollzugsanstalten nicht zulässig ist. Gleichwohl befinden sich in der Praxis Videoüberwachungsanlagen im Einsatz, mit denen Gemeinschaftsräume und Flure in Justizvollzugsanstalten beobachtet werden. Teilweise findet auch eine Aufzeichnung statt. Der Bedarf, bestimmte Bereiche innerhalb einer Vollzugsanstalt technisch zu beobachten und im Rahmen des Erforderlichen Aufzeichnungen anzufertigen, ist nachvollziehbar. Allerdings darf sich die Erlaubnis nicht auf alle Bereiche einer Vollzugsanstalt erstrecken und zum billigen Ersatz von Kontrollen durch das Vollzugspersonal werden.

Videoüberwachung darf dort eingesetzt werden, wo dies für die Gewährleistung der Sicherheit in der Anstalt unbedingt erforderlich und unter Berücksichtigung der Interessen der Gefangenen angemessen ist. Die Vollzugsanstalt ist für die Gefangenen in der Regel der einzige Lebensraum. Daher muss sichergestellt bleiben, dass die Gefangenen von Kameras nicht gewissermaßen rund um die Uhr auf Schritt und Tritt überwacht werden. Persönliche Rückzugsräume müssen erhalten bleiben; hierzu gehören in jedem Fall die Hafträume. Die Einhaltung dieser Vorgaben kann nur über klare gesetzliche Festlegungen gewährleistet werden, die das Sicherheitsinteresse der Anstalt und das Interesse der Gefangenen in einen gerechten Ausgleich bringen.

Was ist zu tun?
Das Untersuchungshaftvollzugsgesetz sollte zügig verabschiedet werden. Dabei sollten aktuelle Fragen des Vollzugs, die vor allem durch neue Technologien bestehen, klar und interessengerecht gelöst werden.

4.3.7 Post vom Gerichtsvollzieher

Post vom Gerichtsvollzieher erfreut niemanden. In einigen Fällen gibt auch die Art und Weise der Zustellung Anlass zu Ärger.

Mehrfach haben wir Beschwerden über Zustellungen durch Gerichtsvollzieher erhalten. Es ging immer um ähnliche Sachverhalte: Ein Gerichtsvollzieher hat z. B. versucht, einem Unternehmer einen Pfändungsbeschluss zuzustellen. Der Unternehmer wurde nicht angetroffen und der Pfändungsbeschluss daraufhin entweder in den Briefkasten des Unternehmens gelegt oder einem Mitarbeiter des Unternehmens überreicht. Soweit in Ordnung, doch leider wurde entgegen der Vorschriften der Pfändungsbeschluss **nicht im verschlossenen Umschlag**, sondern offen zugestellt. Für den Gerichtsvollzieher mag dies eine kleine Nachläs-

sigkeit sein. In einem Fall hat sich der Gerichtsvollzieher damit herausgeredet, dass ihm die Umschläge ausgegangen seien, die Zustellung aber so eilig gewesen sei, dass die Beschaffung neuer Umschläge nicht abgewartet werden konnte. Für die Betroffenen sind solche Versäumnisse mehr als ärgerlich; durch diese Art der Zustellung an eine Beschäftigte wurde etwa die Lohnpfändung einer Mitarbeiterin im Kollegenkreis bekannt.

Was ist zu tun?
Mitteilungen durch Gerichtsvollzieher müssen stets verschlossen sein, es sei denn, dass sie direkt an den Adressaten ausgehändigt werden.

4.4 Videoüberwachung zur Aufklärung von Verkehrsordnungswidrigkeiten

Abstandsmessungen zwischen Fahrzeugen auf Autobahnen, Rotlichtverstöße und Geschwindigkeitsüberschreitungen werden von Polizei und Ordnungsbehörden durch Videoaufnahmen dokumentiert. Die Rechtsgrundlage hierfür steht verfassungsrechtlich infrage.

Polizei und Ordnungsbehörden stützen sich beim Nachweis von Verkehrsordnungswidrigkeiten mittels Videotechnik bisher auf die Vorschriften des Ordnungswidrigkeitengesetzes und die sinngemäße Anwendung der Strafprozessordnung (StPO). Dies wurde bisher von der Rechtsprechung toleriert. Zweifel hieran äußerte nun das Bundesverfassungsgericht im August 2009 mit einem Beschluss im Einzelfall. Es bestritt das Vorliegen einer bereichsspezifischen **normenklaren Rechtsgrundlage** für die dauernde Videobeobachtung von bestimmten Straßenabschnitten zum Herausfiltern von Verkehrssündern. Das zuständige Amtsgericht, an das der Fall zurückverwiesen wurde, stellte das Verfahren daraufhin ein.

Gemeinsam mit dem Bundesverfassungsgericht halten wir die Anwendbarkeit der StPO für die Verfolgung von Verkehrsordnungswidrigkeiten schon seit Längerem für ungenügend. Die **Vorschrift in der StPO** aus dem Jahr 1991 diente der Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität. Die erlaubte Videoüberwachung im öffentlichen Raum soll der Bekämpfung schwerster Kriminalität dienen und nicht der Jagd auf Verkehrssünder. So kommt es, dass für den Einsatz von Videoüberwachung im Straßenverkehr eine hinreichende Rechtsgrundlage fehlt und die bisherige Praxis der Feststellung von Verkehrsverstößen mittels technischer Mittel, also Videokameras und Blitzgeräten, rechtswidrig ist.

Was ist zu tun?
Der Gesetzgeber muss den Einsatz technischer Mittel zur Aufklärung von Verkehrsordnungswidrigkeiten endlich explizit regeln.

4.5 Soziales

4.5.1 3. Auflage der ALG-II-Informationsbroschüre

Es hat sich nichts geändert. Noch immer bestimmen tägliche Eingaben und Fragen von Hartz-IV-Empfängern die Arbeit des ULD. Die Zahl der Beschwerden nimmt immer noch zu. Die dritte Auflage unserer Informationsbroschüre „**Arbeitslosengeld II – Die häufigsten Fragen zum Datenschutz beim Arbeitslosengeld II**“ gibt Antworten auf viele uns gestellte Fragen. Die Informationsbroschüre findet sich im Internet; sie kann auch telefonisch unter 0431/988-1210 oder per Mail (mail@datenschutzzentrum.de) angefordert werden. Darin wird den Betroffenen u. a. aufgezeigt, welche Fragen eine Arbeisgemeinschaft (ARGE) stellen darf, dass ein gesetzlicher Anspruch auf Diskretion und Vertraulichkeit besteht, welche Daten wie lange gespeichert werden, ob andere Behörden oder Personen Daten aus der Akte erhalten dürfen und welche Rechte jeder Einzelne hat. Geschäftsführer von ARGEn fordern die Informationsbroschüre für ihre Mitarbeiterinnen und Mitarbeiter an. Dies verstehen wir als Bestätigung unserer Arbeit.


www.datenschutzzentrum.de/sozialdatenschutz/

Was ist zu tun?
Die Informationsbroschüre „Arbeitslosengeld II – Die häufigsten Fragen zum Datenschutz beim Arbeitslosengeld II“ sollte in jeder ARGE bzw. Optionskommune ausliegen.

4.5.2 Das Problem mit den Mietverträgen

Zum Nachweis der Kosten der Unterkunft hat die Bundesagentur für Arbeit datenschutzkonforme Vorgaben entwickelt. Diese nutzen wenig, wenn sich die ARGEn nicht daran halten.

Dass bei der Berechnung des Arbeitslosengeldes II auch die **Kosten der Unterkunft** (KDU) berücksichtigt werden, ist unstrittig. Gleichwohl werden wir praktisch täglich gefragt, ob

- der vollständige Mietvertrag vorgelegt werden muss,
- die Behörde den Mietvertrag kopieren und ob
- zusätzlich eine vom Vermieter ausgefüllte und unterschriebene Mietbescheinigung verlangt werden darf.

Die Bundesagentur für Arbeit (BA) hat ein datenschutzkonformes und datensparsames Verfahren erarbeitet und den ARGEn Mustervordrucke zur Verfügung gestellt. Der Antragsteller selbst soll die erforderlichen Angaben zur Miete in der **„Anlage KDU“** eintragen. Dieser Vordruck beschränkt sich darauf, nur die wirklich erforderlichen Angaben abzufragen, bzw. weist darauf hin, dass z. B. Angaben zum Vermieter grundsätzlich freiwillig sind. Der Mitarbeiter soll die Angaben anhand des vorzulegenden Mietvertrages kontrollieren und das Ergebnis seiner Kontrolle in einem Aktenvermerk festhalten. Eine Kopie des Mietvertrages ist somit entbehrlich und der Vermieter erfährt nicht, dass sein Mieter ALG II benötigt.

Leider weichen auch in Schleswig-Holstein einzelne ARGEn von diesem Verfahren ab und fordern weitere Angaben bzw. Unterlagen. Es wird zusätzlich eine **Mietbescheinigung** gefordert, die weitaus mehr Fragen enthält und zu allem Überfluss vom Vermieter unterschrieben werden soll. So wird der Antragsteller bei seinem Vermieter zum Bittsteller und gezwungen, diesem seinen Hartz-IV-Bezug auf die Nase zu binden. Der Vermieter soll dabei angeben, ob der Mieter seine Miete stets pünktlich zahlt oder Mietschulden hat. Auch der Name und die Bankverbindung des Vermieters werden erfragt, um bei Bedarf die Miete direkt zahlen zu können.

Wir haben die ARGEn aufgefordert, sich an das Verfahren der BA zu halten. Weiter gehende Angaben können von den Betroffenen gefordert werden, soweit dies erforderlich ist. Selbst in diesem Fall muss verhindert werden, dass der Vermieter „ohne Grund“ von der Notlage seines Mieters Kenntnis erhält. Die ARGEn sagten zu, die Mietbescheinigung grundsätzlich nur als „Serviceangebot“ für die Betroffenen vorzuhalten, die nicht über anderweitige aktuelle Nachweise verfügen.

Dass **Mietverträge in Kopie zur Akte** genommen werden, wird von den ARGEn damit begründet, es reiche für Vorgesetzte oder Rechnungshöfe nicht aus, lediglich anhand eines Aktenvermerkes eines Mitarbeiters dessen Verwaltungshandeln nachzuvollziehen bzw. zu kontrollieren. Der Bundes- und die Landesbeauftragten vertreten überwiegend die Auffassung, dass die Anfertigung von Kopien zumindest von Teilen des vorgelegten Mietvertrages zulässig sein kann, wenn diese Teile Informationen beinhalten, die von den Angaben des Betroffenen abweichen bzw. dessen Angaben im erforderlichen Umfang ergänzen. Dass Kopien gefertigt werden, um das ordnungsgemäße Verwaltungshandeln der Behörde zu dokumentieren, wird zwar kritisch gesehen, aber überwiegend akzeptiert. Für alle ist aber klar, dass eine pauschale Anfertigung sämtlicher vorgelegten Unterlagen unzulässig ist.

Was ist zu tun?
Die ARGEn sollten sich an das bundeseinheitliche datenschutzgerechte und datensparsame Verfahren der BA halten. Nur im begründeten Einzelfall können weitere Angaben oder Nachweise sowie Kopien von Unterlagen gefordert und zur Akte genommen werden.

4.5.3 Die Kundendaten des Unternehmers, der Hartz IV bekommt

Ein Selbstständiger kann Anspruch auf Arbeitslosengeld II haben. Die Behörde muss in diesen Fällen bei der Leistungsberechnung die Einkünfte aus der Selbstständigkeit berücksichtigen. Dies ist in Einzelfällen äußerst schwierig; schließlich kann der Selbstständige ja keine monatliche Lohnabrechnung vorlegen.

In den von der Bundesagentur für Arbeit (BA) zur Verfügung gestellten Hinweisen zum Vordruck „Anlage EKS – Erklärung zum Einkommen aus selbstständiger Tätigkeit, Gewerbebetrieb oder Land- und Forstwirtschaft im Bewilligungszeitraum“ findet sich die allgemeine **Aufforderung, Einnahmen und Ausgaben zu belegen**.

Die Aufforderung, Unterlagen wie z. B. Einnahme-/Überschussrechnung, Gewinn- und Verlustrechnung oder betriebswirtschaftliche Auswertungen vorzulegen, ist datenschutzrechtlich unproblematisch. Schwieriger wird es, wenn z. B. Rechnungen, die der Selbstständige erstellt oder erhalten hat, oder Kontoauszüge von Geschäfts-/Privatkonten angefordert werden, da diese Unterlagen doch oftmals **Daten von Kunden und Geschäftspartnern** beinhalten.

Wir haben im letzten Jahr mit vielen ARGEn gesprochen und nachgefragt, ob es wirklich erforderlich ist, dass Kundendaten offengelegt werden. In keinem der geprüften Fälle war dies der Fall! Wir empfehlen daher allen Selbstständigen, zunächst die Kundendaten zu schwärzen und, sollte die Behörde auf die Offenlegung von Kundendaten bestehen, uns um eine Prüfung zu bitten.

Was ist zu tun?
Die ARGEn und Optionskommunen dürfen auch bei der Ermittlung der Einkünfte aus einer Selbstständigkeit nur die erforderlichen Daten erheben. Die Offenlegung von Kundendaten ist nur in wenigen zu begründenden Einzelfällen erforderlich. Der Betroffene ist auf die Möglichkeit, Kundendaten zu schwärzen, hinzuweisen.

4.5.4 Evaluation des Bundesprogramms „Perspektive 50plus“

Wissenschaftliche Begleitforschung ist im Bereich des Bezugs von Arbeitslosengeld II wichtig: Der Vergleich zwischen regional unterschiedlichen Ansätzen zur Integration älterer Arbeitsloser kann die besten Lösungen aufzeigen und so eventuell mehr Arbeitslose in einen neuen Job bringen. Nach einer intensiven Diskussion zwischen der Forschung und den Datenschutzbeauftragten ist es gelungen, die Evaluation des Bundesprogramms „Perspektive 50plus“ datenschutzfreundlich zu gestalten.

Das Bundesprogramm „Perspektive 50plus“ ist mittlerweile in seiner zweiten Phase. Vom Bund werden in dieser Programmphase rund 275 Millionen Euro Fördergelder gezahlt. Insgesamt sind an den (in der ersten Projektphase entwickel-

ten) regionalen Beschäftigungspakten für ältere Arbeitnehmer zwischen 50 und 64 Jahren inzwischen 292 Träger der Grundsicherung beteiligt. Dies entspricht ca. ⅔ der insgesamt in Deutschland existierenden Grundsicherungsstellen. Darunter sind auch sechs Träger aus Schleswig-Holstein. Das Besondere an dem Programm ist, dass es **regional entwickelte Einzelprojekte** unterstützt, die ganz unterschiedliche Ansätze haben können. Es fehlt an der sonst im Bereich der Arbeitsverwaltung üblichen Zentralisierung durch die Bundesagentur für Arbeit (BA).

Es ist nachvollziehbar, dass ein so umfangreiches Programm auf seine Wirkung hin evaluiert werden soll. Dazu wurden unterschiedliche Institute vom Bundesministerium für Arbeit und Soziales beauftragt. Das ULD wurde erstmalig im Juli 2008 vom damaligen Ministerium für Justiz, Arbeit und Europa des Landes über das Evaluationsvorhaben unterrichtet. Nach den Bestimmungen des Sozialgesetzbuches ist eine Genehmigung dieses Ministeriums für die Durchführung der Forschung erforderlich. Das ULD sollte dazu eine Stellungnahme abgeben. Wie auch andere Landesdatenschutzbeauftragte meinte das ULD, dass die erste Fassung des Antrages wegen **datenschutzrechtlicher Mängel** nicht genehmigt werden sollte. So war vorgesehen, dass die Daten der Betroffenen der zur Evaluation vorgesehenen Grundsicherungsträger unter Nutzung der Sozialversicherungsnummer der Person zur Identifizierung des Datensatzes ausgewertet werden sollten. Eine solche Nutzung der Sozialversicherungsnummer wäre eindeutig gesetzeswidrig. Die Gefahr der Identifizierung der Betroffenen bestand. Es war nicht ohne Weiteres erkennbar, warum nicht – wie gesetzlich vorgesehen – vorrangig die Einwilligung der Betroffenen zu der Forschung eingeholt werden sollte. Außerdem fehlten belastbare Ausführungen zu den technisch-organisatorischen Maßnahmen der Datensicherheit bei der Forschung.

Nach einigem Hin und Her konnten in einer auf Einladung des Bundesministeriums für Arbeit und Soziales durchgeführten Arbeitstagung die gegenseitigen Sichtweisen verdeutlicht werden. Die an der Forschung beteiligten Institute zeigten sich zu erheblichen Anstrengungen zur Verbesserung des Datenschutzes bereit. Auf dieser Basis wurde ein Konzept vorgelegt, wonach die Datensätze durch eine **doppelte Pseudonymisierung** von der Sozialversicherungsnummer abgetrennt werden. Umfangreiche technisch-organisatorische Schutzmaßnahmen, z. B. die Begrenzung des Zugangs zur Datenbank mit einem sogenannten Secure ID Onetime-Token, waren vorgesehen. Dieses Token zeigt im 60-Sekundentakt wechselnde 6- bis 8-stellige Zugangscodes an. Der Zugang zu der Datenbank wurde also nicht nur an das Wissen eines Passwortes, sondern auch an den Besitz dieses Tokens geknüpft.

Letztlich wurde auf einige detaillierte Angaben verzichtet, wie beispielsweise auf tagesgenaue Angaben zur Maßnahmenteilnahme, die zur Identifizierung der Betroffenen hätten führen können. Im **überarbeiteten Antrag** vom Mai 2009 ist detailliert dargelegt, weshalb das Einholen von Einwilligungen nicht praktikabel ist und die Befragung einer repräsentativen Stichprobe nicht ausreicht. Dabei spielt eine Rolle, dass es keine zentrale Übersicht über die Maßnahmenteilnehmer gibt. Die Maßnahmen werden nicht zentral durch die BA koordiniert. Infolgedessen kann eine Sammlung der Daten auch nur über die jeweiligen Grundsiche-

rungsträger realisiert werden. Aus Datenschutzsicht sind diese Prämissen der Sozialforschung schlüssig dargelegt. Durch die Implementierung von Schutzmaßnahmen und die effektive Pseudonymisierung der Daten bei der Forschung können die Datenschutzrisiken effektiv auf ein Minimum reduziert werden. Von Bedeutung ist schließlich, dass die Begleitevaluation einen wichtigen sozialpolitischen Zweck erfüllt.

Insgesamt stellt die Evaluation des Bundesprogramms „Perspektive 50plus“ in der zweiten Phase ein Beispiel für einen **gelungenen Kompromiss** zwischen wichtiger sozialwissenschaftlicher Forschung und notwendigem Schutz der Rechte der Betroffenen dar.

Was ist zu tun?
Sozialwissenschaftliche Forschungsvorhaben sollten frühzeitig mit den Datenschutzbeauftragten abgestimmt werden. In der Regel finden sich Lösungen, um Gefährdungen für die Betroffenen zu minimieren und zugleich zu aussagekräftigen Forschungsergebnissen zu kommen.

4.5.5 Indikations- und Begründungsbögen der Krankenkassen

Seit Jahren mahnen wir die Krankenkassen, sich bei der Informationsbeschaffung an die gesetzlichen Vorgaben zu halten. Doch die ungesetzliche Neugier der Kassen beschäftigt Datenschützer jedes Jahr aufs Neue.

Erst Krankenhausentlassungsberichte, dann Selbstauskunftsbögen, es folgten die Reha-Entlassungsberichte (siehe u. a. 22. TB, Tz. 4.7.3); nun sind es die sogenannten Indikations- und Begründungsbögen. Insbesondere einzelne bundesunmittelbare Krankenkassen nutzen jede Möglichkeit, um an **medizinische Daten** ihrer Versicherten zu kommen, und missachten dabei die gesetzlichen Vorgaben des Sozialgesetzbuches V (SGB V).

Ein Sanitätshaus berichtete uns von „neuen“ Vordrucken verschiedener Kassen. Auf bis zu 7 (!) Seiten wurden die Versicherten oder deren Pflegekräfte aufgefordert, detaillierte Angaben zur gesundheitlichen Situation zu machen. „**Keine Angaben, keine Leistung**“, so lautete die versteckte Botschaft dieser Indikations- und Begründungsbögen.

Wir fragten nach dem Vorgehen der **Landeskassen Schleswig-Holstein**. Die AOK verneinte unsere Frage nach der Nutzung solcher Bögen und verwies zu Recht auf die Zuständigkeit des Medizinischen Dienstes der Krankenversicherung (MDK). Die IKK Nord musste eingestehen, einen vergleichbaren, wenn auch weniger umfangreichen Vordruck einzusetzen.

Wir teilten der IKK Nord mit,

- dass eine pauschale Verwendung von Indikations- und Begründungsbögen unzulässig ist,

- dass lediglich in begründeten Prüfungsfällen eine Datenerhebung durch den MDK erfolgen darf und
- dass eine Krankenkasse zur Vorbereitung der Aufgabenwahrnehmung durch den MDK derartige Vordrucke an die Leistungserbringer bzw. -bezieher nur versenden darf, wenn sichergestellt ist, dass der Rücklauf ausschließlich direkt an den MDK (und nicht über die Krankenkasse) erfolgt.

Die IKK Nord versicherte schriftlich, sich an diese **datenschutzrechtlichen Vorgaben** zu halten.

Was ist zu tun?
Die gesetzlichen Krankenkassen dürfen bei der Datenerhebung die gesetzlichen Vorgaben nicht überschreiten. Medizinische Daten sind durch den MDK zu erheben.

4.5.6 Rabattverträge bei der Hilfsmittelversorgung

Seit einiger Zeit dürfen Krankenkassen Versorgungsverträge über Hilfsmittel mit einzelnen Herstellern bzw. Lieferanten solcher Artikel abschließen. Dies wirft Datenschutzfragen auf.

Aufgeregt schilderten uns viele Anrufende, dass sie von einem völlig unbekannten Unternehmen aus Schleswig-Holstein aufgefordert worden sind, ihre Inkontinenzartikel zukünftig nur noch dort zu kaufen. Die **Barmer Ersatzkasse** hatte mit diesem Unternehmen einen Rabattvertrag abgeschlossen und diesem die Daten von Versicherten übermittelt. So wusste das Unternehmen darüber Bescheid, welcher Versicherte dieser Kasse an Blasenschwäche litt. Die Versicherten selbst waren nicht über die Datenweitergabe informiert worden. Wir informierten den für die Barmer zuständigen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit über dieses hochproblematische Vorgehen.

Gesetzliche Krankenkassen können für die Versorgung ihrer Versicherten mit Hilfsmitteln wie Bildschirmlesegeräten, Rollstühlen, Anti-Dekubitus-Systemen oder Inkontinenzartikeln mit den Anbietern dieser Produkte, den sogenannten Leistungserbringern, **Versorgungsverträge** abschließen. Ziel dessen ist ein einheitlich hoher Qualitätsstandard bei gleichzeitiger Kosteneinsparung. Für die Versicherten bedeutet dies allerdings den Wegfall ihres Wahlrechts. Konnten diese zuvor jede beliebige Apotheke bzw. jedes Sanitätsfachgeschäft aufsuchen, so werden sie durch die Versorgungsverträge gezwungen, die benötigten Hilfsmittel bei dem von der Kasse bestimmten Vertragspartner zu kaufen.

Auch die **AOK Schleswig-Holstein** nutzt diese Möglichkeit. Die AOK versicherte uns, dass sie nicht pauschal Listen mit den Daten der Versicherten an die Vertragspartner übermittelt. Man habe vielmehr alle Leistungserbringer darüber unterrichtet, welche Unternehmen zukünftig für AOK-Versicherte welche Hilfsmittel herstellen oder verkaufen dürfen. Man erwarte, dass, wenn ein Versicherter in einem Sanitätshaus vorspricht, mit dem die AOK keinen Versorgungsvertrag

abgeschlossen hat, dieses Sanitätshaus den Versicherten „ablehnt“ und ihm aufzeigt, wo er sein Hilfsmittel beziehen kann. Die Praxis habe gezeigt, dass sich alle Unternehmer an diese neuen Spielregeln halten würden.

Tatsächlich alle? Ein Unternehmer in Schleswig-Holstein, der seit vielen Jahren Anti-Dekubitus-Systeme anbietet, sträubte sich. Für ihn ist es nicht nachvollziehbar, dass der Versicherte kein Wahlrecht mehr haben soll. Auch fürchtet der Unternehmer um seine wirtschaftliche Existenz. Er will weiterhin AOK-Versicherte als Kunden betreuen dürfen, auch wenn er nicht Rabattpartner der AOK ist. Es ist nicht Aufgabe des Datenschutzes, wirtschaftliche Konflikte zwischen David und Goliath zu klären. Geht es dabei um die Daten der Versicherten, so sind wir gefordert. Der erwähnte Unternehmer hat Kunden auf Nachfrage Kostenvoranschläge erstellt. Diese enthalten naturgemäß auch Angaben zur Erkrankung. Die Kunden reichten diese Kostenvoranschläge bei der AOK ein. Wir untersagten der AOK, eingehende Kostenvoranschläge ohne Einwilligung der Versicherten an den eigenen Vertragspartner weiterzureichen. Ansonsten käme es auch hier zur ungefragten Übermittlung von Gesundheitsdaten an ein privates Unternehmen.

Was ist zu tun?
Gesetzliche Krankenkassen sind berechtigt, für die Versorgung ihrer Versicherten mit Hilfsmitteln Versorgungsverträge abzuschließen. Daraus resultiert aber keine Befugnis, den ausgewählten Unternehmen ohne Kenntnis der Versicherten deren Daten zu übermitteln. Vor der Übermittlung sollte die Einwilligung der Versicherten eingeholt werden. Jedenfalls ist den Versicherten die Möglichkeit zu geben, der beabsichtigten Übermittlung zu widersprechen.

4.5.7 Neue Berater bei den Pflegekassen und ihre Befugnisse

Die Pflegekassen dürfen jetzt eigene Mitarbeiter als Pflegeberater einsetzen. Diese Beratung muss den Versicherten dienen und darf nicht zu einer Kontrolle gegen deren Willen umfunktioniert werden.

Weil es für Pflegeberater der AOK ehedem an einer gesetzlichen Aufgabenzuweisung fehlte, mussten wir deren Tätigkeit kritisieren (28. TB, Tz. 4.6.6). Das Pflege-Weiterentwicklungsgesetz änderte jetzt die Rechtslage. Seit Anfang 2009 haben die Versicherten einen Anspruch auf individuelle Beratung und Hilfestellung. Das Gesetz sieht vor, dass ein **individueller Versorgungsplan** erstellt wird. Anders als zuvor darf die Pflegeberatung nun durch Mitarbeitende der Pflegekassen durchgeführt werden.

Wir wollten genau wissen, ob es bei der Beratung bleibt oder eine Kontrolle durch „die Hintertür“ erfolgt. Nach Auskunft der AOK Schleswig-Holstein sind ca. 100 Personen mit besonderen Kenntnissen im Pflegeversicherungsrecht als Pflegeberater tätig. Man habe aus früheren Fehlern gelernt und die Anregungen des ULD aufgegriffen. Es gehe ausschließlich um **Beratung und Unterstützung**. Die Kontaktaufnahme erfolge grundsätzlich telefonisch. Gemäß den gesetzlichen Vorgaben erfolge eine Pflegeberatung nur, wenn dies vom Versicherten gewünscht

werde. Eine Ablehnung habe keine Konsequenzen. Alle Mitarbeiter seien umfassend geschult und sensibilisiert worden. Kein Versicherter solle den Eindruck erhalten, es gehe hier um Kontrolle.

Eine Eingabe passte nicht in dieses schöne Bild. Die Tochter einer Versicherten schilderte uns, dass ihre Mutter nach einem Telefonat mit einer Pflegeberaterin einen Brief erhalten hat. Diesem lag ein **zehnseitiger Versorgungsplan** bei. Detailliert war aufgeführt, was man zuvor telefonisch besprochen hatte. Die letzte Seite enthielt eine „Datenschutzerklärung“ und die Aufforderung, „alle relevanten Informationen über die persönlichen und sächlichen Lebensverhältnisse mitzuteilen“. Mit Unterschrift sollte bestätigt werden, dass man umfassend unterrichtet wurde und damit einverstanden ist, dass „alle erforderlichen Daten erhoben, gespeichert und übermittelt werden“. Zu allem Überfluss war auch noch der Hinweis aufgenommen, dass „eine fehlende Mitwirkung zu Nachteilen führen könnte“.

Die AOK räumte ein, der vom AOK-Bundesverband entwickelte Vordruck sei **„unglücklich“ formuliert** und werde in der täglichen Praxis von den Mitarbeitern als kontraproduktiv empfunden. Es wurde umgehend vereinbart, dass die AOK den Vordruck unter Beteiligung des ULD datenschutzgerecht überarbeitet und dem Bundesverband zur Übernahme empfiehlt. Die Versicherte war begeistert, dass ihre AOK so schnell und konstruktiv ihre Kritik aufgegriffen hatte.

Was ist zu tun?
Pflegekassen können neuerdings eigene Mitarbeiter mit der Pflegeberatung beauftragen. Dabei muss sichergestellt werden, dass aus der Beratung keine versteckte Kontrolle wird. Der Versicherte kann nicht zur Annahme des Angebots gezwungen werden. Die eigene Verantwortung endet nicht, wenn Vordrucke oder Verfahrensvorgaben vom Bundesverband übernommen werden.

4.5.8 Tonbandaufzeichnungen beim Notdienst der KVSH

Das Aufnehmen des nicht öffentlich gesprochenen Wortes auf einen Tonträger ist eine Straftat. Ausnahmen gibt es nur für wenige gesetzlich benannte Stellen. Ansonsten ist die Einwilligung der Anrufer erforderlich.

01805/119292 – wer in den Nachtstunden oder am Wochenende einen Arzt benötigt, wählt diese Nummer. Der vertragsärztliche Notdienst der Kassenärztlichen Vereinigung Schleswig-Holstein (KVSH) stellt sicher, dass ein Arzt nach Hause kommt oder in einem akuten Notfall der Rettungsdienst unterrichtet wird. 350.000 Anrufende nutzen jährlich diesen Service. Um die ärztliche Versorgung in Schleswig-Holstein zu optimieren, wurden die ehemals über das ganze Land verteilten Arztnotrufzentralen in einer **zentralen Leitstelle** in Bad Segeberg zusammengefasst.

Neu sollte auch sein, dass alle eingehenden **Telefongespräche aufgezeichnet** werden, ohne dass die Anrufenden hierüber unterrichtet werden. Die KVSH

erklärte, die Tonbandaufzeichnungen dienten der Sicherheit der Anrufer, der Ärzte und der Mitarbeiter der Leitstelle. Nur so sei es möglich, Rückfragen zu eingehenden Anrufen umgehend zu klären oder nachzuvollziehen, wie viel Zeit zwischen Anruf und dem Hausbesuch des Arztes verging. Wenn die Rettungsstellen der Polizei und Feuerwehr aufzeichnen dürfen, so müsse dies doch auch für die KVSH gelten.

Unbefugte Aufzeichnung von Telefonaten kann mit einer Gefängnisstrafe von bis zu drei Jahren bestraft werden. Das Rettungsdienstgesetz enthält eine Befugnis zur Aufzeichnung nur für die Rettungsstellen. Daher bleibt der KVSH nach der geltenden Rechtslage nichts anderes übrig, als sich vor der Aufzeichnung die Einwilligung der Anrufer einzuholen bzw. zumindest diesen die Möglichkeit zum Widerspruch einzuräumen. Die KVSH reagierte auf unseren Hinweis. Zukünftig wird jedem eingehenden Anruf ein Informationstext mit einem Hinweis auf die **Widerspruchsmöglichkeit** vorgeschaltet. Durch einen Tastendruck erhält der Anrufer die Möglichkeit, seinen Widerspruch zu erklären. Auch ist ein mündlicher Widerspruch zu Beginn des Telefonates möglich.

Nicht nur die Aufzeichnung zwischen den Patienten und der Leitstelle ist kritisch zu beleuchten. Wir forderten die KVSH auf, vor einer Aufzeichnung der Telefonate der Leitstelle mit den **diensthabenden Ärzten** die rechtlichen Vorgaben zu beachten.

Was ist zu tun?
Tonbandaufzeichnungen von Telefonaten bedürfen stets einer ausreichenden Befugnisgrundlage. Nur wer sich zuvor der Einwilligung seines Gesprächsteilnehmers versichert, begibt sich nicht in die Gefahr, sich strafbar zu machen.

4.5.9 Qualitätskontrollen und Früherkennungsuntersuchungen

Qualitätskontrollen sind im Gesundheitswesen gesetzlich vorgeschrieben und sollen nach dem Willen des Gesetzgebers verstärkt und sektorenübergreifend durchgeführt werden. Bestimmte Früherkennungsmaßnahmen sind für die Versicherten verpflichtend geworden. Das ULD hat zu den dabei entstehenden datenschutzrechtlichen Fragestellungen Patientenvertreter und Beteiligte beraten.

Maßnahmen der **Qualitätssicherung** werden in allen Leistungsbereichen der gesetzlichen Krankenversicherung in unterschiedlichem Ausmaß und auf unterschiedlichen Grundlagen seit Langem durchgeführt. Ziel ist eine bedarfsgerechte und zugleich wirtschaftliche Patientenversorgung auf hohem Niveau. Qualitätssicherung soll in Zukunft verstärkt und sektorenübergreifend stattfinden. Für die Patientinnen und Patienten, also die Versicherten, bedeutet dies, dass sehr viele von deren sensiblen medizinischen Daten an die für die Qualitätssicherung zuständigen Stellen weitergegeben werden oder gar neu erhoben werden müssen. Im Interesse einer rechtmäßigen Datenverarbeitung muss der Gesetzgeber eine Rechtsgrundlage schaffen und transparent machen, welche Daten in welcher Form

dafür verwendet werden. Er muss Vorkehrungen zum Schutz der Patientendaten treffen. Die die Qualitätssicherung durchführende Stelle muss besonderen Anforderungen genügen. Nach unserer Auffassung besteht hier noch Ergänzungsbedarf des Gesetzgebers.

https://www.datenschutzzentrum.de/vortraege/20091119-weichert-sektorenuebergreifende-qualitaetssicherung.html

Mit **Früherkennungsuntersuchungen** sollen Krankheiten in einem Frühstadium entdeckt werden. Schon seit Langem werden sie von der gesetzlichen Krankenversicherung auf freiwilliger Basis angeboten. Seit dem Jahr 2007 gilt, dass die Nichtteilnahme an einigen Früherkennungsmaßnahmen zu höheren Kosten für die Versicherten führen kann. Dem Gesetzeswortlaut nach sind Personen ab einem bestimmten Alter von der Chronikerregelung ausgenommen, wenn diese nicht an bestimmten Krebsfrüherkennungsmaßnahmen teilgenommen haben und später an dieser Krankheit erkranken. Die Folge ist dann, dass die Nichtteilnehmer an den Früherkennungsmaßnahmen höhere Zuzahlungen zu Medikamenten, stationären Behandlungen usw. erbringen müssen als die Teilnehmer. Diese Regelung stellt einen erheblichen Eingriff auch in das informationelle Selbstbestimmungsrecht der Betroffenen dar. Sie sind nicht mehr frei in der Entscheidung darüber, ob sie an den Früherkennungsmaßnahmen teilnehmen wollen. In der Folge kommt es zur Verarbeitung von Gesundheitsdaten, der diese Personen eventuell freiwillig nicht zugestimmt hätten. Unseres Erachtens wäre lediglich eine verpflichtende Beratung über die Vorsorgeuntersuchungen verhältnismäßig und damit zulässig. Diese Meinung wird von vielen Experten geteilt. Es verwundert daher nicht, dass das Gesetz bisher nicht vollständig umgesetzt wurde und de facto nur eine Beratungspflicht besteht.

Es ist angedacht, die mit den Früherkennungsmaßnahmen gewonnenen Daten in ein **zentrales Register** einzupflegen und bzw. oder mit anderen Registerdaten abzugleichen. Jede Speicherung von Gesundheitsdaten ist ein Eingriff in das Recht auf informationelle Selbstbestimmung. Daher bedarf es zum Aufbau und Führen eines solchen Gesundheitsregisters einer gesetzlichen Ermächtigung. Vor Errichtung eines speziellen Registers sollte zunächst überlegt werden, ob für den verfolgten Zweck nicht die Verarbeitung anonymisierter Datensätze genügt.

Was ist zu tun?
Bei der Qualitätssicherung und den Früherkennungsmaßnahmen muss der Datenschutz stärker im Fokus stehen. Der Gesetzgeber muss hier präziser und zurückhaltender regeln.

4.5.10 eGK – Nichts geht mehr?

Die Datenschutzbeauftragten des Bundes und der Länder hatten gerade die „gematik“ auf die Notwendigkeit von Vorkehrungen zur Wahrnehmung der Betroffenenrechte bei der elektronischen Gesundheitskarte hingewiesen, da verkündet der neue Bundesgesundheitsminister ein Moratorium für „die Realisierung weiterer medizinischer Anwendungen“.

Die elektronische Gesundheitskarte (eGK) stößt vor allem bei Ärztinnen und Ärzten auf erhebliche Vorbehalte, was zu Verzögerungen bei ihrer Einführung beitrug (siehe zuletzt 31. TB, Tz. 4.5.4). Die Datenschutzbeauftragten von Bund und Ländern mussten dann feststellen, dass Vorkehrungen zur **Wahrnehmung der Betroffenenrechte** bisher in den praktischen Planungen nicht ausreichend berücksichtigt wurden, und befürchteten, dass die Grundkonzeption der eGK obsolet werden könnte, wonach die Patienten die Datenhoheit über ihre Gesundheitsinformationen haben. Diese setzt voraus, dass es tatsächlich Gelegenheit zur Einsichtnahme in die eigenen Daten gibt. Die Konferenz der Datenschutzbeauftragten wandte sich daher im September 2009 über ihren Vorsitzenden an den Geschäftsführer der gematik und drang auf konkrete Konzepte zur Rechtewahrnehmung durch die Karteninhaber. Im Gespräch ist der sogenannte eKiosk, der an von Patienten stärker frequentierten Orten aufgestellt werden und es ermöglichen soll, sich die Daten auf der Karte anzusehen und zu verwalten. Erörtert wird auch die sogenannte Pin-at-home-Lösung, die einen solchen Zugang in der häuslichen Umgebung ermöglichen würde.

Das sogenannte **Basis-Rollout** der Karten im 4. Quartal 2009 stand in der Region Nordrhein unmittelbar bevor. Gemäß einem Zwiebelschalenprinzip sollten dabei von den Kassen nach und nach die echten Karten an die Versicherten ausgegeben werden. Die gematik antwortete umgehend und sicherte zu, dass ein demnächst zu veröffentlichendes Datenschutzkonzept weitere Informationen zur Einsichtnahme in die Daten für die Versicherten enthalten werde. Szenarien, etwa die Pin-at-home-Nutzung und die eKioske, seien noch in der Prüfung bzw. in Planung.

In diese Situation platzte im November 2009 die Nachricht, dass der neue Bundesgesundheitsminister ein **eGK-Moratorium** festgesetzt hat. Es soll so lange gelten, bis praxistaugliche, höchsten datenschutzrechtlichen Anforderungen entsprechende Lösungen für die weiteren medizinischen Anwendungen vorgelegt werden. Die eGK hat zurzeit faktisch lediglich die technischen Möglichkeiten einer etwas erweiterten Krankenversichertenkarte. Sie enthält das Foto des Versicherten; auch das Speichern eines Notfalldatensatzes auf der Karte soll möglich bleiben. Realisiert werden soll weiterhin der Versichertenstammdatendienst; damit kann beim Einlesen der Karte beim Arzt online überprüft werden, ob die Karte noch gültig ist und welcher Zuzahlungsstatus besteht. Voraussetzung dafür wäre aber die Online-Anbindung der Arztpraxen, gegen die sich viele Ärzte wenden.

Das ursprünglich an erster Stelle stehende elektronische Rezept ist zunächst vom Tisch – genauso wie der elektronische Arztbrief und weitere Anwendungen.

Unklar war zum Redaktionsschluss, ob das Basis-Rollout fortgesetzt wird. Einige Krankenkassen meldeten beim jetzigen Projektstatus Bedenken gegen die Ausgabe neuer Karten an. Die Zukunftsfähigkeit der einhergehenden Investitionen sei nicht sicher.

Aus Datenschutzsicht besteht derzeit keine Dringlichkeit, denn die sensiblen, beobachtungsbedürftigen Anwendungen sollen vorläufig nicht kommen bzw. erübrigen sich: eKioske und Pin-at-home-Lösungen ergeben erst einen Sinn, wenn medizinische Daten über die Karte verfügbar werden. Wichtig bleibt die Begleitung der weiteren Entwicklung. Hierzu gehören auch **Produkte privater Anbieter**, die versuchen, die entstehenden Lücken bei der digitalen Übermittlung und Speicherung von Gesundheitsinformationen zu füllen.

Was ist zu tun?
Bei der weiteren Planung und Umsetzung der eGK wie auch bei privaten IT-Anbietern im Gesundheitswesen kommt dem Datenschutz eine zentrale Rolle zu. Die Datenschutzbeauftragten helfen gerne und stehen für Rat und Tat bereit.

4.5.11 Schweigepflichtentbindungserklärung beim Mammografie-Screening

Am Mammografie-Screening-Programm teilnehmende Frauen haben die Wahl: Darf die Screening-Einheit Informationen über Vorerkrankungen von anderen Ärzten anfordern? Darf die Screening-Einheit Feststellungen an andere Ärzte weitergeben?

Das ULD begleitet laufend das flächendeckende Angebot zum Mammografie-Screening für Frauen zwischen 50 und 69 Jahren (29. TB, Tz. 4.6.3; 30. TB, Tz. 4.6.2; 31. TB, Tz. 4.5.5). Wir wurden nun darauf aufmerksam, dass bei den vier Screening-Einheiten in Schleswig-Holstein **unterschiedliche Formulare** gebraucht wurden, mit denen die Frauen erklären sollten, ob sie mit der Beiziehung von medizinischen Informationen von anderen Ärzten einverstanden sind bzw. ob sie einwilligen, dass die Erkenntnisse aus dem Mammografie-Screening an andere Ärzte weitergegeben werden. Teilweise waren diese Erklärungen mit der grundsätzlichen Einwilligung zur Teilnahme am Screening verbunden.

Das Screening kann und darf nur durchgeführt werden, wenn die Frau in die Teilnahme überhaupt einwilligt. Damit darf aber nicht automatisch die Einwilligung in die Beiziehung von Informationen anderer Ärzte bzw. die Weitergabe von Erkenntnissen des Screening-Programmes an andere Ärzte verbunden werden. Für diese unterschiedlichen Sachverhalte sind jeweils **zwei getrennte Erklärungen** abzugeben. Sicherlich ist die Begutachtung von auffälligen Befunden in der Screening-Einheit oft leichter möglich, wenn früher angefertigte Mammogramme vorher behandelnder Ärzte vorliegen. Jedoch gibt es keinen Automatismus, wonach die Screening-Einheiten diese Informationen ohne Weiteres beiziehen könnten. Nötig ist in jedem Fall die Einwilligung der Frauen. Entsprechendes gilt für die Weitergabe von Erkenntnissen aus dem Screening an andere Stellen.

Die bundesweit agierende Kooperationsgemeinschaft Mammografie-Screening (http://www.mammo-programm.de) hat bereits vor einiger Zeit einen **Anamnesebogen** entwickelt, der den Frauen zusammen mit der Einladung zugeschickt werden soll. Neben einigen Fragen zu Vorerkrankungen und Gesundheitsstatus werden dort auch die beiden oben angesprochenen Erklärungen in gut verständlicher Weise abgefragt. Die Frauen konnten im in der Vergangenheit verwendeten Anamnesebogen die beiden Erklärungen nicht eindeutig und getrennt abgeben. Von den Screening-Einheiten vor Ort wurden zudem teilweise individuelle Zusatzbögen verwendet, was noch mehr zur Unklarheit beitrug, welches der Wille der Frauen ist.

Auf Intervention des ULD wurde die Verwendung **einheitlicher Muster in ganz Schleswig-Holstein** erreicht. Die regionalen Screening-Einheiten verzichten auf zusätzliche eigene Erklärungsbögen. Der im Land verwendete Anamnesebogen, der von der Zentralen Stelle Mammografie-Screening zugeschickt wird, enthält die Möglichkeit zu bestimmen, ob der Hausarzt bzw. der Frauenarzt über das Ergebnis informiert werden soll; die Ärzte sind namentlich aufzuführen. Weiterhin wird gefragt, ob und gegebenenfalls wo bereits in der Vergangenheit Mammografie-Aufnahmen gefertigt wurden. Die Frauen können dann die Frage „Dürfen wir dort nachfragen?“ mit Ja oder Nein beantworten. So steuern die Frauen im Mammografie-Screening selbst, welche Ärzte welche Informationen über sie erhalten.

Was ist zu tun?
Beim Mammografie-Screening wie auch generell müssen Ärzte darauf achten, dass die Einwilligung der betroffenen Patienten vorliegt, bevor medizinische Unterlagen von anderen Stellen angefordert bzw. eigene medizinische Daten an andere Stellen weitergegeben werden.

4.5.12 Bundessozialgericht bremst Einbeziehung von privaten Stellen bei der GKV

Das Bundessozialgericht hat klargestellt, dass die Einbeziehung von privaten Stellen in Datenflüsse der gesetzlichen Krankenversicherung nur bei Vorliegen einer gesetzlichen Regelung erlaubt ist. Das Vorliegen der vermeintlichen Einwilligung der Betroffenen kann Datenübermittlungen nicht legitimieren.

Dem Urteil vom Dezember 2008 lag ein Fall zugrunde, in welchem ein Krankenhaus die ambulant erbrachten Leistungen nicht wie gesetzlich vorgesehen direkt mit der zuständigen Kassenärztlichen Vereinigung (KV) abrechnete. Vielmehr hatte es eine **privatärztliche Verrechnungsstelle** dazwischengeschaltet, die für das Krankenhaus die Abrechnung mit der KV vornehmen sollte. Dazu hatte der Krankenhausträger mit einem Formular die Einwilligung der Patienten eingeholt.

Trotz der Einwilligung kommt das Bundessozialgericht (BSG) zum Ergebnis, dass diese Datenweitergabe unzulässig ist. Eine Einwilligung kann im Bereich der gesetzlichen Krankenversicherung (GKV) eine Datenverarbeitung nur rechtfertigen, wenn es dafür eine **ausdrückliche gesetzliche Grundlage** gibt. Dies ist im

Hinblick auf die Einschaltung von privaten Stellen in die ambulante Abrechnung nicht der Fall. Das Gericht betont die Bedeutung des Datenschutzes im Bereich der GKV. Das Fünfte Buch des Sozialgesetzbuches (SGB V) legt die zulässigen Datenverarbeitungsvorgänge hinsichtlich der Abrechnung für die Leistungserbringer abschließend fest. Die Einbeziehung von externen Dritten würde detaillierte Datenschutzregelungen nötig machen, wie es sie für die Datenflüsse zwischen den öffentlich-rechtlichen Institutionen in der GKV gibt. Es wäre nicht begründbar, an privatrechtliche Stellen insoweit geringere Anforderungen zu stellen. Die eingeholten Einwilligungen rechtfertigten die Datenweitergabe nicht.

Das Urteil hat über den konkreten Fall hinaus Bedeutung. Die Einschaltung privater Stellen ist im Kern in einigen Bereichen angelegt, ohne dass das Gesetz ein Schutzregime definiert, das mit dem öffentlich-rechtlichen System der GKV vergleichbar ist. Dies betrifft z. B. den Bereich der sogenannten **hausarztzentrierten Versorgung**, worauf das Bundessozialgericht selbst hinweist.

Nach unserer Kritik reagierte der Gesetzgeber prompt: Im Schnelllauf vor Ende der Legislaturperiode wurde in einem **Artikelgesetz** zur Änderung arzneimittelrechtlicher und anderer Vorschriften eine Regelung in das SGB V eingefügt, wonach sich Krankenhäuser zur Abrechnung von ambulanten Leistungen „anderer Stellen“ bedienen dürfen. Auch bei der hausarztzentrierten Versorgung „darf eine andere Stelle mit der Verarbeitung und Nutzung der für die Abrechnung dieser Leistungen erforderlichen personenbezogenen Daten beauftragt werden“. Damit wurde aber dem inhaltlichen Anliegen des Bundessozialgerichts, wonach die Einzelheiten der Datenverarbeitung bei der Einbeziehung privater Stellen detailliert geregelt sein müssen, nicht Genüge getan.

Das Urteil ist für einen weiteren Bereich relevant: Krankenkassen versuchen immer wieder, die ihnen gesetzlich zugewiesenen Informationswege zu erweitern, indem sie Schweigepflichtentbindungserklärungen von den Versicherten einholen (22. TB, Tz. 4.7.3). Auf diese Weise sollen **Informationsquellen jenseits des Gesetzes** für die Kassen erschlossen werden; von Interesse sind namentlich OP- und Entlassungsberichte. Nach den Maßstäben des BSG dürfen Krankenhäuser auf der Basis solcher Erklärungen keine Unterlagen an die Kassen herausgeben, da es an einer entsprechenden gesetzlichen Befugnis fehlt.

Nebenbei äußerte das Bundessozialgericht erhebliche **Zweifel an der Freiwilligkeit** von Einwilligungen, wenn diese im Vorfeld notwendiger medizinischer Behandlungen und namentlich bei Notfallbehandlungen abgegeben werden. Anders als die meisten Bundesländer verfügt Schleswig-Holstein nicht über spezielle Datenverarbeitungsvorschriften für den Krankenhausbereich. Als Folge davon wird die in der Praxis als unvermeidlich angesehene Einschaltung von externen Auftragnehmern für bestimmte Dienstleistungen, etwa bei der Wartung medizinischer Geräte, auf genau solche Einwilligungen gestützt. Rechtsunsicherheit wird sich ergeben, wenn weitere Gerichte den Zweifeln des Bundessozialgerichts an der Freiwilligkeit der Einwilligung folgen. Es ist an der Zeit, über die Schaffung einer landesgesetzlichen Grundlage für die Einschaltung privater Auftragsdatenverarbeiter im Krankenhausbereich nachzudenken.

Was ist zu tun?
Alle Institutionen in der gesetzlichen Krankenversicherung dürfen personenbezogene Daten nur auf hinreichender gesetzlicher Grundlage verarbeiten. Die Einwilligung des Betroffenen genügt in der Regel nicht für Datenübermittlungen von Leistungserbringern an andere Stellen. Die Landesregierung sollte den Erlass von spezialgesetzlichen Regelungen für notwendige Datenweitergaben im Krankenhausbereich prüfen.

4.5.13 Wenn Jugendgerichtshilfe und Arbeitsamt zusammenarbeiten …

Zukunftsaussichten für straffällig gewordene Jugendliche und Heranwachsende verbessern sich, wenn diesen eine berufliche Perspektive aufgezeigt werden kann. Unter welchen Bedingungen darf die Jugendgerichtshilfe Kontakt mit den Arbeitsämtern oder Arbeitsgemeinschaften aufnehmen?

Im Juli 2009 bat uns das damalige Ministerium für Justiz, Arbeit und Europa um Klärung, wie ein Datenaustausch zwischen Jugendgerichtshilfe, Polizei, Staatsanwaltschaften, Jugendgerichten und Agenturen für Arbeit bzw. Arbeitsgemeinschaften (ARGEn) auf datenschutzrechtlich sichere Beine gestellt werden kann. Schon aus fachlicher Sicht wurde erkannt, dass nur ausreichendes Wissen über die Datenflüsse und die Möglichkeit für die Jugendlichen, selbst zu entscheiden, diese nachhaltig motivieren, neue Wege einzuschlagen. Der Jugendliche soll nicht von der **Verantwortung für sein Handeln** befreit werden, indem der Staat für ihn entscheidet.

Schnell konnte daher Einigkeit erlangt werden, dass die beabsichtigte Zusammenarbeit der Behörden für die Jugendlichen so transparent wie möglich gestaltet werden muss. Gemeinsam wurden **Hinweise** erarbeitet, die verständlich jede denkbare Datenübermittlung zwischen den beteiligten Stellen aufzeigten.

Schwierig war und ist, dass für die jeweiligen Behörden unterschiedliche Regelungen gelten und diese nicht ausreichende Befugnisse für den geplanten Datenaustausch beinhalten. Die Lösung berücksichtigt das Ziel weitestgehender Autonomie des Jugendlichen für seinen Lebensweg und überträgt ihm auf nachvollziehbare Weise die Verantwortung für sein Handeln, indem wir eine **Einwilligungserklärung** erarbeiteten, die dezidiert die einzelnen Kommunikationswege auflistet. Dabei wird dem Jugendlichen klargemacht, dass ohne bestimmte Kommunikationen spezifische Hilfen nicht möglich sind. Unsere Materialien stehen bundesweit für vergleichbare Vorhaben zur Verfügung.

Was ist zu tun?
Damit Behörden untereinander personenbezogene Daten austauschen dürfen, bedarf es einer ausreichenden Übermittlungsbefugnis. Fehlt es an gesetzlichen Vorschriften, kann gegebenenfalls die informierte Einwilligung des Betroffenen eingeholt werden.

4.5.14 Kontrolle des kontrollierenden Einladungswesens

Das von der Landeshauptstadt praktizierte Verfahren des Einladungswesens zum Kindergesundheitscheck erwies sich bei einer Prüfung im Wesentlichen als vorbildlich. In Einzelfällen erfolgten nicht autorisierte Nachfragen bei den Kinderärzten.

Wir berichteten ausführlich über das sogenannte kontrollierende Einladungs- und Meldewesen zu den Früherkennungsuntersuchungen U4 bis U9 (31. TB, Tz. 4.5.8). Der entscheidende Teil des Verfahrens wird durch die Kreise und kreisfreien Städte umgesetzt; diese müssen **im Einzelfall überprüfen**, was dahintersteckt, wenn das Landesfamilienbüro keine Bestätigung über die Durchführung der Untersuchung erhält. Die Umsetzung dieser Aufgabe prüften wir in Kiel und stellten dabei grundsätzlich fest, dass das eingeführte Verfahren konzeptionell nicht zu beanstanden ist.

Die vom Landesfamilienbüro eingehenden Briefe über nicht durchgeführte Früherkennungsuntersuchungen gehen in Kiel zunächst zum Amt für Gesundheit. Anders als die meisten anderen Kommunen hatte die Landeshauptstadt zum Prüfungszeitpunkt dort schon einen eigenen Besuchsdienst eingerichtet. Der **Hausbesuch bei den Sorgeberechtigten** erfolgt durch einen Mitarbeiter des Gesundheitsamtes nach schriftlicher Ankündigung. Dabei soll festgestellt werden, ob die Untersuchung zwischenzeitlich stattgefunden hat. Falls nicht, sollten die Eltern davon überzeugt werden, die Untersuchung durchführen zu lassen.

Hausbesuche durch eine Behörde sind ein relativ einschneidendes Mittel. Das Vorgehen war aber im Grundsatz nicht zu beanstanden. Wir wiesen darauf hin, dass in der schriftlichen Ankündigung des Besuchs noch klarer herausgestellt werden soll, dass **alternativ zum Hausbesuch** durch den Behördenmitarbeiter auch ein Besuch der betreffenden Eltern im Amt für Gesundheit möglich ist.

Im Schreiben zur Ankündigung des Besuchs wurden die Eltern aufgefordert, beim Besuchstermin das gelbe Heft mit den dokumentierten Früherkennungsuntersuchungen vorzulegen. Es besteht zwar keine „harte“ Rechtspflicht, die Untersuchungen überhaupt durchzuführen, das gelbe Heft zu führen oder es den kommunalen Behörden vorzulegen. Doch haben die Kommunen den gesetzlichen Auftrag, bei den Eltern die Bereitschaft zur Durchführung der Untersuchungen herzustellen. Hierzu ist die **Nachfrage nach dem gelben Heft** ein geeignetes Mittel.

Konnte ein Fall durch das Gesundheitsamt nicht geklärt werden, z. B. weil die Eltern nicht angetroffen wurden oder sich nicht bereit erklärten, das Kind untersuchen zu lassen, so wurde die Sache an das **Amt für Familie und Soziales** weitergegeben. Dort wurde das örtlich zuständige Zentrum der sechs Sozialzentren tätig. Bei diesem Amt konnte von Anfang an auf ausführliche und datenschutzkonforme Richtlinien zum Umgang mit Meldungen über Kindeswohlgefährdungen und das weitere Vorgehen bei solchen Meldungen zurückgegriffen werden. Dabei erfolgt ein angemessener Ausgleich zwischen den Rechten der Betroffenen und dem

Anliegen des Kinderschutzes. Die vom Amt für Gesundheit im Verfahren des kontrollierenden Einladungswesens empfangenen Meldungen wurden beim Amt für Familie und Soziales nach diesen Richtlinien bearbeitet.

Von den Sozialzentren wurde in der Regel zunächst ein Hausbesuch durchgeführt und bei Bedarf wiederholt. Die Prüfung von Einzelfällen wies teilweise Unklarheiten auf, mit welchem Ergebnis der Vorgang abgeschlossen werden konnte. Mitarbeiter meinten offenbar, für einen Abschluss sei die Durchführung der fraglichen Früherkennungsuntersuchung nötig. Dies entspricht jedoch nicht dem Gesetz, das gerade keine Pflicht zur Untersuchung vorsieht. Es geht nur darum, festzustellen, ob eine Kindeswohlgefährdung vorliegt. So war in den meisten von uns geprüften Fällen das Verfahren abgebrochen worden, als festgestellt war, dass das **Kindeswohl nicht gefährdet** ist, unabhängig davon, ob das Kind letztlich untersucht worden war oder nicht.

Bei beiden Ämtern ergaben sich bei der Einzelfallprüfung Datenschutzverstöße, weil die Mitarbeiter ohne entsprechende Einwilligungserklärung der Sorgeberechtigten versuchten, bei den **Kinderärzten durch telefonische Nachfrage** zu klären, ob die Untersuchung stattgefunden habe. Uns überraschte die große Auskunftsbereitschaft aufseiten der Kinderarztpraxen. Ohne Schweigepflichtentbindung durch die Sorgeberechtigten gibt es keine rechtliche Befugnis für eine solche Auskunft gegenüber der Kommune. Etwas anderes gilt nur, wenn unmittelbare Anhaltspunkte für eine Kindeswohlgefährdung vorliegen. Unklarheiten über die Durchführung der Früherkennungsuntersuchung genügen nicht. Aufseiten der Arztpraxis liegt in einer Auskunft ein strafrechtlich relevanter Verstoß gegen die ärztliche Schweigepflicht. Unzulässig und eventuell eine Ordnungswidrigkeit ist aber auch die entsprechende Datenerhebung aufseiten der Ämter. Diese sicherten zu, ihre Praxis insoweit umzustellen und die Mitarbeiter noch besser in dieser Hinsicht zu schulen.

Bereits im letzten Tätigkeitsbericht wiesen wir darauf hin, dass es in den meisten Fällen eine harmlose Erklärung gibt, warum das Landesfamilienbüro die Rückmeldung über die durchgeführte Untersuchung nicht erhalten hat. Es wäre unverhältnismäßig, diese Daten länger als ein Jahr nach Verfahrensabschluss zu speichern. Mit beiden Ämtern der Landeshauptstadt wurde schnell übereingekommen, dass die Mehrzahl der Fälle, in denen nur die Untersuchung versäumt wurde und keine weiteren Besonderheiten vorliegen, nur kurzfristig gespeichert und spätestens ein Jahr **nach der Erledigung gelöscht** werden.

Was ist zu tun?
Die Kreise und kreisfreien Städte sollten ihre Verfahren des kontrollierenden Einladungswesens an den hier dargestellten Erkenntnissen ausrichten. Direkte Nachfragen bei Kinderärzten, ob ein Kind zur Untersuchung vorgestellt worden sei, sind nur erlaubt, wenn diesbezüglich das Einverständnis der Sorgeberechtigten vorliegt.

4.5.15 ELENA – die Datenspeicherung beginnt

Das ELENA-Verfahrensgesetz ist in Kraft getreten; das Sammeln der Daten hat begonnen. Gleich zu Beginn ergaben sich massive Probleme wegen des Inhalts der geforderten Daten.

Der Bundestag verabschiedete das Gesetz zur Einführung des ELENA-Verfahrens (31. TB, Tz. 4.5.11). Damit sollen zunächst fünf Typen von papierbasierten **Entgeltnachweisen durch elektronische Speicherungen ersetzt** werden. Es geht um drei Bescheinigungen im Bereich des Arbeitslosengeldes I (nämlich Arbeitsbescheinigungen, Nebeneinkommensbescheinigungen und Auskünfte über die Beschäftigung nach dem Recht der Arbeitsförderung), um Auskünfte über den Arbeitsverdienst zum Wohngeldantrag sowie um Einkommensnachweise im Zusammenhang mit dem Bundeselterngeld- und Elternzeitgesetz. Diese Nachweise im ELENA-Verfahren sollen 80 % der in der Praxis ausgestellten Bescheinigungen ersetzen.

Das im April 2009 in Kraft getretene Gesetz sieht vor, dass **ab Anfang Januar 2010** alle Arbeitgeber bestimmte Daten an die sogenannte Zentrale Speicherstelle (ZSS) übermitteln, welche bei der Datenstelle der Träger der Rentenversicherung eingerichtet wurde. Der Datenabruf durch die Stellen, die die jeweiligen Leistungen gewähren, und damit der Wegfall der bisherigen Papiernachweise, soll von Anfang 2012 an erfolgen.

Die von den Arbeitgebern an die ZSS **zu übermittelnden Daten** sind im Gesetz aufgeführt: Vor- und Familiennamen, Geburtstag, Anschrift, Versicherungsnummer bzw. Verfahrensnummer, die eigens für die Personen vergeben wird, die keine Versicherungsnummer in der gesetzlichen Rentenversicherung haben. Zu melden sind zudem das erfasste Einkommen in Euro, Beginn und Ende des Zeitraumes, für den das erfasste Einkommen erzielt worden ist, sowie der Name und die Anschrift des Arbeitgebers und die Betriebsnummer des Beschäftigungsbetriebes. Weiterhin sind die für den betreffenden Einkommensnachweis in den Gesetzen vorgesehenen Angaben zu übermitteln. Bei der Arbeitsbescheinigung im Rahmen des Arbeitslosengeldes I handelt es sich z. B. um die Art der Tätigkeit des Arbeitnehmers, Beginn, Ende, Unterbrechungen und Grund für die Beendigung des Beschäftigungsverhältnisses, das Arbeitsentgelt und sonstige Geldleistungen, die der Arbeitnehmer erhalten hat oder zu beanspruchen hat. Das Bundesministerium für Arbeit und Soziales erlässt nach dem Gesetz eine Rechtsverordnung, mit der die Inhalte der Meldungen der Arbeitgeber an die ZSS inhaltlich näher bestimmt werden (sogenannte ELENA-Datensatzverordnung). Anfang des Jahres 2010 war eine solche Verordnung noch nicht in Kraft.

Gemäß dem ELENA-Gesetz bestimmt ein Gremium, das sich aus Vertretern der Sozialversicherungsinstitutionen sowie der Kommunen, der Bundesagentur für Arbeit (BA) und des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) zusammensetzt, den **Aufbau der einzelnen Datensätze**. Das Gremium veröffentlichte im Herbst 2009 eine erste, noch nicht endgültige Beschreibung. Im Datenbaustein „DBKE – Kündigung/Entlassung“ waren viele Angaben zum Arbeits-

vertrag und dessen Ende bzw. Unterbrechung vorgesehen. So sollte gemeldet werden, ob einer Kündigung eine Abmahnung vorausgegangen war; das Datum der Abmahnung war einzutragen. In einem Freitextfeld war das vermeintlich vertragswidrige Verhalten, welches Anlass zur Kündigung gab, zu beschreiben. Im Datenbaustein „DBFZ – Fehlzeiten“ war zu den Arten der Fehlzeiten u. a. anzugeben, ob diese auf einem rechtmäßigen oder unrechtmäßigen Streik beruhten.

Bei der Erstellung der Datensatzbeschreibung wurde offensichtlich von einigen der Handelnden die **Brisanz unterschätzt**, die sich aus dem ELENA-Verfahren ergibt. Der auf Bundesebene in erster Linie zuständige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit war bei der Erstellung der Datensatzbeschreibung nicht einbezogen worden.

Zwar sind die umstrittenen Angaben zur **Kündigung und zur Rechtmäßigkeit von Streiks** auch vor der Einführung von ELENA in Formularen, die vom Arbeitgeber auszustellen sind, enthalten. In der bisherigen Arbeitsbescheinigung für den Bezug von Arbeitslosengeld I ist anzugeben, ob der Kündigung eine Abmahnung vorausgegangen ist; auch das vermeintlich vertragswidrige Verhalten des Arbeitnehmers muss genannt werden. Es ist jedoch ein Unterschied, ob diese Informationen in einem individuellen Verfahren erhoben oder ob sie auf Vorrat für alle Beschäftigten der Bundesrepublik Deutschland in einer zentralen Datenbank gespeichert werden.

Während es bei einem Formular für den Einzelfall genügt, dass dieses z. B. von der BA in Konkretisierung des Gesetzes bezüglich des Datenumfangs selbst gestaltet wurde, ist es verfassungsrechtlich zweifelhaft, ob ein demokratisch nicht legitimiertes Gremium den Aufbau von Datensätzen festlegen darf, die mit ihren hochsensiblen Informationen aus dem Arbeitsverhältnis, die wie z. B. die Teilnahme an Streiks spezifisch durch das Grundgesetz geschützt sind, in einer Zentraldatei gespeichert werden. Die Rechtsprechung des Bundesverfassungsgerichts fordert, dass **wesentliche Entscheidungen**, die in die Rechte aller Beschäftigten in der Bundesrepublik Deutschland eingreifen, durch das Parlament getroffen werden. So ist schon fraglich, ob die vorgesehene Verordnung eine ausreichende Ermächtigungsgrundlage für derart weitreichende Datenspeicherungen darstellt.

Nach Bekanntwerden der Bedenken an der Datensatzbeschreibung wurde mit Zustimmung des Bundesministeriums für Arbeit und Soziales (BMAS) Ende Dezember 2009 die Version 1.2 der **Datensatzbeschreibung** veröffentlicht. Diese Fassung verzichtet auf Angaben zu rechtmäßigen bzw. unrechtmäßigen Streiks. Das BMAS hat angekündigt, dass alle Daten in dem Katalog noch einmal auf ihre Notwendigkeit hin geprüft werden, einschließlich der immer noch enthaltenen Angaben zur Kündigung und Abmahnung sowie einer Anzahl von Freitextfeldern.

Zum Start des Verfahrens im Januar 2010 schlugen die Wellen auch beim ULD hoch. Besorgte Menschen fragten, ob sie sich gegen die Übermittlung ihrer Daten an die ZSS wenden können. Dies ist nicht vorgesehen; die Übermittlung beruht auf einer gesetzlichen **Pflicht des Arbeitgebers**. Arbeitgeber empörten sich über den bürokratischen Aufwand des Meldeverfahrens und fragten, welche Daten genau sie an die ZSS melden müssten. Zwar lag ein vom BMAS genehmigter

Datenkatalog vor, allerdings waren noch Änderungen in Aussicht gestellt. Vor allem gab es aber zu diesem Zeitpunkt keine Rechtsgrundlage für die Übermittlung einer Vielzahl der in der Datensatzbeschreibung enthaltenen Daten, da die vorgesehene ELENA-Datensatzverordnung noch nicht erlassen war. Dies betraf nicht nur die problematischen Angaben zum Ende des Arbeitsverhältnisses, sondern auch Angaben wie den Geburtsort und die Staatsangehörigkeit, die für solche Beschäftigte übermittelt werden sollten, die keine Rentenversicherungsnummer haben, z. B. Beamte. Die Weitergabe solcher Daten wäre demnach nur unter Begehung eines Rechtsverstoßes möglich.

Andererseits ist das **Unterlassen von Meldungen** eine Ordnungswidrigkeit und mit einem Bußgeld bewehrt. Es war aber kaum zu erwarten, dass die für die Verfolgung der Ordnungswidrigkeiten zuständige Deutsche Rentenversicherung Bund bereits zum Start des Verfahrens angesichts des Fehlens einer Rechtsgrundlage von ihrer Befugnis Gebrauch macht.

Was ist zu tun?
Der Datenkatalog muss auf das vertretbare Maß beschränkt und auf eine belastbare Rechtsgrundlage gestellt werden. Die öffentlichen Arbeitgeber in Schleswig-Holstein sollten genau prüfen, ob diese Voraussetzungen erfüllt sind, bevor sie eine Meldung abgeben. Die grundsätzlichen Bedenken der Datenschutzbeauftragten am Verfahren sind weiterhin nicht ausgeräumt.

4.6 Schutz des Patientengeheimnisses

4.6.1 Ärztliche Haftpflichtverfahren – nicht mit dem Versicherungsmakler

Macht der Patient gegenüber einem Arzt einen Behandlungsfehler geltend, so muss der Arzt bzw. das Klinikum die Haftpflichtversicherung über die Details der Behandlung informieren. Versicherungsmakler dürfen diese sensiblen, der Schweigepflicht unterliegenden Informationen nicht erhalten.

Rechtsstreitigkeiten zwischen Klinik und Patient über den Behandlungsverlauf und -erfolg sind leider juristischer Alltag. Die Pflicht zur Haftpflichtversicherung für Ärzte und Kliniken dient auch dem Schutze der Patientinnen und Patienten. Der Versicherer wird bei Haftungsfällen frühzeitig eingeschaltet, um gegebenenfalls eine außergerichtliche Lösung zu finden. Zur **Schadensbeurteilung und -abwicklung** benötigt der Versicherer detaillierte Angaben aus dem Behandlungsvorgang.

Nicht nur der Abschluss solcher Haftpflichtversicherungen für Heilberufe erfolgt über **Versicherungsmakler**, sondern teilweise auch die Korrespondenz im Schadensfall. In dem uns vorliegenden Fall wurden so der ärztlichen Schweigepflicht unterliegende Informationen an den Makler übermittelt. Das betroffene Universitätsklinikum konnte uns bisher nicht schlüssig darlegen, warum der Austausch nicht direkt mit dem zuständigen Versicherer erfolgte. Gründe für die Durchbrechung der Schweigepflicht gegenüber dem Makler und für das Unterlassen der Anonymisierung der Unterlagen sind für uns nicht erkennbar.

Neben der Patientendokumentation übersandte das Klinikum vertrauliche **Angaben über Angehörige** der Patienten an Versicherung und Makler, ohne dass ein Zusammenhang zum Haftungsfall bestand. Diese Übermittlungen an Makler und Versicherer waren rechtswidrig und wurden vom ULD förmlich beanstandet.

Was ist zu tun?
Personenbezogene Daten von Patienten dürfen nicht an Versicherungsmakler oder andere Dritte übermittelt werden. Ist die Einbeziehung Dritter nötig, kann dies in anonymisierter Form erfolgen oder mit der Einwilligung des Betroffenen.

4.6.2 Immer wieder Patientendaten im Müll

Alle Jahre wieder: Patientenakten im Müll, auf der Straße oder wo sie sonst nicht hingehören, gefunden von Bürgerinnen und Bürgern oder der Polizei. Das ULD reagiert in allen Fällen.

Anzeigen über die **unsachgemäße Entsorgung** von Patientenunterlagen durch Ärzte, Physiotherapeuten oder Heilberufler nahmen jüngst wieder zu. Entweder wenden sich besorgte Bürgerinnen und Bürger mit ihrem Fund direkt an uns, oder die Unterlagen werden vor Ort von der Polizei sichergestellt, die das ULD eingeschaltet. In einem Fall erhielten wir so 350 Patientenakten, gefunden in einem Hinterhof. Der Umstand, dass vermehrt solche Hinweise eingehen, zeigt, dass Bürger und Patienten verstärkt für die Datenschutzbelange sensibilisiert sind.

Das ULD geht diesen Hinweisen nach. Bei Verstößen gegen Datenschutz und Schweigepflicht kann das ULD ein Bußgeld bis zur maximalen Höhe von 250.000 Euro verhängen. Gemäß dem Gesetz unterrichtet das ULD zumindest eine Auswahl der betroffenen Patienten über Art und Umfang des Vorfalls. Wenden sich Betroffene an die lokale Presse, so kann für den Behandler ein erheblicher Rechtfertigungsdruck entstehen; er muss mit einem **Vertrauensverlust** seiner Patienten rechnen.

Mit der Unterstützung der Ärztekammer Schleswig-Holstein haben wir in deren Mitteilungsblatt das Problem dargestellt und Hinweise zum korrekten Umgang mit zu vernichtenden Patientenakten gegeben. Medizinische Daten unterliegen der Schweigepflicht und besonderen Datenschutzanforderungen. Papierakten sind so zu vernichten, dass eine Rekonstruktion nicht mehr möglich ist. Alle Datenträger müssen bis zur endgültigen Vernichtung in der **Obhut des Arztes** oder dessen schweigepflichtiger Mitarbeiter bleiben. Eine Vernichtung durch externe Dienstleister ist zu überwachen (31. TB, Tz. 4.6.3).

Was ist zu tun?
Datenträger mit Patientendaten sind bis zur Vernichtung sicher zu verwahren. Außenstehende dürfen bei der Entsorgung vom Inhalt keine Kenntnis erhalten.

4.7 Datenschutz an Schulen und Hochschulen

4.7.1 Appell an die Jugendlichen: „Entscheide DU“

Bildungsminister Ekkehard Klug und das ULD haben eine Broschüre vorgestellt, die Sensibilität für den Datenschutz und generell Medienkompetenz bei Schülerinnen und Schülern vermitteln soll. Die Broschüre, die auch im Unterricht eingesetzt werden kann, wird uns sinnbildlich aus den Händen gerissen.

Das Internet und elektronische Medien sind zu einer unverzichtbaren **modernen Kulturtechnik** geworden. Schülerinnen und Schüler nutzen bereits im jungen Alter das Internet, tummeln sich im SchülerVZ und anderen sozialen Netzwerken; das Handy ist wichtiger als alles andere. Bei der Mediennutzung setzen sie sich, nur zu oft unbewusst, der Gefahr aus, sich selbst und andere in ihren Persönlichkeitsrechten zu verletzen und personenbezogene Daten ungewollt wildfremden Menschen zugänglich zu machen. Um auf diese Gefahren hinzuweisen, gibt das ULD die Broschüre „Entscheide DU – sonst tun es andere für Dich“ heraus und stellt diese in Klassensätzen zur Verfügung. Die Vermittlung zu Lehrkräften und Eltern erfolgt in Kooperation mit dem IQSH, dem Institut für Qualitätsentwicklung an Schulen Schleswig-Holstein. Die Broschüre wird auch im Rahmen der Fortbildungsinitiative „Im Netz der neuen Medien“, an der IQSH und ULD teilnehmen, eingesetzt.

Kindern und Jugendlichen sollen in der altersgerecht gestalteten Broschüre das Wissen und die Werkzeuge an die Hand gegeben werden, einen kritischen und **selbstbestimmten Umgang mit Computern und Handys** zu lernen. Sie haben ein ausgeprägtes Gespür für Privatsphäre. Ihnen muss aber vermittelt werden, welche Unterschiede sich diesbezüglich bei der Nutzung von digitalen Geräten gegenüber den realen direkten menschlichen Beziehungen ergeben. Es ist eine Aufgabe der Schulen und des ULD, schon den jungen Menschen zu vermitteln, dass der Respekt vor den Rechten der anderen und die Wahrung des Datenschutzes in Zeiten von Handys und Internet möglich und nötig sind.

Die erste Auflage in Höhe von 10.000 Exemplaren war innerhalb von zwei Wochen vergriffen, sodass umgehend eine **zweite Auflage** gedruckt werden musste. Die Broschüre kann im Internet angesehen und heruntergeladen werden.

www.datenschutzzentrum.de/download/entscheide-du.pdf

Was ist zu tun?
Datenschutz ist nicht nur eine rechtliche und technische, sondern vor allem auch eine pädagogische Aufgabe, der sich Schulen wie Datenschützer stellen müssen. Weiter gehende Angebote müssen entwickelt und bereitgestellt werden.

4.7.2 Störlauf – ein Volkslauf und seine Folgen im Internet

Die personenbezogenen Daten Ihres Kindes sind noch nicht online? Kein Problem: Lassen Sie Ihr Kind einfach an einer Breitensportveranstaltung teilnehmen, organisiert von einem Verein und unterstützt von der Schule. Danach findet jeder Namen, Alter und Schule Ihres Kindes im Internet.

Besorgte Eltern einer Zweitklässlerin wandten sich Hilfe suchend an uns. Sie hatten nichtsahnend ihr Kind über die Grundschule zum Störlauf – einer bei Jung und Alt beliebten Laufveranstaltung – angemeldet. Die Schule hatte für diese sportliche Veranstaltung geworben. Die Teilnahme ist Ehrensache. Die Anmeldung und das Einsammeln des Startgeldes erfolgte durch die Schule. Danach stellten die Eltern überrascht fest, dass der Name ihres Kindes mit Nennung der Schule und der Altersklasse **im Internet zu finden** war. Der Veranstalter des Störlaufes hatte alle angemeldeten Personen in einer Starterliste auf seiner Webseite veröffentlicht. So ließ sich die siebenjährige Tochter der Petenten per Suchmaschine finden.

Schon die Sachverhaltsaufklärung und die erste rechtliche Bewertung durch das ULD lösten eine **Pressekampagne** aus, die sich nicht nur gegen unser Haus, sondern auch gegen die Eltern richtete. Es sei doch großartig, wenn man im Rahmen dieses Lauf-Events im Internet genannt werde. Der Datenschützer solle sich nicht so anstellen; die Eltern sollten nicht so querulatorisch sein. Der Veranstalter behauptete, die Internetveröffentlichung sei von den Sportordnungen des Deutschen Leichtathletikverbandes (DLV) vorgeschrieben. Dies entpuppte sich allerdings als Schutzbehauptung. Der DLV teilte mit, dass dem nicht so ist.

Erschreckend war anfangs die **mangelnde Sensibilität der Schulleitungen** hinsichtlich der Gefahren, die mit der Veröffentlichung personenbezogener Daten – insbesondere von jungen Kindern – im Internet verbunden sind. Es bedurfte pädagogischen Geschicks bei der Vermittlung der möglichen Konsequenzen für die Kinder und der rechtlichen Situation, bis sich die meisten Verantwortlichen einsichtig zeigten.

Im Dialog mit dem Bildungsministerium suchten wir für die Zukunft eine einheitliche datenschutzkonforme Lösung für die Teilnahme der Schulen und ihrer

Schülerinnen und Schüler an solchen sportlichen Wettkämpfen. Bedingung ist, dass der **Elternwille** tatsächlich Berücksichtigung findet. Hierfür müssen die Eltern eindeutig auf die Konsequenzen einer Internetveröffentlichung der Daten ihrer Kinder hingewiesen werden. Das Bildungsministerium hat aus guten Gründen eine Initiative zur Aufklärung der Schülerinnen und Schüler über die Gefahren der Veröffentlichung personenbezogener Daten im Internet gestartet. Die Schulen müssen einen sensiblen Umgang mit diesen Daten pflegen und mit gutem Beispiel vorangehen.

Was ist zu tun?
Wenn Schulen mit Sportvereinen kooperieren, um die Kinder an den Sport heranzuführen und damit die Gesundheitsförderung zu stärken, ist der Datenschutz der Kinder zu achten. Eine Veröffentlichung im Internet setzt die informierte Einwilligung der Eltern voraus. Daten von Grundschulkindern haben unseres Erachtens im Internet nichts verloren.

4.7.3 LanBSH – ein Erfolg

Das Konzept für eine einheitliche Informationstechnologie in Schulverwaltungen geht auf. Die Schulträger und die Schulleiterinnen und Schulleiter sind offensichtlich von der zentralen IT-Lösung überzeugt.

Mittlerweile sind ca. 500 von ungefähr 950 Schulen am Landesnetz Bildung, kurz LanBSH angeschlossen (30. TB, Tz. 4.7.1). Fast alle weiteren Schulträger bzw. Schulen haben entsprechende Anschlussanträge gestellt. Die erfolgreiche Umsetzung des Konzepts ist auch dem Umstand zu verdanken, dass die Schulen sich an ein eigens dafür eingerichtetes **Helpdesk** beim Institut für Qualitätsentwicklung an Schulen Schleswig-Holstein, also beim IQSH, wenden können, wenn es zu technischen Problemen kommt. Dieses Helpdesk führt das Training der Anwender in den Schulen durch. Wenn das LanBSH ein Erfolgsmodell bleiben soll, muss weiterhin eine effiziente Unterstützung für die Schulen angeboten werden. Ein Helpdesk, welches Störungsmeldungen im IT-System unverzüglich nachgeht und diese abstellt, ist für sichere IT-Strukturen unabdingbar und entspricht dem Stand der Technik.

Allerdings hat die rasante Weiterentwicklung des LanBSH auch einen Wermutstropfen. Aus verschiedenen Gründen wurde offensichtlich bisher auf ein **Update- und Patch-Management** für die LanBSH-Rechner verzichtet. Dies verstärkt Risiken für die Datensicherheit, weshalb dieses Manko unverzüglich beseitigt werden sollte.

Was ist zu tun?
Die personelle Ausstattung des Helpdesks zur Betreuung der LanBSH-Nutzer sollte gemäß den Anforderungen durch die steigenden Zahlen der nutzenden Stellen angepasst werden. Die Software der im LanBSH befindlichen Rechner ist im Interesse der Risikominimierung auf den technisch aktuellen Stand zu bringen.

4.7.4 Videoüberwachung an Schulen

Immer mehr Schulträger und Schulen installieren im Außenbereich von Schulgebäuden Videoüberwachungsanlagen, um der zunehmenden Sachbeschädigung entgegenzutreten.

Der Einsatz von Videotechnik an Schulen wird vom ULD wegen der damit verbundenen Freiheits- und Persönlichkeitseingriffe als besonders heikel betrachtet. Im Interesse der **Erhaltung eines pädagogischen Freiraums** sollte auf den Einsatz möglichst verzichtet werden. Doch ist nicht von der Hand zu weisen, dass Schulen zunehmend von starken Sachbeschädigungen und Einbruchdiebstählen betroffen sind. Diese Straftaten verursachen für die Schulträger immense Kosten. Die Täter können oft nicht überführt werden. In Ermangelung von Ressourcen für eine sonstige ausreichende Objektsicherung wird zunehmend der Einsatz von Videotechnik als letztes Mittel angesehen.

Voraussetzung für eine datenschutzkonforme Videoüberwachungsmaßnahme ist die Alternativlosigkeit als Sicherungsinstrument. Um die Anforderungen zu konkretisieren, haben wir zusammen mit dem Bildungsministerium eine Leitlinie erarbeitet. Danach darf ein Einsatz zeitlich nur **außerhalb des Schulbetriebes** erfolgen. Ausnahmsweise wird die Videoüberwachung von Fahrradunterständen während des Schulbetriebes zugelassen, da in diesem Bereich eine besonders hohe Sachbeschädigungsquote zu beklagen ist und der Schutz des Eigentums von Schülerinnen und Schülern im Vordergrund steht. Einigkeit besteht darüber, dass Videoüberwachung innerhalb von Schulgebäuden ausgeschlossen ist.

Was ist zu tun?
Schulen und Schulträger sollten Videoüberwachungsmaßnahmen nur als letztes Mittel einsetzen. In diesem Fall ist die Leitlinie zu beachten.

4.7.5 Verantwortung der Schulleitungen ja – Schulungen nein?

Die Schulleiterinnen und Schulleiter sind nach der Datenschutzverordnung-Schule für die ordnungsgemäße personenbezogene Datenverarbeitung verantwortlich. Doch müssen sie sich hierzu auch weiterbilden können.

Vor zwei Jahren wiesen wir auf Wissensdefizite der Schulleitungen beim Datenschutz hin (30. TB, Tz. 4.7.2). Das IQSH bietet seitdem in Kooperation mit dem ULD hierzu zwar wieder **Fortbildungsveranstaltungen** an, die Resonanz ist jedoch gering. Dies liegt weniger an der Gleichgültigkeit der Schulleiterinnen und Schulleiter. Uns wird immer wieder großes Interesse signalisiert, aber auch, dass neben dem sonstigen Aufwand solche Fortbildungen eine zu große zeitliche

Belastung darstellen würden. Im Hinblick auf die auch im Schulbereich fortschreitende Datenverarbeitung ist es wichtig, dass die hierfür nötigen Kompetenzen angeeignet werden können, indem der nötige Freiraum geschaffen wird.

Was ist zu tun?
Die Inanspruchnahme von Fortbildungen zum Datenschutz sollte im Interesse der Handlungssicherheit der Schulleiterinnen und Schulleiter erleichtert werden.

4.7.6 Ärztliche Prüfungsunfähigkeitsbescheinigungen

Können Studierende krankheitsbedingt an einer Prüfung nicht teilnehmen, genügt den Hochschulen und Fachhochschulen zur Freistellung kein „gelber Schein". Eine Prüfungsunfähigkeit wird nur anerkannt, wenn man auch nachweist, woran man erkrankt ist.

Was im normalen Berufsleben selbstverständlich ist, gilt nicht für Studierende. Erkrankt eine Arbeitnehmerin oder ein Arbeitnehmer, weist sie/er die Arbeitsunfähigkeit durch eine Arbeitsunfähigkeitsbescheinigung, den „gelben Schein", nach. Es besteht keine Pflicht, dem Arbeitgeber den Grund der Erkrankung mitzuteilen. Anders bei den Studierenden: Die Prüfungskommissionen wollen auch die Symptome der Erkrankung erfahren, sonst wird die Krankmeldung nicht anerkannt. Gemäß der Rechtsprechung kann nicht der Arzt, sondern nur die Prüfungskommission über die Prüfungsunfähigkeit entscheiden. Sie müsse deshalb auch wissen, woran der Studierende erkrankt ist. Wir sehen dies kritisch. Die Studierenden werden gezwungen, ihren Arzt von der Verschwiegenheitspflicht zu entbinden bzw. zu einer schriftlichen Bescheinigung der **Krankheitssymptome** zu veranlassen, damit medizinisch unerfahrene Mitglieder der Prüfungskommissionen über die Freistellung befinden können. Das Thema wurde erhitzt politisch diskutiert.

Nicht zuletzt durch den öffentlichen Druck konnten wir bei einer großen Hochschule erreichen, dass ein verwendeter Vordruck geändert wurde und weniger Daten zu den Krankheitssymptomen erhoben werden. Das Prinzip wird aber beibehalten. Die Hochschule sicherte aber zu, dass die Prüfungsunfähigkeitsbescheinigungen besonders sorgfältig vor dem Zugriff Unbefugter **geschützt aufbewahrt** werden.

Was ist zu tun?
Studierende sollten die Möglichkeit erhalten, ihre Prüfungsunfähigkeit auch ohne die Offenbarung ihrer Krankheitssymptome nachzuweisen.

4.8 Steuerverwaltung

4.8.1 Datenschutz im Finanzamt

Das ULD prüfte ein Finanzamt in den Bereichen der Arbeitnehmerveranlagung und Automation.

Wir mussten beanstanden, dass keine ausreichenden organisatorischen Maßnahmen gegen unbefugte Kenntnisnahme getroffen waren. In den Büroräumen befanden sich überwiegend **nicht verschließbare Schränke**. Der Schließmechanismus war defekt; die Türblätter gaben schon bei leichtem Druck von außen nach. Schrankschlösser waren in den einzelnen Büroräumen identisch, und die Schlüssel wiesen auch keine besonderen Sicherheitsattribute auf. Der Einsatz der elektronischen Schließanlage für die Räume genügte nicht, da in Abwesenheit der Mitarbeitenden des Amtes fremde Reinigungskräfte unkontrollierten Zugriff hatten.

Die datenschutzrechtlichen **Löschfristen** wurden nicht beachtet. Daten sind zu löschen, wenn ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist. Steuerdaten bleiben erforderlich, wenn die Steuerfestsetzung nur vorläufig erfolgt, also noch keine endgültige Festsetzung vorliegt, oder wenn die Zahlungsverjährung noch nicht eingetreten ist. Eine derartige Erforderlichkeit konnte in großem Umfang nicht nachgewiesen werden. Es waren überwiegend pauschale lange Aufbewahrungszeiten festgelegt, ohne dass der zugrunde liegende Sachverhalt berücksichtigt wurde. Positiv konnte festgestellt werden, dass das geprüfte Finanzamt über ein geeignetes Verfahren zur datenschutzgerechten Entsorgung von Steuerunterlagen verfügt.

Was ist zu tun?
Personenbezogene Daten sind durch geeignete Maßnahmen vor unbefugten Zugriffen zu schützen. Nicht mehr benötigte Steuerunterlagen sind zeitnah zu vernichten.

4.8.2 Wer wurde am Kopf operiert?

Ärzten steht bei steuerlichen Betriebsprüfungen ein Auskunftsverweigerungsrecht zum Schutz des Patientengeheimnisses zu; sie können die Auskunft verweigern.

Ein Arzt bat uns, das Vorgehen von Betriebsprüfern eines Finanzamtes im Zusammenhang mit der **Einsichtnahme in Klinik- und Arztrechnungen** zu prüfen. Die Betriebsprüfer verlangten die Nennung von Namen und Anschriften von Patienten, obwohl sich der Arzt auf sein Auskunftsverweigerungsrecht berief.

Nach der Rechtsprechung des Bundesfinanzhofes können sich z. B. Rechtsanwälte im Hinblick auf die Angaben zu den Teilnehmern einer Bewirtung nicht auf ihre anwaltliche Schweigepflicht bzw. auf ihr Auskunftsverweigerungsrecht berufen, wenn die Bewirtungskosten als Betriebsausgaben geltend gemacht werden. Der Mandant habe bereits in die Offenlegung seiner Daten gegenüber dem Finanzamt eingewilligt; er müsse stets damit rechnen, dass die Bewirtungskosten von dem Rechtsanwalt als Betriebsausgaben geltend gemacht würden.

Diese Wertung ist jedoch nicht auf den geschilderten Fall übertragbar. Es existiert kein Erfahrungssatz, dass der Patient mit dem Abschluss des **Behandlungsvertrages** einwilligt, dass Angaben zum Namen, Vornamen und zur Anschrift gegenüber dem Finanzamt offenbart werden. Der Arzt hatte sein Auskunftsverweigerungsrecht zu Recht geltend gemacht; es war bei der Betriebsprüfung zu beachten.

Was ist zu tun?
Im Rahmen von Betriebsprüfungen müssen die Finanzbehörden die ärztlichen Auskunftsverweigerungsrechte beachten. Bei unbefugter Offenbarung der Angaben würde sich der Arzt der Gefahr strafrechtlicher Verfolgung aussetzen.

4.8.3 Erneut Zusendung falscher Steuerunterlagen

Weiterhin gilt: Finanzämter müssen bei der Versendung von Steuerunterlagen das Steuergeheimnis wahren. Steuerunterlagen dürfen nicht in falsche Hände geraten.

Wir berichteten zuletzt von drei Vorfällen, in denen Steuerpflichtige vom Finanzamt Steuerunterlagen fremder Personen zugesandt bekamen (31. TB, Tz. 4.7.3). Dieses Mal war ein anderes Finanzamt Auslöser für eine Beanstandung. Wieder sollten Steuerbelege wie etwa Kontoauszüge oder Arztrechnungen, die bei der Steuererklärung eingereicht worden waren, nach Prüfung an die Steuerpflichtigen zurückgesandt werden. Ursache für die Zusendung falscher Steuerunterlagen war wiederum eine falsche **Befüllung von Postumschlägen**.

Was ist zu tun?
Weiterhin gilt: Die Mitarbeiterinnen und Mitarbeiter in den Finanzämtern müssen bei der Bearbeitung von Steuerfällen mit den Steuerunterlagen sorgsam umgehen und Verwechslungen vermeiden.

4.8.4 Zur Anerkennung einer ausländischen Insolvenz

Finanzbehörden müssen insolvenzrechtliche Entscheidungen anderer EU-Mitgliedstaaten anerkennen. Für die Überprüfung der Entscheidungen und eine damit verbundene Datenerhebung beim Steuerpflichtigen besteht in der Regel keine Rechtsgrundlage.

Einem Steuerpflichtigen war von einem englischen Gericht nach dortigem Insolvenzrecht **Restschuldbefreiung** gewährt worden. Nach den europarechtlichen

Vorgaben müssen die Wirkungen eines Insolvenzverfahrens in einem anderen Mitgliedstaat auch von den deutschen Behörden anerkannt werden, es sei denn, dass die Anerkennung der jeweiligen Entscheidung zu einem Ergebnis führt, welches offensichtlich mit der Rechtsordnung im Widerspruch steht.

Ein Finanzamt mit einer Steuerforderung gegen den Betroffenen weigerte sich gleichwohl, die Entscheidung des englischen Gerichts anzuerkennen. Es erklärte die gegen den Steuerpflichtigen eingeleitete Pfändung nicht für erledigt und forderte die Nachreichung des Schriftverkehrs mit dem Insolvenzverwalter und die Einreichung diverser Unterlagen. Eine solche Erhebung personenbezogener Daten des Steuerpflichtigen ist nur im Rahmen der Erforderlichkeit und auf Basis einer Rechtsgrundlage zur Aufgabenwahrnehmung zulässig. Das Finanzamt konnte die Erforderlichkeit nicht darlegen. Es bestanden keine Anhaltspunkte dafür, dass die **Anerkennung der richterlichen Entscheidung** zu einem Ergebnis führt, das offensichtlich mit der Rechtsordnung im Widerspruch steht.

Was ist zu tun?
Eine Datenerhebung beim Steuerpflichtigen muss zur Erfüllung zugewiesener Aufgaben erforderlich sein. Die Finanzbehörden müssen dies sorgfältig prüfen.

5 Datenschutz in der Wirtschaft

Die Schwergewichte haben sich verschoben: War der Datenschutz im nicht öffentlichen Bereich, also die Wahrung des Rechts auf informationelle Selbstbestimmung insbesondere im Bereich der Privatwirtschaft seit den 70er-Jahren, also den Frühzeiten des gesetzlich geregelten Datenschutzes, ein Randthema, so hat dessen Bedeutung seitdem kontinuierlich zugenommen. Zugleich ist es immer schwieriger, eine klare Grenze zwischen beiden Bereichen zu ziehen, da z. B. die Spezialgesetze zu den Neuen Medien keine Unterscheidung nach der Rechtsform vornehmen und insofern ein einheitliches Recht gilt, aber auch weil die Datenkommunikation zwischen beiden Bereichen zunimmt, indem Private zu Datenhaltungen und Datenlieferungen für die öffentlichen Stellen verpflichtet werden und nicht öffentliche Stellen für ihre geschäftliche Tätigkeit auf öffentliche Daten zugreifen. Die **Schwerpunktverlagerung** äußert sich darin, dass neben einem anhaltend hohen Beschwerdeaufkommen im öffentlichen Bereich die Zahl der Eingaben im nicht öffentlichen Bereich kontinuierlich zunimmt. Dies hat im ULD zur Folge, dass hierfür immer mehr Mitarbeiter benötigt werden.

5.1 Kurz vor Torschluss – Neuerungen im Bundesdatenschutzgesetz

Ende der letzten Legislaturperiode wurden im Bundestag zahlreiche Änderungen des Bundesdatenschutzgesetzes beschlossen. Zum Teil sind diese aus Datenschutzsicht unbefriedigend, zum Teil sind brauchbare Regelungen entstanden, die z. B. mehr Transparenz für die Betroffenen bringen.

Die Änderungen betreffen insbesondere die Werbung, die Tätigkeiten von Auskunfteien sowie den Einsatz von Scoring-Verfahren und setzen europarechtliche Vorgaben im Bereich von Verbraucherkrediten um.

5.1.1 Von allem ein bisschen – BDSG-Novelle II

Die Neuregelungen der BDSG-Novelle II sind zum größten Teil bereits im September 2009 in Kraft getreten. Wesentliche Änderungen wurden erst ganz am Ende des Gesetzgebungsverfahrens gegenüber dem ursprünglichen, aus dem Bundesinnenministerium stammenden Entwurf vorgenommen (31. TB, Tz. 5.1.2). Herausgekommen ist ein **Kompromiss**, der viele Fragen aufwirft, aber in mancher Hinsicht in die richtige Richtung weist.

Die Schwerpunkte der Änderung werden im Folgenden dargestellt:

- **Kündigungsschutz für betriebliche Datenschutzbeauftragte und Auftragsdatenverarbeitung**

Zu begrüßen sind eine Regelung zum **Kündigungsschutz** für den betrieblichen Datenschutzbeauftragten sowie konkretisierende Vorgaben für eine wirksame Auftragsdatenverarbeitung. Die insbesondere für den Teilzeitdatenschutzbeauftragten, der neben der Funktion des Beauftragten noch andere Aufgaben im

Unternehmen wahrnimmt, im Hinblick auf eine Kündigung des zugrunde liegenden Arbeitsverhältnisses bestehenden Unsicherheiten sind nun durch einen expliziten Kündigungsschutz, vergleichbar mit dem eines Betriebsratsmitgliedes, ausgeräumt. Bei der Auftragsdatenverarbeitung ist im Gesetz ausdrücklich neu geregelt, zu welchen Punkten ein Auftragsdatenverarbeitungsvertrag Aussagen treffen muss. Was nun ausdrücklich geregelt ist, wurde von den Datenschutzaufsichtsbehörden auch schon bisher gefordert. Dennoch ist die Konkretisierung, etwa im Hinblick auf mögliche Sanktionen und Bußgeldverfahren, hilfreich.

- **Datenverarbeitung zum Zweck der Werbung**

Die Regelungen zur Datenverwendung zu Werbezwecken hätten konsequenter und verständlicher ausfallen können. Dem Grundsatz nach sollen Daten für fremde Werbezwecke nur noch mit Einwilligung der Betroffenen verwendet werden dürfen. Geregelt wurden aber viele Ausnahmen, die nicht nur für die Betroffenen undurchsichtig, sondern auch für die Unternehmen verwirrend sind und **Rechtsunsicherheit** schaffen.

Ohne ausdrückliches Einverständnis bleibt erlaubt, **listenmäßig zusammengefasste Daten** über Angehörige einer bestimmten Personengruppe mit deren Berufs-, Branchen- oder Geschäftsbezeichnung, Namen, Titel (akademischer Grad), Anschrift und Geburtsjahr für Werbung mit eigenen Angeboten, für Zwecke der Werbung im Hinblick auf die berufliche Tätigkeit der Betroffenen sowie für Zwecke der Spendenwerbung zu gebrauchen. Erfreulich ist, dass der Betroffene bereits bei der Erhebung seiner Daten darauf hingewiesen werden muss, dass er der Nutzung zu Werbezwecken widersprechen kann und dies nicht erst bei der Ansprache zu Werbezwecken erfolgt.

> **?** ***BDSG-Novelle I bis III***
>
> *In Veröffentlichungen, Pressemitteilungen oder Berichten ist häufig von den BDSG-Novellen I bis III die Rede. Die BDSG-Novelle I erfasst alle Neuregelungen, die sich auf die Tätigkeit von Auskunfteien und den Einsatz von Scoring-Systemen beziehen. In der BDSG-Novelle II sind alle Änderungen im Zusammenhang mit der Werbung und der Markt- und Meinungsforschung zusammengefasst. Die BDSG-Novelle III bezeichnet Regelungen zur Umsetzung der europäischen Verbraucherkreditrichtlinie.*
>
> *Diese Unterscheidung wird z. B. im Zusammenhang mit dem Zeitpunkt des Inkrafttretens der Regelungen relevant. Bis auf wenige Ausnahmen sind die Änderungen der BDSG-Novelle II bereits am 1. September 2009 in Kraft getreten. Die Neuregelungen in der BDSG-Novelle I sind vom 1. April 2010 an zu beachten. Am 11. Juni 2010 erlangen die Vorgaben zum Verbraucherkreditrecht Rechtskraft.*

Die Unternehmen sollen andere Erkenntnisse über den Betroffenen zu den Listendaten hinzuspeichern dürfen. Auch die Übermittlung von Listendaten ist weiterhin zulässig. Wollen Unternehmen allerdings zukünftig in Listen zusammengefasste Daten, die nach einem Gruppenmerkmal selektiert sind, an andere Stellen weiterübermitteln, müssen sie dokumentieren, woher die Daten stammen und an wen diese weitergegeben werden. Diese Informationen sind dem Betroffenen auf Anfrage mitzuteilen. Der Betroffene erhält hierdurch –

jedenfalls mehr als bisher – eine Chance, bezüglich seiner Daten die **Übermittlungskette nachzuvollziehen** und die einzelnen Stellen, die im Besitz seiner Daten sind, zu identifizieren. An diese kann er dann herantreten und eine weitere Nutzung bzw. Übermittlung zu Werbezwecken untersagen.

Viele praktische Fragen harren noch der Klärung. Das ULD steht als **Ansprechpartner für Beratungen** bereit und hat eine verstärkte Diskussion unter den Aufsichtsbehörden im Düsseldorfer Kreis angeregt. In diesem Zusammenhang wurde ein erster Beschluss gefasst.

http://www.bfdi.bund.de/cae/servlet/contentblob/814758/publicationFile/50536/Nov09DVWerbezwecke.pdf

Was ist zu tun?
Die Regelungen müssen zu massiven Änderungen der Werbepraxis führen. Ein „Weiter-so-wie-bisher“ verstößt gegen das neue Datenschutzrecht. Die bisher bereits unzulässige, aber weitverbreitete Praxis der Übermittlung von nach mehr als einem Merkmal selektierten Adressen ist ohne Einwilligung unzulässig. Die neuen Transparenzvorgaben müssen zuverlässig umgesetzt werden.

- **Arbeitnehmerdatenschutz**

Angesichts vieler Überwachungsskandale im Arbeitnehmerbereich sah sich der Gesetzgeber veranlasst, in letzter Sekunde dem Arbeitnehmerdatenschutz einen neuen Paragrafen zu widmen. So heiß die Nadel beim Stricken der Norm war, so wenig hilft sie bei den meisten Problemen weiter. Sie soll auch nicht der Weisheit letzter Schluss sein: Die neue Regierungskoalition auf Bundesebene hat angekündigt, den Arbeitnehmerdatenschutz in der aktuellen Legislaturperiode zu verbessern. Dabei wird voraussichtlich in das BDSG ein Kapitel zum Arbeitnehmerdatenschutz eingefügt werden. Allerdings ist jetzt schon klar: Ein **Arbeitnehmerdatenschutzgesetz** wird viel Gegenwind bekommen.

Die Neuregelung der BDSG-Novelle II wird von der Wirtschaft bereits für eine unerfreuliche Angstkampagne genutzt. Es wird öffentlich behauptet, die Unternehmen könnten ihren Compliance-Aufgaben, insbesondere der Korruptionsbekämpfung, nicht mehr ordnungsgemäß nachkommen. Dem stehe der Datenschutz entgegen. Dies trifft nicht zu. Der Gesetzgeber hat vielmehr für Verarbeitungen zu Zwecken des Beschäftigungsverhältnisses eine abschließende Regelung formuliert und die Verarbeitungen zu diesen Zwecken unter einen konsequenten **Erforderlichkeitsvorbehalt** gestellt.

Was ist zu tun?
Ein wenig mehr Besonnenheit könnte nicht schaden. Es ist an der Zeit, dass Wirtschaftsvertreter den Datenschutz endlich als gleichwertige Compliance-Aufgabe begreifen und dies auch in der Praxis umsetzen.

- **Informationspflicht bei Sicherheitslecks und Datenpannen**

Brandneu ist die Einführung einer Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten. Damit hat der Gesetzgeber den europarechtlichen Entwicklungen vorgegriffen. Eine solche Informationspflicht bei Datenpannen sieht die Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) vor, die am 18. Dezember in Kraft getreten ist und innerhalb von 18 Monaten in deutsches Recht umgesetzt werden muss. Dort gilt die Verpflichtung nur für Telekommunikationsunternehmen. Diese zukünftig gesetzlich umzusetzende Pflicht gilt bereits jetzt für alle Datenverarbeiter. Danach sind sowohl die Betroffenen als auch die zuständige Datenschutzaufsicht grundsätzlich zu informieren, wenn bestimmte Arten von personenbezogenen Daten, z. B. besondere Arten personenbezogener Daten oder Daten zu Bank- und Kreditkartenkonten, unrechtmäßig übermittelt oder Dritten auf andere Weise unrechtmäßig zur Kenntnis gelangt sind.

- **Erweiterte Befugnisse der Aufsichtsbehörde**

Neben den Erweiterungen des Bußgeldkatalogs und der Erhöhung des Bußgeldrahmens ist auch das aufsichtsbehördliche Instrumentarium wesentlich ausgeweitet und die bisher auf technisch-organisatorische Maßnahmen beschränkte Anordnungsbefugnis der Aufsichtsbehörden ausgedehnt worden. Die Aufsichtsbehörden können bei allen festgestellten Verstößen gegen das Datenschutzrecht Maßnahmen zur Beseitigung anordnen. Bei besonderen Gefährdungen für das Persönlichkeitsrecht und Nichtbefolgung der Anordnung dürfen die Aufsichtsbehörden die Datenverwendungen bzw. einzelne Verfahren sogar untersagen.

5.1.2 Mehr Transparenz bei Auskunfteien und Kreditwirtschaft – BDSG-Novelle I

Verbesserte Transparenz für die Betroffenen bei der Tätigkeit der Auskunfteien und den von diesen praktizierten Verfahren, insbesondere bei Scoring-Verfahren, war das erklärte Hauptziel der BDSG-Novelle I. Die Neuregelungen treffen in der Hauptsache Auskunfteien und die Kreditwirtschaft. Von den Vorgaben zum Scoring und zur Bonitätsbewertung sind aber auch andere Bereiche wie etwa Telekommunikationsunternehmen und Versandhandel tangiert. Das Gesetz tritt am 1. April 2010 in Kraft.

Was ist zu tun?
Das ULD hat die Verbände der Banken und Kreditinstitute sowie einzelne Banken in Schleswig-Holstein angeschrieben, um sich über den Stand der Umsetzungsbemühungen zu informieren. Es hat angeboten, über die Umsetzung der Vorgaben frühzeitig in einen Dialog einzutreten. Dieses Angebot ist bisher nicht von allen Banken und Verbänden angenommen worden.

- **Automatisierte Einzelentscheidung**

Der Gesetzgeber hat an vielen Stellen des Gesetzes angesetzt, um die **Informations- und Auskunftsrechte** der Betroffenen zu stärken. Er reagierte u. a. darauf, dass die Vorgaben zur automatisierten Einzelentscheidung in der Praxis hartnäckig ignoriert wurden.

Typischerweise ist die Regelung zur automatisierten Einzelentscheidung beim Einsatz von **Scoring-Verfahren** anwendbar. Beim Scoring wird anhand eines Sets von Merkmalen basierend auf statistischen Erfahrungswerten ein Wert errechnet. Dieser Wert soll die Wahrscheinlichkeit ausdrücken, mit welcher ein bestimmtes Ereignis eintritt oder ein bestimmtes Verhalten zukünftig erfolgt. Dem Betroffenen, der diese Merkmale aufweist, wird dieser Wert in einem Entscheidungsverfahren, z. B. im Rahmen einer Kreditvergabeentscheidung, mit entsprechenden Konsequenzen zugerechnet.

Automatisierte Einzelentscheidung

Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dient. Zulässig war eine solche Entscheidung nach der alten Fassung des BDSG, wenn der Betroffene z. B. die Möglichkeit erhielt, seinen Standpunkt geltend zu machen, und die verantwortliche Stelle daraufhin die Entscheidung erneut geprüft hat.

Die Regulierung solcher Entscheidungsverfahren erfolgt zum Schutze der Betroffenen: Das Gesetz will verhindern, dass der Betroffene zum reinen Objekt einer Bewertung wird, ohne auf einen voll automatisiert ablaufenden Prozess Einfluss nehmen zu können. Deswegen soll ein menschlicher Ansprechpartner existieren, der die Entscheidung gegenüber dem Betroffenen verantwortet und bei dem der Betroffene auch eine Gegendarstellung abgeben kann.

Wie viel **Einfluss der Scorewert** auf z. B. die Kreditvergabeentscheidung hatte und ob angesichts dessen von einer automatisierten Entscheidung die Rede sein konnte, war ein lange währender Streitpunkt zwischen Aufsichtsbehörden und Wirtschaftsvertretern. Die Kreditwirtschaft behauptete, der Scorewert sei nur eine Entscheidungshilfe für den Kreditsachbearbeiter. Dem standen Berichte von Betroffenen und Erfahrungen eines Praxistests entgegen, wonach die Kreditsachbearbeiter häufig gar keinen Einfluss auf den Vorschlag des Computersystems haben und diesen übernehmen müssen, weil sie ansonsten intern in Erklärungsnöte geraten.

Der Gesetzgeber macht nun deutlich, dass die Regelungen zur automatisierten Einzelentscheidung nicht mehr umgangen werden können, indem eine mehr oder minder formale **Bearbeitung durch einen Menschen** nachgeschaltet wird. Dem Betroffenen ist bei einer automatisierten Entscheidung mitzuteilen, „woran es gelegen hat“. Dies hat zur Konsequenz, dass eine Stelle im Unternehmen eingesetzt werden muss, die die Hintergründe des Scoring-Verfahrens kennt und die Kompetenz besitzt, Entscheidungen unter Berücksichtigung etwaiger Gegendarstellungen durch den Betroffenen neu zu bewerten.

- **Einmeldung von Forderungen bei einer Auskunftei**

Erstmalig hat der Gesetzgeber in einem konkreten Katalog festgelegt, unter welchen Umständen Daten über eine Forderung bei einer Auskunftei eingemeldet werden dürfen. Problematisch ist in diesem Zusammenhang die gesetzlich legitimierte Einmeldung von sogenannten **nicht titulierten Forderungen**. Dabei handelt es sich um Forderungen, deren Bestehen weder durch einen Vollstreckungsbescheid noch durch einen Titel vor Gericht, d. h. von unabhängiger dritter Seite, festgestellt wurde. Diese Forderungen dürfen zukünftig unter bestimmten Verfahrensvoraussetzungen bei einer Auskunftei eingemeldet werden, wenn der Betroffene der Forderung nicht widersprochen hat. Rechtzeitig vor der Einmeldung ist der Betroffene zu unterrichten.

Was ist zu tun?
Selbst wenn der Verbraucher sich im Recht fühlt – ignorieren ist keine Lösung: Wird dem Betroffenen fälschlicherweise vorgehalten, einen Vertrag geschlossen zu haben, so muss er aktiv werden und bestreiten, dass die Forderung besteht.

- **Einmeldung von Vertragsdaten durch Kreditinstitute**

Eine der wichtigsten Änderungen der BDSG-Novelle I betrifft die Einmeldung von Informationen über die Begründung, ordnungsgemäße Durchführung und Beendigung des Vertragsverhältnisses bei Auskunfteien durch Kreditinstitute. Der Gesetzgeber hat grundsätzlich anerkannt, dass diese Informationen über die Auskunfteien anderen Banken und Kreditinstituten zur Verfügung stehen sollen. Damit soll das Einholen einer Einwilligung der Betroffenen als Grundlage für den Datenaustausch nicht mehr nötig sein. Entgegen den Vorgaben des Gesetzes wurde diese nicht freiwillig erteilt. Der Betroffene hatte ohne Unterzeichnung der Erklärung letztlich keine Chance, die gewünschte Leistung zu erhalten. Egal ob bei der **Eröffnung eines Girokontos**, der Beantragung einer Kreditkarte oder eines Kredits, die Kunden mussten einwilligen, dass die Bank Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung des Vertragsverhältnisses an eine Auskunftei übermittelt (sogenannte Schufa-Klausel). Diese Einwilligung wurde von fast allen Banken eingesetzt, und dem Betroffenen blieb letztlich nichts anderes übrig, als sie zu unterschreiben. Nun darf die Datenübermittlung aufgrund der Neuregelung stattfinden. Die Einwilligung ist nicht mehr nötig.

Etwas anderes gilt für den Fall eines **Kontos ohne Überziehungsmöglichkeit**. Hier ist die Einmeldung von Daten gesetzlich nicht erlaubt.

Was ist zu tun?
Die Kunden müssen vor Abschluss des Vertrages konkret darüber unterrichtet werden, dass eine Übermittlung von ihren Daten an Dritte erfolgt, zu welchem Zweck die Übermittlung durchgeführt wird, was beim Empfänger mit den Daten geschieht und wer Empfänger der Daten ist.

- **Nachberichtspflicht**

Diejenigen Stellen, die Daten an Auskunfteien übermitteln, müssen dafür sorgen, dass die übermittelten Daten gelöscht oder berichtigt werden, wenn sich Änderungen ergeben und die Übermittlung so nicht erfolgen durfte.

Was ist zu tun?
Die Betroffenen sollten die Berichtigung durch die einmeldende Stelle aktiv einfordern, wenn eine Einmeldung zu Unrecht erfolgt ist.

- **Scoring**

Der Gesetzgeber hat erstmalig das Scoring-Verfahren (siehe oben) gesetzlich geregelt. Allerdings wurde versäumt, die wohl wichtigste Frage zu klären: Welche **Merkmale** dürfen beim Scoring genutzt werden? Hier wird auch im neuen BDSG auf eine Interessenabwägung zwischen den berechtigten Interessen des Unternehmens und den schutzwürdigen Interessen der Betroffenen verwiesen – mit einer Einschränkung: Scoring-Verfahren, bei denen ausschließlich Anschriftendaten genutzt werden, sind nicht erlaubt. Festgelegt ist zukünftig, dass die zum Einsatz kommenden Verfahren wissenschaftlich anerkannte mathematisch-statistische Verfahren sind und die genutzten Daten nachweisbar für die Berechnung der Wahrscheinlichkeit erheblich sein müssen.

Was ist zu tun?
Die Unternehmen müssen auf Verlangen der Aufsichtsbehörde die Erheblichkeit der Daten für die Berechnung der Wahrscheinlichkeit nachweisen können. Dieser Zusammenhang sowie die Tatsache, dass das Verfahren wissenschaftlich anerkannt ist, müssen dokumentiert werden.

- **Auskunftsrecht der Betroffenen**

In der BDSG-Novelle I wird klargestellt, dass und wie die Betroffenen auf Verlangen Auskunft erhalten sollen, wenn ein **Scoring-Verfahren** zum Einsatz kommt. Dabei müssen sowohl die innerhalb der letzten sechs Monate erhobenen oder gespeicherten Scorewerte als auch die zur Berechnung genutzten Datenarten beauskunftet werden. Darüber hinaus muss den Betroffenen das Zustandekommen und die Bedeutung des Wahrscheinlichkeitswertes bezogen auf den konkreten Einzelfall erläutert werden. Auskunfteien müssen darüber hinaus die innerhalb der letzten zwölf Monate übermittelten und die tagesaktuellen Scorewerte auf Anfrage mitteilen und Auskunft geben, an wen die Daten weitergegeben wurden.

Der Gesetzgeber hat auch für die **Kosten der Auskunftserteilung** eine Neuregelung getroffen. Grundsätzlich war die Auskunft bereits nach dem alten Recht unentgeltlich. Etwas anderes galt, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen konnte. Diese Ausnahmeregelung wurde von mancher Auskunftei zum Anlass genommen, pauschal Geld für eine schriftliche Auskunft zu verlangen. Für den Betroffenen blieb undurchsichtig, wie

die Kosten für sein Auskunftsersuchen berechnet wurden. Dies hat zukünftig ein Ende: Jedenfalls einmal pro Jahr kann der Betroffene auch von Auskunfteien eine unentgeltliche Auskunft verlangen.

5.2 Neues aus der Versicherungswirtschaft

Die Verhandlungen zur Erstellung einer Schweigepflichtentbindungs- und datenschutzrechtlichen Einwilligungserklärung mit dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) sind noch nicht abgeschlossen. Auch die Erörterung der Verhaltensregeln der Versicherungswirtschaft wird fortgeführt. Das ULD führt weiter den Vorsitz der AG Versicherungswirtschaft des Düsseldorfer Kreises.

- **Einwilligungserklärungen und Verhaltensregeln**

Die Entwürfe der Verhaltensregelung sowie die Mustererklärungen zur datenschutzrechtlichen Einwilligung und zur Schweigepflichtentbindung wurden im Düsseldorfer Kreis nicht abschließend abgestimmt (31. TB, Tz. 5.5.1). Vonseiten der Datenschutzaufsichtsbehörden wurde weiterer Nachbesserungsbedarf angemeldet. Wir gehen davon aus, dass die Erklärungen zwischen dem GDV und den Datenschutzaufsichtsbehörden im Jahr 2010 abgestimmt und die Verhaltensregeln der Versicherungswirtschaft zu einem Abschluss gebracht werden können. Die gesetzlichen Neuregelungen im BDSG haben nun in einigen Punkten Klarheit geschaffen, die in den Erörterungen im Hinblick auf die zukünftigen gesetzlichen Entwicklungen bisher offengeblieben waren.

- **Bonitätsabfrage und Scoring in der Versicherungswirtschaft**

Intensiv beschäftigen sich die Datenschutzaufsichtsbehörden in der AG Versicherungswirtschaft mit der Frage der Zulässigkeit von Bonitätsabfragen und Scoring durch Versicherungsunternehmen. Die an der AG teilnehmenden Aufsichtsbehörden haben den Umgang mit Bonitätsabfragen und Scoring im Wege einer Umfrage bei den Versicherungsunternehmen ermittelt. Die Erkenntnisse wurden in einem umfangreichen Sachbericht zusammengestellt. Dabei stellte sich heraus, dass in der Praxis Bonitätsauskünfte sowohl im Antragsfall als auch bei der Leistungsprüfung gang und gäbe sind. Beim Scoring sind die Versicherungsunternehmen bisher etwas zurückhaltender. Derzeit wird die rechtliche Bewertung der ermittelten Sachverhalte in der AG abgestimmt, um diese über den GDV an die Mitgliedsunternehmen weiterzugeben.

- **Hinweis- und Informationssystem der Versicherungswirtschaft (HIS)**

Der Versicherungswirtschaft ist es bisher nicht gelungen, das HIS, oft nach der Software auch „Uniwagnis“ genannt, datenschutzkonform umzugestalten (31. TB, Tz. 5.5.2). Das System zur Risikobewertung und Betrugsprävention war von den Datenschutzaufsichtsbehörden für datenschutzwidrig erklärt worden. Die Versicherungswirtschaft hat unter Federführung des GDV zugesagt, das System in eine Auskunftei umzugestalten. Dieses befindet sich in der Umgestaltungsphase. Für

das alte System haben die Aufsichtsbehörden – als Übergangsvorgehen – gefordert, dass der GDV Auskunftsanfragen von Betroffenen beantwortet und die Versicherungsunternehmen die Betroffenen bei Einmeldung in das HIS benachrichtigen. Dies ist inzwischen umgesetzt: Seit April 2009 können Betroffene auf Anfrage beim GDV Auskunft erhalten, ob sie im HIS eingemeldet sind; die Versicherungsunternehmen benachrichtigen nach unseren Erkenntnissen die Betroffenen bei der Einmeldung. Die AG Versicherungswirtschaft und der GDV diskutieren über die konkreten Kriterien der Einmeldung. Die Erörterungen sind noch nicht abgeschlossen. Es ist davon auszugehen, dass der GDV das neue HIS nicht selbst betreiben wird, sondern an einen Auskunfteibetreiber abgeben wird.

5.3 Illegaler Datenhandel – kein Ende in Sicht

Die Anfragen und Eingaben zu unerwünschten Werbeanrufen sowie zur unberechtigten Nutzung von Kontodaten zeigen, dass der illegale Datenhandel weiter stattfindet.

Die beim ULD im Jahre 2008 erlangten **Datenbestände aus illegalem Datenhandel** werden weiterhin vorgehalten, um Betroffenen Auskunft zu erteilen (31. TB, Tz. 5.4). Bei Beschwerden über ungerechtfertigte Kontoabbuchungen prüfen wir, ob die zur Abbuchung genutzten Daten auch im vorgehaltenen Datenbestand sind. Ist dies der Fall, so geben wir den Betroffenen den Rat zu prüfen, ob ein Wechsel der Kontoverbindung möglich ist.

Doch auch bei einer Negativauskunft kann keine Entwarnung gegeben werden. Andere **„frische“ illegal beschaffte Kontodaten** sind im Umlauf. Wir verweisen weiterhin darauf, im Falle einer bereits erfolgten unzulässigen Abbuchung oder eines entsprechenden Versuches regelmäßig und sorgsam die Kontoauszüge zu kontrollieren und den Wechsel der Kontoverbindung zu erwägen. In Kooperation mit der Verbraucherzentrale Schleswig-Holstein e.V. hat das ULD zur Thematik „Illegaler Datenhandel“ eine gleichnamige Broschüre erstellt, die Wissenswertes zum Umgang mit unerwünschten Telefonanrufen, fingierten Verträgen und unberechtigten Abbuchungen vom Konto vermittelt.

www.datenschutzzentrum.de/blauereihe/blauereihe-kontodatenhandel.pdf

Was ist zu tun?
Von der Preisgabe sensibler Informationen wie z. B. Kontodaten gegenüber nicht bekannten Dritten, z. B. im Internet oder am Telefon, ist abzuraten. Bei unerwünschten Telefonanrufen ist Vorsicht angezeigt: Häufig werden die Betroffenen durch trickreiche Überredungskünste unfreiwillig zur Preisgabe ihrer Informationen gebracht.

5.3.1 Das moderne „Drückergeschäft“ bei Zeitschriftenabos

Illegal erlangte Kontodaten werden in großem Maße für Zeitschriftenabonnements zur Begründung fingierter Verträge genutzt.

Ein beträchtlicher Teil der Eingaben zur illegalen Nutzung von Kontodaten bezieht sich auf den Abschluss von Zeitschriftenabonnements. Betroffene berichteten von Telefonanrufen, bei denen der Anrufer bereits die Kontodaten kannte und um die Bestätigung der Bestellung bat. Betroffene erhielten dann oft Vertragsbestätigungen, obwohl sie während des Gesprächs deutlich einen Vertragsschluss abgelehnt hatten. Diese Bestätigungen geben uns einen Ermittlungsansatz, weil die Identität der vermeintlichen Vertragspartner genannt wird. Da schriftliche Anfragen keine zufriedenstellenden Resultate brachten, führten wir in Schleswig und Kiel **unangekündigte Betriebsprüfungen** durch.

Bei einer Prüfung konnte das ULD nähere Erkenntnisse über das System der **Nutzung der Kontodaten** gewinnen. Kleine bzw. durch Einzelpersonen betriebene Callcenter waren als Unterauftragnehmer tätig und erhielten von deren Auftraggebern ausgedruckte Listen oder Dateien mit Name, Adresse, Telefonnummer, Kontoverbindungsdaten und in einigen Fällen Alter der Betroffenen. Dies war die Grundlage für Anrufe mit Angeboten für Zeitschriftenabonnements. Im Fall eines realen oder vermeintlichen Abschlusses wurden die Vertragsdaten an den Auftraggeber weitergegeben und der Callcenterbetreiber erhielt eine Provision. In einigen Fällen führte der Auftraggeber Kontrollanrufe zur Bestätigung des Aboabschlusses durch. Bei den Betriebsprüfungen konnten wir Einblick in die Widersprüche von Betroffenen gegen den Abschluss der Abos nehmen; dabei verstärkte sich der Verdacht, dass häufig mit bereits vorhandenen Kontodaten der Abschluss eines Zeitschriftenliefervertrages fingiert wurde.

Die Betreiber der Callcenter legten weder die Herkunft der Daten offen, noch konnten sie Einwilligungserklärungen der Betroffenen zur Nutzung der Daten vorlegen. Einige Listen enthielten Hinweise auf deren Ursprung, etwa auf klassische Glücksspiele oder Telekommunikationsdienstleistungen, aber auch auf Internetseiten mit Werbung für Preisausschreiben und Ähnliches. Bei einem Stichprobenabgleich mit der im ULD befindlichen Datenbank zum illegalen Datenhandel ergaben sich viele Treffer. Wegen der Erhärtung des Verdachts der Beteiligung am illegalen Datenhandel hat das ULD **Strafanzeige** gegen die verantwortlichen Stellen gestellt. Die Ermittlungen sind nach Kenntnis des ULD bisher noch nicht abgeschlossen.

5.3.2 Aus gegebenem Anlass: die Betretungsrechte des ULD

Betriebsprüfungen des ULD zur Aufklärung und Verfolgung des illegalen Datenhandels stießen nicht bei allen Stellen auf Zustimmung. In zwei Fällen wurde den ULD-Prüfenden der Zutritt zu den Geschäftsräumen verwehrt und die Duldung der Prüfung verweigert.

Dies verstieß gegen die gesetzliche Duldungspflicht. Die Beauftragten der Aufsichtsbehörden sind befugt, zur Erfüllung der übertragenen Prüf- und Kontrolltätigkeit während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume zu betreten und Prüfungen und Besichtigungen vorzunehmen. Die Befugnis erstreckt sich auch auf das Recht, Einsicht in geschäftliche Unterlagen, die gespeicherten Daten und die Datenverarbeitungsanlagen zu nehmen. Prüfungen sind schon dann berechtigt, wenn sie dazu dienen festzustellen, ob überhaupt personenbezogene Daten verarbeitet werden und in welcher Form dies geschieht. Eine vorherige Ankündigung oder ein besonderer Anlass ist nicht zwingend erforderlich. Gerade bei Ermittlungen zum illegalen Datenhandel sind wir auf unangekündigte Betriebsprüfungen angewiesen, um eine Vernichtung von belastenden Beweisen, z. B. durch Datenlöschung, zu verhindern. Die Feststellung der illegalen Aktivitäten würde dadurch unmöglich gemacht oder zumindest erschwert. Die verantwortlichen auskunftspflichtigen Stellen haben die Prüfungsmaßnahmen zu dulden. Im Fall einer Be- oder **Verhinderung von Prüfungs- und Besichtigungshandlungen** kann die Aufsichtsbehörde ein Bußgeld bis zu 50.000 Euro verhängen.

Im Rahmen ihrer Prüfung wurde Mitarbeiterinnen und Mitarbeitern des ULD der Zugang zu den Räumen untersagt und sie wurden an der Einsicht in Geschäftsunterlagen und Datenverarbeitungsanlagen gehindert. Ein Unternehmen meinte, sich mit einem Hausverbot der Kontrolle entziehen zu können. In einem Verfahren wurde der vom ULD erlassene **Bußgeldbescheid** nach dem Einspruch des Unternehmens vom Amtsgericht Kiel bestätigt.

Für das Gericht war es unerheblich, ob die verantwortliche Person während einer Prüfung anwesend ist. Die Aufsichtsbehörde muss sich nicht auf einen späteren Prüfungszeitpunkt verweisen lassen, um deren Anwesenheit zu ermöglichen. Vor allem dann nicht, wenn die Verantwortlichen nicht in unmittelbarer zeitlicher Nähe in der Lage sind, der Prüfung beizuwohnen. Der **Auslandsaufenthalt des Verantwortlichen** ist kein Hinderungsgrund für eine Betriebsprüfung, soweit ein ordnungsgemäßer Zugang zu den Räumen, z. B. über einen Vertreter, gewährleistet ist. Das Gericht erklärte, dass es keinen besonderen Anlasses oder einer vorherigen Ankündigung der Betriebsprüfung bedarf. Zudem bestätigte das Gericht, dass eine Nichtduldung der Prüfung durch konkludentes Handeln ausgedrückt werden kann. Die Ankündigung, während der üblichen Geschäftszeit die Betriebsräume gegenüber den Beschäftigten der Aufsichtsbehörde zu verschließen, ist Ausdruck der Nichtduldung der Prüfung. Den Beschäftigten der Aufsichtsbehörde ist es auch nicht zuzumuten, sich einschließen zu lassen.

www.datenschutzzentrum.de/wirtschaft/20091102-betreuungsrecht-aufsichtsbehorde-bdsg.html

Was ist zu tun?
Daten verarbeitende Stellen haben die zu den üblichen Betriebs- und Geschäftszeiten durchgeführten Besichtigungen und Einsichtnahmen durch die Aufsichtsbehörde zu dulden. Einer vorherigen Ankündigung oder eines besonderen Anlasses der Betriebsprüfung bedarf es nicht.

5.3.3 Anrufe krimineller „Datenschützer“

Schon seit Längerem bieten angebliche Daten- oder Verbraucherschützer telefonisch „Datenschutzdienstleistungen“ an. Die Betroffenen werden am Telefon mit ihren eigenen Bankdaten konfrontiert, deren Schutz sie sich knapp 50 Euro kosten lassen sollen.

Die Daten der Angerufenen werden telefonisch abgeglichen. Sie erhalten wenige Tage später ein Bestätigungsschreiben, eventuell zu einem ganz anderen Thema wie z. B. zur Teilnahme an einem Glücksspiel. Seit einiger Zeit geben sich die Anrufer als **Mitarbeiter des „Datenschutzzentrums“** oder einer „Datenschutzzentrale“ aus und verweisen zum Beleg ihrer „Glaubwürdigkeit“ auf die Webseite des ULD oder des Virtuellen Datenschutzbüros.

Diese unseriösen Anrufer nutzen die Angst der Verbraucherinnen und Verbraucher vor dem Missbrauch ihrer Daten aus, indem sie z. B. behaupten, die Kontodaten der Betroffenen im Internet entdeckt zu haben, und bieten gegen einen **monatlichen Beitrag von etwa 50 Euro** an, sich um den Schutz der Daten zu „kümmern“. Tatsächlich arbeiten auch solche Anrufer mit illegal angekauften Kontodaten und nutzen die Bestürzung der Angerufenen, um eine Dienstleistung zum Schutze der Daten im Abonnement anzubieten und dazu die Daten beim Betroffenen zu verifizieren. Die Zustimmung zur Erbringung einer Dienstleistung und zum Datenabgleich werden in vielen Fällen – auch das ist illegal – aufgezeichnet. Wenige Tage nach dem Anruf des „Datenschutzzentrums“ erhalten die Angerufenen ein Bestätigungsschreiben für die Teilnahme an einem – im Telefonat angeblich vereinbarten – Gewinnspiel.

Was ist zu tun?
Im Falle solcher Anrufe sollten auf keinen Fall persönliche Angaben gemacht oder Aufträge erteilt werden. Betroffene sollten unbedingt regelmäßig ihre Kontoauszüge kontrollieren. Sollten den Anrufern ermittlungsrelevante Informationen entlockt werden können, ist das ULD für eine Benachrichtigung dankbar, um diesen Hinweisen weiter nachgehen zu können.

5.4 Bonitätsabfragen durch Energieversorger

Zunehmend finden sich in vorgefertigten Energielieferverträgen der Energieversorgungsunternehmen in Schleswig-Holstein Vertragsklauseln zu datenschutzwidrigen Bonitätsabfragen.

Zweck der Vertragsklauseln ist es, die Bonität des zukünftigen Kunden durch Anfragen bei Auskunfteien ermitteln zu können. Fällt die Bonitätsprüfung negativ aus, wird keine Energie geliefert. Die Zulässigkeit solcher Bonitätsabfragen und die Wirksamkeit entsprechender Einwilligungserklärungen durch die Betroffenen sind von der **Art des Vertrages** abhängig, also ob inner- oder außerhalb des Versorgungsgebietes geliefert werden soll oder nach Grund- oder Sondertarif.

- **Kunden im Versorgungsgebiet mit Grundtarif**

Eine Bonitätsabfrage, d. h. die Übermittlung von personenbezogenen Daten an eine Auskunftei und die Rückübermittlung von Negativinformationen, ist nur gesetzlich gerechtfertigt, wenn für das abfragende Unternehmen ein **finanzielles Ausfallrisiko** besteht, wenn es also in nicht unerheblichem Maße in Vorleistung tritt. Schutzwürdige Interessen stehen einer solchen Abfrage nicht entgegen, soweit die übermittelten Daten sich auf Angaben zur Zahlungsfähigkeit und Zahlungswilligkeit des Betroffenen beschränken. Bei Vorliegen dieser gesetzlichen Voraussetzungen ist eine Einwilligung der Betroffenen nicht erforderlich und auch nicht der richtige Weg.

Für Kunden im Versorgungsgebiet besteht für die Energieversorger ein sogenannter Kontrahierungszwang. Die Unternehmen sind danach gesetzlich zum Abschluss von Energielieferverträgen verpflichtet, es sei denn, dass ein Vertragsschluss unzumutbar ist. Die Entscheidungsfreiheit über den Abschluss eines Vertrages ist für die Energieversorger damit stark eingeschränkt und kann nicht vom Ergebnis einer Bonitätsprüfung des Kunden abhängig gemacht werden. Die Bonitätsprüfung ist also nicht erforderlich und unzulässig.

Einwilligung versus gesetzliche Grundlage

Datenverarbeitungen können aufgrund von Gesetzen, z. B. des Bundesdatenschutzgesetzes, gerechtfertigt sein, etwa für die Abwicklung eines Vertragsverhältnisses. In solchen Fällen ist das Einholen einer Einwilligungserklärung irreführend, denn den Betroffenen wird suggeriert, mit ihrer Unterschrift selbst bestimmen zu können, ob ihre Daten verwendet werden oder nicht. Dies ist nicht der Fall, wenn die Daten verarbeitet werden müssen, damit der geschlossene Vertrag durchgeführt werden kann. So kann ein Versandhändler Ware nur versenden, wenn er die Adresse des Bestellers kennt. Das Abverlangen von Einwilligungserklärungen in diesen Fällen ist jedenfalls dann ein unzulässiges und widersprüchliches Verhalten, wenn trotz eines Widerrufs der Einwilligung oder bei Verweigerung der Einwilligung die Daten verarbeitet werden.

Das ULD empfiehlt vom Einholen einer Einwilligung abzusehen, wenn die Datenverarbeitung auf gesetzliche Füße gestellt werden kann. Wichtig ist in jedem Fall ein aussagekräftiger Hinweis auf die beabsichtigten Verarbeitungen mit sämtlichen nach § 4 Abs. 3 BDSG relevanten Informationen.

- **Kunden im Versorgungsgebiet mit Sondertarif**

Auch für die Fälle der Sondertarife bei Kunden innerhalb des Versorgungsgebietes können wir ein kreditorisches Risiko bzw. die Erforderlichkeit einer Bonitätsprüfung auf gesetzlicher Grundlage nicht erkennen. Im Versorgungsgebiet dürfen die Energieversorgungsunternehmen typischerweise keine Kunden ablehnen, d. h., sie müssen mit diesen Kunden wegen des Kontrahierungszwanges zumindest einen Vertrag mit normalem Tarif schließen.

Allein ein Sondertarif mit **günstigeren Konditionen** begründet kein kreditorisches Risiko. Der Energielieferant muss ein Ausfallrisiko so oder so tragen. Eine

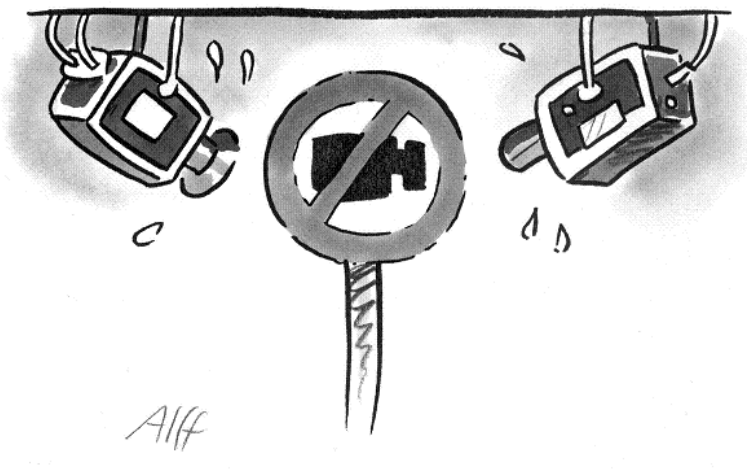
Bonitätsprüfung ist in diesen Fällen, wenn überhaupt, nur mit Einwilligung des Betroffenen, die freiwillig sein muss, möglich, d. h., die Betroffenen müssen eine Wahl haben, wenn sie eine Bonitätsprüfung ablehnen und stattdessen in Vorleistung gehen.

- **Neukunden außerhalb des Versorgungsgebietes**

Für Neukunden außerhalb des Versorgungsgebietes besteht kein Kontrahierungszwang. Hier kann ein zusätzliches finanzielles Ausfallrisiko beim Energieversorger bestehen. Die in der Praxis gegebenen Informationen für die Betroffenen sind häufig nicht ausreichend. Aus den Klauseln zur Bonitätsabfrage geht weder hervor, bei welchen Auskunfteien Auskünfte eingeholt werden, noch welchen Inhalt die Auskünfte haben, d. h., welche Daten über den Betroffenen zurückübermittelt werden. Dies und der Zweck der Datenverarbeitung müssen in einem **Datenschutzhinweis** spezifiziert werden. Die Kundinnen und Kunden müssen erkennen können, welche Folgen eine negative Bonitätsauskunft oder eine Nichtunterzeichnung bzw. Streichung der Klausel hat. Grundsätzlich muss eine Vorauszahlung bei den Energieunternehmen ermöglicht werden, die dann höher als die Abschlagszahlungen ist. Kann eine Bonitätsprüfung aufgrund eines finanziellen Ausfallrisikos auf gesetzlicher Basis erfolgen, sollte vom Einsatz einer Einwilligungserklärung abgesehen werden.

Was ist zu tun?
Die Datenschutzklauseln in den Energielieferverträgen sind zu überprüfen. Eine gesetzliche Rechtfertigung für Bonitätsabfragen besteht grundsätzlich nur für Kunden außerhalb des Grundversorgungsgebietes. Für die Kunden muss erkennbar sein, mit welchen Auskunfteien zusammengearbeitet wird und welche Daten für welchen Zweck abgefragt und eingemeldet werden.

5.5 Videoüberwachung



Die **Flut illegaler Videoüberwachung** ist durch das ULD an den rechtlichen Dämmen nicht allein zu stoppen. Eine Gesellschaft, die an Privatsphäre und Freiheitsrechten interessiert ist, muss sich überall dieser oft unsinnigen technischen Sozialkontrolle entgegenstemmen.

5.5.1 Letztes Mittel − Nachbarschaftsstreit per Kamera

Nachbarschaftsstreitigkeiten werden zunehmend mittels Videoüberwachung ausgetragen. Dies trägt weder zur Beilegung der Konflikte bei, noch nutzt es den Betroffenen in anderer Weise. Im Gegenteil: Den Beteiligten ist oft nicht bewusst, dass die Videoüberwachung illegal sein und dies empfindliche rechtliche Konsequenzen haben kann.

Nachbarschaftsstreitigkeiten sind wahrscheinlich so alt wie der menschliche Siedlungsbau. Ging es zunächst um die genaue Platzierung des Grenzsteins, so kamen im Laufe der Zivilisation Grillgeruch, Wegerechte oder laubende Bäume hinzu. Die Technik ermöglicht jetzt die Austragung auf höherer Ebene. Videokameras sind bei Sicherheitstechnikanbietern, aber auch im Baumarkt mittlerweile **niedrigpreisig erhältlich**. Als Bewegungsmelder getarnt, sind sie im Versandhandel für einen zweistelligen Betrag zu haben.

Die Eingaben zerstrittener Nachbarn wegen Beobachtung mittels Videotechnik schilderten uns vielfältigste **Fallgestaltungen**:

- Der Platzierung von Videokameras in verschiedenen Fenstern eines Wohnhauses waren zahlreiche Anzeigen von Nachbarn beim Ordnungsamt vorausgegangen, in welchen der Eigentümer des Hauses der illegalen Verbrennung von Müll bezichtigt wurde.
- Der Bau eines Brunnens kann Stein des Anstoßes sein. Der befürchtete Verlust von Grundwasser veranlasste den Nachbarn, eine Videokamera an der Grundstücksgrenze zu installieren, um einen Fortgang der Baumaßnahmen feststellen und intervenieren zu können.
- In einer Reihenhaussiedlung wollten Bewohner durch Installation mehrerer Videokameras verhindern, dass der böse Nachbar weiterhin heimlich Glasscherben und Nägel auf dem Grundstück ausstreut, was angeblich bereits zu erheblichen Pfotenverletzungen ihres Hundes geführt hatte.
- Ein Webcambetreiber in einer als „Karnevalszentrum“ bekannten Stadt an der Westküste Schleswig-Holsteins wollte diese mit seinen Aufnahmen noch bekannter machen. Dass er damit die gesamte Nachbarschaft ins Internet stellte, stieß bei dieser auf wenig Frohsinn.
- Auch der Wunsch eines Hobbyfunkers, seinen Freunden in aller Welt seine Umgebung per Webcam zu zeigen, stieß bei den Nachbarn auf wenig Gegenliebe, da nun weltweit beobachtet werden konnte, welcher Nachbar wann mit welchem Wagen vom Hof fuhr, welcher Gast zu Besuch kam und welcher Nachbar wie viele Schafe auf die Weide ließ.

Derartige Verhaltensweisen sind aus verschiedenen Gründen unzulässig. Es ist strafrechtlich verboten, unbefugt Bildaufnahmen von Personen in ihren Wohnungen herzustellen oder zu übertragen und dadurch deren **höchstpersönlichen Lebensbereich** zu verletzen. Entsprechendes gilt für andere Räume, die gegen Einblick besonders gesichert sind, z. B. durch Hecken oder Mauern sicht-

geschützte Gärten. Die Ausrichtung der Videokamera auf das Fenster des Nachbarn oder auf dessen ummauerten Garten kann Strafverfolgungsmaßnahmen auslösen.

Die Veröffentlichung von Videoaufnahmen, z. B. im Internet, kann als ein öffentliches Zurschaustellen von Bildnissen ohne Einwilligung des Betroffenen nach dem Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie, dem sogenannten **Kunsturhebergesetz**, ebenfalls strafbar sein.

Videoüberwachten Nachbarn stehen **zivilrechtliche Mittel** zur Verfügung. Die zielgerichtete ständige Beobachtung von Dritten mittels Videokamera ohne eine Einwilligung ist eine Verletzung von deren Persönlichkeitsrechten und kann für die Nachbarn Unterlassungs-, Beseitigungs-, aber auch Schadensersatzansprüche begründen. Ein Gericht bejahte schon einen vorbeugenden Unterlassungsanspruch eines betroffenen Nachbarn, weil eine Kamera auf sein Grundstück ausgerichtet installiert war und eine dauernde Videoüberwachung angedroht wurde.

Für Datenschutzaufsichtsbehörden stellen sich bei der nachbarschaftlichen Videoüberwachung verschiedene Fragen. Das **Bundesdatenschutzgesetz** (BDSG) ist häufig nicht anwendbar, wenn die Videoüberwachung keine öffentlichen Räume, z. B. Bürgersteige oder Straßen, erfasst. Die Verarbeitung von Daten ausschließlich für persönliche oder familiäre Tätigkeiten ist vom Anwendungsbereich des BDSG ausgeschlossen. In bestimmten Fällen sind wir auf den Appell beschränkt, sich eine dauernde Überwachung der Wohnung am eigenen Leibe vorzustellen, und auf den Hinweis der möglichen zivil- und strafrechtlichen Konsequenzen. Zudem sind die Kontrollbefugnisse des ULD begrenzt, wenn es um die Betretung von Privatwohnungen und -grundstücken geht. Die Überprüfung einer Eingabe zur nachbarschaftlichen Videoüberwachung eines Privatgrundstücks am Objekt ist dem ULD nicht möglich. Kann von außen durch Augenschein und durch Beweismittel eine unzulässige Videoüberwachung festgestellt werden und gehen die Verantwortlichen nicht auf unsere gesetzlich begründeten Forderungen ein, so müssen sie mit Bußgeldern rechnen.

Was ist zu tun?
Bei Videoüberwachungen im rein nachbarschaftlichen Verhältnis sollten sich die Bürger zivilrechtlich beraten lassen. Gegen die Verletzung von Persönlichkeitsrechten durch die dauernde Videoüberwachung kann mit Schadensersatz- und Beseitigungsansprüchen, d. h. der Verpflichtung des Nachbarn zum Abbau der Videokamera, vorgegangen werden.

5.5.2 Videoüberwachung im Restaurant

In Restaurations- und Freizeitbetrieben ist eindeutig ein Trend zu mehr und ungezügelterer Videoüberwachung feststellbar. Es bleibt ein Geheimnis der Verantwortlichen, wie die Beobachtung von Gästen in Freizeitbereichen der Sicherheit dienen soll.

Unverändert hoch ist die Anzahl der Beschwerden von Bürgern über Videobeobachtung in Restaurants und Freizeitbetrieben. Oft konnte dem ULD nicht plausibel dargelegt werden, wie die Videobeobachtung von Tresen- und Toilettenbereichen in Gaststätten zur Aufrechterhaltung und **Verbesserung der Sicherheit** führt:

- Mehrere Strandgaststätten beobachteten die Sitzplätze ihrer Außenterrasse – mit Strand und Meer im Hintergrund – per Videokamera und stellten die Bilder auch ins Internet. In manchen Fällen sahen die Betreiber schnell ein, dass ihren Gästen dies unangenehm sein könnte, und positionierten die Kamera so, dass nur noch Meer und Strand erfasst wurden. Andere Gastwirte zeigten sich zunächst unbeirrbar.
- Diverse Diskotheken meinten, mit Videobeobachtung der Toiletten die Sicherheit und Sauberkeit wesentlich erhöhen bzw. Vandalismus verhindern zu können.
- Restaurationsbetriebe beobachteten ihre Gäste an den Tischen und am Tresen ständig mit Kameras.
- Sportvereine installierten in ihren Vereinsheimen diverse Videokameras und kontrollierten damit sowohl Mitglieder als auch Besucher.
- Spielhallen beobachteten – abgesehen von der Kasse – jeden einzelnen Automaten und die dazwischen liegenden Gänge.

Das ULD hatte mehr als einmal den Eindruck, die Kameras dienten weniger der Sicherheit der Gäste als der – unzulässigen – Kontrolle der eigenen Belegschaft. Nach Einschalten des ULD wurden die Kameras zumeist abgebaut, der Erfassungswinkel verändert oder das Bild unscharf gestellt.

Was ist zu tun?
Die Videobeobachtung in Restaurations- und Freizeitbetrieben ist auf reine Sicherheitsfunktionen, z. B. an der Außenfassade, an Ein- und Ausgängen, Treppen, Kassen und Tresoren, zu beschränken. Reine Aufenthaltsbereiche − wie z. B. Sitzgruppen, Bar oder Tresen – dürfen nicht überwacht werden. Die Beobachtung von Toiletten und Umkleideräumen verbietet sich schon wegen der damit einhergehenden Verletzung der Intimsphäre.

5.6 Betriebsvereinbarungen und Datenschutz

Die Kontrolle der Leistung und des Verhaltens von Arbeitnehmerinnen und Arbeitnehmern bedarf grundsätzlich einer Rechtfertigung. Betriebsvereinbarungen als Rechtsgrundlage für die Verarbeitung personenbezogener Daten dürfen die Schutzvorgaben des BDSG nicht unterlaufen.

Das ULD wird häufig bei der Erstellung von Betriebsvereinbarungen um Beratung gebeten, zumeist von **Betriebsräten**. Der immer weiter reichende Einsatz von Technik am Arbeitsplatz eröffnet auch weiter gehende Kontrollmöglichkeiten durch den Arbeitgeber. Beim Einsatz von technischen Mitteln fallen zu Kontroll-

zwecken auswertbare Nutzungsdaten an. Die Betriebsräte sind gefordert: Nach dem Betriebsverfassungsgesetz ist die Einführung und Anwendung von technischen Einrichtungen, die geeignet sind, das Verhalten und die Leistung der Arbeitnehmer zu überwachen, mitbestimmungspflichtig. Eine Betriebsvereinbarung kann Rechtsgrundlage für die Verarbeitung von Arbeitnehmerdaten sein und ist damit ein wichtiges datenschutzrechtliches Gestaltungsinstrument. Für die Betriebsräte wird es daher immer wichtiger, sich auch in Fragen des Datenschutzes bzw. bei technischen Zusammenhängen auszukennen bzw. sich umfassend hierüber zu informieren.

5.6.1 GPS-Tracking bei Fahrzeugen im Außendienst

In einem Unternehmen sollte eine Betriebsvereinbarung über den Einsatz eines GPS-Tracking-Systems in die Fahrzeuge der Außendienstmitarbeiterinnen und -mitarbeiter geschlossen werden.

Das GPS-Tracking-System dient dem zügigen und koordinierten **Einsatz von Servicefahrzeugen**, die bei Notrufen aus Aufzügen losgeschickt werden. Zudem sollte der Einsatz der gesamten Fahrzeugflotte aus wirtschaftlicher Sicht optimiert werden. Das Unternehmen versprach sich von dem System auch die Erstellung elektronischer Fahrtenbücher, die Nachweisführung der Anwesenheit von Monteuren gegenüber Kunden und einen besseren Diebstahlschutz.

Das GPS-Tracking-System erfasst lückenlos Standort und Route der überwachten Fahrzeuge, welche die Beschäftigten auch außerhalb der Dienstzeit für die An- und Abfahrt zum Dienstort nutzen dürfen. Besondere Brisanz des Systems ergibt sich dadurch, dass neben Aufenthalt und **Route der Fahrzeuge weitere technische Angaben**, z. B. Betriebszustand des Motors, Drehzahlbereiche und Bremsverhalten, erhoben und verarbeitet werden können. Der Hersteller bewirbt das Produkt offensiv mit diesem „Vorteil“. Derart durch das System erhobene Daten sind personenbeziehbar. Positiv hervorzuheben ist ein „Privat-Schalter“ im System.

Bei der Gestaltung der Betriebsvereinbarung war darauf zu achten, dass die Daten nicht für eine **Leistungs- und Verhaltenskontrolle** der Beschäftigten eingesetzt würden. Ein zulässiger, weil gesetzlich vorgesehener Zweck ist das Führen des elektronischen Fahrtenbuches. Als berechtigt anerkannt und in der Betriebsvereinbarung geregelt wurden die Einsatzkoordinierung für den Notfall (Notrufleitanbindung und Störungseinsatzsteuerung) sowie die Sicherung des Eigentums (Diebstahlschutz). Für diese Zwecke ist jedoch nur die kurzfristige und nicht dauerhafte Erfassung des Aufenthaltsortes des Fahrzeuges und keine Erhebung von Betriebsdaten erforderlich.

Das Unternehmen hat grundsätzlich ein **berechtigtes Interesse** an der wirtschaftlichen Optimierung des Flotteneinsatzes. Eine dauerhafte Überwachung der Beschäftigten und die Erhebung und Verarbeitung von Daten über Privatfahrten lässt sich mit diesem Zweck allerdings nicht rechtfertigen. Auch Wettbewerbsvorteile, welche durch den Einsatz des Systems erzielt werden sollen, rechtfertigen

nicht die lückenlose Überwachung der Beschäftigten. Es muss vielmehr für diese transparent werden, welche Daten durch das GPS-System erhoben und verarbeitet werden und zu welchen Zwecken dies geschieht.

Wenn es um die Optimierung des Einsatzes von Fahrzeugen, z. B. Verminderungen von Fahrtzeiten zum nächsten Einsatzort, geht, genügt eine Erhebung der Position in Echtzeit. Eine Speicherung ist **nicht erforderlich**. Sollen zusätzlich statistische Erkenntnisse gewonnen werden, so reicht eine Auswertung aggregierter Daten ohne Personenbezug aus. Die Erhebung von Informationen über Privatfahrten bei erlaubter Privatnutzung des Fahrzeuges ist grundsätzlich nicht erforderlich und gesetzlich verboten. Für die Beschäftigten muss insgesamt transparent sein, welche Daten zu welchen Zwecken bei der Nutzung der mit GPS-Technik ausgestatteten Fahrzeuge anfallen und wer Zugriff auf diese Daten erhält.

Die Betriebsvereinbarung war um die folgenden **Punkte zu ergänzen**:

- die konkrete Festlegung der Zwecke des Einsatzes des GPS-Tracking-Systems und das Verbot der Nutzung der Daten zur Leistungs- und Verhaltenskontrolle,
- die Installation einer technischen Einrichtung zur Begrenzung der Datenerhebung während der Privatfahrten („Privat-Schalter“),
- die konkrete Nennung der zu erhebenden Daten unter Begrenzung auf die erforderlichen Parameter (Ausschluss von Betriebsdaten) und das Verbot der Ausweitung der Erhebung weiterer Datenarten (Datensparsamkeit),
- die Nennung der zugriffsberechtigten Personen anhand des Zwecks des Einsatzes des Systems und die Pflicht zur restriktiven Vergabe der Zugriffsrechte,
- eine Benachrichtigungspflicht des Unternehmens und die Auskunftsrechte der Beschäftigten,
- die Begrenzung der Speicherfristen auf das für den jeweiligen Zweck erforderliche Maß und
- die Pflicht zur Aggregierung der erhobenen Daten mit dem Ziel der Vermeidung einer Profilbildung.

Was ist zu tun?
Beim Einsatz von GPS-Technik ist konkret zu überprüfen, welche Daten erhoben werden und ob diese für den angestrebten Zweck überhaupt erforderlich sind.

5.6.2 Erstellung einer Rahmenbetriebsvereinbarung

Der Einsatz von Kommunikationstechnik kann in einer Rahmenbetriebsvereinbarung zur Datenverarbeitung geregelt werden.

Die **Rahmenbetriebsvereinbarung** des Gesamtbetriebsrates sollte einen grundsätzlichen Rahmen für den Einsatz von technischen Einrichtungen und Methoden abstecken, bei denen Daten von Beschäftigten verarbeitet werden und die die Überwachung von deren Leistung und Verhalten ermöglichen. Die einzelnen Bereiche sollten dann durch konkrete Einzelbetriebsvereinbarungen konkretisiert werden.

Eine Rahmenbetriebsvereinbarung kann zunächst allgemeine Weichen für einen datenschutzkonformen Einsatz von technischen Einrichtungen und Methoden am Arbeitsplatz stellen. Konkret zeigte sich erneut, dass zum Teil elementare Grundsatzfragen bei dem Einsatz von technischen Betriebsmitteln vor Erstellung der Vereinbarung geklärt und festgelegt werden mussten. Ganz oben steht die Frage, ob die **Privatnutzung von Kommunikationsmitteln** am Arbeitsplatz zulässig sein soll oder nicht, da die Antwort hierauf Ausstrahlungswirkung in alle Bereiche der Datenverarbeitungsbefugnisse des Arbeitgebers rund um den Mitarbeitercomputer hat.

Die Beteiligung des **betrieblichen Datenschutzbeauftragten** wird sowohl im Erstellungsprozess einer Betriebsvereinbarung als auch hinsichtlich der zu vereinbarenden Kontrollrechte oft vergessen. Gerade in komplexen Datenschutzfragen sollte sich der Betriebsrat der Expertise des Datenschutzbeauftragten bedienen und diesen aktiv einbinden.

Weitergabe von Mitarbeiterdaten im Konzern

Wenn personenbezogene Mitarbeiterdaten an eine Konzernmutter übermittelt werden sollen, ist die Betriebsvereinbarung als Gestaltungsinstrument besonders wichtig. Im Datenschutzrecht gibt es kein Konzernprivileg, d. h., die Übermittlung von Mitarbeiterdaten an die Konzernmutter ist nach den gleichen Datenschutzprinzipien zu prüfen, die für eine Weitergabe an eine Stelle außerhalb des Konzerns gelten. Soll die Datenverarbeitung nicht im Wege der Auftragsdatenverarbeitung erfolgen, muss eine explizite Rechtsgrundlage vorliegen. Die Einwilligung als Rechtfertigung der Datenübermittlung scheidet mangels Freiwilligkeit im Arbeitsverhältnis in der Regel aus.

Eine Betriebsvereinbarung kann die Grundlage für eine Datenübermittlung im Konzern schaffen, wenn gewährleistet ist, dass die Datenschutzrechte der betroffenen Arbeitnehmer ausreichend geschützt werden. Beim internationalen Datenverkehr ist zudem zu beachten, dass eine Datenübermittlung an einen Empfänger außerhalb der Europäischen Union oder eines Vertragsstaates der Europäischen Union nur gestattet ist, wenn gemäß den Vorgaben der Europäischen Datenschutzrichtlinie (95/46/EG) ein angemessenes Datenschutzniveau beim Empfänger gewährleistet ist oder bestimmte Ausnahmetatbestände vorliegen.

Als Erstes ist allerdings immer zu überprüfen, ob die Übermittlung von Arbeitnehmerdaten an einen Dritten, egal wo dieser seinen Sitz hat, überhaupt zulässig ist.

5.7 Einzelfälle

5.7.1 Inkasso im Verein

Um säumige Mitglieder, bei denen die dritte Mahnung erfolglos blieb, zur Zahlung des Mitgliedsbeitrags zu bewegen, vermerkte ein Sportverein diese Mitglieder auf einer Mahnliste.

Ein Sportfreund staunte, als er von einem Vereinskollegen gefragt wurde, ob er auf der sogenannten „Mahnliste“ stünde. Verärgert aufgrund dieser peinlichen Situation, fragten er und seine Frau beim Vorstand des Sportvereins nach. Die Erstellung dieser Liste erwies sich als gängige Praxis. Die Liste erhielten **alle Abteilungsleiter**, welche die jeweiligen Mitglieder in einem persönlichen Gespräch auf die Säumnis ansprechen sollten. Über die Ansprache durch eine dem Betroffenen bekannte Person, zu der vielleicht gar eine persönliche Bindung besteht, könnte eine individuelle Lösung bei Zahlungsengpässen gesucht und gefunden und sollte ein sofortiger Ausschluss säumiger Vereinsmitglieder vom Sportbetrieb nach erfolgloser dritter Mahnung vermieden werden. Weil für den Verein nicht nachvollziehbar war, welche Mitglieder in welchen Abteilungen Sport treiben – alle Mitglieder können ohne spezifische Anmeldung alle Angebote im Verein nutzen –, wurden die Listen mit allen säumigen Mitgliedern an alle Abteilungsleiter übergeben. Damit erhielten diese Kenntnis über die Säumnis auch der Mitglieder, die mit der eigenen Abteilung nichts zu tun hatten. Die Aufnahme des äußerst bestürzten Ehepaars in die Mahnliste, so stellte es sich nach der Prüfung heraus, war auf Probleme im Buchungssystem beim Einzug des Familienbeitrags zurückzuführen.

Bei der Offenbarung von Informationen zur finanziellen Situation und insbesondere z. B. über die Zahlungssäumigkeit besteht die besondere Gefahr einer Stigmatisierung der Betroffenen. Diese haben grundsätzlich ein schutzwürdiges Interesse am vertraulichen Umgang mit diesen Informationen. Ein Auslegen von Listen säumiger Vereinsmitglieder zur Erzeugung eines gewissen Zahlungsdrucks ist unzulässig. Auch die Aushändigung der Mahnlisten an alle Abteilungsleiter war nicht erforderlich. Zunächst muss geprüft werden, ob ein Abteilungsleiter gefunden werden kann, der das Vereinsmitglied direkt auf den ausstehenden Beitrag ansprechen kann. Nur wenn dies nicht möglich ist, kann eine abteilungsübergreifende Mahnliste zur Verhinderung von Inkassoverfahren unter **eingrenzenden Voraussetzungen** zum Einsatz kommen:

- Es muss durch ein zuverlässiges Verfahrensmanagement hinsichtlich der mehrfachen erfolglosen Mahnungen sichergestellt werden, dass nur tatsächlich säumige Vereinsmitglieder auf der Liste stehen.
- Die Aufnahme in die Mahnliste darf frühestens nach der zweiten erfolglosen Mahnung erfolgen.
- Die Abteilungsleiter als Empfänger der Liste sind schriftlich auf das Datengeheimnis zu verpflichten.

- Den Abteilungsleitern sind präzise Hinweise zu geben, wie sie mit der Liste zu verfahren haben, etwa bei der vertraulichen Ansprache des Vereinsmitglieds oder in Bezug auf die Pflicht zur Löschung bzw. Vernichtung der Liste nach Gebrauch.

Was ist zu tun?
Im Umgang mit sensiblen Informationen muss im Verein der Grundsatz der Datensparsamkeit besonders ernst genommen werden. Vor einem breiten Streuen von Informationen muss geprüft werden, wie durch Konkretisierungen der Empfängerkreis auf das unbedingt erforderliche Maß eingeschränkt werden kann.

5.7.2 Faires Verfahren bei Kreditangeboten

Wer von einer Bank einen Kredit haben will, wird für diese zwangsläufig von einer oder mehreren Auskunfteien hinsichtlich der Kreditwürdigkeit durchleuchtet. Bonitätsanfragen haben für die Betroffenen weitreichende Konsequenzen. Zwischen verbindlichen und unverbindlichen Kreditangeboten muss klar unterschieden werden.

Holt eine Bank im Falle eines **Kreditgesuchs** eine Bonitätsauskunft ein, so wird diese Anfrage bei der Auskunftei gespeichert, auf Anfrage auch an Dritte, z. B. an andere Kreditinstitute, beauskunftet und fließt möglicherweise in die Berechnung eines Scorewertes ein. Dies konnte sich früher nachteilig für die Betroffenen auswirken, wenn sie innerhalb kurzer Zeit bei mehreren Banken Kreditangebote einholten. Aus der Vielzahl der Anfragen wurde auf eine schlechte Bonität geschlossen. Je mehr Anfragen, umso schlechter die Bewertung und umso ungünstiger die angebotenen Kreditkonditionen.

Im Jahre 2006 wurde – zumindest bei der größten Verbraucherauskunftei, der Schufa – auf Druck der Datenschutzaufsichtsbehörden Abhilfe geschaffen. Die Schufa unterschied von da an zwischen einer Kredit- und einer **Konditionenanfrage**. Bei einer Konditionenanfrage übermittelt die Schufa auf Anfrage an die Bank bestimmte Daten über den Kunden zur Berechnung unverbindlicher Kreditkonditionen. Diese Anfrage fließt nicht in die Scoreberechnung ein und wird auch nicht an Dritte übermittelt. Holt der Betroffene danach mehrere Kreditangebote bei verschiedenen Banken ein, um diese vergleichen zu können, hat die Auskunfteianfrage der ersten Bank keine Auswirkung auf die folgenden Anfragen – die Einholung vergleichbarer Angebote ist also möglich. Konditionenanfragen können ohne schriftliche Einwilligung des Betroffenen von der Bank eingeholt werden. Hier besteht ein beiderseitiges Interesse, dass dem potenziellen Kreditnehmer reale Kreditkonditionen berechnet werden können, ohne dass der Betroffene dadurch Folgenachteile hat.

Anders bei **Kreditanfragen**. Hier übermittelt die Schufa auf Anfrage der Bank auch Daten zur Berechnung der Kreditkonditionen, jedoch zur Erstellung eines für den Kunden verbindlichen Angebots. Anders als bei einer Konditionenanfrage wird das Merkmal „Kreditanfrage“ für 10 Tage von der Schufa gespeichert und

des Weiteren an Dritte übermittelt. Außerdem fließt dieses Datum für ein Jahr in den Scorewert ein. Die Anfrage an die bzw. Übermittlung der Daten von der Schufa ist daher bisher nur auf der Grundlage einer Einwilligung des Betroffenen zulässig (zur künftigen Rechtslage siehe Tz. 5.1.2).

In der Praxis fehlte es allerdings an einer konsequenten Umsetzung dieses Verfahrens. In einem Fall hatte die Bank vorgesehen, dass der Kunde sowohl für eine Konditionenanfrage als auch für eine Kreditanfrage eine Einwilligung in Form der Schufa-Klausel unterschreibt. Zwar hatte die Bank tatsächlich nur eine Konditionenanfrage durchgeführt, für den Kunden war aber nicht ersichtlich, welche der beiden Abfragen durchgeführt worden ist. Der Betroffene muss wissen, in welche Anfrage er genau einwilligt und welche Folgen diese für ihn hat. Bei einer Konditionenanfrage kann die Bank ganz auf eine Einwilligung verzichten, was sie jedoch nicht davon entbindet, den Kunden über die Datenerhebung zu informieren. Die Bank konnte zudem nicht im Einzelnen darlegen, nach welchen **Kriterien eine Abgrenzung** zwischen den beiden Anfragen erfolgt. Da jede „versehentlich“ als Kreditanfrage gemeldete Konditionenanfrage empfindliche Nachteile für die Betroffenen nach sich ziehen kann, ist eine klare Unterscheidung unerlässlich.

Für die **Betroffenen** ist es wichtig zu wissen, dass es zwei verschiedene Arten von Bonitätsauskünften bei der Erstellung eines Kreditangebotes gibt. Möchte der Betroffene zunächst nur Konditionenauskünfte einholen, um den Markt zu sondieren und ohne einen verbindlichen Kreditantrag zu stellen, sollte er die Banken darauf hinweisen, dass er seine Anfrage als Konditionenanfrage verstanden wissen will.

Was ist zu tun?
Nach den neuen, ab 2010 geltenden Vorschriften des BDSG zur Datenübermittlung an Auskunfteien bleibt die Unterscheidung zwischen Konditionen- und Kreditanfrage bestehen. Banken und Auskunfteien müssen klare und transparente Verfahren festlegen, die eine Diskriminierung von vergleichenden selbstbewussten Verbrauchern verhindern.

5.7.3 Die Gehaltsliste fürs Frühstück

Die Mitarbeiterin eines mittelständischen Unternehmens war verwundert, als sie im Frühstücksraum ihrer Firma eine Liste mit Namen und detaillierten Gehaltsangaben einer Vielzahl ihrer Kollegen inklusive ihrer eigenen Daten vorfand.

Zunächst stand im Raum, der Betriebsrat habe auf diese außergewöhnliche Weise Arbeitnehmerdaten veröffentlicht. Er lehnte die **Verantwortung** für die Auslage der Gehaltsliste ab und zeigte zugleich Interesse daran, dass sich Derartiges nicht wiederholt. Nach Darstellung der Geschäftsführung waren die Gehaltsdaten lediglich verfahrensbezogen einem Richter zur Durchführung eines Schlichtungsverfahrens in einer Tarifauseinandersetzung überlassen worden.

Es stellte sich heraus, dass die betreffende Gehaltsliste Gegenstand eines sich zwischen der Geschäftsführung des Unternehmens und der zuständigen Gewerkschaft verhandelten sogenannten **Anerkennungstarifvertrages** war. Mit einem solchen Verfahren sollen die generell in einer bestimmten Branche bestehenden Tarifverträge durch einen eigentlich nicht tarifgebundenen Arbeitgeber übernommen werden. Die im Verfahren erstellte Schlichtungsvereinbarung enthielt im Anhang die in Rede stehende personenbezogene Gehaltsliste und wurde für Zwecke der Urabstimmung den abstimmenden Gewerkschaftsmitgliedern zur Verfügung gestellt. Auf diese Weise erfuhren die an der Urabstimmung teilnehmenden Mitarbeiter die Gehaltsdaten sämtlicher ebenfalls gewerkschaftlich organisierter Kollegen.

Die Datenübermittlung war nicht erforderlich. Das ULD wird sich dafür einsetzen, dass entsprechende Urabstimmungen künftig ohne die Preisgabe von personenbezogenen Arbeitnehmerdaten durchgeführt werden. Dies kann z. B. dadurch erreicht werden, dass die zur Veröffentlichung bestimmten Exemplare einer Schlichtungs- oder einer Tarifvereinbarung entweder keine Anlage mit personenbezogenen Daten enthalten oder diese **Angaben geschwärzt** werden. Durch diese Anonymisierung verliert eine Tarifvereinbarung nicht an Aussagekraft.

Was ist zu tun?
Zwischen den Tarifparteien sollte für die Durchführung von Urabstimmungen in den Betrieben ein datenschutzfreundliches Verfahren zur Anwendung kommen, bei dem die Bekanntgabe von Personendaten in Schlichtungsergebnissen gegenüber den abstimmenden Gewerkschaftsmitgliedern vermieden wird.

5.7.4 Ehekrise wegen telefonischer Versicherungsauskunft

Die telefonische Auskunft einer Versicherungsgesellschaft an die Ehefrau eines Versicherungsnehmers über einen inzwischen abgelaufenen und ausgezahlten Lebensversicherungsvertrag ihres Mannes führte zu ehelichen Auseinandersetzungen zwischen dem Versicherungsnehmer und dessen Ehefrau.

Ein Bürger hatte im Jahre 2002 einen seinerzeit bestehenden Lebensversicherungsvertrag aufgelöst und sich den Rückkaufswert auf sein Konto überweisen lassen. So weit, so gut. Im Jahre 2008 stieß seine Ehefrau beim Aufräumen auf die alten Vertragsunterlagen ihres Mannes, von deren Existenz sie offensichtlich

keine Kenntnis hatte, und **erkundigte sich telefonisch** bei der Versicherungsgesellschaft nach den Einzelheiten des Vertrages einschließlich der Vertragsabwicklung und Auszahlung des Guthabens. Der Ehemann beschwerte sich beim ULD über die telefonische Auskunftserteilung durch die Versicherung.

Die Lebensversicherungsgesellschaft gab an, sie könne das mit der Ehefrau des Versicherungsnehmers geführte Telefonat nicht mehr nachvollziehen. Es müsse sich um einen Irrtum des zuständigen Sachbearbeiters gehandelt haben. Nach einer schon vor dem Vorfall geltenden unternehmensinternen Weisung waren die Beschäftigten gehalten, sich bei telefonischen Auskünften von der **Identität des Anrufers** bzw. der Anruferin zu überzeugen.

Das ULD hat die Auskunft an die Ehefrau gegenüber dem Versicherungsunternehmen beanstandet und eine erhöhte Sicherheit bei fernmündlichen Auskünften angemahnt. Die Mitarbeiterinnen und Mitarbeiter im Service Center wurden, so das Unternehmen, noch einmal eindringlich auf die Problematik der Telefonauskünfte hingewiesen. Die **betriebsinternen Datenschutzrichtlinien** wurden aktualisiert und neu veröffentlicht. Danach bekommen Ehepartner jetzt überhaupt keine telefonischen Auskünfte mehr. Bei Telefonauskünften an den Versicherungsnehmer bzw. Vertragspartner selbst wird versucht, durch gezielte Fragen nach der Versicherungsnummer und dem Geburtsdatum Gewissheit über die Identität des Anrufenden zu gewinnen. Nach Information des ULD haben sich die Eheleute wieder vertragen.

Was ist zu tun?
Unberechtigte telefonische Auskünfte von Unternehmen zu Vertragsdaten ihrer Kunden sind Auslöser unterschiedlichster Konflikte. Es bedarf hierzu klarer innerbetrieblicher Weisungen. Durch Rückfragen kann die Identität der Anrufenden überprüft werden. Auch individuelle Passwörter oder andere Absprachen können die Gefahr unberechtigter Telefonauskünfte verringern. Im Zweifel dürfen keine telefonischen Auskünfte erteilt werden.

5.7.5 Tanzkurs: „Du kommst hier nicht rein!“

Ein Auszubildender einer Tanzschule wollte zwecks Vervollkommnung seiner Fähigkeiten bei einer anderen Tanzschule in der gleichen Stadt einen Tanzkurs belegen. Doch hatte er die Rechnung ohne den Wirt gemacht.

Mit der Bemerkung „Sie können bei uns keinen Kurs besuchen, weil Sie bei unserem Konkurrenzunternehmen in einem Arbeitsverhältnis stehen!“ hätte der Auszubildende vielleicht leben können. Wegen eines früheren geschäftlichen Konflikts zwischen den beiden Tanzschulen war nämlich im Jahre 2007 ein generelles Hausverbot für Mitarbeiter der anderen Seite erteilt worden. Als er jedoch erfuhr, dass die Tanzschule seinen Arbeitgeber per **E-Mail über den versuchten tänzerischen Ausflug** zur Konkurrenz informiert hatte, fühlte er sich massiv verletzt.

„Er hätte von dem ausgesprochenen Hausverbot wissen müssen“, meinte die Daten übermittelnde Tanzschule. Doch eine Rechtsgrundlage für die mittels E-Mail vorgenommene Datenübermittlung an den Arbeitgeber konnte sie nicht vorweisen. Das ULD hat die **unzulässige Datenübermittlung** beanstandet. Die Tanzschule entschuldigte sich beim Petenten für die Datenweitergabe.

Was ist zu tun?
Hausverbote sind keine Rechtsgrundlage für die Übermittlung personenbezogener Daten an Dritte.

5.7.6 Verantwortungslose Wahlwerbung

Wahlwerbung erreicht uns heutzutage auch per elektronischer Post. Werbung mittels E-Mail und SMS ist nur zulässig, wenn eine explizite Einwilligung des Empfängers vorliegt.

Während des zeitgleichen Bundestags- und Landtagswahlkampfes erreichten uns vielfältige Beschwerden wegen Wahlwerbung per SMS und E-Mail. Die Petenten schilderten, dass sie am Tag vor den Wahlen eine Werbe-SMS von einer Partei mit der **Aufforderung des Spitzenkandidaten** erhielten, seiner Partei die Stimme zu geben. Die Partei hatte sowohl auf Bundes- als auch Landesebene zum Zweck der Durchführung von Wahlwerbung ein parteinahes Unternehmen in Berlin beauftragt. Dieses bediente sich wiederum eines Unternehmens in Baden-Württemberg. Für die Werbeaktion wurden die Daten des baden-württembergischen Unternehmens sowie von fünf weiteren Kooperationspartnern in Deutschland und Österreich verwendet. Diese Partner hatten die E-Mail-Adressen und SMS-Nummern teilweise wiederum von Dritten bezogen.

Einen direkten Zugriff auf die Adressdaten hatte weder die Partei auf Bundes- noch auf Landesebene. Alleinige Dateninhaber waren teilweise das Unternehmen in Baden-Württemberg sowie teilweise deren Partner, die diesem gegenüber versichert haben sollen, dass Einwilligungen zur Datennutzung vorlägen. Die Vertreter der Partei teilten mit, sie seien **davon ausgegangen**, dass die Dienstleister bei ihren Werbemaßnahmen rechtmäßig vorgehen würden. Das schwäbische Unternehmen hatte es unterlassen, das Vorliegen der Einwilligungen auch nur stichprobenweise zu überprüfen; eine solche Prüfung war im Vertrag mit dem Unternehmen in Berlin auch nicht vorgesehen.

Für eine Nutzung von E-Mail-Adressen und Handynummern zum Zweck der Werbung ist datenschutzrechtlich wie wettbewerbsrechtlich eine **ausdrückliche Zustimmung** erforderlich, die nur durch eine gesondert abzugebende Erklärung, ein sogenanntes Opt-In, erteilt werden kann. Das Vorliegen der Einwilligung des Empfängers hat das Daten verarbeitende und nutzende Unternehmen zu beweisen. Die Datenschutzaufsichtsbehörde Baden-Württemberg teilte uns mit, die Daten hätten ursprünglich u. a. aus Internetangeboten gestammt, in denen sich die Webseitenbetreiber über allgemeine Geschäftsbedingungen die Werbenutzung erlauben ließen. Die Verantwortlichkeiten seien in den Auftragsverträgen nicht eindeutig geregelt.

Die Partei hatte den Inhalt der Werbung vorgegeben, ohne selbst in den Besitz der Daten zu kommen. Die Abwicklung der Werbeaktion war vollständig an das Unternehmen in Berlin ausgelagert worden, das wiederum die Baden-Württemberger einschaltete, welche wieder weitere Unternehmen einbezog, die wiederum von anderen Unternehmen Daten erhalten hatten. **Adressinhaber** waren ausschließlich die baden-württembergische Firma und deren Kooperationspartner. Diese sind dafür verantwortlich und nachweispflichtig, dass ausdrückliche Einwilligungserklärungen der SMS-Empfänger vorliegen.

Die **Partei** ist nicht frei von Verantwortung: Wenn sie einen Dritten mit der Durchführung von Werbeaktionen beauftragt, dann hat sie diesen Dienstleister sorgfältig auszuwählen und vertraglich sicherzustellen, dass ausschließlich Adressdaten verwendet werden, bei denen eine ausdrückliche Einwilligung in die Nutzung für elektronische Werbung vorliegt und nachgewiesen werden kann. Dies dient auch dem eigenen Image: Die Partei geht aus der Werbung als Urheber hervor und sollte ein ureigenes Interesse daran haben, keine Personen mit unverlangter elektronischer Post zu belästigen.

Was ist zu tun?
Bei elektronischer Werbung ist eine ausdrückliche Einwilligung des Empfängers erforderlich. Werden zum Zweck der Durchführung von Werbeaktionen Dritte beauftragt, ohne dass dabei im rechtlichen Sinne Datenübermittlungen erfolgen, ist zu vereinbaren, dass nachweisbar nur mit ausdrücklicher Einwilligung erhobene Daten verwendet werden.

5.7.7 Bewerbungsfotos im Schulungssystem

Eine Fortbildungseinrichtung stellte die Bewerbungsbilder von Kursteilnehmern ins allgemein zugängliche Schulungssystem. Die Kontaktdaten der Teilnehmer wurden genutzt, um Vermittlungsgespräche zu vereinbaren.

Die Teilnehmerin eines **Bewerbungstrainings** bei einer privaten Fortbildungseinrichtung war über digitale Bewerbungsbilder aller Kursteilnehmer im für alle zugänglichen Schulungssystem der Einrichtung erstaunt. Die Bilder wurden im Rahmen eines freiwilligen Fototermins vom Kursleiter gefertigt. Dieser legte einen Ordner mit den Bildern auf einem gemeinsamen Laufwerk an. Die Teilnehmer sollten dann ihre Bilder einsehen und auf ein eigenes, externes Speichermedium übertragen. Nach Angaben der Fortbildungseinrichtung wurden alle Kursteilnehmer darauf hingewiesen, sich eigenverantwortlich um das Löschen der Bilder sowie anderer Dokumente mit Personenbezug im Schulungssystem zu kümmern. In der verwendeten „Verpflichtungserklärung zur EDV-Nutzung“ fand sich dieser Hinweis aber damals noch nicht. Kursteilnehmer konnten also bis zur Löschung der Dokumente Fotos anderer Teilnehmer auf ein eigenes Speichermedium übertragen und später anderweitig verwenden – manchmal wurde die Löschung sogar ganz vergessen.

Die Teilnehmerin des Bewerbungstrainings beschwerte sich auch darüber, dass sie von der Fortbildungseinrichtung telefonisch und per E-Mail kontaktiert worden war, um einen Termin für ein Vermittlungsgespräch zu vereinbaren. Hintergrund ist, dass die Fortbildungseinrichtung auch Dienstleistungen zur Vermittlung auf dem Arbeitsmarkt erbringt. Daten dürfen aber nur für den Zweck verwendet werden, für den sie erhoben wurden. Hier hatte die Fortbildungseinrichtung die Daten der Teilnehmerin für die Durchführung des Bewerbungstrainings erhoben. Einer Nutzung ihrer Daten für andere Zwecke hatte die Petentin nicht zugestimmt, insbesondere hatte sie keine Einwilligung hinsichtlich einer Kontaktaufnahme zur **Vereinbarung eines Vermittlungsgesprächs** erteilt.

Was ist zu tun?
In Schulungssystemen müssen zugriffsgeschützte Bereiche für die Kursteilnehmer eingerichtet werden. Das Verfahren für die Kursteilnehmer muss transparent sein. Auf die Konsequenzen bei bestehenden Zugriffsmöglichkeiten auf Personendaten muss hingewiesen werden. Nach der Beendigung einer Schulung ist die Löschung von Teilnehmerdaten sicherzustellen. Kontaktaufnahmen zur Vereinbarung eines Vermittlungsgesprächs bedürfen der Einwilligung der Schulungsteilnehmer.

5.7.8 Bonitätsabfragen beim Tierarzt

Ist des Menschen bester Freund krank, soll ein Tierarzt schnell helfen. Da dieser seine verfügbare Zeit lieber dem kranken Tier als dem Abrechnungsaufwand in seiner Praxis widmen möchte, wird die Abrechnung zunehmend an externe Dienstleister übertragen.

Dienstleister wollen sichergehen, dass sie ohne großen Aufwand schnell an das Geld kommen. Aus diesem Grund wurde in einer Tierarztpraxis bei jedem Besuch, der nicht bar beglichen wurde, eine Bonitätsabfrage gestartet. So sollten schwarze Schafe im Vorwege erkannt werden. Will sich der Tierarzt die Abrechnungsmodalitäten erleichtern und schaltet einen externen Dienstleister ein, so legitimiert dies noch nicht standardmäßige Bonitätsabfragen. Eine Einwilligung ist erforderlich. Ein finanzielles Ausfallrisiko des Tierarztes kann z. B. durch Vorauszahlung ausgeschlossen werden. Tierbesitzer müssen vor der Inanspruchnahme einer Bezahlung per Rechnung über die damit eventuell verbundenen Auswirkungen wie Abwicklung durch einen Dritten sowie Durchführung einer Bonitätsabfrage informiert werden. Als **Alternative** muss Barzahlung bzw. Vorkasse ermöglicht werden.

Was ist zu tun?
Eine Bonitätsabfrage bei einer Auskunftei ist nur gesetzlich gerechtfertigt, wenn ein finanzielles Ausfallrisiko besteht, d. h., wenn das Unternehmen nicht unerheblich in Vorleistung geht. Auch dann sind aber die schutzwürdigen Belange der Betroffenen zu wahren.

5.7.9 Datenschutzrechtliches Trauerspiel bei der Dopingprävention

Der Radsportverband Schleswig-Holstein verlangte von Personen, die eine Radrennlizenz beim dafür zuständigen Bundesverband beantragten, die Unterzeichnung der „Nutzungsbedingungen für Rennlizenzen".

Diese Nutzungsbedingungen verpflichteten zur Meldung von „**verschreibungspflichtigen Medikamenten** und Arzneimitteln unter Angabe des Handelsnamens und der Wirkstoffkombination an den Verband". Die Meldung sollte per E-Mail an eine angegebene Adresse erfolgen. Das Formular wies darauf hin, dass der Anti-Dopingbeauftragte des Landesverbandes zur Verschwiegenheit gegenüber Dritten verpflichtet sei. Die meldenden Sportlerinnen und Sportler sollten eine Rückmeldung erhalten, ob die Medikamente aus Sicht des Dopingbeauftragten eingenommen werden dürfen. Der Landesverband machte die Zustimmung zu diesen Nutzungsbedingungen zur Voraussetzung für die Erteilung der Lizenz, die vom Bundesverband unter Anerkennung der nationalen Regularien der nationalen und der internationalen Anti Doping Agentur, also der NADA und der WADA, vergeben wird. Der Landesverband entscheidet also inhaltlich nicht über die Erteilung der Lizenz, sondern fungiert als Mittler zwischen Bundesverband und Lizenzfahrer.

Der Petent weigerte sich, die vom schleswig-holsteinischen Verband geforderte Erklärung zu unterzeichnen, sodass ihm die bereits durch den Bundesverband erteilte Lizenz vom Landesverband nicht weitergeleitet wurde. Das Tätigwerden des ULD führte zur **Veröffentlichung des Namens** des Petenten in einem Bericht von der Hauptversammlung des Verbandes im Internet: Darin wurde vom namentlich genannten Petenten und dessen Verein berichtet. Er bereite dem Landesverband zusehends Probleme und nähme die Arbeit der ehrenamtlich Tätigen über Gebühr in Anspruch; er habe den Verband beim Datenschutz „angezeigt".

Das ULD beanstandete die erzwungene Einholung der Einwilligung und die Internetveröffentlichung. Nach Intervention des ULD wurde der Name des Petenten aus dem Internet entfernt und auf das Abfordern der Einwilligung verzichtet. Unabhängig von der datenschutzrechtlichen Bewertung der Regularien der NADA und WADA war das Vorgehen des Sportverbandes unzulässig. Die **Zulässigkeit einer Einwilligungserklärung** setzt die Information der Betroffenen, die Freiwilligkeit der Erteilung und die Widerruflichkeit voraus.

Im konkreten Fall fehlte es bereits am Erfordernis der Information über Art, Umfang, Zweck und Dauer der Datenverarbeitung. Die **Erklärung informierte nicht** über mögliche Konsequenzen einer Einmeldung. Unklar blieb, aus welchem Grund nur verschreibungspflichtige Medikamente zu melden waren. Der Unterschied zwischen Medikament und Arzneimittel wurde nicht erläutert. Besondere Brisanz lag darin, dass die verschriebenen Medikamente Rückschlüsse auf die Gesundheit des Athleten ermöglichten. In der Einwilligungserklärung hätte die hohe Datensensibilität berücksichtigt werden müssen.

Einwilligungen dürfen grundsätzlich **nicht erzwungen** werden. Die Sportlerinnen und Sportler unterwerfen sich bei der Beantragung der Lizenz den Vorgaben der NADA und der WADA. Einer zusätzlichen zwingenden Landesregelung bedurfte es zur Verhinderung des Dopings nicht. Die Erlaubniserteilung zur Datenübermittlung war somit unfreiwillig und daher unzulässig.

Zudem fehlte es an den notwendigen organisatorischen und technischen Maßnahmen der Datensicherheit. Die Übermittlung sensibler **Gesundheitsdaten mittels E-Mail** entspricht dem Versenden einer Postkarte gleichen Inhalts. Die Ermöglichung einer verschlüsselten Übermittlung durch Bereitstellung einer entsprechenden Infrastruktur wäre das Mindeste gewesen.

Das Einfordern der Einhaltung von Datenschutzgesetzen ist **kein querulatorischer Akt**. Petenten nehmen ihr verfassungsrechtlich verbrieftes Recht auf Privatsphäre und Schutz ihrer Daten wahr. Weder der unterstützenswerte Kampf gegen Doping im Sport noch die anzuerkennende ehrenamtliche Tätigkeit rechtfertigen einen Verstoß gegen die Grundrechte und das An-den-Pranger-Stellen derjenigen, die die Beachtung dieser Rechte einfordern.

Was ist zu tun?
Beim Kampf gegen Doping sind die Privatsphäre der Sportlerinnen und Sportler und die Vorgaben des Bundesdatenschutzgesetzes zu beachten.

5.7.10 Kfz-Kennzeichen vor dem Lebensmittelladen

Ein Kunde beschwerte sich, dass sein Kfz-Kennzeichen von einem privaten Wachmann vor der Filiale einer großen Lebensmittelkette notiert wurde. Der Ladeninhaber konnte ein berechtigtes Interesse an der Erhebung der Daten geltend machen.

Die Nutzung des unternehmenseigenen Parkplatzes ist gemäß deutlich sichtbaren Schildern nur für Kundinnen und Kunden und nur für die Dauer von einer Stunde erlaubt. Bei **widerrechtlichem Parken** wird ein Abschleppen des Fahrzeuges angedroht. Der Lebensmittelhändler hatte festgestellt, dass wiederholt Nichtkunden den Parkplatz nutzen, und beauftragte deshalb einen Sicherheits- und Wachdienst mit der Kontrolle der parkenden Autos. Die Wachleute notierten handschriftlich die Kfz-Kennzeichen mit Ankunfts- und Abfahrtszeiten. Die so erhobenen Daten werden täglich gelöscht und nur im Fall einer widerrechtlichen Nutzung des Parkplatzes und des Abschleppens genutzt.

Dieses Vorgehen war nicht zu beanstanden. Inhaber von Privatparkplätzen, die für jedermann zugänglich sind, haben ein Selbsthilferecht gegen die unberechtigte Nutzung sowie einen Schadenersatzanspruch im Rahmen der Beseitigung einer Störung. Voraussetzung der Ansprüche ist, dass die Nutzungsbedingungen des Parkplatzes z. B. durch gut lesbare Hinweisschilder kenntlich gemacht und die Maßnahmen zur Rechtsdurchsetzung verhältnismäßig sind. Der Inhaber darf ein unbefugt abgestelltes Fahrzeug auch ohne konkrete Behinderung abschleppen lassen. Die Erhebung der Kfz-Kennzeichen und der Parkzeit dient der Feststellung der Parkberechtigung und, für den Fall der unberechtigten Nutzung, des Kfz-Halters bzw. -Führers und damit der Verpflichteten. Das Unternehmen kann an der Datenerhebung ein **berechtigtes Interesse** geltend machen. Werden die Daten nach Wegfall des Bedarfs unverzüglich gelöscht, so gibt es keinen Grund zur Beanstandung. Den Betroffenen ist erkennbar und zumutbar, dass ihre Parkplatznutzung kontrolliert wird. Die Kontrolle erfolgt auf eine wenig belastende Art: Durch die handschriftliche Aufzeichnung ist die Gefahr einer unberechtigten Weiternutzung zu anderen Zwecken und einer Verknüpfung mit anderen Daten gering.

Was ist zu tun?
Ein berechtigtes Interesse zur Erhebung von personenbezogenen Daten ist anzuerkennen, wenn diese zur Verfolgung von Rechtsansprüchen benötigt werden.

5.7.11 Kinogutschein gegen Daten von Kindern

Ein Kreditinstitut wollte Fünftklässlern den Start in den neuen Schulabschnitt versüßen und versprach ihnen einen Kinogutschein. Dafür mussten die etwa 11 Jahre alten Kinder einen mit persönlichen Informationen ausgefüllten Coupon in den Institutsfilialen abgeben.

Eltern empörten sich, dass ihre Kinder **in der Schule** ein Anschreiben eines Kreditinstituts bekamen, das sich direkt an die Fünftklässlerinnen und Fünftklässler richtete. Den Kindern wurde gegen Abgabe eines ausgefüllten Coupons ein Kinogutschein versprochen. Anzugeben waren Name, Adresse, Geschlecht, Geburtsdatum und Schule. Eine Einwilligungserklärung der Eltern war nicht vorgesehen. Das Kreditinstitut teilte auf dem Coupon mit, dass die Daten der Kinder genutzt würden, um sie über seine Produkte zu informieren.

Das Kreditinstitut erkannte nach Konfrontation mit der Rechtslage sofort die Unzulässigkeit dieser Datenerhebung zu Werbezwecken bei Kindern an. Fünftklässler verfügen in der Regel noch nicht über die hier **nötige Einsichtsfähigkeit** für wirksame Einwilligungserklärungen. Das Kreditinstitut versicherte, dass die Daten der abgegebenen Gutscheine nicht elektronisch gespeichert und vor allem nicht zu Werbezwecken verwendet werden. Eine solche Kampagne soll auch nicht wiederholt werden.

Was ist zu tun?
Sollen Daten von Kindern und Jugendlichen erhoben werden, so ist sorgfältig zu prüfen, ob sie bereits über die nötige Einsichtsfähigkeit hinsichtlich der Konsequenzen ihres Handelns verfügen. Fehlt diese, so ist die Einwilligung der Eltern als gesetzliche Vertreter einzuholen.

5.7.12 Tankvorgang mit schwer ermittelbaren Folgen

Nach dem Tanken gab ein Kunde beim Bezahlen mit EC-Karte und PIN-Code versehentlich die falsche Tanksäule an und zahlte zu wenig. Als er seinen Fehler bemerkte und sich bei der Tankstelle meldete, sagte man ihm, der Fall sei schon erledigt.

Der Differenzbetrag wurde acht Tage nach dem Tankvorgang vom Konto des Kunden abgebucht. Diese Abbuchung war mit dem Textschlüssel „einlösungsgarantiert, ec-cash-Verf. Inland“ versehen. Die Buchung im sogenannten EC-Cash-Verfahren setzt voraus, dass der Kunde am Terminal seine EC-Karte einsetzt und seinen PIN-Code eingibt. Die Bank des Kunden konnte ihm keine Auskunft darüber geben, wie diese Abbuchung ohne den nochmaligen Einsatz der EC-Karte und vor allen Dingen **ohne die nochmalige Eingabe des PIN-Codes** möglich war. Der Tankstellenbetreiber gab an, der Betrag sei in zwei Raten abgebucht worden. Wie die zweite Abbuchung ohne Vorlage der EC-Karte möglich war, verschwieg er zunächst gegenüber dem Petenten.

Der Kunde befürchtete eine Manipulation des EC-Terminals der Tankstelle und eine Speicherung seines PIN-Codes. Der Tankstellenbetreiber erläuterte dem ULD sein Vorgehen nach der Säulenverwechslung, um den „Schaden zu minimieren“: Er habe anhand der Kopie des EC-Belegs aus der ersten Zahlung die Kontonummer und Bankleitzahl in Erfahrung gebracht und den Differenzbetrag einfach im **Lastschriftverfahren** eingezogen. Klar ist, dass die Nutzung von Bankverbindungsdaten zur Einziehung einer Forderung ohne Einzugsermächtigung unzulässig ist. Ungeklärt blieb, warum die Forderung als EC-Cash-Abbuchung, also als Abbuchung mit PIN-Eingabe, auf dem Kontoauszug des Petenten erschien.

Die Mineralölgesellschaft, die die gesamte Abrechnung durchführte, bot auf Nachfrage des ULD eine ähnliche Erklärung: Der Tankstellenbetreiber habe eine Mitarbeiterin der Abrechnungsabteilung veranlasst, anhand der Belegdaten einen manuellen Abbuchungsvorgang auszulösen. Die Hausbank des Tankstellenbetreibers hatte nach Auskunft der Bank des Kunden die Buchung mit dem Textschlüssel „einlösungsgarantiert, ec-cash-Verf. Inland“ versehen.

Wir baten um eine Erklärung, wie dies möglich gewesen war, obwohl die Mineralölgesellschaft behauptete, im Lastschriftverfahren abgebucht zu haben. Die Bank verwies darauf, dass der Netzbetreiber, der die Kartendaten vom Terminal übermittelt, verloren gegangene Transaktionen ein zweites Mal sende. Da hier das zweite Mal nicht eine identische Transaktion durchgeführt wurde, konnte auch diese Antwort das Rätsel nicht lösen.

Ein erneuter Erklärungsversuch der Mineralölgesellschaft war, die Abbuchung im EC-Cash-Verfahren sei von einer Mitarbeiterin „gebastelt“ worden. Die zur Abwicklung von Kartentransaktionen genutzte Software erlaube für Transaktionen die **Wahl einer Typenzuordnung**. Die Zuordnung der fraglichen Buchung zum EC-Cash-Verfahren sei „schlichtweg falsch“ gewesen.

Zu prüfen bleibt, ob Software, die zur Abrechnung eingesetzt wird, tatsächlich eine gezielte Typenzuordnung zur Transaktion zulässt. Dies dürfte für die Banken, die die Einlösung einer im EC-Cash-Verfahren als „einlösungsgarantiert“ gebuchten Lastschrift grundsätzlich nicht verweigern können, von Interesse sein. Auch für Kunden, die einer Abbuchung im Lastschriftverfahren ohne Einzugsermächtigung widersprechen können, ist dies von Bedeutung. Der Vorgang zeigt die Wichtigkeit eines funktionierenden betrieblichen Datenschutzmanagements.

Die beteiligten Unternehmen hatten anscheinend keine genaue Vorstellung von den Verfahrensabläufen im eigenen Betrieb und damit auch **keine Kontrolle** über die Beachtung des Datenschutzes durch die Mitarbeitenden.

Was ist zu tun?
Buchungen dürfen nicht eigenmächtig im Lastschriftverfahren ohne Einzugsermächtigungen vorgenommen werden. Datenschutzrelevante Vorgänge sollten im Rahmen eines Datenschutzmanagements klar dokumentiert und auf Risiken hin geprüft sein.

Abbuchung im Lastschriftverfahren

Ohne eine zuvor erfolgte Einzugsermächtigung des Kontoinhabers dürfen Dritte keine Beträge vom fremden Konto abbuchen. Dennoch ist es beim sogenannten Lastschriftverfahren möglich, dass Beträge abgebucht werden, ohne dass eine Einzugsermächtigung vorliegt.

Das Lastschriftverfahren funktioniert so: Der aufgrund der erteilten Einzugsermächtigung Einzugsberechtigte übergibt seinem Geldinstitut ein als Lastschrift ausgewiesenes Formular mit dem Namen und der Bankverbindung des Zahlungspflichtigen sowie dem abzubuchenden Betrag. Das Geldinstitut wendet sich daraufhin an die Bank des Zahlungspflichtigen, welche aufgrund der erklärten Einzugsermächtigung eine Belastung des Kontos des Zahlungspflichtigen vornimmt.

Im Massenverfahren der Lastschrifteinlösung können solche Stellen Beträge von fremden Konten per Lastschrifteinzug abbuchen, die durch die Bank im Wege einer sogenannten Inkassovereinbarung zugelassen wurden. Die Ermächtigung des Kontoinhabers zum Einzug durch Lastschrift wird im Einzelfall in der Regel nicht überprüft. Der Zahlungsempfänger muss sich nur verpflichten, diese auf Verlangen vorzulegen. So kann es zu Abbuchungen vom Konto kommen, obwohl keine Einzugsermächtigung vorliegt. Zum Schutz vor unberechtigten Kontobelastungen kann der Kontoinhaber innerhalb einer 6-Wochenfrist bei seinem kontoführenden Institut der Abbuchung widersprechen. Die kontoführende Stelle ist dann verpflichtet, die Rückbuchung zu veranlassen.

5.7.13 Bitte einmal waschen, schneiden und daten

Kaum zu glauben: Die Mitarbeiterin einer größeren Friseurkette wollte einen Kunden nur bedienen, wenn dieser vorher umfangreiche personenbezogene Daten über sich für eine Bonuskarte herausgibt.

Erst nach einem kurzen Wortgefecht wurden dem Kunden auch ohne Preisgabe seiner Daten die Haare geschnitten. Eigentlich wollte die Friseurkette mit ihrem freiwilligen **Bonusprogramm** die Kunden nur enger und längerfristig an sich binden, so das Unternehmen in seiner ersten Stellungnahme. Als Bonus war u. a. bei jedem dreizehnten Friseurbesuch ein Nachlass von 50 % vorgesehen. Die Kunden sollten auch bei der Auswahl ihrer Haarfärbemittel durch Vergleich mit den zuletzt benutzten – kundenbezogen gespeicherten – Produkten besser beraten werden. Die Mitarbeiterin war wohl über ihr Ziel der Aufklärung hinsichtlich des neuen Kundenbindungsprogramms etwas hinausgeschossen.

Dem Geschäftsführer der Ladenkette war dies peinlich. Die Reaktion der Mitarbeiterin beruhe auf einem bedauernswerten Irrtum. Die Erhebungsbögen für das Bonusprogramm enthielten tatsächlich einen optisch hervorgehobenen Freiwilligkeitshinweis, den die Mitarbeiterin offensichtlich nicht kannte. Er sagte zu, die **Information der Beschäftigten** bezüglich des Datenschutzes insgesamt durch Besuche in den Filialen vor Ort zu verbessern.

Was ist zu tun?
Unternehmen sollten in regelmäßigen Abständen ihre Beschäftigten über die Freiwilligkeit von Bonusprogrammen und den hierbei zu beachtenden Datenschutz informieren.

5.7.14 Segelfliegen nur gegen Personalausweisdaten

Der Besitzer eines auf einem Flughafengelände beheimateten Segelflugzeuges ärgerte sich, dass wegen neuer Sicherheitsvorschriften von seinen Gästen die Personalausweisdaten erhoben werden und drei Jahre gespeichert bleiben sollten.

Der Flughafen verwies auf Sicherheitsvorschriften in einer europäischen Verordnung sowie auf das Luftsicherheitsgesetz. Eine konkrete Regelung konnte nicht genannt werden. Die örtliche Ausweisordnung sieht das Speichern von Personalausweisdaten nicht vor. Nach Abstimmung der zuständigen Luftsicherheitsbehörde mit dem Bundesinnenministerium wurde nun festgelegt, dass künftig auf die Speicherung von Personalausweisdaten verzichtet wird. **Lediglich der Name** wird in eine Besucherliste eingetragen; der Personalausweis ist für die Dauer des Aufenthalts auf dem Flughafengelände zu hinterlegen.

Was ist zu tun?
Die Verwendung von Personalausweisnummern durch Wirtschaftsunternehmen ist grundsätzlich nur in den gesetzlich bestimmten Fällen zulässig.

6 Systemdatenschutz

6.1 Professionelle Informationstechnik

Ambitionierte Heimwerkerinnen und Heimwerker schauen gern einmal Profis bei der Arbeit über die Schulter und erkennen: Professionelle Werkzeuge unterscheiden sich von Geräten für den Heimgebrauch. Sie müssen anderen Anforderungen genügen und sind vor allem auf Stabilität und gleichbleibend gute Arbeitsergebnisse hin optimiert.

Diese Unterscheidung gilt auch bei der Technik zur Verarbeitung personenbezogener Daten. Nicht alles, was im Heimbereich zur Anwendung kommt, ist **für den professionellen Einsatz geeignet**. Bei Beratungen und Prüfungen stoßen wir häufig auf Informations- und Kommunikationstechnik (IuK-Technik), die professionellen Anforderungen nicht genügt. Dies erkennt man häufig daran, dass das für die IuK-Technik zuständige Personal sich primär mit der Technik und weniger mit den täglichen Anforderungen der Anwender beschäftigt. Um beim obigen Bild zu bleiben: Man beauftragt einen Handwerker damit, einen Holzboden zu verlegen; dieser ist einen Großteil der Zeit damit beschäftigt, seine Stichsäge einzustellen, umzustellen, zu prüfen und zu reparieren. Wertvolle Arbeitskraft wird für das Werkzeug verschwendet und steht nicht für die eigentliche Aufgabenerledigung zur Verfügung.

Welchen Anforderungen muss professionelle Informationstechnik genügen? Es geht darum, den Aufwand für den laufenden Betrieb zu reduzieren und gleichzeitig eine stabile und gleichbleibend hohe Leistung zu gewährleisten. Hierfür muss ein System über Funktionen zur **Selbstauskunft** verfügen. Der aktuelle Betriebszustand eines Programms oder eines Gerätes muss leicht ablesbar sein. Jedes IuK-System sollte Auskunft über seine aktuelle Auslastung und Fehlersituation geben können, ohne dass diese Daten aufwendig durch eigene Messungen oder Abfragen selbst erhoben werden müssen. Es muss **Prüfpunkte** bereitstellen, anhand derer man schnell und einfach die korrekte Funktion wichtiger Systembestandteile prüfen kann.

Die Datenschutzverordnung (DSVO) Schleswig-Holstein fordert, dass für jedes Verfahren eine Installations- und Konfigurationsdokumentation erstellt wird. Dies ist nur dann ein zusätzlicher Aufwand, wenn bei der Systemauswahl und -beschaffung nicht darauf geachtet wurde, dass das System über ausreichende Mechanismen zur **Selbstdokumentation** verfügt. Jedes IuK-System sollte die aktuellen

Einstellungen und Parameter automatisiert so dokumentieren, dass die Konfiguration für eine sachkundige Person in angemessener Zeit nachvollziehbar ist. Die Dokumentation darf hierbei nicht „im System eingeschlossen“ sein, sondern muss z. B. als Ausdruck auch in einer Systemakte oder in elektronischer Form in der Dateiablage abgelegt werden können.

Jedes System muss eine **zentrale Verwaltung** unterstützen. Dies kann über das Einbinden in vorhandene Verzeichnisdienste geschehen, um die dort hinterlegten Informationen zur Authentifizierung und Autorisierung nutzen zu können. Das ansonsten notwendige mehrfache Pflegen von Daten für die Zugriffskontrolle sorgt für erhöhten Aufwand im Betrieb und führt häufig zu Sicherheitsproblemen, weil das Umsetzen einheitlicher Vorgaben für die Verarbeitung personenbezogener Daten erschwert wird. Das System muss von zentraler Stelle aus konfiguriert werden können. Fehlen diese zentralen Funktionen, kommt es zur „Turnschuh-Administration“: Systemververwalter müssen für jede Konfigurationsänderung zum System laufen. In solchen Situationen wird auf datenschutzrechtlich gebotene Änderungen der Technik oft wegen des hohen Personalaufwands verzichtet.

Grundvoraussetzung jeder professionellen Datenverarbeitung sind verlässliche Funktionen zur **Datensicherung**. Systemverwalterinnen und Systemverwalter müssen ein großes Interesse daran haben, dass die Konfiguration eines Systems und die auf dem System verarbeiteten Daten komfortabel gesichert und wiederhergestellt werden können. Hieran hapert es häufig: Das korrekte Vorgehen zur Datensicherung und -wiederherstellung ist seitens der Hersteller nicht dokumentiert. Oft ist zweifelhaft, ob auch wirklich alles so gesichert ist, dass man das System in derselben Konfiguration und mit demselben Datenbestand nach einem Systemfehler wiederherstellen kann.

Werden personenbezogene Daten ausschließlich automatisiert verarbeitet, so sind Funktionen zur Protokollierung zwingend nötig. Für die Revisionsfähigkeit des Systems ist es zusätzlich wichtig zu wissen, wer wann welche Einstellungen durchgeführt hat. Immer wieder weisen wir auf die Notwendigkeit einer aussagekräftigen **Protokollierung** hin, etwa in unseren Tätigkeitsberichten (28. TB, Tz. 6.5) oder durch die gemeinsame Arbeit mit unseren Kollegen in anderen Bundesländern (Tz. 6.5). Dennoch finden wir noch Systeme vor, deren Protokollierung nicht vollständig oder nicht aussagekräftig ist.

Das Landesdatenschutzgesetz (LDSG) definiert als zentrale Anforderung, dass eine Datenverarbeitung nur stattfinden darf, nachdem die **Berechtigung der Benutzer** festgestellt worden ist. Werden Daten automatisiert verarbeitet, so müssen die beteiligten Programme und Systeme über Möglichkeiten zur Berechtigungsvergabe und zur Dokumentation der vergebenen Berechtigungen verfügen. Die Nutzung von Berechtigungen muss protokolliert werden können.

Behördliche und betriebliche Datenschutzbeauftragte kennen die obigen Funktionen: Sie fordern diese regelmäßig von den Administratorinnen und Administratoren zur Dokumentation und zum Nachweis ordnungsgemäßer Datenverarbeitung. Professionelle IuK-Technik bedeutet, die obigen **Anforderungen möglichst auto-**

matisiert erfüllen zu können, um eine schlanke Umsetzung des Nachweises ordnungsgemäßer Datenverarbeitung zu ermöglichen.

Was ist zu tun?
Daten verarbeitende Stellen müssen ihre Informations- und Kommunikationssysteme daraufhin überprüfen, ob sie die oben dargestellten Anforderungen erfüllen. Mangelhafte Systeme sollten schnell durch besser geeignete Systeme ersetzt werden. Die Anforderungen sollten bei der Vergabe in einem Pflichtenheft als unabdingbar aufgeführt werden.

6.2 Die neue DSVO – Bilanz nach einem Jahr

Vor etwas mehr als einem Jahr wurde die neue Datenschutzverordnung (DSVO) veröffentlicht. Diese kommt gut an. Datenschutzbeauftragte, Systemplaner und Sicherheitsbeauftragte schätzen ihre modulare Struktur.

Evolution statt Revolution: So kann man das Vorgehen zur Aktualisierung der neuen DSVO bezeichnen. Im Geiste der kontinuierlichen Verbesserung haben wir die neue DSVO an den Stellen modernisiert, wo es in der Umsetzung der alten hakte: Die modularisierte Sicherheitskonzeption und kooperative Vorgehensweisen für Test- und Freigabeverfahren sind detaillierter ausgearbeitet. Der Erfolg kann sich sehen lassen. Viele Beispiele zeigen, dass die neue DSVO durch ihre Struktur und genaue Vorgaben das Umsetzen der Anforderungen des LDSG an Sicherheitskonzepte und Test- und Freigabeverfahren erleichtert.

Das Landesvermessungsamt war einer der Pilotkunden der neuen DSVO: Bei der **Vorabkontrolle des Geoservers** wurden die vorigen monolithischen Sicherheitskonzepte auf kleinere, handhabbare Module heruntergebrochen. Die Vorabkontrolle ließ sich effektiv und effizient durchführen. Dabei griffen wir auf uns bekannte Module aus vorherigen Prüfungen und Auditverfahren zurück.

Das Finanzministerium hat inzwischen für **ressortübergreifende Verfahren** ebenfalls diese modularisierte Vorgehensweise zur Dokumentation von Verfahren übernommen. Mit dem ULD wurde ein gemeinsames modulares Vorgehen für die E-Government-Verfahren des Landes vereinbart. Betroffen ist hiervon die technische Plattform für den „Einheitlichen Ansprechpartner“ in Schleswig-Holstein (Tz. 6.4). Auch hier werden bestehende Sicherheitskonzepte, z. B. für die elektronische Aktenführung, in einem Dokumentenmanagementsystem (eAkte) und das vom ULD auditierte Landesnetz genutzt.

Die neue DSVO soll die **Wiederverwertung** von bestehenden Sicherheitskonzepten steigern. Doppelarbeit wird vermieden.

Was ist zu tun?
Systemplaner und Datenschutzbeauftragte sollten modularisiert vorgehen. So kann unter steigendem Kostendruck ein effektives und effizientes Datenschutzmanagement aufgebaut und betrieben werden.

6.3 Tele-, Heim- und mobile Arbeit

Wir stellen steigenden Beratungsbedarf bei neuen Arbeitsformen fest, bei denen die Beschäftigten von zu Hause aus oder von einem anderen Platz außerhalb der Organisation tätig sind und häufig dafür Zugriff auf die IT-Systeme über das Internet erhalten. Was muss man dabei bedenken?

Immer mehr öffentliche und nicht öffentliche Organisationen versuchen, das Idealbild des „vernetzten Wissensarbeiters“ zu erreichen. Sei es wegen der besseren Vereinbarkeit von Beruf und Familie, um Teilzeitbeschäftigten unangemessene Reisezeiten zu ersparen, oder um bestehendes Wissen an wechselnden Einsatzorten verfügbar zu machen: **Mobilere Arbeitsformen** lösen die klassische Arbeit am Schreibtisch in der Behörde oder im Betrieb ab, die ortsunabhängige, vernetzte Wissensarbeit nimmt zu. Das ULD berät bei der datenschutzkonformen und sicheren Umsetzung solcher Arbeitsformen.

Die wichtigsten Maßnahmen bei der Einführung von neuen Arbeitsformen sind organisatorisch und nicht technisch: Die Rechte und Pflichten der Beschäftigten müssen schriftlich festgelegt werden. Unter Wahrung der Mitbestimmung des Betriebs- oder Personalrates müssen geeignete **Vereinbarungen** abgeschlossen werden. Das ULD berät hierbei sowohl die Arbeitgeber als auch die Arbeitnehmervertretung.

Durch eine datenschutzfreundliche Technikgestaltung kann das zusätzliche Risiko einer Datenverarbeitung außerhalb der Organisation deutlich verringert werden. Wir empfehlen häufig die **Nutzung von Terminaldiensten**. Bei der Beratung z. B. der Stadt Flensburg oder des Zweckverbands Kommunit konnte erreicht werden, dass durch den Einsatz von Terminaldiensten die eigentliche Datenverarbeitung weiterhin im sicheren Rechenzentrum stattfindet und auf den Geräten der mobilen Nutzerinnen und Nutzer nur die Bildschirme zur Darstellung der Inhalte genutzt werden.

Bei der Planung neuer Arbeitsformen muss immer darauf geachtet werden, dass **Datentransport, -verarbeitung und -speicherung** mindestens ein gleich hohes Schutzniveau aufweisen wie die bisherige „klassische“ Arbeitsumgebung. Häufig kann durch eine vollständige Festplattenverschlüsselung auf tragbaren Rechnern, eine Verschlüsselung der Datenübertragung durch VPN-Techniken (virtuelles, privates Netz) und eine Absicherung der Datenverarbeitung durch Softwarebeschränkungen und zentrale Einstellungen ein angemessenes Sicherheitsniveau erreicht werden.

Immer wieder stellten wir Lücken bei der Ausgestaltung der „klassischen“ **papierenen Datenverarbeitung** fest. Obwohl immer mehr personenbezogene Datenverarbeitung ausschließlich elektronisch erfolgt, werden häufig noch Akten auf Papier geführt und zur besseren Übersicht Ausdrucke erstellt. Am häuslichen Arbeitsplatz ist für diese Fälle vorzusorgen: Abschließbare Schränke und eine Möglichkeit, Papier ordnungsgemäß zu vernichten, z. B. mit einem Schredder, sollten stets vorhanden sein.

Was ist zu tun?
Neue Arbeitsformen müssen geplant und projektorientiert umgesetzt werden. Die Datenschutzbeauftragten sind bereits bei der Planung hinzuzuziehen, müssen den gesamten Prozess der Einführung beratend begleiten und die Durchführung durch regelmäßige Kontrollen überprüfen.

6.4 Gerade der EAP braucht einen modernen Datenschutz

Nach Vorgabe der EU-Dienstleistungsrichtlinie müssen alle Länder sogenannte „Einheitliche Ansprechpartner" installieren, über die Dienstleister ihre Genehmigungsverfahren an zentraler Stelle komfortabel abwickeln können. Datenschutzanforderungen sind von Anfang an in die Konzepte eingeflossen.

Die aufwendigen Vorarbeiten in Schleswig-Holstein sind vollbracht. Der Einheitliche Ansprechpartner (EAP) soll als **Verfahrensvermittler** zwischen einem Dienstleistungsanbieter aus dem europäischen Raum und den Behörden agieren, ohne dass der EAP an den bestehenden Zuständigkeiten für behördliche Prüfungen oder Genehmigungen etwas ändert (31. TB, Tz. 6.3). In Arbeitsgruppen haben Vertreter der Kommunen, der Handwerks- und Industrie- und Handelskammern, des Landes sowie der IT-Dienstleister mit unserer Beteiligung begonnen, die behördenübergreifenden Prozesse zu konzipieren, zu dokumentieren und mit ihren jeweils lokalen Prozessen zu verbinden. Mit dieser nötigen Vorarbeit konnten die verschiedenartigen Genehmigungsverfahren samt Beteiligungen der jeweiligen Parteien über den EAP abgebildet werden.

Die durch den EAP ausgelöste Integration der Verwaltungskommunikation und die angestoßenen Änderungen der internen Informationsverarbeitung erzeugen allerdings neue – und damit auch rechtlich neu zu bewertende – **Risiken für den Datenschutz**. Diese Risiken bestehen sowohl für die Verarbeitung der Daten betroffener Bürger als auch der Mitarbeiter der Verwaltungen. An den technisch aufbereiteten Datenbeständen von Antragstellern bestehen Begehrlichkeiten. Für die Mitarbeiter in den Verwaltungen bewirkt die Vermessung der Verwaltungsprozesse, dass diese erkennbar auch mit eigenen Kennzahlen zu ihrer Produktivität konfrontiert werden. Mit dem EAP steigt somit das Risiko, dass in der Verwaltung der Umgang mit solchen Kennzahlen eingeübt und schleichend zur Normalität wird, was auf eine automatisierte Verhaltens- und Leistungskontrolle hinauslaufen kann.

Die gegenseitigen technischen Abhängigkeiten der Kommunen, Länder und Nationen untereinander steigern die **Fehleranfälligkeit der Systeme**, wenn keine übergreifend wirksame Gesamtplanungsinstanz mit einem wirksamen Qualitätsmanagement eingerichtet wird. Kleine Ungereimtheiten können sich zu Fehlern aufschaukeln. Dieses Risiko wird durch die vorgegebene Trennung von Organisationseinheiten reduziert, sei es durch Gewaltenteilung, Ressorthoheit und in diesem Falle vor allem durch die kommunale Selbstverwaltung. Bestehende Vorschriften, die in diesem Sinne Funktionstrennungen gebieten, sollten bewahrt bzw. ausgebaut werden.

Das ULD sieht seine Aufgabe darin, diese **funktional gebotene Trennung** zu unterstützen. Die Komponenten der EAP-Infrastruktur müssen untereinander lose gekoppelt sein. Damit wird die Fortpflanzung von Fehlern vermieden und die Anpassung an lokale Besonderheiten erleichtert; zudem müssen und können immer nur einzelne Teile eines technischen Großsystems kontrolliert geplant und geplant kontrolliert werden. Dieses Vorgehen bietet sich an, zumal es keinen alles regulierenden europäischen Gesamtplan für den EAP gibt. Es wäre fatal, die Fehler zu wiederholen, die sich Anfang 2007 im durchdigitalisierten Meldeverfahren in Deutschland zeigten, bedingt durch die Schwierigkeit, organisationsübergreifend Fehler als solche zu kennzeichnen und deren Ursachen bei einer anderen Verwaltung zu belegen und zuzurechnen, damit diese nachhaltig an der Quelle behoben werden (29. TB, Tz. 6.6).

Die Umsetzung der EU-Dienstleistungsrichtlinie (EU-DLR) bietet die Chance zur Verbesserung des Datenschutzes in der öffentlichen Verwaltung. Die zunehmende Automation der Verwaltungsprozesse führt zum Offenlegen der Zwecke der Datenbestände und Schnittstellen sowie zu einer Standardisierung der Verfahren und Techniken. Der **gesteigerte Grad an Transparenz** und Standardisierung macht wiederum die Verbindung zwischen Organisation und Technik besser kalkulierbar. Alle Beteiligten – die Verantwortlichen, die Nutzer, die Betreiber, die Auftraggeber und die Betroffenen – können künftig leichter klären, welche Datenverarbeitung zu welchem Zeitpunkt stattfinden soll, welche Datenverarbeitung aktuell stattfindet oder stattfand. Eine wesentliche Voraussetzung zur Beherrschung dieser Prozesse ist, dass mit der Entwicklung der neuen Informations- und Kommunikationshochleistungssysteme auch die Mechanismen zu deren Beobachtung, Regulation, Kontrolle und Prüffähigkeit als wesentliche Systembestandteile mitentwickelt werden. Dies bedeutet, dass mit der Automation sowohl der organisationsübergreifenden als auch der internen Verwaltungsprozesse die Instrumente zu deren Controlling automatisiert werden müssen, selbstverständlich ohne dazu auf die Inhaltsdaten zuzugreifen.

Schon aus haftungsrechtlichen Gründen kommt der revisionsfesten und beweissicheren **Protokollierung der Verwaltungstätigkeiten** mit starkem Bezug zu Unternehmen eine große Bedeutung zu. Der EAP kann die eigene Rechtssicherheit durch detaillierte Prozessvorgaben, eine sicherheitstechnisch einwandfreie Ablaufumgebung, eine transparente Prozessdurchführung und eine revisionsfähige Ablaufdokumentation erreichen. Im Systemdesign sind deshalb von vornherein die Mechanismen zur Einrichtung eines effektiven Datenschutzmanagements – und somit auch des Qualitätsmanagements – vorzusehen.

Der Datenschutzbeauftragte des EAP steht vor der Aufgabe, die Wirksamkeit und Angemessenheit der technischen und organisatorischen Maßnahmen zu prüfen, mit denen die besonderen Risiken der Mitarbeiterüberwachung und der unerlaubten Verkettung normalerweise isolierter Verwaltungsverfahren verringert werden sollen. Zunächst wird es darum gehen, eine Dokumentation der Prozesse zur automatisierten und zur klassischen papierbezogenen Datenverarbeitung des EAP zu erstellen. Dann ist zu prüfen, ob und inwieweit die verwendete Informations- und Kommunikationstechnik sicher und datensparsam eingesetzt wird. Letztendlich muss der Datenschutzbeauftragte darauf hinwirken, dass durch eine **General-**

dokumentation des EAP für Antragsteller und am EAP-Prozess teilnehmende Behörden die notwendige Transparenz und Nachvollziehbarkeit in allen Prozessschritten hergestellt wird. Das Finanzministerium erarbeitet eine DSVO-gerechte Dokumentation des gesamten EAP-Systems, das auf einer ganzen Reihe bereits existierender Komponenten der E-Government-Infrastruktur des Landes Schleswig-Holstein aufsetzt.

Was ist zu tun?
Die rechts- und damit datenschutzkonforme Kontrolle des EAP als komplexes, automatisiertes System setzt ein Qualitätsmanagement auf hohem Technisierungsniveau voraus, das sich an den funktionalen Aspekten des Verfahrens orientiert.

6.5 Die unendliche Geschichte: Protokollierung

Die datenschutzkonforme Ausgestaltung der Protokollierung in automatisierten Verfahren ist ein Dauerthema. Das ULD unterstützt Daten verarbeitende Stellen durch konkrete Vorgaben.

Die Protokollierung ist nach wie vor das wichtigste Instrument zur Herstellung von Transparenz für den Nachweis rechtskonformer Verwaltungstätigkeit. Auf der Basis von Protokolldaten müssen **Sachverhalte rekonstruiert und bewertet** werden können. Die automatisierte Protokollierung darf aber nicht zur unzulässigen Verhaltens- und Leistungskontrolle von Mitarbeitern eingesetzt werden.

Protokolldaten unterliegen – ebenso wie andere Datenbestände – einer spezifischen **Zweckbindung**: Es darf keine Protokollierung, also z. B. keine Einträge in Logdateien geben, über deren Erforderlichkeit, Umfang und Speicherdauer nicht Rechenschaft abgelegt werden kann. Protokolldaten ergeben nur einen Sinn, wenn sie tatsächlich ausgewertet werden. Die Erforderlichkeit und Korrektheit der Protokolldaten müssen durch Tests sichergestellt werden. Insbesondere ist zu prüfen, ob sich bestimmte unerwünschte Ereignisse mithilfe der Protokolldaten belegen lassen. Die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit sind zu berücksichtigen. Dabei können kryptografische Verfahren zum Einsatz kommen.

Die **Protokollierung** umfasst sowohl Änderungen an informationstechnischen Systemen durch Administratoren als auch deren Nutzungen bei der Verarbeitung personenbezogener Daten. Zu protokollieren sind hierbei Tätigkeiten

- der Authentisierung und Autorisierung,
- der Dateneingabe und Datenveränderung,
- der lesenden Dateneinsicht,
- der Datenübermittlung und
- der Datenlöschung.

Zu den jeweiligen Ereignissen ist der Zeitpunkt sowie die auslösende Systemkomponente oder Person zu erfassen. Das Format, in dem die Daten gespeichert werden, muss so ausgewählt werden, dass diese **automatisiert mit einem Analysewerkzeug auswertbar** sind. In der Praxis hat sich bei großen Datenvorkommen das zeilenweise Speichern im CSV-Format bewährt.

Bei der Konzeption der Protokollierungsregelungen zu jedem einzelnen Verfahren empfiehlt sich eine Orientierung am Lebenszyklus der Protokollierung:

- Für die **Erzeugung** der Protokolldaten sind die Anforderungen der Gesetze sowie die des organisationsinternen Datenschutzmanagements zu berücksichtigen. Jede als relevant eingestufte Tätigkeit muss zu einem Protokolleintrag führen. Wichtig: Änderungen an der Konfiguration der Protokollierung müssen ihrerseits einen Eintrag in den Protokolldaten erzeugen.
- Art und Umfang der **Speicherung** der Protokolldaten müssen festgelegt werden. Die Zugriffsmöglichkeiten auf Protokolldaten sind zu minimieren, insbesondere für die Administratoren, deren Tätigkeiten anhand dieser Protokolldaten kontrolliert werden. Protokolldaten sollten deshalb nicht auf den Produktionsmaschinen, sondern auf eigens betriebenen Protokollservern gespeichert werden. Ausschließlich automatisiert gespeicherte Protokolldaten sind nach einem Jahr zu löschen.
- Bei der **Übertragung** von Protokolldaten mit Personenbezug und/oder erhöhtem Schutzbedarf über Netzwerke, z. B. bei zentraler Protokollspeicherung oder entfernter Auswertung, sind zur Wahrung der Vertraulichkeit, Integrität und Authentizität geeignete und für den Schutzbedarf angemessene kryptografische Verfahren nach dem Stand der Technik zu nutzen.
- Das Verfahren zum **Löschen** der Protokolldaten muss beschrieben sein. Dabei müssen diejenigen Protokolldaten einbezogen werden, die auf Datensicherungsmedien oder bei einem Auftragsdatenverarbeiter gespeichert sind. Bei der Protokollierung von Löschvorgängen für Protokolldaten dürfen keine personenbezogenen Daten in den Inhalten des Löschprotokolls enthalten sein. Stattdessen sind gegebenenfalls Hinweise auf Aktenzeichen oder Dateinamen aufzunehmen. Ferner müssen Angaben darüber ergänzt werden, welche Entität die Löschung dieser Protokolldaten zu welchem Zeitpunkt vorgenommen hat. Beispiel:

  „Gelöscht
  Protokolldaten_Fachverfahren_AA200_bis_ZZ620_von200106_bis_200606,
  Admin_A, 20090302_1510_35“

Wie wichtig eine vollständige Protokollierung auch der **lesenden Zugriffe** ist, wenn ein Verfahrensschritt direkt auf die Ermittlung personenbezogener Daten – wie für die Polizeiarbeit typisch – abzielt, zeigte sich jüngst an einem Beispiel in Rheinland-Pfalz. Dort hatte in der sogenannten Nürburgring-Affäre ein Mitglied des Landtages ehemalige Kollegen bei der Polizei gebeten, im dortigen Polizei-Informationssystem nach Daten über Geschäftspartner der Nürburgring GmbH zu fahnden. Aufgrund der Protokollierung konnte nachgewiesen werden, dass die getätigten Abrufe nicht dienstlich veranlasst waren. Das ULD wird die Angemes-

senheit und Wirksamkeit der erzeugten Protokolldaten in ähnlichen Verwaltungsverfahren prüfen.

Eine **Orientierungshilfe zur Protokollierung** ist veröffentlicht unter:

http://www.lfd.m-v.de/dschutz/informat/protokol/oh-proto.pdf

Was ist zu tun?
Die automatisierte Verarbeitung personenbezogener Daten ist vollständig zu protokollieren. Zielt ein Verfahrensschritt direkt auf die Ermittlung personenbezogener Daten ab, so muss die vollständige Protokollierung auch lesende Zugriffe umfassen. Protokolldaten mit Personenbezug unterliegen ebenfalls dem Datenschutzrecht.

6.6 Staatskanzlei: „interamt“

Arbeitgeber bieten die Möglichkeit für E-Mail-Bewerbungen auf Stellenangebote oder nutzen Online-Stellenbörsen. Das Land Schleswig-Holstein ist mit einer Online-Stellenbörse für den öffentlichen Dienst namens „interamt“ im Netz.

Da es sich dabei um ein Verfahren mit personenbezogenen Daten handelt, bat die Staatskanzlei das ULD um Beratung. Das Verfahren „interamt“ ist eine **Jobbörse**, die sich an den speziellen Anforderungen der Personalsuche des öffentlichen Dienstes orientiert. Sie steht grundsätzlich allen Institutionen und Mitarbeiterinnen und Mitarbeitern des öffentlichen Dienstes zur Verfügung. Behörden können ihre offenen Stellen in der Stellenbörse ausschreiben sowie gezielt nach potenziellen Kandidaten für ihre offenen Stellen suchen. Mitarbeiterinnen und Mitarbeiter des öffentlichen Dienstes können in der Jobbörse ein Profil mit ihren Bewerbungsdaten hinterlegen und nach neuen passenden Stellen suchen. Die Hinterlegung und Veröffentlichung von Daten in dieser Plattform ist für alle registrierten Personen **freiwillig**.

Die Staatskanzlei ist sich bewusst, dass bei diesem Verfahren sensible personenbezogene Daten verarbeitet werden. Die konzeptionelle Vorarbeit und die bestehende Teststellung lassen erkennen, dass großes Gewicht auf Datensicherheit und Datenschutz gelegt wird. Kleine Lücken taten sich bei der Dokumentation des Verfahrens auf. Die Schieflage zwischen umgesetzten technischen Maßnahmen und lückenhafter Dokumentation ist – oft in deutlich größerem Ausmaß – auch andernorts im Land anzutreffen. Neben einer Verfahrensbeschreibung, der Dokumentation des IT-Einsatzes und der Sicherheitsmaßnahmen einschließlich eines Berechtigungskonzepts, Prozessbeschreibungen und einigen Referenzdokumenten waren bereits Formulare zu Tests und zur Freigabe sowie ein Datenschutzleitfaden erstellt worden. Es fehlten lediglich die Risikoanalyse und die Restrisikobetrachtung. Durch dieses **Fundament an Dokumentation** zum Verfahren „interamt“ und die effektive Zusammenarbeit hat die Staatskanzlei die Dokumentations-

anforderungen nach der DSVO so konsequent umgesetzt, wie wir dies nur selten vorfinden. Die Dokumentation der Sicherheitsmaßnahmen einschließlich einer Risikoanalyse mit Restrisikobetrachtung wird von vielen IT-Verantwortlichen eher stiefmütterlich behandelt. Vollkommen vernachlässigt wird immer wieder die Dokumentation von Tests und Freigaben.

Als rühmliche Ausnahme war bei der Jobbörse „interamt“ von Anfang an die Dokumentation ein zentraler Bestandteil der Entwicklung des Verfahrens. Begleitend wurde das ULD als Berater hinzugezogen, um etwaige Fragen zu Inhalten und Struktur schnell zu klären. Herausgekommen ist ein vorbildlich nach LDSG und DSVO erstelltes Paket, das die Staatskanzlei als **Vorlage – aber auch Messlatte** – für weitere Verfahren nutzen kann.

Was ist zu tun?
IT-Verantwortliche oder Administratoren, die an der Erarbeitung der erforderlichen Dokumentation scheitern, weil sie nicht wissen, wie sie diese zu erstellen haben, sollten per E-Mail oder telefonisch mit dem ULD einen Beratungstermin vereinbaren. Andere Verfahren sollten mit derselben Systematik wie bei „interamt“ dokumentiert werden.

6.7 Datenschutzerklärung im Webangebot der Stadt Heide

Häufig wird das ULD um Unterstützung bei der Gestaltung der Datenschutzerklärung eines Webauftritts gebeten. Nachfragen kommen sowohl aus dem öffentlichen als auch aus dem nicht öffentlichen Bereich. Oberstes Gebot einer Datenschutzerklärung ist immer die Transparenz: Wann werden welche Nutzerdaten zu welchem Zweck erhoben und wie lange werden sie gespeichert?

Positiver Nebeneffekt bei der Erstellung einer solchen Erklärung ist die zwangsläufig erfolgende Prüfung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten im Bereich des Webangebots. Nach dem Telemediengesetz ist jeder Anbieter eines Webauftritts verpflichtet, den Nutzer über Art, Umfang und Zweck der Erhebung und Verwendung seiner personenbezogenen Daten zu informieren. Meist ist den Verantwortlichen der Umfang der bei ihnen verarbeiteten Daten nicht bewusst, da ihnen das technische Know-how fehlt. Mit der Bitte um Hilfe bei der Erstellung der **Datenschutzerklärung** für ihren Webauftritt wandte sich auch die Stadt Heide an das ULD. Ihr Webauftritt vereint die Stadtverwaltung, die Stadtbücherei, die Volkshochschule und den Verein „Heide-rundum“.

Beschränkt sich ein Webangebot nicht auf die Informationsdarstellung, sondern ermöglicht es auch Dateneingaben, so empfiehlt es sich, in einem Workshop mit den Beteiligten – unter Einbeziehung der technischen Dienstleister – die Verantwortlichkeiten zu klären und zu erarbeiten, welche personenbezogenen Daten bei der Nutzung des Webangebots anfallen. Dabei darf nicht vergessen werden: **IP-Adressen**, die fast immer aus statistischen Gründen mitgeloggt werden, sind personenbezogene Daten.

Das ULD unterstützte die Stadt Heide bei der Zusammenstellung aller möglichen anfallenden personenbezogenen Daten und ihrer Bewertung in Bezug auf ihren Nutzen und die **Rechtmäßigkeit** dieser Erhebungen. Gerade beim Logging auf Webservern werden häufig mehr Daten gespeichert, als zur gewünschten Auswertung notwendig sind. Dann kann der Umfang der Logdaten reduziert werden. Gerade im öffentlichen Bereich ist das Verhalten des einzelnen Webnutzers nicht von Interesse, ganz im Gegensatz zur Anzahl einzelner Seitenabrufe.

Die Stadt Heide beschreibt in der Datenschutzerklärung explizit, welche **Daten von Nutzenden** sie beim Logging erfasst. Sie stellt dar, welche Form von Cookies sie einsetzt und wann diese gelöscht werden. Eine kurze Erklärung zu diesen kleinen Textdateien und wie der Nutzer seinen Browser in Bezug auf Cookies konfigurieren kann, ergänzt diesen Absatz. Es wird konkret auf Formulare eingegangen, bei denen der Nutzer Daten von sich eingeben und Kontakt mit den jeweiligen Ansprechpartnern aufnehmen kann. Hier wird der Bearbeitungsprozess beschrieben und den Nutzenden erklärt, dass ihre Daten nur für die erforderliche Anfrage genutzt und anschließend gelöscht werden.

Die Stadtbücherei Heide bietet als Zusatzdienst ein Bücherforum an, in dem die Nutzer Kommentare zu Büchern abgeben können. Die Datenschutzerklärung stellt genau dar, welche Daten zur Registrierung und Nutzung notwendig sind und wie mit diesen umgegangen wird. Die Stadt klärt die Nutzer darüber auf, dass deren Nutzername und die von ihm abgegebenen Kommentare für alle sichtbar sind und von Suchmaschinen erfasst werden, und empfiehlt **Pseudonyme als Nutzernamen**.

All dies dient der Information der Nutzer über die von ihnen erhobenen Daten. Alle Aspekte müssen **klar und leicht verständlich formuliert** werden. Die Datenschutzerklärung muss dann von jeder Seite des Webangebots schnell auffindbar und durch einen Klick erreichbar sein. Transparenz ist oberstes Gebot. Die Nutzer müssen wissen, welche Daten bei Nutzung des Angebots über sie gesammelt, zu welchem Zweck diese genutzt sowie wann diese gelöscht werden und an wen sie sich bei Nachfragen wenden können. Die Stadt Heide hat eine beispielhafte Datenschutzerklärung erstellt, die Vertrauen schafft.

Was ist zu tun?
Jeder Webseitenanbieter muss eine Datenschutzerklärung veröffentlichen. Er muss sich hierzu Gedanken machen, wo und wann welche Daten des Nutzers auf seiner Webseite entstehen. Die Transparenz zu Erfassung, Verarbeitung und Löschung seiner Daten wird beim Nutzer Vertrauen schaffen.

6.8 E-Mail – Sicher oder nicht sicher?

Ob personenbezogene Daten sicher per E-Mail verschickt werden können, hängt vom Weg einer E-Mail durchs Netz und von den genutzten Systemen ab. Immer wieder wird uns die Frage gestellt, ob man personenbezogene Daten nicht einfach unverschlüsselt per E-Mail versenden darf.

Beim Versenden von Daten muss man sich immer darüber im Klaren sein, welchen **Schutzbedarf** diese haben. Im Umfeld von Verfahren, die einem Amts- oder Berufsgeheimnis unterliegen, z. B. bei Steuer- oder Patientendaten, ist dieser bereits gesetzlich festgelegt. In anderen Fällen ist aus Sicht der Betroffenen zu prüfen, welche Nachteile entstehen können, wenn eine E-Mail von Unbefugten gelesen oder verändert wird. Allein die Tatsache, dass ein Antrag auf Unterstützungsleistungen gestellt wurde, kann bei unbefugter Kenntnisnahme negative Auswirkungen für den Betroffenen haben.

Um einschätzen zu können, wie hoch das Risiko einer unberechtigten Einsichtnahme oder Veränderung von E-Mails ist, müssen die Quell- und Zielsysteme und der zur E-Mail-Übertragung genutzte Weg betrachtet werden. Für jedes beteiligte System ist zu prüfen, ob eine **ausreichende Sicherheitskonzeption** vorliegt. Darin muss das Risiko der unberechtigten Einsichtnahme in die Daten durch angemessene und wirksame Maßnahmen behandelt werden. Ist diese Prüfung für alle beteiligten Systeme nicht möglich, z. B. weil die Zielsysteme nicht bekannt sind, so müssen die E-Mail-Inhalte durch zusätzliche Sicherheitsmaßnahmen wie Verschlüsselung geschützt werden. Genau diese Situation findet man in der Regel bei der Kommunikation mit Bürgern oder Kunden vor. Die wenigsten Kundinnen und Kunden betreiben eigene E-Mail-Systeme und können die Sicherheit des Übertragungsweges beeinflussen. Die Systeme ihrer Internetprovider oder von Drittanbietern haben zumeist kein definiertes Schutzniveau. Häufig verbleiben sämtliche E-Mails auf den Rechnern der Anbieter. In solchen Situationen kann keine ausreichende Aussage über die Sicherheit der Endsysteme getroffen werden.

Ergibt die eigene Analyse, dass die lokale IuK-Umgebung und die E-Mail-Server, der Transportweg zum Zielsystem und die dortige IuK-Umgebung ausreichenden Schutz gegen eine unberechtigte Einsichtnahme und Veränderung von E-Mails bieten, so kann auf zusätzliche Sicherheitsmaßnahmen verzichtet werden. Dies kann der Fall sein, wenn zwei Landesbehörden über das **Landesnetz** E-Mails versenden. Das Landesnetz wird u. a. vom ULD im Rahmen eines Audits regelmäßig überprüft. Die Endsysteme der Landesbehörden sind größtenteils nach einheitlichen Vorgaben standardisiert – aktuell IKOTECH III, demnächst „+1“ –, konfiguriert und kontrolliert. Das ULD stuft das Landesnetz als ein abgeschlossenes Netz ein, in dem personenbezogene Daten der Nutzer unverschlüsselt, aber isoliert von anderen Nutzergruppen transportiert werden können. Eine Verschlüsselung ist erforderlich, wenn die in dem Sicherheitskonzept des Finanzministeriums beschriebenen Restrisiken als nicht tragbar bewertet werden. Problematisch ist, dass noch nicht alle öffentlichen Stellen E-Mails über das Landesnetz austauschen oder andere Möglichkeiten zur Absicherung des E-Mail-Transports, z. B. über eine Transportverschlüsselung, (TLS) getroffen haben.

Die Entscheidung, ob E-Mails verschlüsselt werden müssen oder nicht, kann meistens nicht vom Endanwender getroffen werden. Ihm fehlen häufig die Einsichten, um eine genaue Analyse durchzuführen und eine valide Entscheidung treffen zu können. Insofern muss die Daten verarbeitende Stelle Hilfestellung liefern, z. B. durch **schriftliche Anweisungen**. Auf Basis einer sicherheitstechnischen und datenschutzrechtlichen Betrachtung können in einer Dienstanweisung Festlegungen getroffen werden, bei welchen Empfängern und bei welchen Inhalten auf Verschlüsselung verzichtet werden kann.

Das ULD bietet im Rahmen seiner Beratungstätigkeit an, Analysen der Endsysteme und des Transportweges durchzuführen, um eine **belastbare Entscheidungsgrundlage zur E-Mail-Verschlüsselung** zu erhalten.

Was ist zu tun?
Personenbezogene E-Mails sollten grundsätzlich verschlüsselt werden. Ausnahmen sollten vorher sicherheitstechnisch und datenschutzrechtlich begutachtet und in Form einer schriftlichen Anweisung festgelegt werden.

6.9 „Schutzziele“ sind mehr als „CIA“

Unter führender Beteiligung des ULD wird von den Datenschutzbeauftragten für die Novellierung des Bundesdatenschutzgesetzes ein Entwurf zur Festlegung „neuer Schutzziele“ erarbeitet. Die Schutzziele dienen als konstruktiv umsetzbare Vorgaben zur Herstellung von Datensicherheit in IuK-Systemen.

Die wichtigsten traditionellen Schutzziele der Datensicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit (**Confidentiality**, **Integrity**, **Availability** – kurz: CIA). Hierzu gibt es Kataloge von Maßnahmen. Welche Schutzmaßnahmen in welcher Form zu treffen sind, wird anhand einer an den dokumentierten Risiken bemessenen Schutzbedarfsfeststellung festgelegt.

Die Schutzziele der Datensicherheit, die zumeist aus der Perspektive eines zu sichernden Betriebsablaufs formuliert sind, müssen aus Datenschutzsicht im Hinblick auf den Persönlichkeitsschutz der jeweiligen Betroffenen spezifiziert werden. Für ein gutes Datenschutzniveau von technischen Systemen reichen allerdings allein die Schutzziele der Datensicherheit nicht aus. Es wurden speziell auf den Datenschutz zugespitzte „neue“, die klassischen der Datensicherheit ergänzende **spezifische Datenschutz-Schutzziele** erarbeitet: Transparenz, Zweckbindung sowie Intervenierbarkeit.

Das Schutzziel **Transparenz** zielt darauf ab, Organisationen, Verfahren und technische Systeme durch Offenlegung sowohl der Verfahrensabläufe als auch der Zugänge zu den Systemen und Verfahren so einzurichten, dass diese datenschutzrechtlich prüfbar und bewertbar werden – für die Zukunft, die Gegenwart und die Vergangenheit. Transparenz für die Zukunft bedeutet, dass bei neuen Projekten prüffähige Konzepte und Pläne auszuarbeiten sind. Gegenwärtige Transparenz umzusetzen fordert vom verantwortlichen Systembetreiber die Bereitstellung von

Maßnahmen, mit denen jederzeit ermittelbar ist, in welchem Zustand sich die Systeme gegenwärtig befinden. Transparenz für die Vergangenheit bedeutet Revisionsfähigkeit, nämlich bei Rückfragen z. B. von Betroffenen, um nachweisen zu können, wie ein Sachverhalt war.

Das Schutzziel der **Zweckbindung** operationalisiert, dass rechtlich gebotene Trennungen von zweckgebundenen Datenverarbeitungen – etwa bezüglich der Gewaltenteilung, der Ressorthoheit, der Zuständigkeit oder allgemein der Funktionstrennungen von Organisationen – nicht durch technische Kurzschlüsse unterlaufen werden. Technik ist unter Berücksichtigung rechtlich gebotener Zweckbindungen bzw. Funktionstrennungen zu planen und zu betreiben.

Intervenierbarkeit zielt darauf ab, dass ein Betroffener von seinen ihm zustehenden Rechten technisch auch wirksam Gebrauch machen kann. Systeme, bei denen Hersteller beispielsweise angeben, die Daten seien aus welchen Gründen auch immer nicht löschbar, dürfen wegen Verletzung dieses Schutzziels nicht zum Einsatz in Verfahren mit Personenbezug kommen. Betroffene dürfen nicht Opfer von Systemen werden, die sich angeblich nicht stoppen und ändern lassen.

Die neuen Schutzziele bilden bereits die Grundlage zur Entwicklung von Regeln für WebServices – sogenannte **Policies** – für OSCI 2.0 (Online Services Computer Interface, 31. TB, Tz. 6.4), welches der inzwischen verabschiedete Nachfolgestandard zur sicheren Kommunikation in der öffentlichen Verwaltung in Deutschland werden soll. Noch nutzt kein Verfahren OSCI 2.0; zunächst müssen alle Sicherheits- und Datenschutzmaßnahmen praxisgerecht umgesetzt werden.

Die Entwicklung von WebService Policies wird unter Beteiligung des ULD intensiv fortgeführt werden, was wegen der Komplexität der Anforderungen dringend nötig ist. Diese Arbeit kann sich durchaus **über Deutschland hinaus** positiv auf das Datenschutzniveau der kommunikationstechnischen Infrastruktur auswirken. Die Teilnahme des ULD an internationalen Arbeitsgruppen der ISO (International Organization for Standardization) und des W3C (World Wide Web Consortium) ist insofern äußerst wertvoll (Tz. 2.3.2). Auch die Kriterienkataloge für das ULD-Datenschutz-Gütesiegel, das ULD-Datenschutz-Audit sowie für das europäische Datenschutz-Gütesiegel EuroPriSe profitieren von der Arbeit an den neuen Schutzzielen.

Was ist zu tun?
Die Arbeiten zur Modernisierung des Abschnitts über technisch-organisatorische Bestimmungen im Bundesdatenschutzgesetz sind fortzusetzen. Ein Schwerpunkt muss auf die Entwicklung von praktikablen Maßnahmen zur Umsetzung der „neuen“ Datenschutz-Schutzziele gelegt werden.

6.10 Datenschutz messbar gemacht – KPIs fürs Datenschutzmanagement

Datenschutzaktivitäten dienen dazu, Prozesse in einer Organisation im Hinblick auf Personenbezug zu beobachten, zu bewerten und gegebenenfalls zu korrigieren. Die Beobachtung von Prozessstrukturen unterliegt dabei den gleichen Anforderungen an Transparenz und Steuerbarkeit wie die vom Datenschutz beobachteten Prozesse selber.

Für Datenschutzprozesse gilt die klassische Aussage zum Controlling allgemein: Prozesse, die man nicht messen kann, kann man auch nicht kontrollieren, bewerten oder steuern. Hilfreich sind dabei sogenannte **Key-Performance-Indikatoren** (KPIs).

Datenschutzaktivitäten in einer Organisation müssen geplant werden und gesteuert geschehen. Im Rahmen der Ausrichtung auf das Prozessmanagement von ITIL (IT Infrastructure Library) führen Organisationen zunehmend ein entsprechendes Datenschutzmanagementsystem ein. Dazu gehört, den oder die Datenschutzbeauftragte in die Prozesse des Konfigurations-, Problem- und Change-Managements einzubinden. Weiterhin können eigene Prozesse entwickelt werden, mit denen sich die Umsetzung von Datenschutzanforderungen systematisch beobachten lassen und die neben den anderen Prozessen des Controllings bzw. des Qualitätsmanagements zur Verfügung gestellt werden. Datenschutzmanagement ist ein **Teilaspekt einer Compliance-Strategie**, die im Wesentlichen die Regeltreue in Bezug auf Bestimmungen zum Umgang mit personenbezogenen Daten und Prozessen transparent macht.

Ein systematisches **Datenschutz-Controlling** identifiziert zunächst datenschutzrelevante Funktionen und Tätigkeiten. Dann gilt es, verschiedene Prozesse aufzusetzen, mit denen sich diese Funktionen und Tätigkeiten gemäß den Datenschutzanforderungen systematisch beobachten lassen. Darüber hinaus muss die Leitung der Organisation einen Prozess etablieren, mit dem nach festgestellten Abweichungen gemessener Istwerte von den festgelegten Sollwerten Korrekturen oder zumindest Korrekturanforderungen ausgelöst werden. In einem solchen „zweistufigen“ Datenschutzprozess – erst einen Prozess zur Beobachtung und dann einen Prozess zur Behebung von Fehlern, Problemen oder Verstößen mit Korrekturvorschlägen – sind mindestens die folgenden Funktionen und Tätigkeiten zu begleiten:

- Strategie (z. B. Planung von neuen Prozessen),
- Sicherheitsanalyse von Systemen, Verfahren, Prozessen,
- Restrisikoanalyse,
- Patch-Management und Updates für Systeme,
- Test und Freigabe (z. B. Entwickeln eines Testplans für neue Verfahren),
- Dokumentation von Verfahren,
- Protokollierung von Prozessen,

- regelmäßige oder anlassbezogene Kontrollen für laufende Verfahren, Prozesse und Systeme (z. B. für Patches, Back-ups, Sicherheitsmaßnahmen, Berechtigungsmanagement, Entsorgung),
- Back-up,
- Entsorgung (z. B. von Datenträgern wie Akten, Festplatten oder Disketten),
- Besuchermanagement,
- Berechtigungsmanagement,
- Personalmanagement,
- Wartung.

Zur Vermessung von Prozessen im Hinblick auf die Frage, ob diese ihre Ziele effizient und effektiv erreichen bzw. erreicht haben, setzen Organisationen heute typischerweise KPIs ein. Dabei sind generell **drei Ebenen für KPIs** zu unterscheiden:

1. KPIs, die aus dem **technisch-automatisierten Betrieb der Systeme** stammen, z. B. aus Protokolldaten: Hier lassen sich die Verfügbarkeit, Störungen oder abgewiesene Zugriffsversuche bei Log-ins automatisiert erkennen. Beispiele für KPIs mit unmittelbarem Datenschutzbezug sind die Anzahl der eingeführten Compliance-Prüfpunkte, der Anteil gesichteter Protokolleinträge oder der Grad an Verringerung von Datenbankfeldern bei bereits bestehenden Verfahren.

2. KPIs des **innerorganisationellen Datenschutzmanagements**, die teilweise auf den KPIs des Betriebes aufsetzen: KPIs lassen sich auf der Basis von Zahlen für die folgenden Verfahren ermitteln:

   - Anzahl von Verfahren, die einen vollständigen Test- und Freigabeprozess durchlaufen haben,
   - Anzahl von Verfahren, die gemäß den Datenschutznormen (z. B. nach DSVO) dokumentiert sind,
   - Anzahl von Dokumenten eines Verfahrens, die gemäß DSVO die Dokumentation vervollständigen,
   - Anzahl von Verfahren, an deren Planung der oder die Datenschutzbeauftragte beteiligt war,
   - Anzahl von Verfahren, die von dem oder der Datenschutzbeauftragten innerhalb eines Zeitrahmens geprüft wurden,
   - Anzahl der Probleme mit Datenschutzbezug (Störungen, unzulässige Datenverarbeitung, Beschwerden).

3. KPIs mit **organisationsexterner Relevanz**, die die oberste Führungsebene der Organisation für Entscheidungen heranziehen: Neben den aggregierten Indikatoren, die aus den KPIs der unteren Ebenen zusammengesetzt werden, sind hier

Indikatoren zur Erfassung des Anteils von Verfahren innerhalb der gesamten Organisation sinnvoll, für die z. B. Datenschutzrichtlinien erarbeitet wurden oder die Auskunft zum generellen Datenschutzbewusstsein der Mitarbeiter und Mitarbeiterinnen der Organisation geben.

Um die Kennzahlen für Bewertungen nutzen zu können, müssen sie zu Bezugsgrößen in ein Verhältnis gesetzt werden (Benchmarking): Sinnvolle Bezugsgrößen sind normative Sollvorgaben – etwa die Anforderung gemäß DSVO, dass Verfahren vollständig und fortschreibend zu dokumentieren sind –, die entsprechende Anzahl aus der vorigen Messperiode, z. B. vom letzten Jahr, oder Maßzahlen, die man zum Vergleich aus anderen Organisation(seinheit)en bezieht. Wie auch immer: Dem oder der Datenschutzbeauftragten wird es anhand des Benchmarkings erleichtert, differenziert **Auskunft über die Datenschutzsituation** in seiner Organisation zu geben. Die Organisation wiederum kann gegenüber einer Aufsichtsbehörde belegen, dass – selbst wenn noch nicht alles perfekt ist – ein Weg der systematisch überwachten, kontinuierlichen Verbesserung eingeschlagen wurde.

Die Datenschutzorganisation muss dafür sorgen, dass die Prozesse einer Einheit in Bezug auf den rechtskonformen Umgang mit personenbezogenen Daten zunehmend verbessert werden, doch auch die Datenschutzprozesse unterliegen der Anforderung nach ständiger Verbesserung. Hier hat sich als bekanntestes Planungswerkzeug der **Deming-Zyklus** etabliert, wonach sich ein kontinuierlicher Verbesserungsprozess in vier Phasen („Plan – Do – Check – Act“) unterteilen lässt: Beim „Plan“ muss ein Problem exakt beschrieben und eine mögliche Verbesserung konzipiert werden; beim „Do“ sind notwendige Daten zu sammeln, zu analysieren und mögliche Fehlerquellen zu untersuchen; beim „Check“ sind Daten mit den Annahmen aus der „Plan“-Phase zu vergleichen und zu bewerten – entsprechend sind Maßnahmen zur Prozessveränderung vorzunehmen; beim „Act“ sind Entscheidungen für oder gegen eine Prozessänderung zu treffen und umzusetzen, und die Änderungen sind zu dokumentieren. Dann beginnt der nächste Zyklus einer Prozessverbesserung, wieder mit der „Plan“-Phase.

Was ist zu tun?
Es müssen Erfahrungen mit KPIs für Datenschutzprozesse gesammelt werden. Das ULD beteiligt sich an einem Pilotprojekt, dessen Ziel es ist, die Praxistauglichkeit der KPIs nachzuweisen und eine Vorlage zur Nutzung durch verschiedene Organisationen zu entwickeln.

6.11 Ergebnisse aus Kontrollen vor Ort

Im Zuge der Verwaltungsstrukturreform sollen die öffentlichen Verwaltungen in Schleswig-Holstein auf Landes- und Kreisebene sowie auf der Ebene der Städte, Gemeinden, Ämter und Zweckverbände „professioneller, bürgernäher und wirtschaftlicher“ gestaltet werden. Vor allem die mangelnde Steuerung von externen Dienstleistern führt häufig zu datenschutzrechtlichen Defiziten.

Das ULD hat die Verwaltungsstrukturreform zum Anlass genommen, **fusionierte Amtsverwaltungen** datenschutzrechtlich zu überprüfen. Warum sind hier immer noch so viele Beanstandungen nötig, wenn bei den zusammengelegten Verwaltungen das bestehende Wissen im Bereich Datenschutz doch verschmelzen und somit eher anwachsen konnte? Nachfolgend finden sich die häufigsten Fragestellungen, die sich bei Überprüfungen im Berichtszeitraum ergaben:

- Warum werden externe Dienstleister ohne vertragliche Regelungen eingeschaltet und deren Arbeit nicht kontrolliert?
- Warum existieren Nutzerkonten, deren Zweck niemand kennt?
- Warum wird durch einen Dienstleister eine Firewall installiert und dieser erklärt nicht, welche Regeln konfiguriert wurden?
- Warum ist es möglich, dass sich Nutzer mit einem „leeren“ Passwort im System anmelden können?
- Warum werden Sicherheitskomponenten des Betriebssystems, wie z. B. Gruppenrichtlinien, nicht eingeschaltet?
- Warum erfolgt keine Löschung der für die eigentliche Aufgabenerfüllung nicht mehr notwendigen Daten?
- Warum sind die installierten technischen Systeme, die eingesetzte Software und die gespeicherten Datenbestände so schlecht dokumentiert?

Die **Hitliste der Antworten** auf unsere Fragen:

- Der Abschluss der Fusion ist vorrangiges Ziel und der Datenschutz muss erst einmal „hinten anstehen“.
- Wir vertrauen den externen Dienstleistern, diese werden schon alles richtig machen.
- Wir, die Systemverantwortlichen, führen die Administration nur so „nebenbei“ aus und sind oft überfordert.

Die IuK-Systeme sowie die Datenverarbeitungsprogramme werden immer komplexer und damit störungsanfälliger. Gleichzeitig steigt quer durch alle Verwaltungen die **Abhängigkeit von den Systemen und Programmen**. Selbst kleinste Störungen können dazu führen, dass ein Verfahren ganz oder teilweise ausfällt. Deshalb entschließen sich öffentliche Verwaltungen dazu, ihre EDV-Systeme nicht mehr selbst zu warten, sondern externe Dienstleister damit zu beauftragen.

In einem Fall der datenschutzrechtlichen Prüfung einer einzigen Amtsverwaltung wurden **gleich drei externe Dienstleistungsfirmen** vorgefunden. Diese waren zuständig für

- die Administration der Terminalserver,
- die Administration und Konfiguration der Firewall sowie der Software zur Kontrolle der E-Mail- und Internetnutzung und
- die Administration des Verwaltungsnetzwerks.

Die Wartungsarbeiten erfolgten per Fernzugriff sowie vor Ort.

Wir **beanstandeten** folgende Punkte:

- Die Wartung der Systeme erfolgte stets unter derselben Nutzerkennung der Administration, unabhängig davon, wer gerade am System arbeitete.
- Eine Kontrolle der externen Dienstleister fehlte.
- Eine nachvollziehbare Dokumentation der administrativen Tätigkeiten war nur teilweise vorhanden.
- Die Dokumentation der installierten Firewallregeln wurde durch den Dienstleister nicht erstellt.
- Konfigurationseinstellungen der Internetverbindungen wurden nicht schriftlich vorgelegt.
- Vertragliche Regelungen für die externen Dienstleistungen bestanden nicht.

Dieses Bild hat sich in mehreren Prüfungen immer wieder gezeigt. Wir mussten feststellen: **Die Ämterfusion hat dem Datenschutz nicht genützt.** Die bereits vor der Fusion bestehenden Defizite in der Steuerung einer zunehmend komplexen IuK-Umgebung traten vielmehr noch deutlicher hervor.

Was ist zu tun?
Bei der Zusammenlegung von Verwaltungseinheiten muss das Wissen um den Datenschutz konzentriert werden. Die Systemadministratoren sind diesbezüglich auszubilden und zu fördern. Sie benötigen genügend Zeit und ausreichende Ressourcen für eine ordentliche Arbeit. Der Einsatz von externen Dienstleistern entbindet die Verwaltung nicht von der Pflicht, alle gesetzlichen Vorgaben für den Datenschutz und die Datensicherheit einzuhalten.

7 Neue Medien

7.1 Google Analytics und Dienste zu Tracking oder Reichweitenanalyse

„Wollen Sie Ihre Webseiten optimieren und für Werbung die beste Wirkung erzielen? Wollen Sie wissen, wo Ihre Besucher leben und wie sie mit Ihren Webseiten interagieren?“ So werben Dienste für das Tracking der Nutzer oder für Reichweitenanalysen. Viele Betreiber von Webseiten setzen solche Dienste ein, ohne diese auf Einhaltung der Datenschutzanforderungen überprüft zu haben.

Bereits im Jahr 2008 hatten wir den Webtracking-Dienst Google Analytics unter die Lupe genommen und festgestellt, dass der Einsatz dieses Dienstes in verschiedenen Punkten **gegen deutsches Recht verstößt** (31. TB, Tz. 7.2). Wir konfrontierten die Firma Google Inc. bzw. Google Germany GmbH als deutscher Google-Niederlassung mit unseren Feststellungen und drängten auf Änderung ihres Dienstes. Dies ist bis zum Redaktionsschluss nicht geschehen:

> **?** ***Tracking***
>
> *Unter Tracking versteht man das Nachverfolgen von Objekten oder Subjekten. Tracking von Webseitenbesuchern erfordert eine Wiedererkennbarkeit der jeweiligen Nutzer. Dies lässt sich z. B. über die Zuordnung von individuellen Cookies erreichen. Außerdem kann man über den sogenannten „Referer“, der vom Browser übertragen wird, auslesen, über welchen Link der Besucher auf die aktuelle Webseite gekommen ist. Während die statistischen Informationen darüber, welche Wege Besucher hauptsächlich auf einer Webseite nehmen, aus Datenschutzsicht unkritisch sind, kann das individuelle Tracking sehr viel über Interessen und Persönlichkeitsausprägungen eines Nutzers enthüllen.*

- Besucher von Webseiten bleiben im Unklaren über die genaue Verarbeitung ihrer Daten. Auch Webseitenbetreiber, die den Dienst Google Analytics nutzen, erhalten keine genauen Informationen darüber.
- Die Erstellung von Nutzungsprofilen ist nach dem Telemediengesetz nur bei Verwendung von Pseudonymen zulässig; die Profile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Da sich die Firma Google bestimmte Verknüpfungen mit anderen Daten und Weitergaben an Dritte vorbehält, konnten unsere Bedenken in diesem Punkt bislang nicht ausgeräumt werden.
- Nutzungsprofile dürfen nur erstellt werden, sofern der Webseitenbesucher nicht widerspricht; auf das Widerspruchsrecht muss der Diensteanbieter ihn hinweisen. Die Software von Google Analytics sieht diese Widerspruchsmöglichkeit jedoch nicht vor.
- Nach eigenen Informationen der Firma Google stehen die Server außerhalb der Europäischen Union. Eine Einwilligung der Betroffenen, dass ihre Nutzungsdaten dorthin übermittelt werden dürfen, liegt in der Regel nicht vor.

Unsere Auffassung wurde mittlerweile durch den **Düsseldorfer Kreis** als Zusammenschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich bestätigt: Der Beschluss „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internetangeboten“ vom November 2009 verdeutlicht die Anforderungen, die sich aus dem Telemediengesetz ableiten. Diese einheitliche Rechtsauffassung der Aufsichtsbehörden müssen Webseitenbetreiber nunmehr bei der Einbindung von Diensten zum Tracking und zur Reichweitenanalyse berücksichtigen.

> **?** ***Reichweitenanalyse***
>
> *Eine Reichweitenanalyse liefert Informationen über den Anteil der Zielpersonen, die über ein Medium oder einen Werbeträger erreicht werden. Auf ihrer Basis werden die Abrechnungen für Werbekunden erstellt.*

 http://www.lfd.m-v.de/dschutz/beschlue/Analyse.pdf

Auf dieser Basis haben wir **Webseitenbetreiber in Schleswig-Holstein** angeschrieben, die Google Analytics einsetzen, und sie dazu aufgefordert, den Einsatz des Dienstes einzustellen, die dazugehörigen Analytics-Konten zu löschen und die Firma Google Inc. schriftlich aufzufordern, die erlangten Nutzungsdaten zu löschen. Fast alle Betreiber kamen unserer Aufforderung umgehend nach.

Was ist zu tun?
Webseitenbetreiber müssen sich datenschutzkonform verhalten. Dies gilt auch beim Einbinden von zusätzlichen Diensten, an die Daten ihrer Besucher weitergeleitet werden. Anbieter und Entwickler von Diensten zum Tracking oder zur Reichweitenanalyse sollten etwaige datenschutzrechtliche Mängel abstellen, da anderenfalls der Einsatz der Dienste in Deutschland unzulässig ist.

7.2 Google Street View

Die Sonne scheint, der Himmel ist blau – schönes Wetter in Schleswig-Holstein. Dies war im Jahr 2009 das Signal für schwarze Autos mit Kameras auf dem Dach, die Straßen in vielen Städten abzufahren und die anliegenden Häuser zu fotografieren. Doch viele Hausbesitzer und Mieter sind damit nicht einverstanden.

Vor über einem Jahr waren erste Kamerawagen von Google Street View in **Schleswig-Holstein** „aus logistischen Gründen“ unterwegs, so die Auskunft des Konzerns (31. TB, Tz. 7.3). Seit Frühjahr 2009 gehört Schleswig-Holstein zum unmittelbaren Erfassungsgebiet. Zunächst kamen die größeren Städte dran, dann folgten einige Kreise.

Der Datenschutzbezug dieser Fotos liegt auf der Hand und wurde vom Düsseldorfer Kreis im November 2008 bestätigt: Veröffentlichungen von digitalen Straßenansichten und Bilddaten von Gesichtern, Kraftfahrzeugkennzeichen oder Hausnummern sind unzulässig, wenn keine hinreichende Anonymisierung erfolgt und

den betroffenen Bewohnern und Grundstückseigentümern keine ausreichenden **effektiven Widerspruchsmöglichkeiten** zur Verfügung gestellt werden. Um einen Widerspruch auszuüben, muss man allerdings erst mal wissen, dass und wo solche Kamerawagen unterwegs sind – und schon diese Vorabinformation seitens der Firma Google fehlte zunächst. Die Diskussionen mit Google Germany GmbH, die teilweise auch im Innen- und Rechtsausschuss des Schleswig-Holsteinischen Landtags geführt wurden, mündeten schließlich insbesondere in den folgenden Zusagen:

- Google gibt die geplanten Befahrungen mit einem Hinweis auf die Widerspruchsmöglichkeit im Internet rechtzeitig vorher bekannt und aktualisiert diese Information ständig.
- Vor der Veröffentlichung der Daten wendet Google eine Technik zur Verschleierung von Gesichtern und Kfz-Kennzeichen an.
- Google berücksichtigt die Widersprüche zu Personen, Kennzeichen und Gebäuden bzw. Grundstücken. Rechtzeitig vor der Veröffentlichung eingehende Widersprüche führen dazu, dass die entsprechenden Bilder so nicht veröffentlicht, sondern unkenntlich gemacht werden. Dies wirkt sich auch auf die Rohdaten aus. Voraussetzung ist eine Identifizierung des Grundstücks, der Person oder des Fahrzeugs.

Google informiert über die Befahrungen unter dem nicht gerade intuitiven Link:

http://maps.google.de/intl/de/help/maps/streetview/faq.html#q9

Wir haben angeregt, dass Google zusätzlich direkt Kontakt mit den betroffenen Kommunen aufnimmt, damit die Nachricht über die geplante Bilderfassung über lokale Magazine, Zeitungen oder sonstige Medien die Betroffenen erreichen kann. Dieser Vorschlag wurde unseres Wissens nirgends von Google umgesetzt. Im letzten Jahr musste Google sogar mehrfach einräumen, noch nicht einmal auf ihren eigenen Webseiten über die Erfassung größerer Städte vollständig und korrekt informiert zu haben. Bezeichnungen von Kreisen wie „Nordfriesenland“ oder „Segenberg“ zeugen nicht von besonderer Sorgfalt.

Widersprüche können per E-Mail unter Angabe des Absenders an streetview-deutschland@google.com oder schriftlich an „Google Germany GmbH, betr.: Street View, ABC-Straße 19, 20354 Hamburg“ eingelegt werden. Die Google Germany GmbH leitet dann die jeweilige Nachricht an die Google Inc. weiter. Google hat zugesagt, die Widersprüche zu bestätigen – auch dies war anfangs keine Selbstverständlichkeit. Für die Zukunft plant Google die Bereitstellung eines Online-Tools zum Einlegen des Widerspruchs mit unmittelbarer Kennzeichnung der Ortsinformation auf einer Karte. Natürlich muss der Widerspruch auch ohne Internetzugang möglich sein. Widersprüche können übrigens jederzeit eingelegt werden, also auch dann, wenn die Bilder schon veröffentlicht sein sollten.

Die Aufsichtsbehörden haben sich darauf verständigt, dass bei Einhaltung bzw. **Umsetzung eines 13-Punkte-Katalogs** keine weiteren grundsätzlichen Einwände gegen die Veröffentlichung im Internet erhoben werden. Gefordert wird darin u. a.

eine Beschreibung der Datenverarbeitungsprozesse und der technischen und organisatorischen Maßnahmen. Google hat zugesichert, diese Informationen nachzureichen. Dies betrifft auch den Umgang mit den Daten, die durch das Einlegen von Widersprüchen bei Google auflaufen. Die vollständige Liste der Zusagen von Google findet sich auf den Webseiten des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit.

www.hamburg.de/datenschutz/aktuelles/1569338/google-street-view-zusage.html

Was ist zu tun?
Google muss sich an seine Zusagen halten, d. h. vollständig über Befahrungspläne informieren, Widersprüche zum frühestmöglichen Zeitpunkt beachten und den Aufsichtsbehörden ausstehende Informationen nachreichen. Kommunen, in denen Google Street View Daten erfasst, sollten ihre Bürger darüber und über die Widerspruchsmöglichkeiten informieren.

7.3 Smart Meter – die Zukunft der Energieversorgung

Das Energiewirtschaftsgesetz regelt, dass von Januar 2010 an in Neubauten und bei Renovierungen von Gebäuden zur Verbesserung der Gesamtenergieeffizienz „intelligente“ Stromzähler einzubauen sind. Kundinnen und Kunden haben das Recht, von ihrem Versorger oder einem Dritten den Einbau dieser Messeinrichtungen zu verlangen.

Das Gesetz verpflichtet Energieversorgungsunternehmen, mit Ablauf des Jahres 2010 Verbrauchern Stromtarife anzubieten, die Anreize zur Einsparung oder Steuerung des Energieverbrauches mit sogenannten lastvariablen und tageszeitabhängigen Tarifen setzen. Zu diesem Zweck kommen „intelligente“ Zähler, sogenannte **Smart Meter**, zum Einsatz.

Zur Bewältigung der dabei anfallenden Datenmengen erlauben solche Zähler das kontaktlose Auslesen der erhobenen Informationen und die Übermittlung an Sammelstellen via Internet oder Funkverbindung. Die Besonderheit der Smart Meter besteht somit in der **Menge und der Qualität der Daten**, die erhoben und verarbeitet werden können. Diese Datenverarbeitung wäre durch die bisher üblichen Ferraris-Zähler nicht zu bewältigen.

? Smart Meter

„Intelligente“ Zähler für die Messung des Verbrauches von Strom, Gas und weiteren Versorgungssparten werden Smart Meter genannt. Sie messen nicht nur den Gesamtverbrauch, sondern den Verbrauch geräte- und zeitbezogen in einer Form, dass spezifische Verhaltens- und Nutzungsprofile erstellt werden können.

Durch Smart Meter erhobene Verbrauchsinformationen von Privathaushalten sind oft **personenbezogene Daten**. Sie geben Auskunft über die persönlichen und

sachlichen Lebensverhältnisse der Nutzerinnen und Nutzer. Die menschliche Existenz in einer modernen Gesellschaft in einer hoch technisierten und automatisierten Umgebung ist eng mit dem Verbrauch von Energie verbunden. Es gibt kaum noch menschliche Aktivitäten, die nicht unmittelbar oder zumindest mittelbar zu einem spezifischen Energieverbrauch führen. Ein Großteil des heutigen Kommunikations- und Freizeitverhaltens ist ohne Elektrizität nicht denkbar. Tagesabläufe spiegeln sich in der Nutzung von Energie wider. Diese Abhängigkeit führt dazu, dass die gerätegenaue Erfassung verbrauchter Energie zu einer Ausforschung der Lebensgewohnheiten der Betroffenen führen kann.

Die elektronische Verarbeitung von Energieverbrauchsdaten erlaubt die jederzeitige und quantitativ unbegrenzte Erfassung, die Speicherung und Auswertung ohne Rücksicht auf Entfernungen in Sekundenschnelle sowie entsprechende Abrufe. Diese Informationen können mit anderen Daten verschnitten werden und bergen das Potenzial für anderweitige Nutzungen. Fernübermittlung bzw. Fernabruf gefährden zugleich die **Transparenz für die Verbraucher** und eröffnen ohne hinreichende Sicherungsmaßnahmen Missbrauchsrisiken.

Smart Meter sind nur eine Wegmarke in der Entwicklung der modernen Mess- und Regelungstechnik. Es ist absehbar, dass sie nur ein Baustein in „intelligenten“ Versorgungsnetzen, sogenannten **Smart Grids**, sein werden. Bereits jetzt muss bei der technischen Entwicklung der Geräte und Geschäftsprozesse dieser weitere Schritt berücksichtigt werden. Die Transparenz der Datenverarbeitung, Datensparsamkeit und -minimierung sowie die Datensicherheit sollten bereits von Beginn an im technischen Gerätedesign implementiert werden. Der Verbraucher soll selbst entscheiden können, wer zu welchem Zweck seine Verbrauchsdaten verarbeiten und nutzen darf.

Das ULD hat in einem ersten **Gutachten** zu den datenschutzrechtlichen Fragen beim Einsatz von Smart Metern Position bezogen, ist in die Diskussionen mit Herstellern, Anwendern und Verbänden einbezogen und wird weiter aktiv die Entwicklung und den Einsatz „intelligenter“ Zähler und Versorgungsnetze begleiten.

https://www.datenschutzzentrum.de/smartmeter/

7.4 Veröffentlichungen im Internet

Die Übermittlung personenbezogener Daten im Internet an einen nicht einschränkbaren Empfängerkreis, also die globale elektronische Veröffentlichung, stellt eine rechtlich noch nicht ansatzweise gelöste Herausforderung dar.

Um nicht zu dem Ergebnis zu kommen, dass personenbezogene Daten überhaupt nichts im Internet verloren haben, hatte im November 2003 der Europäische Gerichtshof in der Lindqvist-Entscheidung gemeint, **personenbezogene Daten im Internet** würden nicht aus der Europäischen Union heraus übermittelt. In der Spickmich-Entscheidung vom Juni 2009 entschied nun der Bundesgerichtshof

(BGH), dass es sich bei Internetveröffentlichungen wohl um eine Datenverarbeitung zum Zweck der Übermittlung nach dem BDSG handelt, erklärte aber – contra legem – einige gesetzliche Anforderungen hierfür einfach für nicht anwendbar und rechtfertigte dies mit den in Art. 5 Grundgesetz garantierten Rechten auf Meinungsäußerung und Informationsfreiheit.

Beide Entscheidungen zeigen, dass unser Datenschutzrecht auf europäischer wie nationaler Ebene **keine adäquaten Antworten** parat hat, um Persönlichkeitsschutz und Informationsfreiheit im Internet zu einem Ausgleich zu bringen (30. TB, Tz. 2.2). Tatsächlich werden die Datenschutzaufsichtsbehörden täglich genau mit dieser Ausgleichsaufgabe betraut, ohne hierfür eine gesetzliche Richtschnur zu haben. Zumindest mittelfristig kann gegenüber öffentlichen Stellen, z. B. Schulen, mit Mühe noch die Wahrung des Persönlichkeitsschutzes durchgesetzt werden (Tz. 4.7.1). Doch bei der Masse der Beschwerden gegen private Webseitenanbieter fehlen uns rechtlich oder faktisch häufig die nötigen Mittel.

Mit der Spickmich-Entscheidung des BGH wurde die bisherige Position des ULD bestätigt, dass bei personenbezogenen Veröffentlichungen generell das BDSG anwendbar ist und – bei Fehlen einer wirksamen Einwilligung des Betroffenen – regelmäßig eine **Abwägung** zwischen Veröffentlichungs- und Geheimhaltungsinteresse vorgenommen werden muss. Neben dieser groben Linie gibt es viele spezifische Fragen, zu denen unser Recht – wenn überhaupt – oft nur zufällig eine Antwort gibt. Nötig bleibt ein gesondertes separates Kapitel im BDSG mit der Überschrift „Veröffentlichung im Internet“. Bedauerlich ist, dass dieser Bedarf im Bundesinnenministerium nicht erkannt wird, wie eine aktuelle Stellungnahme des dortigen zuständigen Staatssekretärs offenbarte.

https://www.datenschutzzentrum.de/internet/200909-weichert-vur-datenschutz-bei-internetveroeffentlichungen.pdf

Was ist zu tun?
Ins BDSG muss ein Kapitel aufgenommen werden, das materielle Voraussetzungen und datenschutzrechtliche Verfahren bei Internetveröffentlichungen regelt.

7.4.1 Werbung mit Schülerdaten

Wieder wurden wir mit dem problematischen Umgang mit Kundendaten durch Veranstalter von Schüler- und Sprachreisen konfrontiert.

Veranstalter greifen gerne zum Mittel der „**Referenzen**“, um für ihre Angebote zu werben. Dafür werden Namen und Adressen, Telefonnummern oder Bilder von Teilnehmerinnen und Teilnehmern von Reisen im Internet einer weltweiten Öffentlichkeit zur Verfügung gestellt. Derartige Veröffentlichungen sind datenschutzrechtlich nur zulässig, wenn die Betroffenen explizit eingewilligt haben. Bei Minderjährigen ist darauf zu achten, dass diese die Tragweite ihrer Entscheidung nicht übersehen können.

Was ist zu tun?
Es muss Allgemeinwissen werden, dass Informationen im Internet potenziell für unbestimmte Zeit einer weltweiten Öffentlichkeit zur Verfügung stehen. Vor und nicht nach der Veröffentlichung ist zu prüfen, ob Datenschutzbelange einer Veröffentlichung entgegenstehen.

7.4.2 Unfallfahrzeug im Netz

Ein Bürger entdeckte im Internet Bilder des bei einem Verkehrsunfall stark beschädigten Kraftfahrzeuges seiner Tochter. Das mit der Bergung beauftragte Abschleppunternehmen hatte es sich zur Gewohnheit gemacht, an der Unfallstelle und in der Werkstatt aufgenommene Bilder der beschädigten Fahrzeuge zu Werbezwecken auf seine Homepage zu stellen.

Zwar war das Kfz-Kennzeichen des abgebildeten Fahrzeuges mit einem Balken abgedeckt, doch erinnerten die Bilder den Vater auf unangenehme Weise an den Verkehrsunfall und die Verletzungen seiner Tochter. Das Abschleppunternehmen weigerte sich, die entsprechenden Bilder von der Homepage zu nehmen. Wir konnten dem Vater nicht helfen. Die veröffentlichten Fahrzeugbilder waren nicht personenbezogen, da für Dritte keine Rückschlüsse auf natürliche Personen möglich waren. Durch **Unkenntlichmachung des Kennzeichens** hat das Abschleppunternehmen bereits das Erforderliche getan, um eine hinreichende Anonymisierung der Fotos zu erreichen.

Der Vater meinte, Neugierige könnten auf Grundlage der veröffentlichten Bilder bei der Polizei das Kennzeichen oder den Fahrer telefonisch erfragen. Nach den Vorschriften des Landesverwaltungsgesetzes darf und wird nach allen vorliegenden Erfahrungen die Polizei solche Auskünfte nur zur konkreten Gefahrenabwehr – eine hier nicht vorstellbare Konstellation – übermitteln. Abbildungen von **Gegenständen** ohne Bezug zum Eigentümer oder Nutzer fallen grundsätzlich nicht unter den Schutzbereich des Bundesdatenschutzgesetzes.

8 Modellprojekte und Studien

Neben seiner Prüf- und Beratungstätigkeit beteiligt sich das ULD an drittmittelfinanzierten Projekten und Studien mit besonderem Datenschutzbezug. Für Forscher und Entwickler werden Datenschutzkriterien erarbeitet, die sie in ihrer wissenschaftlichen Tätigkeit oder bei der Erstellung von Produkten berücksichtigen können oder müssen. Mit unserer Hilfe versuchen sie über das gesetzlich notwendige Mindestmaß an Datenschutz hinauszugehen und sogenannte „**datenschutzfördernde Technik**“ zu entwickeln. Seit Mitte der 1990er-Jahre wird dieses Ziel zunehmend von Datenschutzdienststellen unterstützt; im Jahr 2007 erhielt dieser Trend Rückenwind durch die „Mitteilung der Kommission an das Europäische Parlament und den Rat über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre“. Über das ULD-i (Tz. 8.1) haben wir auch im Berichtsjahr deutsche und europäische Fördermittel eingeworben, um an Projekten (Tz. 8.2 bis Tz. 8.4, Tz. 8.6 bis Tz. 8.9) mitwirken zu können. Weitere Einnahmen sind für die Erstellung von Studien (Tz. 8.5) zu verzeichnen.

8.1 ULD-i – das Innovationszentrum Datenschutz & Datensicherheit

Das Innovationszentrum Datenschutz & Datensicherheit engagiert sich für die Integration des Datenschutzes in Anwendungen und Produkte von Anfang an und berät Interessenten bei allen Fragen zu Datenschutz und Datensicherheit. Schleswig-holsteinische Unternehmen und Hochschulen nehmen diese Serviceleistungen weiterhin gerne in Anspruch. Dies führt zu einer Stärkung des Datenschutz-Know-hows im Norden.

Im Jahre 2009 konnten neben den Projekten mit der Wirtschaft die **Kooperationen mit den wissenschaftlichen Einrichtungen** des Landes Schleswig-Holstein intensiviert werden. Neben der Fortsetzung mehrerer erfolgreicher Vorlesungsreihen zu Datenschutz und Datensicherheit wurde die wissenschaftliche Zusammenarbeit in einem Projekt zur Standardisierung von Datenschutzprozessen mit der Christian-Albrechts-Universität zu Kiel, Bereich Wirtschaftsinformatik, ausgebaut.

Auch künftig gehört es zu den Zielen des ULD-i, das Thema Datenschutz auf **Messen und Veranstaltungen** publikumswirksam zu platzieren. Wie in den vorangegangenen Jahren vermittelt das ULD-i dazu Vortragende und Diskutanten u. a. für die CeBIT und die „Mediatage Nord“.

Was kann das ULD für Sie tun?

Nehmen Sie Kontakt zu uns auf:

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

8.2 PrimeLife – Identitätsmanagement im Fokus

Das von der EU geförderte Projekt PrimeLife verfolgt das Ziel, Menschen in ihrer informationellen Selbstbestimmung durch nutzergesteuertes Identitätsmanagement zu unterstützen. Die Arbeit an den Konzepten ist weit fortgeschritten. Nun sollen Prototypen zeigen, dass sich die Ideen auch in die Praxis umsetzen lassen.

> **?** ***PrimeLife***
>
> *Das auf drei Jahre ausgerichtete Projekt PrimeLife (Privacy and Identity Management in Europe for Life) ist im März 2008 gestartet. Zusammen mit 14 Projektpartnern aus neun Ländern arbeiten wir an Datenschutzkonzepten für Identitätsmanagement, wobei die Selbstbestimmung der Nutzer und innovative Datenvermeidungsstrategien im Vordergrund stehen.*

Unsere Rolle besteht darin, die Forschung und Entwicklung der anderen Projektpartner datenschutzrechtlich zu begleiten, Konzepte für besseren Datenschutz in interdisziplinären Teams zu entwickeln, ihre Handhabbarkeit in der Praxis, die „Usability“, zu verbessern, Projektergebnisse mit einer externen Expertengruppe zu diskutieren, sie in geeigneter Form in die Standardisierung zu geben (Tz. 8.3) und über die Projektwebseite und andere Medien zu veröffentlichen (30. TB, Tz. 8.3). Im Berichtsjahr waren wir Co-Ausrichter der „PrimeLife Summer School“ mit 60 Teilnehmenden. Diese Veranstaltung diente dem Austausch und **wissenschaftlichen Diskurs** zwischen langjährigen Datenschutzforschenden auf der einen Seite und Studierenden auf der anderen Seite, die in ihrem Studium einen Fokus auf Datenschutzfragen legen.

Ein wichtiges Thema ist für uns Datenschutz in **sozialen Netzwerken**: Der Empfehlung, möglichst wenige personenbezogene Daten über sich preiszugeben oder lediglich unter Pseudonym aufzutreten, wollen viele Nutzerinnen und Nutzer nicht folgen, weil sie ja gerade die sozialen Netzwerke als Treffpunkt und Plattform für Nachrichtenaustausch verwenden. PrimeLife arbeitet an Konzepten, bei denen die Daten verschlüsselt vorliegen und die Betroffenen definieren können, für welche ihrer Freunde welche Daten im Klartext sichtbar sind. Diese Methode verringert die Missbrauchsmöglichkeiten deutlich. Anhand eines Prototyps wird erprobt, wie gut sich die Datenschutzkonzepte in der Praxis behaupten.

Ein weiterer Fokus unserer Arbeit liegt auf der Entwicklung von Konzepten für Delegation bei der Wahrnehmung der eigenen Datenschutzrechte. Wenn in Systemen zum „**nutzergesteuerten Identitätsmanagement**“ die Nutzer stärker einbezogen werden, ist es nötig, ihnen Hilfe zu bieten, wenn sie für eine kurze oder längere zeitliche Periode ihre Rechte nicht selbst wahrnehmen können. Sie sollen Personen ihres Vertrauens benennen können, die in ihrem Auftrag handeln und sie insbesondere in Datenschutzfragen nach außen vertreten. Heutzutage nicht selten praktizierte Lösungen, einer anderen Person einfach seinen Log-in-Namen und das Passwort oder eine Chipkarte und die dazugehörige PIN zu geben, die online so dem Diensteanbieter gegenüber auftritt, sind unbefriedigend und sogar riskant für die Beteiligten – es ist nämlich für den Diensteanbieter nicht unterscheidbar, ob ein Identitätsdiebstahl oder ein autorisiertes Delegationsverhältnis vorliegt. Auch ist es für den Betroffenen schwierig nachzuprüfen, was in seinem Namen getan wurde, und effektiv einzugreifen, wenn er damit nicht einverstanden ist. Diese Probleme lassen sich lösen, indem der Betroffene für seine Vertreter eigene Zugriffsdaten besorgt und die Regeln, nach denen die Vertreter für ihn agieren sollen, im Vorfeld festlegt. Im nächsten Schritt werden wir untersuchen, wie eine solche Delegation in Identitätsmanagementsystemen praktisch umsetzbar ist.

Die PrimeLife-Arbeiten sind von Nutzen bei Prüfungen und Beratungen des ULD. Lösungen für **handhabbare Delegationsmethoden** und Realisierungsmöglichkeiten für Datensparsamkeit und Selbstbestimmung der Betroffenen werden in langfristig angelegten Datenschutzkonzepten dringend benötigt. Neben Großprojekten wie der elektronischen Gesundheitskarte, die in Schleswig-Holstein getestet wurde, betrifft dies beispielsweise E-Government- und E-Commerce-Anwendungen im Kontext des elektronischen Personalausweises, der Ende 2010 eingeführt werden soll.

www.primelife.eu/

Was ist zu tun?
Wer Software entwickelt, die personenbezogene Daten verarbeitet, sollte sich überlegen, wie sich die Prinzipien Datensparsamkeit und Selbstbestimmung der Nutzer technisch umsetzen oder unterstützen lassen.

8.3 FIDIS – ein Projekt geht erfolgreich zu Ende

Nach mehr als fünf Jahren hat das Exzellenznetzwerk FIDIS (Future of Identity in the Information Society) seine Ergebnisse auf einer Abschlussveranstaltung vorgestellt – und die können sich sehen lassen.

Seit Beginn des FIDIS-Projekts im März 2004 haben wir jährlich über Fortschritte berichtet (31. TB, Tz. 8.4). Im Sommer 2009 wurde das Projekt abgeschlossen. Es hinterlässt einen reichen Schatz an Ausarbeitungen, die sogenannten „Deliverables“, die in englischer Sprache Themen rund um die Identität mit unmittelbarem Bezug zum Datenschutz bearbeiten: Zumeist geht es direkt um personenbezogene Daten. Aber selbst dann, wenn der Bezug zu einer einzelnen Person nicht unmittelbar bekannt ist, können Risiken durch **Auswirkungen auf die Privatsphäre** der Betroffenen bestehen.

> **?** ***FIDIS***
>
> *Im Projekt FIDIS (Future of Identity in the Information Society) arbeitete das ULD mit weiteren 23 Partnern aus 12 Ländern zusammen in einem sogenannten „Network of Excellence“. Ergebnisse des Projekts sind europäische Studien, Berichte und Artikel zu verschiedenen Aspekten von Identität, Identifizierung und Identitätsmanagement, die unter www.fidis.net, als Broschüren oder in Zeitschriften publiziert werden.*

Wir waren bei datenschutzrechtlichen wie auch bei technischen Aspekten im Umfeld von Datenschutz und Datensicherheit gefragt, beispielsweise in den Bereichen Biometrie, E-Government, elektronische Ausweise (eIDs) wie maschinenlesbare Reisedokumente, Funkchips, Identitätsmanagementsysteme, Profiling oder Public-Key-Infrastrukturen. Die FIDIS-Resultate dienen als Materialsammlung für Datenschutzdiskussionen auf nationaler und europäischer Ebene – die Artikel-29-Datenschutzgruppe oder die Europäische Agentur für Netz- und Informationssicherheit (ENISA) haben mehrfach auf Ergebnisse der FIDIS-Arbeiten Bezug genommen. Der im Rahmen von FIDIS diskutierte und modellierte Prozess eines Datenschutzmanagements analog zu bekannten IT-Sicherheitsmanagementprozessen wurde von uns in die neuen Fassungen der IT-Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI) eingebracht. Die **Ergebnisse des FIDIS-Projekts**, die jeweils von mehreren europäischen Experten zusammen erarbeitet und qualitätsgesichert worden sind, helfen dem ULD konkret bei der Arbeit, z. B. wenn wir Konzepte auf Basis neuer Technologien bewerten sollen oder wenn wir um Beratung in Fragen der zukünftigen Gestaltung von Datenschutzgesetzen gebeten werden.

Weitere Informationen rund um das Thema Identität und FIDIS-Projektergebnisse sind verfügbar unter:

www.fidis.net/

Was ist zu tun?
Auch nach dem Projektende von FIDIS lohnt sich bei identitätsbezogenen Themen eine Recherche in den erstellen Materialien. Interessierte können die Experten in dem ehemaligen Netzwerk direkt ansprechen, wenn sie einen Informations- und Erfahrungsaustausch wünschen.

8.4 Erfolgreicher Abschluss des Projekts bdc\Audit

Biobank Data Custodianship/Audit Methodology and Criteria – unter diesem Langtitel präsentiert das ULD Methoden, Kriterien und Handlungsempfehlungen für die Datenschutzauditierung der Datentreuhänderschaft in der Biobankforschung.

Seit mehreren Jahren befassen wir uns intensiv mit dem Thema **Datenschutz in der Biobankforschung**. Dabei waren wir insbesondere in dem vom Bundesministerium für Bildung und Forschung geförderten Projekt bdc\Audit engagiert (31. TB, Tz. 8.10; 30. TB, Tz. 8.11). Es ging um die Entwicklung von Methoden und Kriterien für eine praxisgerechte und zugleich datenschutzfreundliche Biobankforschung. Die empirischen Erhebungen haben ergeben, dass der Datenschutz bei Biobanken in Deutschland stark verbesserungsfähig und -bedürftig ist.

Der aus dem Projekt resultierende Bericht analysiert die bestehenden nationalen und internationalen Regelungen zum Datenschutz bei Biobanken und zu deren Auditierung und leitet daraus einen **umfassenden Kriterienkatalog** ab. Dieser Katalog für die datenschutzgerechte Gestaltung von Biobanken gibt Betreibern die Möglichkeit, ihre Biobank einer Überprüfung aus datenschutzrechtlicher Sicht zu unterziehen und so eine Verbesserung des Datenschutzniveaus vorzunehmen. Zentrales Instrument ist dabei ein differenziertes Verfahren der technischen Pseudonymisierung von medizinischen und genetischen Forschungsdatensätzen, verbunden mit einer strikten Trennung der identifizierenden Daten von den pseudonymisierten Forschungsdaten. Insbesondere bei langjährig geführten Biobanken sind zur effektiven Wahrung der Privatsphäre eine größtmögliche Transparenz für die Öffentlichkeit und die Probanden sowie differenzierte Wahlmöglichkeiten für die Betroffenen nötig. Die Probanden müssen über die gesamte Dauer der Forschungsprojekte kontinuierlich informiert werden; außerdem müssen sie die Möglichkeit haben, bestimmte Forschungszwecke und Forschungsprojekte auszuschließen und über die Rückmeldung von Forschungsergebnissen zu entscheiden.

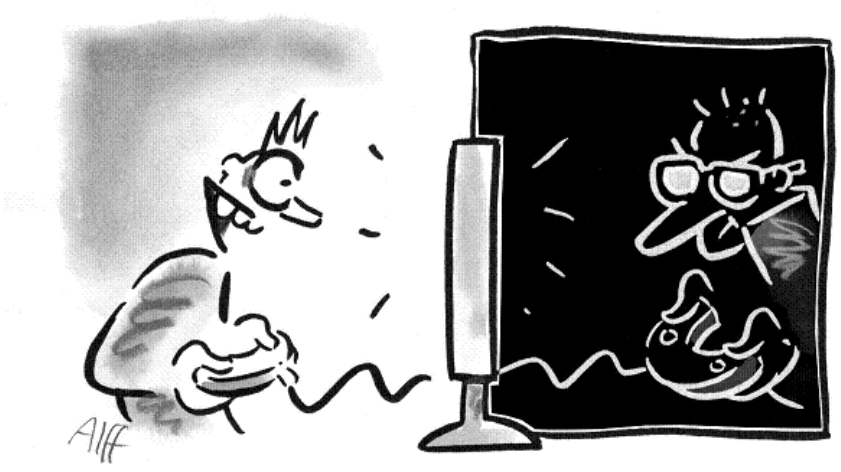

www.datenschutzzentrum.de/biobank/

Was ist zu tun?
Die praktischen Handlungsanleitungen müssen umgesetzt werden. Nötig bleibt eine gesetzliche Regelung der Biobankforschung, die die Rechte der Probanden angemessen schützt.

8.5 Der datengeschützte Online-Spieler

Das Projekt DOS (Datenschutz in Online-Spielen) wurde erfolgreich abgeschlossen. Ein Leitfaden erleichtert es nationalen und internationalen Anbietern solcher Spiele, diese datenschutzgerecht zu entwickeln und zu betreiben. Der Leitfaden und die ausführlichere Studie informieren Spieler über Gefahren und ihre Rechte.

Das DOS-Projekt wurde von September 2007 bis Dezember 2009 vom Bundesministerium für Bildung und Forschung gefördert (31. TB, Tz. 8.7). Wir untersuchten und systematisierten das Angebot an solchen Spielen und identifizierten 27 einzelne **Funktionen mit Datenschutzrelevanz**. Diese Funktionen umfassen generelle Punkte wie die Internetanbindung als auch Spezielles, etwa zu Highscore-Listen, der möglichen Einbindung von Webcams oder der gezielten Werbung innerhalb von Online-Spielen. Neue Entwicklungen während der Projektlaufzeit wurden betrachtet, z. B. die Integration von Spielen in soziale Netzwerke wie Facebook und studiVZ.



Ein von uns entwickelter **Leitfaden** gibt für jede der 27 Funktionen Hinweise, welche Rechtsnormen einschlägig sind und was diese konkret für Hersteller und Betreiber der Spiele bedeuten. Beispiele erleichtern Anbietern die Umsetzung unserer Empfehlungen. Die ausführlichen rechtlichen Hintergrundinformationen werden in einer umfassenden Studie beschrieben. Diese wird durch Ergebnisse einer Umfrage, die Darstellung von möglichen Geschäftsmodellen, sozio-ökonomische Erwägungen und einen Ausblick auf zukünftige Entwicklungen abgerundet.

Wir haben 2009 zahlreiche Vorträge zum Datenschutz in Online-Spielen gehalten und **zwei Workshops** veranstaltet. Dabei wurden Spielerinnen und Spieler eingebunden. Die Ergebnisse wurden Herstellern und Betreibern der Spiele und ihren juristischen Beratern vorgestellt und hinsichtlich der Praxisrelevanz und Umsetzbarkeit diskutiert. Dabei wurde eine bei allen Beteiligten bestehende große Unsicherheit beim Umgang mit dem Thema Datenschutz offenbar.

Kaum ein auf dem Markt befindliches Spiel erfüllt die **deutschen Datenschutzbestimmungen**. Datenschutzerklärungen sind kaum verständlich und oft rechtlich zu kritisieren: Viele Anbieter stufen fälschlicherweise die übertragenen IP-Adressen der Spielenden als nicht schutzbedürftige Daten ein; Informationen werden abgefragt, ohne dass deren Erforderlichkeit erkennbar ist; teilweise erfolgen weitgehende Überwachungen des Spielverhaltens und der Kommunikation, ohne dass der Spieler hierüber informiert wird, geschweige denn um seine Einwilligung gebeten wird. Doch wir haben auch positive Beispiele insbesondere von deutschen Anbietern erlebt, die gezielt über das Thema Datenschutz Vertrauen bei den Spielern aufbauen wollen.

Weitere Informationen zum Projekt und die Dokumente befinden sich im Internet unter:

www.datenschutzzentrum.de/dos/

Was ist zu tun?
Viele Hersteller und Betreiber müssen ihre Online-Spiele an die gesetzlichen Forderungen anpassen. Die Spieler sind über ihre Rechte und Möglichkeiten zu informieren. Dazu werden wir unsere Erkenntnisse weiterverbreiten. Der im Projekt entwickelte Leitfaden sollte regelmäßig fortgeschrieben werden. Hierfür suchen wir Kooperationspartner.

8.6 AN.ON – Anonymität.Online

Internetnutzende haben weiterhin die Möglichkeit, anonym im Web zu surfen, indem sie den Anonymisierungsdienst „AN.ON – Anonymität.Online“, der u. a. vom ULD betrieben wird, nutzen. Trotz Pflicht zur Vorratsdatenspeicherung wird die Anonymität der Webzugriffe gewahrt.

? Wie nutzt man den AN.ON-Dienst?

Mithilfe der kostenlosen Software JAP (bzw. nunmehr Jondo) wird die anonyme Nutzung von Diensten des World Wide Web ermöglicht. Dabei wird der Kontakt zu den Webservern nicht, wie normalerweise üblich, unmittelbar aufgenommen, sondern für den Nutzer unsichtbar über eine Kette von Anonymisierungsservern (sogenannte Mixserver) geleitet. Diese sorgen dafür, dass niemand Kenntnis von der IP-Adresse des Nutzers erlangen kann. Die Kette von Mixservern mit dem ULD-Rechner wird in der Regel von mehr als 1.000 Personen gleichzeitig genutzt.

Seit 2001 betreibt das ULD gemeinsam mit Partnern den Anonymisierungsdienst für Webzugriffe „AN.ON – Anonymität.Online“ (31. TB, Tz. 8.5). Seit Anfang 2009 ist die **Vorratsdatenspeicherung** durch Internetprovider umzusetzen, weshalb zu klären war, ob dies auch für AN.ON gilt. Nach unserer Interpretation ist der AN.ON-Dienst vor allem ein Telemediendienst, der nicht gegen Entgelt angeboten wird und für den keine Pflicht zur Vorratsdatenspeicherung besteht. Die Bundes-

netzagentur meint aber, dass anfallende Verbindungsdaten auch vom AN.ON-Dienst für sechs Monate aufzubewahren sind. Daher aktivierten wir diese Speicherung in unserem Mixserver und informierten die Nutzer hierüber auf der Webseite des Dienstes.

Trotz Vorratsdatenspeicherung können die über den AN.ON-Dienst abgewickelten Webzugriffe von den einzelnen Betreibern **keinen individuellen Nutzern zugeordnet** werden. Eine solche Zuordnung ist nur möglich, wenn die von uns gespeicherten Daten von Ermittlungsbehörden mit denen der anderen Mixserver in derselben Kette zusammengebracht werden. Es bleibt also trotz Vorratsdatenspeicherung bei der Aussage, dass der Dienst vor der Identifikation durch den einzelnen Betreiber eines Mixservers schützt.

Die Anfragen der Ordnungsbehörden beschränkten sich 2009 in der Regel auf einfache Bestandsdatenabfragen. Mangels Registrierungspflicht der Nutzenden des Dienstes konnten und mussten wir diese nicht beantworten. Gerichtliche Anfragen mit Bezug auf die Vorratsdatenspeicherung blieben aus. Wir erhielten **eine gerichtliche Überwachungsanordnung**, der wir entsprechend nachgekommen sind. Die Anordnung war sehr allgemein gefasst und in der uns zunächst übermittelten Fassung erst nach weitgehender Interpretation und Rücksprache mit den ermittelnden Beamten ausführbar. Der von uns dagegen eingereichten Beschwerde wurde vom Beschwerdegericht weitgehend entsprochen; wir erhielten daraufhin eine präzisere Ausfertigung.

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

Was ist zu tun?
Wir werden mit dem ULD-Mixserver unseren Beitrag, wie gesetzlich gefordert, zu einer anonymen Nutzungsmöglichkeit des Webs leisten. Im Kontakt mit Behörden und Gerichten werden wir auf die Präzisierung etwaiger Überwachungsanordnungen hinwirken, um Eingriffe in die Rechte der Internetnutzer so gering wie möglich zu halten.

8.7 RISERid (Registry Information Service on European Residents Initial Deployment)

Die europäische Melderegisterauskunft RISER geht 2010 ins sechste Jahr und zeigt, wie erfolgreiches E-Government und Datenschutz zugleich vorbildlich umgesetzt werden können.

Dieses E-Government-Projekt kann auf eine erfolgreiche Geschichte zurückblicken: Seit März 2004 wird das in Berlin entwickelte und von der Europäischen Kommission im Rahmen des eTEN-Programms geförderte Verfahren auf europäischer Ebene ausgerollt. Im Meilensteinbericht der EU-Kommission heißt es dazu:

„RISER is an **excellent success story** for EU funded implementation of new telematics solutions and for the eTEN programme in particular."

Die datenschutzgerechte Ausgestaltung des Dienstes, der seit 2007 kommerziell von der RISER ID Services GmbH betrieben wird, war stets ein Anliegen aller Beteiligten. RISER leitet elektronische **Anfragen an Einwohnermeldebehörden** in zehn europäische Länder weiter. Bis zu 150.000 Anfragen an Meldebehörden werden bei RISER monatlich zentral angefragt und abgeholt. Slowenien und Finnland sollen als Nächstes hinzukommen. Die Reichweite für elektronische Anfragen in Deutschland erlangte 72 % im Jahr 2009. In Europa werden 246 Millionen Einwohner erreicht; das sind 52 % der Bevölkerung. Der Dienst bietet seinen Kunden einen einheitlichen Zugang zu einer sehr heterogenen und unübersichtlichen Melderegisterlandschaft in Europa. Über das Serviceportal werden Meldeanfragen als Datei- oder Einzelanfrage über das Internet an die zuständige Meldebehörde weitergeleitet. RISER übernimmt die Funktion eines Vermittlers und Zustellers. Im Sinne der Auftragsdatenverarbeitung werden die von den RISER-Kunden überlassenen personenbezogenen Daten ausnahmslos zu den vertraglich festgelegten Zwecken und nach den vertraglich festgelegten datenschutzkonformen Verfahren verarbeitet. Auskünfte werden ausschließlich fallbezogen für den jeweiligen Kunden verarbeitet, die Ergebnisse ausschließlich für diesen bereitgehalten. RISER speichert keine Ergebnisse aus Melderegisterauskünften für eigene Zwecke, macht sie nicht Dritten zugänglich und überführt die Adressen auch nicht in einen sogenannten Treuhandpool.

Das Angebot von RISER unterscheidet sich durch die strikte Zweckbindung im Rahmen der Auftragsdatenverarbeitung von dem Angebot der sogenannten Adresshändler und Auskunfteien. Insbesondere das Sammeln von Adressdaten in sogenannten **Treuhandpools** (31. TB, Tz. 4.1.3) für eine eventuelle Weiterverwendung ist datenschutzrechtlich problematisch. Der Adresssammler oder der Pool muss sich seinerseits auf eine eigene Rechtsgrundlage für die Datenverarbeitung berufen können. Eine Datenverarbeitung im Auftrag liegt in diesen Fällen in der Regel nicht vor. Der Dienstleister bzw. Treuhänder speichert die Daten für eigene Zwecke. Die Einstellung der im Rahmen einer einfachen Melderegisterauskunft erlangten Adressdaten in den Pool ist nicht mehr vom durch den vom Auftraggeber verfolgten Geschäftszweck abgedeckt. Diesem geht es um die Erlangung der gewünschten Auskunft; mehr sieht das Melderecht auch nicht vor. Ein weiteres Vorhalten der Daten ist für den Auftrag nicht erforderlich. Es dient ausschließlich dem Dienstleister, der aus dem Pool der gespeicherten Adressen andere anfragende Stellen beauskunftet. Der Geschäftszweck der Auftraggeber lässt sich wegen der melderechtlichen Restriktionen auch nicht auf eine Auftragsdatenverarbeitung im Rahmen eines treuhänderisch verwalteten Datenpools ausweiten.

Das über RISER bei einer Meldebehörde anfragende Unternehmen darf die durch die Meldeauskunft akualisierte Adresse nur dann für **Zwecke der Werbung und Markt- oder Meinungsforschung** nutzen, wenn diese Nutzungen durch eine Rechtsgrundlage im BDSG abgedeckt sind.

Bei der einfachen Melderegisterauskunft, die an Anfragende bei Nennung von Namen und Adresse oder Geburtsdatum über eine dadurch eindeutig identifizierte Person erteilt wird, handelt es sich um **keine allgemein zugängliche Quelle**. Sie wird nicht voraussetzungslos erteilt: Die gesuchte Person muss eindeutig identifizierbar sein; deren schutzwürdige Interessen dürfen der Auskunft nicht entgegenstehen (31. TB, Tz. 4.1.3).

Für Mai 2010 plant RISER die 5. Konferenz für **E-Services im europäischen Meldewesen** in Berlin. Die Konferenz hat sich in den letzten Jahren zu einem zentralen Forum für Interessenvertreter aller entwickelt, die mit dem Meldewesen zu tun haben. Behandelt werden lokale, nationale und europäische Fragen, insbesondere mit Datenschutzbezug.


www.riserid.eu

Was ist zu tun?
Die Berücksichtigung einheitlich hoher datenschutzrechtlicher Standards bei Einwohnermeldeauskünften und der Ausschluss der Weiterverwendung von Adressauskünften ist Voraussetzung für deren gesellschaftliche Akzeptanz.

8.8 Datenschutzdiskurse im „Privacy Open Space“

Die Erfahrungen von Entwicklern, Nutzern und Datenschutzbehörden zeigen, dass die Anforderungen des Datenschutzes bei jeder Art von E-Service bereits im frühen Stadium berücksichtigt, umgesetzt und in Prozesse integriert werden müssen. „Privacy Open Space“ – kurz „PrivacyOS“ – hilft dabei, die Perspektiven verschiedener Akteure zusammenzubringen und Lösungsvorschläge zu erarbeiten.

Das Projekt PrivacyOS wird im Rahmen des „**ICT Policy Support Programme**“ der Europäischen Kommission gefördert. Es führt Vertreter aus den Bereichen Wirtschaft, Wissenschaft, Regierung und Gesellschaft zusammen, um die Entwicklung und Anwendung von Datenschutzinfrastrukturen in Europa zu fördern und zu unterstützen. Alle 15 Projektpartner aus 12 europäischen Ländern und das ULD als Koordinator können langjährige Datenschutzerfahrungen vorweisen und einbringen.

Kern von PrivacyOS ist der Datenschutzdiskurs auf Konferenzen mit der sogenannten **Open-Space-Methode**: Die Teilnehmerinnen und Teilnehmer bringen eigene Themen ein und gestalten dazu Vorträge und Diskussionen. Die Agenda eines Open Space – also des offenen Raums – wird erst zu Beginn der Konferenz erstellt. Jeder kann ein Thema mit datenschutzrechtlichem Bezug einbringen und bekommt in Abhängigkeit des Interesses der anderen Teilnehmer einen Zeitblock und einen Raum zugeordnet. Diese Dynamik ermöglicht es besonders, neue und aktuelle Themen zu behandeln. Ziele sind eine dauerhafte Zusammenarbeit und ein nachhaltiger Austausch innerhalb der Mitgliedstaaten und den verschiedenen EU-Projekten zum Thema Datenschutz.

PrivacyOS eröffnet ein Diskussionsforum für Best Practices, Datenschutzherausforderungen und Lösungen. Themen wie Electronic ID-Cards, eParticipation, Datenschutz-Gütesiegel oder Kryptomechanismen werden diskutiert und Anwendungsmöglichkeiten erarbeitet. Über einen Zeitraum von zwei Jahren werden vier Open-Space-**Konferenzen** parallel zu Veranstaltungen mit datenschutzrechtlicher Relevanz für Vertreter aus den Bereichen Wirtschaft, Wissenschaft, Regierung und Gesellschaft angeboten.

Die erste PrivacyOS-Konferenz fand im Oktober 2008 in den Räumen des Europäischen Parlaments (EP) unter der Schirmherrschaft des EP-Mitglieds Alexander Alvaro zeitgleich mit der 30. Internationalen Konferenz der Datenschutzbeauftragten statt. Teilnehmer aus 11 Mitgliedstaaten entwickelten die Agenda zu aktuellen Datenschutzthemen, z. B. eHealth, Standardisierung im Datenschutz, Datenschutz-Gütesiegel oder Vorratsspeicherung. Die zweite PrivacyOS-Konferenz wurde unter der Schirmherrschaft des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Peter Schaar, im April 2009 in Kombination mit der „re:publica“-Tagung in Berlin veranstaltet. Über 80 Personen aus 11 Mitgliedstaaten referierten und diskutierten zu sozialen Netzwerken, E-Government oder Identity Management. Die dritte PrivacyOS-Konferenz unter der Schirmherrschaft von Hans G. Zeger, Obmann der ARGE DATEN, stand im Oktober 2009 im Zusammenhang mit den österreichischen Big Brother Awards. Unter dem Thema „Rising Awareness“ diskutierten über 50 Teilnehmer aus 10 Ländern über die bestehenden Möglichkeiten der europäischen Datenschutzbehörden, den Umgang mit Medizindaten und die Sensibilisierung von Jugendlichen in Bezug auf Datenschutz.

www.privacyos.eu

Was ist zu tun?
Dem bestehenden Mangel an Vernetzung und Kommunikation der Akteure im Datenschutz, insbesondere zu Forschungsansätzen, Geschäftsmodellen, zivilgesellschaftlichen Bedürfnissen und staatlichen Anforderungen, muss weiter abgeholfen werden.

8.9 EuroPriSe (European Privacy Seal)

Das europäische Datenschutz-Gütesiegel EuroPriSe hat die Marktvalidierungsphase mit Erfolg abgeschlossen. Die steigende Nachfrage und die positiven Erfahrungen legen den Grundstein für eine erfolgreiche Fortführung des Projektes aus der Pilotphase in den Wirkbetrieb.

Die rasante Entwicklung von Technologien und elektronischen Dienstleistungen vom Smartphone über soziale Netzwerke bis zum elektronischen Personalausweis schaffen neue Möglichkeiten, bergen aber ebenso neue und für viele Bürgerinnen und Bürger unüberschaubare Gefahren. Im Dschungel der Technologien und Angebote brauchen die Menschen ebenso wie Unternehmen richtungweisende Hilfestellungen, denen sie guten Gewissens vertrauen können. EuroPriSe hat zum Ziel, ein wirkungsvolles **Instrument zur Herstellung von Vertrauen** in Informationstechnologien und eine Messlatte für die Datenschutzfreundlichkeit von Produkten und Dienstleistungen bereitzustellen.

Das europäische Datenschutz-Gütesiegel wird nach einer eingehenden Prüfung an IT-Produkte und IT-Dienstleistungen verliehen, die sich in puncto Datenschutz vorbildlich an die Vorgaben der europäischen Datenschutzrichtlinie halten. Für Verbraucher bietet das EuroPriSe-Siegel eine informative und zuverlässige Orientierungshilfe. Unternehmen und Diensteanbieter können mit dem von einer unabhängigen, kompetenten Stelle verliehenen Siegel ihren Kunden effektiv nachweisen, dass ihre Produkte und Dienstleistungen **dem europäischen Datenschutzrecht entsprechen** und eine faire und rechtskonforme Datenverarbeitung ermöglichen.

Über 21 Monate förderte die **Europäische Kommission** im Rahmen des eTEN-Programms das Marktvalidierungsprojekt European Privacy Seal, kurz EuroPriSe, mit 1,3 Millionen Euro (30. TB, Tz. 9.2). Von Juni 2007 bis Februar 2009 hat das ULD zusammen mit acht Partnern an der Umsetzung des schleswig-holsteinischen Gütesiegels (Tz. 9.3) auf europäischer Ebene gearbeitet. An dem vom ULD geleiteten Projekt waren die Datenschutzbehörde APDCM von Madrid, die nationale französische Datenschutzbehörde CNIL, das Institut für Technikfolgenabschätzung der Österreichischen Akademie der Wissenschaften, das Institut für Menschenrechte der London Metropolitan University, die TÜViT aus Deutschland, VaF aus der Slowakei, Borking Consultancy aus den Niederlanden und Ernst & Young aus Schweden beteiligt.

Im Rahmen von **drei Projektabschnitten** wurden zunächst die Anforderungen des schleswig-holsteinischen Verfahrens den europäischen Anforderungen angepasst. Zusätzlich zu einem europäischen Kriterienkatalog wurde eine Kommentierung mit Hinweisen zum europäischen Datenschutzrecht sowie zu nationalen

Besonderheiten erarbeitet. In einem zweiten Projektabschnitt wurden die Anforderungen für ein Zulassungsverfahren von Gutachtern erstellt. Sachverständige aus den Bereichen Technik und Recht wurden für die Gutachtenerstellung ausgebildet und konnten ein Zulassungsverfahren durchlaufen. Innerhalb der Projektlaufzeit konnten zwei Gutachterworkshops mit insgesamt 120 Teilnehmenden aus acht Ländern durchgeführt werden. 2009 konnten wir zwei weitere Gutachterworkshops in Kiel anbieten (Tz. 9.4.3). Neben der Teilnahme am Workshop, der in das EuroPriSe-Verfahren, die Bearbeitung von Gutachten und die Durchführung von Auditierungen einführt, ist von den Teilnehmenden ein Gutachten über ein eigens für die Gutachterausbildung entwickeltes Produkt anzufertigen. Die Trainingsgutachten zeigten große Unterschiede hinsichtlich der Prüftiefe und Anwendung der Kriterien bei den Gutachtern und machten deutlich, dass für die Sicherstellung eines einheitlichen Niveaus eine intensive Ausbildung nicht ausreicht. Ein hohes Niveau kann effektiv von einer übergeordneten, unabhängigen Zertifizierungsstelle gewährleistet werden.

Der dritte Projektabschnitt umfasste die Durchführung von Pilotverfahren zur Zertifizierung. Aus den 24 Bewerbungen, die wir Anfang 2008 erhielten, starteten zusätzlich zu den geplanten sechs Piloten 12 weitere in das Pilotverfahren. Sechs Verfahren wurden innerhalb der Projektlaufzeit erfolgreich abgeschlossen; ein Verfahren konnte bereits rezertifiziert werden. Insgesamt sind bis Ende 2009 13 Verfahren abgeschlossen worden. Die Hersteller kommen aus den Niederlanden, Luxemburg, Deutschland, Spanien, Schweden und den USA. Mittlerweile läuft auch ein Verfahren in Südamerika.

Die **Nachfrage nach Zertifizierungen** ist nach Abschluss der Projektphase weiter gestiegen, obgleich die Verfahren hohe Anforderungen an die Unternehmen stellen. Die Auswertung des Feedbacks der Pilotteilnehmer ergab, dass die Evaluierungen eingehender sind als erwartet, aber im Gegenzug der Nutzen auch größer als erwartet ausfällt. So konnten die beteiligten Hersteller ihre Produkte bzw. Dienstleistungen im Ergebnis verbessern und den Umsatz mit der Gütesiegelerteilung teilweise erheblich steigern.

Die Pilotverfahren wurden zum Teil gemeinsam mit den Datenschutzbehörden aus Madrid und Frankreich durchgeführt. Wichtig war für die Zusammenarbeit eine Abstimmung der Zertifizierungsanforderungen im Hinblick auf die Auslegung der Kriterien, der Plausibilitäts- und Vollständigkeitsprüfung. Das EuroPriSe-Verfahren ist als **Basisbaustein** konzipiert und soll eine schlanke Prüfung von speziellen nationalen Anforderungen im Rahmen von nationalen Zertifikaten ermöglichen. In Frankreich steht das nationale Gütesiegelverfahren kurz vor dem Abschluss des Gesetzgebungs- und Verordnungsverfahrens, für das das schleswig-holsteinische Verfahren Vorbild war (Tz. 9.4.5). Das ULD stellt gern, sowohl auf internationaler als auch auf nationaler Ebene, auch nach Abschluss der Projektphase seine Gütesiegelerfahrungen zur Verfügung – mit dem Ziel, wirkungsvolle und glaubwürdige Anreize für datenschutzfreundliche Produkte und Verfahren zu schaffen.

EuroPriSe wurde auf zahlreichen **Konferenzen und Veranstaltungen** im In- und Ausland vorgestellt. Im Rahmen des Projekts wurde ein Informationsvideo in englischer und deutscher Sprache produziert.


www.european-privacy-seal.eu/about-europrise
www.datenschutzzentrum.de/europrise/

Das EuroPriSe-Projekt ist im März 2009 in den **Wirkbetrieb** überführt worden. Interessierte Hersteller und Anbieter von IT-Produkten und IT-basierten Diensten können diese weiterhin beim ULD nach den Kriterien des europäischen Datenschutz-Gütesiegels zertifizieren lassen (Tz. 9.4). Um dem Nachfrageaufkommen der Unternehmen gerecht werden zu können, gibt es auch in Schleswig-Holstein noch einen Bedarf an qualifizierten Gutachtern. Der Projektabschlussbericht ist auf der EuroPriSe-Webseite abrufbar.


www.european-privacy-seal.eu

Was ist zu tun?
Die erfolgreiche europäische Zertifizierung ist im Wirkbetrieb fortzuführen.

9 Audit und Gütesiegel

9.1 Datenschutzauditgesetz – reloaded

Die Bundesregierung hat eine neue Initiative zur Einführung eines Datenschutz-Audits auf Bundesebene angekündigt – über eine Stiftung Datenschutz.

Wie vermutet wurde der **Entwurf eines Datenschutzauditgesetzes** der Bundesregierung von der Fachöffentlichkeit nicht für gut befunden (31. TB, Tz. 9.1). In einer Anhörung des Innenausschusses des Bundestages im März 2009 wurde das Anliegen des Entwurfes, freiwillige Anreize im Wettbewerb für eine Verbesserung des Datenschutzes zu geben, von allen Sachverständigen unterstützt. Die zur Diskussion stehende Lösung war hierfür aber nicht geeignet, da in einem äußerst bürokratischen Verfahren eine Zertifizierung durch private Kontrollstellen vorgesehen war, ohne dass die Qualität der Zertifikate durch eine unabhängige Stelle oder auch nur über hinreichende Transparenz durch eine kritische Öffentlichkeit geprüft werden konnte. Das Zertifikat sollte schon durch eine reine Bereitschaftserklärung zur Überprüfung erlangt werden können. Während die BDSG-Novelle II vom Bundestag kurz vor Ende der Legislaturperiode verabschiedet wurde (Tz. 5.1.1), blieb die zugleich geplante Normierung des Audits unerledigt.

In der **Koalitionsvereinbarung** von CDU, CSU und FDP für die 17. Legislaturperiode wird das Thema wieder angesprochen: „Darüber hinaus werden wir eine Stiftung Datenschutz errichten, die den Auftrag hat, Produkte und Dienstleistungen auf Datenschutzfreundlichkeit zu prüfen, Bildung im Bereich des Datenschutzes zu stärken, den Selbstdatenschutz durch Aufklärung zu verbessern und ein Datenschutz-Audit zu entwickeln. Wir sind überzeugt, dass mit dieser Lösung auch der Technologiestandort Deutschland gestärkt wird, wenn datenschutzfreundliche Technik aus Deutschland mit geprüfter Qualität weltweit vertrieben werden kann."

Die Idee einer **Stiftung Datenschutz** ist ein äußerst innovativer Ansatz, über dessen Umsetzung aber bisher wenige Vorstellungen bekannt sind. Zunächst schien es so, als solle die neue Stiftung mit seinen Überprüfungen – ähnlich der Stiftung Warentest als Instrument des Verbraucherschutzes – eine Lücke zwischen staatlicher Datenschutzaufsicht und freiwilliger Zertifizierung füllen, und zwar durch Untersuchungen von Marktangeboten, inwieweit diese die Datenschutzvorschriften beachten. Das ULD präsentierte gegenüber den zuständigen Ressorts auf der Basis der Erfahrungen mit Kontrollen und Zertifizierungen Überlegungen für eine wirkungsvolle Umsetzung der Stiftungsidee.

Die Federführung für das Projekt liegt beim Bundesministerium des Innern. Die Bundesministerin der Justiz signalisierte, dass sich ihr Ressort in das Projekt einbringen wird. Die Stiftung soll nach ihrer Vorstellung als **unabhängige Stelle** ausgestaltet werden, die auch freiwillige Zertifizierungsverfahren mit einer großen Prüftiefe durchführen können soll. Der Charme einer solchen Stiftung kann darin liegen, dass eine von den Länderverwaltungen unabhängige Einrichtung bundesweit ein einheitliches Vorgehen bei der Auditierung gewährleisten kann.

Bei den weiteren Diskussionen wird es darauf ankommen, die bisher gemachten Erfahrungen mit Datenschutzzertifizierungen zu berücksichtigen. Zwar gibt es **vonseiten der Wirtschaft** vielversprechende Ansätze. Diese leiden aber durchgängig an mangelnder Transparenz und Unabhängigkeit mit der Folge unzureichender Vertrauenswürdigkeit für den Markt und die Öffentlichkeit. Derartige Auftragsaudits erfüllen eine wichtige Rolle als Rückversicherung bei der internen Compliance, also der Beachtung der von außen gesetzten Datenschutzregeln. Sie können aber nicht für andere Marktteilnehmer als Orientierungshilfe genutzt werden, da ihre Verfahren und Kriterien unklar bleiben. So ergab z. B. eine Anfrage bei der Schufa, die ein eigenes „DatenschutzSiegel“ als „Zeichen für mehr Sicherheit und Vertrauen“ anbietet, dass weder das Zertifizierungsverfahren und die Kriterien im Detail noch dessen Ergebnisse offengelegt werden.

Das ULD hat seine Kooperationsbereitschaft bei der Etablierung eines nationalen Datenschutzauditverfahrens signalisiert. Dabei sollte hinsichtlich der technischen, organisatorischen und rechtlichen Anforderungen an die zu zertifizierenden IT-Anwendungen bei den schon vorliegenden Kriterienkatalogen angeknüpft werden. Für alle Beteiligten, also Hersteller, Anbieter, Marktteilnehmer, Verbraucher, private Datenschutzdienstleister, Datenschutzbeauftragte in den Unternehmen und Datenschutzaufsichtsbehörden, sollte eine größtmögliche Transparenz hinsichtlich der datenschutzrelevanten Eigenschaften der zertifizierten Produkte geschaffen werden. Die Unabhängigkeit und Neutralität sowie die Vergleichbarkeit der Zertifizierungsentscheidung müssen gesichert sein. Bei einer nationalen Lösung kann es nicht um eine Eins-zu-eins-Übertragung der schleswig-holsteinischen Praxis gehen. Dies erlaubt weder die größere Dimension eines nationalen Verfahrens noch die föderale Struktur des Datenschutzes in Deutschland. Doch sollte sich das Audit der Stiftung Datenschutz in die sich derzeit entwickelnde **europäische Auditierungslandschaft** einfügen, sodass keine Konkurrenz, sondern ein gegenseitiges Ergänzen bewirkt wird.

Was ist zu tun?
In einem Dialog der interessierten Stellen sollte ein nationales Auditierungskonzept entwickelt und umgesetzt werden, das positive Anreize zur Verbesserung des Datenschutzes gibt und das neue Impulse für europäische und internationale Zertifizierungen setzt.

9.2 Audits in Schleswig-Holstein

9.2.1 ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz

Das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz bietet den Behörden die Möglichkeit, ihre positiven Aktivitäten im Bereich Datenschutz und IT-Sicherheit unter Beweis zu stellen.

Interesse und Bereitschaft von Behörden wie Unternehmen, internationale Sicherheitsstandards anzuwenden, nehmen ständig zu. Im Behördenumfeld ist der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) vorgegebene IT-Grundschutzstandard schon lange bekannt. Aufgrund der Anlehnung an die ISO 27001-

Norm, die ausführlich die Anforderungen eines **Informationssicherheitsmanagementsystems** (ISMS) beschreibt, erhält der IT-Grundschutzstandard eine internationale Ausrichtung und gewinnt somit zunehmend an Bedeutung.

> **?** ***ISO/IEC 27001***
>
> *„Information technology – Security techniques – Information security management systems – Requirements" spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation.*

Das ULD hat schon früh die Voraussetzungen für die Durchführung derartiger Audits geschaffen und verfügt über **drei Auditoren** mit dem erforderlichen Know-how, ISO 27001-Zertifizierungen auf der Basis von IT-Grundschutz durchzuführen. Für die Vergabe dieses Zertifikats muss ein Audit durch einen externen, vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierten Auditor für ISO 27001-Audits auf der Basis von IT-Grundschutz durchgeführt werden. Das Ergebnis des Audits ist ein vom Auditor erstellter Auditreport, welcher der Zertifizierungsstelle beim BSI vorgelegt wird. Diese entscheidet abschließend über die Vergabe des Zertifikats.

Bei einem **Grundschutzaudit** werden das IT-Sicherheitsmanagement sowie die konkrete Umsetzung der IT-Sicherheitsmaßnahmen geprüft. Der Umfang der zu prüfenden IT-Sicherheitsmaßnahmen ist in den IT-Grundschutzkatalogen festgelegt. In diesen Katalogen erfolgt eine Auflistung geeigneter organisatorischer, personeller, infrastruktureller und technischer Maßnahmen zur Erreichung eines Sicherheitsniveaus für IT-Systeme, das für den normalen Schutzbedarf angemessen und ausreichend ist und als Basis für hoch schutzbedürftige IT-Systeme und Anwendungen dienen kann. Die IT-Grundschutzkataloge erklären, wie Informationssicherheit konzipiert und realisiert werden sollte, und geben sehr konkrete Hinweise, wie eine Umsetzung auf technischer Ebene aussehen kann.

Einige größere **Behörden in Schleswig-Holstein** verfahren bereits nach dem IT-Grundschutzstandard. Eine Zertifizierung streben jedoch bis jetzt nur sehr wenige an. Aufgrund der in letzter Zeit bekannt gewordenen Datenskandale steigt der öffentliche Druck auf Unternehmen und Behörden, IT-Sicherheit und Datenschutz gründlicher anzugehen, z. B. durch Überprüfung der ordnungsgemäßen Datenverarbeitung durch einen externen Gutachter mit dem Ziel einer Zertifizierung.

> ***Hinweis***
>
> *Die DATENSCHUTZAKADEMIE Schleswig-Holstein bietet in ihrem Programm Fortbildungsseminare für die Einführung und Umsetzung des IT-Grundschutzstandards an.*

Das ULD bietet die ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz separat, aber auch in **Kombination mit dem Datenschutz-Audit** an. Beide Verfahren zielen auf eine Verbesserung der IT-Sicherheit und des Datenschutzes ab.

Was ist zu tun?
Behörden und Unternehmen in Schleswig-Holstein sollten ihre automatisierte Datenverarbeitung nach dem IT-Grundschutzstandard und bzw. oder mit dem bewährten Datenschutz-Audit des ULD zertifizieren lassen.

9.2.2 azv Südholstein

Das neue Kommunalunternehmen azv Südholstein hat zusätzliche Aufgaben übernommen und verarbeitet verstärkt Kundendaten. Durch ein Auditverfahren möchte es sicherstellen, dass die Verarbeitung personenbezogener Daten nach aktuellem Stand der Technik und datenschutzfreundlich erfolgt.

Für das gemeinsame Projekt mit dem ULD könnte die Ausgangsbasis nicht besser sein. Der azv Südholstein, vor 2009 tätig als Abwasser-Zweckverband Pinneberg, verfügt bereits über **umfangreiche Auditerfahrung** aus erfolgreich durchgeführten Verfahren der ISO 9000er-Reihe zum Qualitätsmanagement und der ISO 14000er-Reihe zum Umweltmanagement. Wir konnten beim Datenschutzauditverfahren sofort damit beginnen, bestehende technisch-organisatorische Lücken im Rahmen der üblichen Mängelbehebung zu schließen. Gemeinsames Ziel ist es, das Datenschutz-Behördenaudit in Übereinstimmung mit den Anforderungen der ISO 2700er-Reihe zum Informationssicherheitsmanagement auszugestalten.

Was ist zu tun?
Der azv Südholstein sollte seine bestehende Auditerfahrung nutzen und das neue Datenschutzauditverfahren in die bestehenden innerbetrieblichen Prozesse zum Qualitätsmanagement integrieren.

9.2.3 Rezertifizierung Landesnetz

Das Landesnetz ist ein zentraler Baustein in der gemeinsamen E-Government-Strategie des Landes und der Kommunen. Im Rahmen einer Rezertifizierung wurde das bestehende Auditsiegel erneuert.

Auf der Sommerakademie 2009 erhielt der Staatssekretär im Finanzministerium für das Landesnetz erneut das Siegel nach einem erfolgreichen Datenschutz-Behördenauditverfahren. Das ULD prüfte bei der Rezertifizierung nicht nur die technischen und organisatorischen Sicherheitsmaßnahmen beim Finanzministerium, bei Dataport und bei T-Systems, sondern legte einen Schwerpunkt auf das Datenschutzmanagement mit regelmäßig durchgeführten Kontrollen und einem geordneten Vorgehen beim Umgang mit Sicherheitsproblemen. Wir stellten eine **kontinuierliche Weiterentwicklung** der technischen und organisatorischen Sicherheitsmaßnahmen im Landesnetz fest, was durch Detailverbesserungen gegenüber der Erstzertifizierung zu einer Verbesserung des Sicherheits- und Datenschutzniveaus führte.

Was ist zu tun?
Das Finanzministerium muss seiner besonderen Verantwortung als Betreiber des integrierten Sprach- und Datennetzes der schleswig-holsteinischen Landesverwaltung weiterhin nachkommen. Das dazugehörige Datenschutz- und Sicherheitsmanagement muss stetig weiterentwickelt werden.

9.2.4 ZIAF-Audit beim Landwirtschaftsministerium

Das Ministerium für Landwirtschaft, Umwelt und ländliche Räume hat für den sicheren und datenschutzfreundlichen Betrieb des ZIAF-Verfahrens erneut ein Auditsiegel erhalten. Die erreichten Sicherheitsstandards müssen stetig fortgeschrieben werden.

Im vorigen Jahr hat das ULD das ZIAF-Verfahren des Ministeriums für Landwirtschaft, Umwelt und ländliche Räume (MLUR) zur Agrarförderung erfolgreich auditiert (31. TB, Tz. 9.2.2). Zur Erinnerung: Der ländliche Raum wird durch den Europäischen Ausrichtungs- und Garantiefonds für die Landwirtschaft (EAGFL) und den Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) gefördert. Die Kommission der Europäischen Gemeinschaft (EU-Kommission) hat für die ordnungsgemäße Abwicklung der zur Verfügung gestellten Finanzmittel Anforderungen erlassen, die von den eingerichteten **Zahlstellen der Bundesländer** einzuhalten sind. Für die Umsetzung dieser Verordnung haben sich die Bundesländer auf die Anwendung des IT-Grundschutzstandards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verständigt (Tz. 9.2.1). Die beim Ministerium durchgeführten Audits sollen bestätigen, dass die Zahlstelle und die dort für die Fördermaßnahmen eingesetzten IT-Systeme (ZIAF) nach den nationalen und europarechtlichen Vorgaben betrieben werden.

Rückblick: Das MLUR hat das ULD im Juni 2005 mit der Begutachtung der IT-Sicherheit in der Zahlstelle beauftragt, um die Einhaltung der von der Europäischen Gemeinschaft (EG) vorgegebenen IT-Sicherheitsanforderungen zu überprüfen. Als Basis für die Umsetzung der Anforderungen wurde zunächst eine Generaldokumentation als **Konzeption der Zahlstelle** des MLUR erstellt. Sie sollte zunächst inhaltlich auf ihre Norm- und Rechtskonformität sowie ihre Umsetzbarkeit hin überprüft werden. Neben dem Datenschutz ging es vor allem um die Erfüllung der spezifischen Anforderungen des IT-Grundschutzstandards durch die in der Zahlstelle eingesetzten ZIAF-Fachverfahren.

Im Oktober 2007 verlieh das ULD für drei Jahre dem Konzept mit seiner Generaldokumentation das Datenschutzauditzertifikat. Auf dieser Basis sollte die **Umsetzung** zur Erreichung der BSI-Grundschutzkonformität durch eine Zertifizierung nach ISO 27001 nachgewiesen werden. Als dies erreicht war, verlieh das Bundesamt für Sicherheit in der Informationstechnik (BSI) dem Konzept im April 2009 das Zertifikat nach ISO 27001 auf der Basis von IT-Grundschutz für drei Jahre. Da auch die datenschutzrechtlichen Anforderungen erfüllt waren, erfolgte durch das ULD im August 2009 die ergänzende Datenschutzauditierung.

Die erreichten Sicherheitsstandards müssen nun dauerhaft aufrechterhalten werden. Dafür hat das MLUR sein IT-Sicherheitsmanagement nachhaltig und effektiv bei der ZIAF-IT einzusetzen. Mit der IT-Grundschutzzertifizierung verpflichtet sich das MLUR zu jährlichen Nachprüfungen durch einen anerkannten BSI-Auditor im Rahmen von sogenannten **Überwachungsaudits**. Das erste Überwachungsaudit wird bereits im Jahr 2010 erfolgen. Nach den Vorgaben des BSI müssen folgende Aspekte geprüft werden:

- Fortführung und Stand der Dokumentation,
- Wirksamkeit des IT-Sicherheitsmanagements,
- Abarbeitung der bei der Zertifizierung erteilten Auflagen,
- Änderungen an dem IT-Verbund bzw. der IT-Systemzusammenstellung.

Was ist zu tun?
Das MLUR muss seinem IT-Sicherheitsmanagement ausreichende Ressourcen zur Verfügung stellen, damit der erreichte Sicherheitsstandard dauerhaft gewährleistet werden kann.

9.2.5 Amt Viöl[1]

An de 31. August 2009 wurr de Amtsverwaltung Viöl in Rohmen vun de Sommerakademie 2009 een Dotenschutzauditzertifikot för de vörbildliche Verarbeidung vun personenbetruckene Doten op IT-Systeme dörch dat ULD verlehnt.

Dat bi't Amt Viöl vörwiegend Platt sproken warrt, gehört to de gode Service vun't Huus, de Bürger in de gewohnte Sprook to begegnen. De Amtsvörsteher Hans Jes Hansen mit sien Lüüd ist nämli **foortschrittli opstellt**: Ünner dat Motto „Unse Verwaltung arbeitet ortsnoh, effektiv un kostengünstig" hett he de Dotenverarbeidung in't Huus op de Inholung dotenschutzrechtliche Belange dör dat ULD pröven loten. Nofolgend een poor Eenzelheiten ut dat Godachten:

- De Amtsverwaltung hat för ehr Informationstechnik un ehr Verwaltungsnetz een Dotenschutzmanagement etableert.
- De op de Arbeitsplatz-PC verfögbore Funktionen sind op een Mindestmoot reduzeert.
- De Disketten- un CD-ROM-Loopwarke un de USB-Port sind standardmäßig deaktiveert.
- De Fachanwendungen warrn struktureert zentrol op Servern verwaltet.
- De Internet-Togang is dör een Firewall un een qualifizeerte Virenschutzsoftware schützt.

[1] Übersetzung ins Plattdeutsche durch Frau Marion Engel aus dem Amt Viöl

Grundlaag vör de Överprövung vun de IT-Systeme dör dat ULD weer een detailleerte Dokumentation. Prövt wurr uk, op all de inschlägigen Dotenschutzvörschriften vun de Amtsverwaltung beachtet warrn. De erfolgrieke Zertifizeerung wiest, dat sik een Dotenschutz-Audit uk för een lüdde Amtsverwaltung as een wirksome Middel to **noholdige Verbedderung vun IT-Sekerheit** un Bürgervertrun nutzen lett.

Wat is to doon?
Dat Amt Viöl schull dat sette Moot duerhaft oprechterholn un dordörch to een Vörbild för annere Amtsverwaltungen warrn.

Hochdeutsche Sprachvariante:

Amt Viöl

Am 31. August 2009 wurde der Amtsverwaltung Viöl im Rahmen der Sommerakademie 2009 ein Datenschutzauditzertifikat für die vorbildliche Verarbeitung personenbezogener Daten auf IT-Systemen durch das ULD verliehen.

Dass beim Amt Viöl vorwiegend Platt gesprochen wird, gehört zum guten Service des Hauses, den Bürgern in der gewohnten Sprache zu begegnen. Der Amtsvorsteher Jes Hansen mit seinem Team ist nämlich fortschrittlich aufgestellt: Unter dem Motto „Unsere Verwaltung arbeitet ortsnah, effektiv und kostengünstig“ hat er die Datenverarbeitung des Hauses auf die Einhaltung datenschutzrechtlicher Belange durch das ULD prüfen lassen. Nachfolgend ein paar Details aus dem Gutachten:

- *Die Amtsverwaltung hat für ihre Informationstechnik und ihr Verwaltungsnetz ein Datenschutzmanagement etabliert.*
- *Die auf den Arbeitsplatz-PC verfügbaren Funktionen sind auf ein Mindestmaß reduziert.*
- *Die Disketten- und CD-ROM-Laufwerke sowie der USB-Port sind standardmäßig deaktiviert.*
- *Die Fachanwendungen werden strukturiert zentral auf Servern verwaltet.*
- *Der Internetzugang ist durch eine Firewall und durch eine qualifizierte Virenschutzsoftware geschützt.*

Grundlage der Überprüfung der IT-Systeme durch das ULD war eine detaillierte Dokumentation. Geprüft wurde zudem, ob alle einschlägigen Datenschutzvorschriften von der Amtsverwaltung beachtet werden. Die erfolgreiche Zertifizierung zeigt, dass sich ein Datenschutz-Audit auch für eine kleine Amtsverwaltung als ein wirksames Mittel zur nachhaltigen Verbesserung von IT-Sicherheit und Bürgervertrauen erfolgreich nutzen lässt.

Was ist zu tun?
Das Amt Viöl sollte den gesetzten Maßstab dauerhaft aufrechterhalten und dadurch zum Vorbild anderer Amtsverwaltungen werden.

9.2.6 Audit für Internetdienste im Kreis Plön

Die IT-Abteilung des Kreises Plön setzt erneut Maßstäbe beim Betrieb des Rechenzentrums. Der Landrat des Kreises erhielt ein weiteres Datenschutzauditzertifikat für die Internetdienste E-Mail und WWW.

Die Kreisverwaltung Plön ist unter den Kommunen des Landes schon lange Vorreiter im Bereich Datenschutz und IT-Sicherheit. Vor zwei Jahren ließ sie ihr Kreisnetz vom ULD erfolgreich zertifizieren. Nun folgte die Zertifizierung der Internetanbindung und der Internetdienste E-Mail und WWW für die Kreisverwaltung und über das Kreisnetz angeschlossene Kommunen. Folgende von der IT-Abteilung umgesetzte **Sicherheitsmaßnahmen** wurden festgestellt:

- Zum Schutz vor Angriffen von außen wurden die Übergänge vom internen Verwaltungsnetz zum Internet mit abgestuften Firewallsystemen ausgestattet.
- Die Überwachung und Administration der eingesetzten Firewallkomponenten werden ausschließlich von der Kreisverwaltung durchgeführt.
- Die ergriffenen Sicherheitsmaßnahmen werden regelmäßig von qualifizierten Mitarbeitern auf ihre Wirksamkeit hin überprüft.
- Veränderungen der Sicherheitseinstellungen bedürfen nach Abstimmung mit dem IT-Sicherheitsmanagement und der behördlichen Datenschutzbeauftragten der Zustimmung des Leiters der IT-Abteilung.
- Alle Einstellungen auf den Internetkomponenten werden nachvollziehbar dokumentiert.
- Nicht zugelassene Zugriffe werden auf der physikalischen Ebene protokolliert und abgewehrt. Bei Ereignissen von sicherheitsrelevanter Bedeutung werden gesonderte Warnmeldungen ausgegeben.
- Eine Fernadministration der Firewallkomponenten ist nicht gestattet.
- Es werden nur die E-Mails an den Arbeitsplatz geleitet, die virenüberprüft sind und zugelassene Anhänge enthalten.
- Der Zugriff auf die Webseiten wird in Bezug auf die sicherheitskritischen Komponenten ActiveX, Java und VBScript gefiltert.
- Webseiten werden nach Inhalten gefiltert und gegebenenfalls für den Aufruf nicht zugelassen.
- Das Herunterladen ausführbarer Programme und Dateien auf die Arbeitsplatzrechner ist nicht zugelassen.

Was ist zu tun?
Die IT-Abteilung des Kreises Plön sollte für andere Kommunalverwaltungen Leitbild bei der Umsetzung von IT-Sicherheit und Datenschutz werden.

9.2.7 Amt Trave-Land

Das Amt Trave-Land schreitet voran: Als Pionier der Ämterfusionen nimmt man sich des Datenschutzes und der Datensicherheit im Rahmen eines Auditverfahrens intensiv an.

Mit rund 20.000 Einwohnern in 27 Gemeinden und einer Flächengröße von 318 Quadratkilometern ist das Amt Trave-Land eine der größten Amtsverwaltungen in Schleswig-Holstein. In einem gemeinsamen Auditverfahren unterstützt das ULD die Amtsverwaltung bei der datenschutzfreundlichen Ausgestaltung ihrer Verwaltungsprozesse und der technischen Infrastruktur. Nach einer ersten Analyse rechtlicher Rahmenbedingungen nimmt das Amt eine **umfassende Bestandsaufnahme** der technischen Gegebenheiten vor Ort vor.

Was ist zu tun?
Das Amt Trave-Land sollte den positiv begonnenen Auditprozess erfolgreich zu Ende führen.

9.3 Datenschutz-Gütesiegel Schleswig-Holstein

9.3.1 Abgeschlossene Gütesiegelverfahren

Im Jahr 2009 wurde wieder zahlreichen Produkten ein Datenschutz-Gütesiegel verliehen. Sechs Produkte wurden erstmalig zertifiziert. Weitere sechs Produkte wurden nach Fristablauf einer bestehenden Zertifizierung in einem vereinfachten Verfahren rezertifiziert.

Das anhaltende Interesse der IT-Hersteller an Zertifizierungen und Rezertifizierungen zeigt, dass das Gütesiegel einen echten Wettbewerbsvorteil bietet, der sich lohnt, regelmäßig erneuert zu werden. Mehr und mehr Hersteller machen von einer **Doppelzertifizierung** zusammen mit EuroPriSe (Tz. 9.4) Gebrauch, um die Datenschutzfreundlichkeit sowohl für den europäischen wie für den deutschen Markt zu dokumentieren. Bei der Doppelzertifizierung können sowohl bei den Gutachtern als auch bei uns als Zertifizierungsstelle Synergieeffekte genutzt und Kosten gespart werden. So ist es möglich, ein gemeinsames Gutachten auf Deutsch oder Englisch einzureichen, das beide Zertifizierungsverfahren einschließt (Tz. 9.3.3).

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

- „Dokumentenprüfer ALDO-L“, Hardware Release 01/Software 0023: Altersverifikation mittels Personalausweisen und Führerscheinen,
- Magellan/da Vinci (Version 6): Schulverwaltungssoftware und Stundenplan-, Kursplan-, Vertretungsplansoftware,
- Scola Schulverwaltung (Version 2009, multiuser-server-edition): Schulverwaltungssoftware zur Verwaltung der Daten von Schülern, Lehrern und sonstigen zur Verwaltung und zum Betrieb einer Schule erforderlichen Personen,

- mobiler Schredder (Stand Juli 2009): Akten- und Datenträgervernichtung im Rahmen einer Auftragsdatenverarbeitung durch die Firma Rhenus Data Office GmbH,
- TGPopen (Version 1.0): IT-Produkt für Vermarkter und Betreiber von Telemediendiensten zur Steuerung von zielgruppenspezifischen Inhalten, wie z. B. Werbeeinblendungen,
- Durchzugsleser DC3 und DC Mini, Multiakzeptor MA3 und Führerscheinleser LC3 (Stand November 2009): automatische Lesegeräte zur Altersverifikation mittels Personalausweis, Reisepass und EU-Führerschein.

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

- TeamDrive (Version 2.1 für Windows): Kollaborationstool für den Zugriff mehrerer Benutzer auf einen verschlüsselten Datenbestand zur gemeinsamen Bearbeitung von Dokumenten,
- SpeechMagic (Version 1.0): Verarbeitung und Verwaltung von digitalen ärztlichen Diktaten,
- Dataport Firewall Altenholz (Stand: 14.10.2008): Schutz der Ressourcen im Netzwerk von Dataport gegen unberechtigte Zugriffe aus dem Internet durch Einschränken der Verbindungen von und zum Internet auf zulässige Dienste,
- Altersverifikation (Stand: 25. Juni 2009): Altersüberprüfung durch Einlesen des Personalausweises oder des Führerscheins,
- „DIBIKO mit Fotokabine VC 100“ und „DIBIKO Small Business“ (Stand: Juli 2009): digitale Bildintegration für Kommunen mit und ohne Fotokabine,
- Predictive Targeting Networking (PTN) (Version 2.0): Generierung von statistischen Annahmen aus Nutzungsinformationen von Nutzern von Webdiensten.


www.datenschutzzentrum.de/guetesiegel/infos_hersteller.htm

Was ist zu tun?
Die Hersteller von Produkten sind weiterhin auf die Vorzüge des Gütesiegels hinzuweisen. Dabei werden wir eng mit dem Projekt EuroPriSe zusammenarbeiten, um Synergien zu nutzen und Hersteller zielgerichtet beraten zu können.

9.3.2 Sachverständige

Weitere Sachverständige und Prüfstellen konnten für das Gütesiegelverfahren anerkannt werden.

Beim Gütesiegelverfahren erfolgt die Begutachtung der zu zertifizierenden Produkte durch beim ULD anerkannte Datenschutzsachverständige. Deren Akkreditierung kann je nach **Qualifikation** entweder für den Bereich Recht oder Tech-

nik oder für beides beantragt werden. Möglich ist auch die Anerkennung einer ganzen Prüfstelle. Voraussetzungen für die Akkreditierung sind stets die Zuverlässigkeit, die Unabhängigkeit und der Nachweis der erforderlichen spezifischen Fachkunde im Datenschutzbereich.

Hinzugekommen als Sachverständige sind 2009:

- Sachverständige Dipl.-Ing. (FH) Silke Jacob (Technik),
- Sachverständiger Dr. Ing. Klaus-Dieter Frankenstein (Technik).

Inzwischen sind beim ULD 33 Einzelsachverständige **registriert**. 14 Sachverständige sind für den Bereich Recht und 13 für den Bereich Technik anerkannt. Sechs Sachverständige haben die Anerkennung für beide Bereiche. Hinzu kommen noch neun Prüfstellen, von denen zwei für Recht, drei für Technik und vier für beides bei uns eingetragen sind.

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.

Im September 2009 fand der jährliche **Gutachterworkshop** in Kiel statt. Von dieser Möglichkeit des Erfahrungsaustausches machten 19 Sachverständige Gebrauch. Diskutiert wurden aktuelle Erfahrungen mit Neu- und Rezertifizierungen, die Änderungen der Datenschutzverordnung, die erforderliche Prüftiefe wie auch Fragen des Marketings des Gütesiegels. Ein Schwerpunkt war die Zusammenarbeit mit dem europäischen Gütesiegel EuroPriSe (Tz. 9.3.3).

Ende 2009 kam es im Zuge der EG-Dienstleistungsrichtlinie zu einer **Änderung der Datenschutzauditverordnung**. Damit kann nunmehr das Anerkennungsverfahren über eine einheitliche Stelle abgewickelt werden. Außerdem wurde die Anerkennung von Sachverständigen auf Bundesebene oder aus anderen Bundesländern aufgenommen.


www.datenschutzzentrum.de/guetesiegel/akkreditierung.htm

Was ist zu tun?
Die Sachverständigen sind ein wichtiger Faktor, um Werbung für das Gütesiegel zu machen und dieses generell voranzubringen. Ihr Antrieb, neue Produkte für das Gütesiegelverfahren zu gewinnen, ist sehr zu unterstützen.

9.3.3 Zusammenarbeit mit EuroPriSe

Die Vergleichbarkeit der Verfahren von EuroPriSe und dem Datenschutz-Gütesiegel Schleswig-Holstein ermöglicht es den Herstellern von IT-Produkten, kostengünstig beide Siegel zu erlangen.

Sowohl EuroPriSe (Tz. 9.4) als auch das ULD-Gütesiegel basieren auf einem **qualitätsgesicherten Verfahren**. Anerkannte Gutachter analysieren ein IT-Produkt auf Konformität mit Datenschutzrecht und Datenschutztechnik. Das ULD als Zertifizierungsstelle überprüft die Gutachten und verleiht die Siegel. Auch die Kriterienkataloge der beiden Siegel sind in weiten Teilen vergleichbar. Unterschiede gibt es hinsichtlich dessen, dass bei EuroPriSe besondere europäische Vorgaben und beim ULD-Gütesiegel spezielle deutsche bzw. schleswig-holsteinische Gesetze relevant sind.

Die Verfahren für das ULD-Gütesiegel und für EuroPriSe können verbunden werden. So ist es möglich, ein einziges Gutachten entweder auf Deutsch oder Englisch einzureichen, das beide Kriterienkataloge abdeckt. Hierdurch können sowohl die Gutachterkosten als auch die Kosten für uns als Zertifizierungsstelle verringert werden. Voraussetzung ist, dass die Gutachter sowohl für das Gütesiegel des ULD als **auch für EuroPriSe anerkannt** sind. Derzeit erfüllen 20 Sachverständige diese Voraussetzung.

Auch außerhalb der gemeinsamen Verfahren erfolgt ein stetiger Austausch über **Auslegungen von Kriterien** zwischen EuroPriSe und dem ULD-Gütesiegel. So wird sichergestellt, dass es nicht zu Wertungswidersprüchen zwischen den Siegeln kommt. Gemeinsame Workshops werben auch bei Gutachtern dafür, die Vorteile der einzelnen Zertifizierungen zu nutzen.

Weitere Informationen für Hersteller finden sich im Internet unter:

www.datenschutzzentrum.de/guetesiegel/
www.european-privacy-seal.eu/

Was ist zu tun?
Die Hersteller von IT-Produkten sind auf die Vorzüge beider Siegel hinzuweisen. Eine stetige Abstimmung der Kriterienkataloge ist notwendig, um Wertungswidersprüche zu vermeiden.

9.4 EuroPriSe

Das von der Europäischen Union geförderte Projekt des europäischen Datenschutz-Gütesiegels – European Privacy Seal (EuroPriSe) – ist seit März 2009 im Wirkbetrieb.

EuroPriSe als Projekt ist erfolgreich abgeschlossen (Tz. 8.9). Im Wirkbetrieb ist es uns weiterhin möglich, IT-Produkte und IT-basierte Dienstleistungen aus aller Welt auf ihre Vereinbarkeit mit den europäischen Datenschutzregelungen zu prüfen und datenschutzfreundliche Angebote für unsere Bürgerinnen und Bürger sichtbar zu machen. Die Erfahrungen aus der Pilotphase gaben wertvolle Hinweise für den **Markteinsatz** und die Wirtschaftlichkeitsplanungen, was ein Ziel des Marktvalidierungsprojektes war. Das Verfahren wurde für den Markteinsatz ergänzt (Tz. 9.4.2), das Gebührenmodell, Vertragsmuster für Zertifizierungen und Gutachterzulassung wurden überarbeitet. Der Übergang wird zudem durch die Änderung vom Projektlogo zum Markenlogo deutlich.

Die **hohe Nachfrage** nach EuroPriSe-Zertifizierungen durch Unternehmen aus ganz Europa, den USA und Südamerika bestätigt die Anerkennung unserer Datenschutzgrundsätze über die Landesgrenze hinaus. Europäische Datenschutzstandards, bescheinigt durch eine deutsche Zertifizierungsstelle, sind ein internationales Qualitätsmerkmal und Wettbewerbsfaktor in der globalen Informationsgesellschaft. Das Beispiel der Internetsuchmaschine Ixquick (31. TB, Tz. 9.4.4) hat gezeigt, dass die Zertifizierung den internationalen Markt nachhaltig beeinflussen kann und Wettbewerber wie auch Regulationsbehörden auf die datenschutzfreundlichen Lösungen als State-of-the-Art-Standard reagieren.

9.4.1 Zertifizierungskriterien

Das EuroPriSe-Siegel bescheinigt die Vereinbarkeit eines IT-Produkts oder einer IT-basierten Dienstleistung mit den Bestimmungen des EU-Datenschutzrechts. Die im Rahmen einer Zertifizierung zu prüfenden Kriterien sind aus den einschlägigen EU-Richtlinien abgeleitet und in einem Anforderungskatalog aufgelistet.

Der **Katalog** benennt neben den Kriterien die Rechtsnormen, aus denen diese jeweils abgeleitet sind, und listet die Fragen auf, die im Hinblick auf ein Kriterium regelmäßig von Relevanz sind. Er setzt sich aus vier thematischen Komplexen zusammen (31. TB, Tz. 9.4.1):

- 1. Komplex: grundsätzliche Fragestellungen,
- 2. Komplex: Rechtmäßigkeit der Datenverarbeitung,
- 3. Komplex: technische und organisatorische Maßnahmen der Datensicherheit,
- 4. Komplex: Betroffenenrechte.

Der in englischer Sprache verfasste Anforderungskatalog liegt gegenwärtig in der Version 1.0 vor und kann im Internet abgerufen werden unter:

www.european-privacy-seal.eu/criteria/

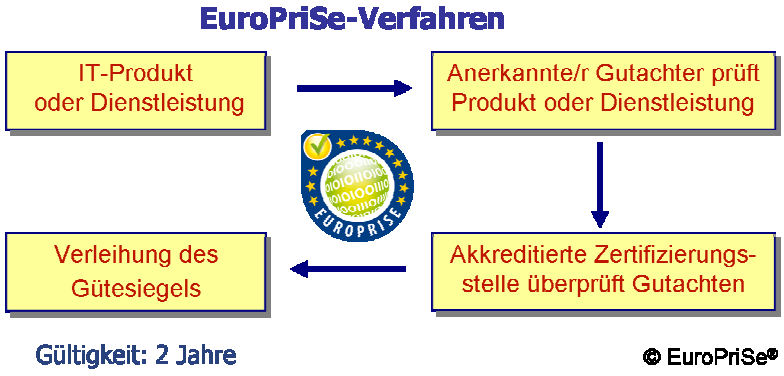
Eine aktualisierte Version des Katalogs wird nach Einarbeitung des Telekom-Reformpakets der EU veröffentlicht werden.

Was ist zu tun?
Der Kriterienkatalog ist kontinuierlich weiterzuentwickeln und an alle wesentlichen Veränderungen im Bereich der Gesetzgebung und der Technik anzupassen.

9.4.2 Zertifizierungsverfahren

Das qualitätsgesicherte Verfahren ist mit einem „Monitoring“ und einem „Update Check“ um zwei neue Instrumente ergänzt worden. Beide können nach erfolgreicher Erstzertifizierung relevant werden.

Das EuroPriSe-Zertifizierungsverfahren besteht aus **zwei Hauptbestandteilen** (31. TB, Tz. 9.4.2): Zunächst wird das IT-Produkt oder die IT-basierte Dienstleistung von akkreditierten Sachverständigen evaluiert. In einem zweiten Schritt überprüft eine unabhängige Zertifizierungsstelle das von den Sachverständigen eingereichte Gutachten auf Vollständigkeit, Nachvollziehbarkeit und Datenschutzkonformität. Sind alle Zertifizierungskriterien erfüllt, verleiht die Zertifizierungsstelle das EuroPriSe-Zertifikat. Dieses ist zwei Jahre lang gültig. Nach Ablauf dieser Zeitspanne oder bei wesentlichen Änderungen kann ein vereinfachtes Rezertifizierungsverfahren durchgeführt werden.



IT-basierte Dienstleistungen und insbesondere webbasierte Dienste werden oft in kurzen zeitlichen Intervallen geändert, ohne dass dies für die Nutzer transparent ist. Deshalb ist bei EuroPriSe das „**Monitoring**“ eingeführt worden: Wurde ein IT-basierter Dienst zertifiziert, so muss er während der zweijährigen Gültigkeitsdauer des Siegels von den in das Verfahren involvierten Gutachtern auf seine fortwährende Vereinbarkeit mit den Zertifizierungskriterien überprüft werden. Aufgabe der Gutachter ist es zu verfolgen, ob datenschutzrelevante Änderungen an dem jeweiligen Dienst vorgenommen werden, und – falls ja – zu prüfen, ob der Dienst trotz der Änderungen noch alle anwendbaren EuroPriSe-Kriterien erfüllt. Die Anbieter von IT-basierten Dienstleistungen sind verpflichtet, acht Monate nach der Zertifizierung einen Monitoring Report bei der Zertifizierungsstelle einzureichen, der alle relevanten Änderungen und deren Bewertung beinhaltet. Ein weiterer Bericht ist nach 16 Monaten vorzulegen. Das Monitoring ersetzt nicht das erfolgreiche Durchlaufen eines Rezertifizierungsverfahrens.

Hersteller bzw. Anbieter können sich nach erfolgter Zertifizierung freiwillig dafür entscheiden, ihr Produkt bzw. ihre Dienstleistung von akkreditierten EuroPriSe-Gutachtern in regelmäßigen Abständen daraufhin überprüfen zu lassen, ob es nach wie vor allen relevanten Zertifizierungskriterien genügt. Werden solche „**Update Checks**“ durchgeführt, ersetzen diese sowohl das für IT-basierte Dienstleistungen obligatorische Monitoring als auch die Durchführung eines vereinfachten Rezertifizierungsverfahrens. Im Anschluss an die Zertifizierung sind alle sechs Monate von den Gutachtern angefertigte sogenannte Update Check Reports bei der Zertifizierungsstelle einzureichen. Bescheinigen die Gutachter dem IT-Produkt bzw. der -Dienstleistung fortdauernde Compliance mit den EuroPriSe-Zertifizierungskriterien und hat die Zertifizierungsstelle insoweit keine Einwände, so stellt sie nach Überprüfung des letzten einzureichenden Reports nach zwei Jahren eine Rezertifizierungsurkunde aus. Die Gültigkeit des EuroPriSe-Zertifikats verlängert sich dann um weitere zwei Jahre.

9.4.3 Zulassung von Gutachtern

Als EuroPriSe-Gutachter werden nur Datenschutzexperten tätig, die das strenge EuroPriSe-Akkreditierungsverfahren erfolgreich durchlaufen haben. Bis zum Ende des Jahres 2009 sind mehr als 80 Sachverständige aus 13 Staaten zugelassen worden.

Die Evaluierung der zu zertifizierenden IT-Produkte und -Dienstleistungen wird bei EuroPriSe durch akkreditierte Gutachter vorgenommen. Die Akkreditierung kann für den Bereich Recht und den Bereich Technik erfolgen, bei entsprechender **Fachkunde** ist eine Doppelzulassung möglich.

Datenschutzexperten müssen für ihre Akkreditierung nicht nur ihre Fachkunde und Zuverlässigkeit nachweisen, sondern auch an einem Ausbildungsworkshop teilnehmen und ein Trainingsgutachten anfertigen, das den hohen EuroPriSe-Anforderungen entspricht. Im Jahr 2009 wurden zwei kostenpflichtige **Ausbildungsworkshops** in Kiel durchgeführt. Ingesamt wurden bislang vier Workshops veranstaltet, an denen mehr als 150 Datenschutzexperten aus 13 Staaten teilgenommen haben.

2009 wurden **17 neue EuroPriSe-Gutachter** akkreditiert. Insgesamt sind damit zum Ende des Jahres 81 Datenschutzexperten als Gutachter zugelassen. 36 Sachverständige sind für den Bereich Recht und 35 für den Bereich Technik akkreditiert, zehn Sachverständige sind für beide Bereiche anerkannt. Die Gutachter können für ihre Tätigkeit als Sachverständige mit dem EuroPriSe-Expertenlogo werben.

Die akkreditierten Gutachter verteilen sich auf die folgenden EU-Mitgliedstaaten: Deutschland (33), Finnland (1), Frankreich (3), Großbritannien (1), Kroatien (2), Niederlande (2), Österreich (6), Schweden (3), Slowakei (1), Spanien (27). Zudem ist auch in Argentinien und den USA jeweils ein Datenschutzexperte als EuroPriSe-Gutachter zugelassen worden. Eine **Liste der zugelassenen EuroPriSe-Gutachter** ist abrufbar unter:

www.european-privacy-seal.eu/experts/register-experts/

Die Akkreditierung eines Gutachters ist **drei Jahre lang gültig**. Sie verlängert sich um weitere zwei Jahre, wenn der Gutachter aktiv an einem EuroPriSe-Verfahren mitwirkt oder an einschlägigen Fortbildungsveranstaltungen, z. B. an vom ULD angebotenen Workshops, teilnimmt.

Was ist zu tun?
Wegen des weiterhin bestehenden großen Interesses unter Datenschutzexperten an einer EuroPriSe-Akkreditierung wird das ULD im Verlauf des Jahres 2010 weitere Ausbildungsworkshops für Gutachter anbieten.

9.4.4 Abgeschlossene und laufende EuroPriSe-Verfahren

Bis zum Abschluss der EuroPriSe-Pilotphase im Februar 2009 konnten sechs Gütesiegel an IT-Produkte bzw. IT-basierte Dienstleistungen verliehen werden. Im weiteren Verlauf des Jahres wurden sechs Erstzertifizierungen und eine Rezertifizierung erfolgreich abgeschlossen.

Das **Interesse der Hersteller** von IT-Produkten und der Anbieter von IT-basierten Dienstleistungen an einer EuroPriSe-Zertifizierung ist hoch. 2009 konnten insgesamt sechs Produkte bzw. Dienstleistungen mit einem EuroPriSe-Zertifikat ausgezeichnet werden. Der Metasuchmaschine Ixquick gelang als erstem IT-basierten Dienst die erfolgreiche Rezertifizierung. Ende des Jahres 2009 gab es insgesamt mehr als 25 laufende EuroPriSe-Zertifizierungsverfahren.

2009 wurden folgende IT-Produkte und -Dienstleistungen **neu zertifiziert**:

- **KiwiVision Privacy Protector** (Version 1.0): Das Softwaremodul „Privacy Protector“ ist Teil von KiwiVision, einer Lösung für Videoüberwachung, die in jedes bestehende Videoüberwachungssystem integriert werden kann. Das Modul ermöglicht die Verschleierung von Videoklardaten in Echtzeit. Bewegte Personen oder personenbeziehbare Objekte (z. B. Kfz-Kennzeichen) können in digitalen Videobildern unkenntlich gemacht werden. Das restliche Videobild bleibt unverändert. Mit dem Modul können Videoüberwachungsanlagen so eingesetzt werden, dass sie weniger intensiv in das Recht auf informationelle Selbstbestimmung der überwachten Personen eingreifen.

- **Predictive Targeting Networking** (Version 2.0): PTN ist ein Verfahren zur gezielten Ansprache von Internetnutzern im Bereich der Online-Werbung („predictive behavioral targeting“). Die Ansprache der Nutzer erfolgt auf der Grundlage ihres Surfverhaltens, welches mit Umfragedaten einer kleinen Zahl zufällig ausgewählter Nutzer kombiniert und mithilfe mathematischer Algorithmen ausgewertet wird. Hierbei werden weder anbieterübergreifende Profile von Nutzern erstellt noch sensitive Daten im Sinne des Datenschutzrechts verwendet. Nutzer können den Einsatz des PTN-2.0-Verfahrens durch Verwendung eines sogenannten Block-Cookies unterbinden („Opt-Out“).

- **ICAM Legal Aid Solution** (Stand: Juli 2009): Die Anwaltskammer von Madrid (Ilustre Colegio de Abogados de Madrid – ICAM) hat den gesetzlichen Auftrag, an der Ernennung von Pflichtanwälten mitzuwirken, die bedürftige Personen vor Gericht vertreten. ICAM hat eine Softwarelösung zur Bearbeitung entsprechender Verfahren entwickelt und implementiert. Diese ermöglicht die Bearbeitung von Anträgen bedürftiger Personen, zudem können Anwälte über ein Webinterface ausstehende Gebühren für ihre Tätigkeit als Pflichtanwalt einsehen.

- **Iberemec CRM** (Stand: September 2009): Das spanische Unternehmen Iberemec, S.A. bietet seinen Kunden kostenlos und auf freiwilliger Basis die Nutzung eines internen Bereiches auf der Unternehmenswebsite http://www.iberemec.es an. Registrierte Kunden können u. a. online aktuelle Konditionen und Preise abfragen, Bestellungen vornehmen und Rechnungen einsehen. Dieser Service dient der Verbesserung der Kommunikation zwischen Iberemec und seinen Kunden (Customer Relationship Management – CRM).

- **telemed.net** (Version 2.7): Telemed.net ist eine Kommunikationslösung, die eine Echtzeitkommunikation zwischen Ärzten im Wege eines sogenannten Instant Messaging über das Internet ermöglicht. Zweck des Produktes ist es, Ärzten eine vor der Kenntnisnahme Dritter geschützte Direktkommunikation in Echtzeit über das Internet zu ermöglichen und darüber hinaus Gesundheitsdaten von Patienten zur Übernahme in ein Arztinformationssystem (AIS) zu übermitteln.

- **eBGempresa** (Version 2009.09.28.10.10): eBGempresa ist ein Online-Banking-Dienst, den die spanische Bank „Banco Guipuzcoano“ ihren Geschäftskunden (Unternehmen, Selbstständigen und Freiberuflern) anbietet. Kunden können sich nach Abschluss eines Online-Banking-Vertrags unter https://www.ebgempresa.com einloggen und neben Standardfunktionen wie Kontostandsabfrage oder Vornahme einer Überweisung weitere unternehmensspezifische Funktionalitäten nutzen.

Im Rezertifizierungsverfahren wurde die Wortsuche der **Metasuchmaschine Ixquick** (Stand: Januar 2009, http://www.ixquick.com) in einem vereinfachten Verfahren erneut überprüft und zertifiziert: Das Angebot leitet Suchanfragen von Internetnutzern an diverse Suchmaschinen weiter, kombiniert die von diesen erhaltenen Ergebnisse und stellt sie bereit. Bemerkenswert ist eine weitere Datenschutzverbesserung seit der Erstzertifizierung: Wurden damals die IP-Adressen der Nutzer für einen Zeitraum von 48 Stunden in Logfiles gespeichert, so werden sie heute gar nicht mehr über das Ende der Verbindung hinaus vorgehalten.

Die öffentlichen **Kurzgutachten** zu allen verliehenen EuroPriSe-Gütesiegeln (inklusive der Rezertifizierungen) sind in englischer Sprache abrufbar unter:

www.european-privacy-seal.eu/awarded-seals/

9.4.5 Zusammenarbeit mit nationalen Datenschutz-Gütesiegeln

Synergien zwischen den Verfahren für das europäische und das schleswig-holsteinische Datenschutz-Gütesiegel ermöglichen den Antragstellern eine Überprüfung der Vereinbarkeit sowohl mit europäischem als auch mit dem nationalen und lokalen Datenschutzrecht **in einem Gutachten** (Tz. 9.3.3). Inhaltsgleiche Prüfpunkte werden nur einmal bearbeitet. Dadurch können für Antragsteller und Zertifizierungsbehörde Kosten gesenkt werden.

Das europäische Datenschutz-Gütesiegel ist von Anfang an als Basis für eine „**Baukasten-Zertifizierung**“ konzipiert worden. Die Überprüfung eines Produktes oder einer Dienstleistung auf der Grundlage der harmonisierenden EU-Regelungen sichert weitgehend die Vereinbarkeit mit nationalem Datenschutzrecht, das insbesondere in sektorspezifischen Bereichen (z. B. Schulrecht, Medizinrecht) ergänzende Regelungen vorsehen kann. Eine auf EuroPriSe aufbauende Zertifizierung nach dem schleswig-holsteinischen Gütesiegel als sogenanntes Add-on kann dadurch ohne großen Mehraufwand realisiert werden. Da Gütesiegel und EuroPriSe „Pate“ für andere nationale Zertifizierungssysteme, z. B. in Frankreich, stehen, erwarten wir weitere Synergien.

9.4.6 Zusammenarbeit mit anderen Datenschutzbehörden

Auch nach Abschluss der Projektphase wurden der Kontakt und die Zusammenarbeit mit anderen Datenschutzbehörden weitergeführt.

Die Kolleginnen und Kollegen in Europa wurden auf der Europäischen Konferenz der Datenschutzbeauftragten über die Erfahrungen und den Stand von EuroPriSe unterrichtet. Auf Wunsch wurde am Tag vor der 31. Internationalen **Datenschutzkonferenz** in Madrid im Regierungssitz der Regionen, in der Real Casa de Correos, ein Workshop für Datenschutzbehörden mithilfe unseres Partners, der Datenschutzbehörde von Madrid (APDCM), ausgerichtet. Ziel des Workshops war eine vertiefte Information und Diskussion über zukünftige Kooperationen.

Der Kontakt mit der **französischen Datenschutzbehörde** CNIL wurde fortgesetzt. In einem Rapport des französischen Senats vom Juni 2009 zum Datenschutz (La vie privée à l'heure des mémoires numériques), der als wichtigste legislative Initiative in Frankreich seit der Implementation der EU-Datenschutzrichtlinie im Jahre 2004 bezeichnet wird, wird die Schaffung eines Datenschutz-Gütesiegels in Anlehnung an EuroPriSe empfohlen. Das Gesetzgebungsverfahren, das der CNIL die Durchführung von Zertifizierungsverfahren ermöglicht, wird voraussichtlich 2010 abgeschlossen sein.

Im Rahmen der Anhörung der **Europäischen Kommission** zur Überarbeitung des Rechtsrahmens des Grundrechts auf Datenschutz haben wir eine Stellungnahme zur Kooperation und Institutionalisierung von Datenschutzzertifizierungen mit dem Ziel abgegeben, weiter gehende Kooperationen zu ermöglichen.

Was ist zu tun?
Die Kooperation mit den Institutionen der EU und den Datenschutzbehörden in Europa ist fortzusetzen und weiter zu intensivieren.

10 Aus dem IT-Labor

10.1 Mobile Geräte – ob Spielzeug oder Werkzeug: jedenfalls absichern!

Mobile Geräte sind fester Bestandteil in der IT-Umgebung vieler Organisationen. Zu einem hohen Anteil werden hierauf personenbezogene Daten verarbeitet. Hersteller bieten Managementlösungen an, um IT-Sicherheit und Datenschutz zentral zu definieren und dezentral umzusetzen.

Unabhängig davon, aus welchem Grund ein mobiles Gerät angeschafft wird: Sein Einsatz geht fast immer mit der Verarbeitung personenbezogener Daten einher. Häufig sind die verwendeten Geräte mit vielen Funktionen ausgestattet, die zur Aufgabenerfüllung nicht benötigt werden und ein **zusätzliches Sicherheitsrisiko** darstellen. Den Risiken des Verlustes oder des Diebstahls, des Abhörens oder Manipulierens der Geräte muss mit wirksamen Sicherheitsmaßnahmen begegnet werden.

Der hohe **Beratungsbedarf** beim Einsatz von BlackBerry-Geräten besteht unvermindert fort (31. TB, Tz. 10.1). Stark angestiegen sind im kommunalen Bereich Nachfragen zum Einsatz des iPhones der Firma Apple.

Wir empfehlen, mobile Geräte nicht einzeln über die jeweils dezentrale Konfiguration zu verwalten, sondern eine **zentrale Managementlösung** einzuführen. Alle großen Hersteller bieten hierzu Mittel und Wege an. Zu nennen sind hier vor allem der BlackBerry Enterprise Server, das iPhone Enterprise Kit und der Windows Mobile Management Server. Diese Lösungen ermöglichen eine profilbasierte Vorkonfiguration der Geräte, durch die dann viele der sicherheitskritischen Funktionen abgeschaltet und zugleich alle notwendigen Sicherheitsmaßnahmen aktiviert werden können. Zusätzlich bieten die zentralen Managementsysteme Funktionen, die bei Verlust des Gerätes ausgeführt werden können, z. B. ein „Remote Wipe“, bei dem die Datenbestände auf den Geräten über einen zentral abgesetzten Befehl sicher gelöscht werden können.

Beim Einsatz mobiler Geräte sollten zumindest die folgenden **Sicherheitsmaßnahmen** geplant, umgesetzt und regelmäßig kontrolliert werden:

- Sicherung der personenbezogenen Daten auf dem Gerät durch Passwortschutz,
- bei Daten mit erhöhtem Schutzbedarf: Verschlüsselung der Daten auf dem Gerät,

- Deaktivieren nicht benötigter oder sicherheitskritischer Funktionen (Tethering, Bluetooth, WiFi),
- Verschlüsselung des Datentransfers in und aus den organisationsinternen Systemen sowie
- Authentisierung der Nutzer und der Geräte beim Aufbau einer Verbindung zu organisationsinternen Systemen.

Weiterhin gilt: Ein ungeplanter und unbedachter Einsatz mobiler Geräte ist mit dem LDSG und der DSVO nicht vereinbar. Analysiert man jedoch die Risiken, trifft **geeignete Sicherheitsmaßnahmen** und setzt diese über eine zentrale Lösung um, so ist ein datenschutzkonformer Einsatz mobiler Endgeräte möglich.

Was ist zu tun?
Daten verarbeitende Stellen müssen die zur Verfügung stehenden Enterprise-Funktionen aktueller Gerätegenerationen für eine zentrale Verwaltung nutzen, um das notwendige Niveau an Datenschutz und Datensicherheit zu gewährleisten.

10.2 Instant Messaging

Instant Messaging hat sich neben E-Mails als schnelle Kommunikationsform im privaten Bereich etabliert. Die Chats sind vor allem bei jüngeren Internetnutzern beliebt, aber auch viele Firmen nutzen inzwischen Online-Chats – beispielsweise für die Kundenberatung. Der Einsatz von Instant-Messaging-Diensten im Behördenumfeld wirft aber grundlegende Fragen auf.

Die technische Struktur von Instant-Messaging-Diensten basiert auf einem zentralen Vermittlungsserver, an dem sich alle Nutzer des jeweiligen Dienstes anmelden. So kann der Server dann anderen Nutzern anzeigen, wer gerade online ist. Nachrichten, die Nutzer einander schreiben, werden über den zentralen Server vom Absender zum Empfänger geleitet. Dienste wie MSN, ICQ oder Google Talk haben daher vollständige Kontrolle der über sie gesendeten Nachrichten. Es gibt keinen Weg für die Nutzer, zuverlässig die Identität des Gegenübers zu prüfen. Für den **Versand vertraulicher Informationen** sind solche Dienste daher **ungeeignet**. Zwar existiert für einige Dienste die Möglichkeit, Verbindungen per SSL zu verschlüsseln. Da es sich hierbei jedoch um eine Ende-zu-Server-Verschlüsselung handelt, erhält der zentrale Server nach wie vor Einblick in die Daten. Auch damit ist eine Authentisierung zwischen Nutzern nicht gegeben.

Zwei Wege sind denkbar, um Instant Messaging in Behörden im Zusammenhang mit vertraulichen Informationen zu nutzen:

- Eine Behörde kann einen **eigenen XMPP-Server** (XMPP steht für „Extensible Messaging and Presence Protocol“) betreiben. Nutzer müssen sich dort ein Konto anlegen und an diesem Server anmelden. Zusammen mit einer SSL-verschlüsselten Verbindung ergibt sich so eine Ende-zu-Ende-Verschlüsselung

zwischen Nutzer und Behörde, da sich der Server im Hoheitsbereich der Behörde befindet. Nachteil dieser Lösung ist, dass der Betrieb des Servers gewährleistet werden muss und die Nutzer im Regelfall nicht mit ihren gewohnten Chat-Diensten arbeiten können, sondern sich ein neues Nutzerkonto auf dem Behördenserver anlegen müssen. Eventuell müssen sie auch zusätzliche Software installieren, wenn die von ihnen bisher genutzte Chat-Anwendung das XMPP-Protokoll nicht beherrscht. Ebenfalls ungelöst bleibt hier das Problem der Authentisierung der Nutzer.

- Behörde und Nutzer, die miteinander kommunizieren wollen, könnten echte **Ende-zu-Ende-Verschlüsselungen** einsetzen. Hier sind verschiedene Verfahren denkbar, die jedoch in den meisten Fällen eine Installation von Zusatzsoftware auf Nutzerseite sowie ein gewissenhaftes Schlüsselmanagement erfordern. Auch ist die Authentisierung – z. B. beim klassischen PGP/GPG – aufwendig, da sie über einen zweiten Kanal erfolgen muss.

Eine einfache Möglichkeit bietet das Verschlüsselungsverfahren OTR (**Off-the-Record Messaging**). Um eine OTR-gesicherte Verbindung aufzubauen, müssen beide Kommunikationspartner Software verwenden, die OTR unterstützt. Einige gängige Chat-Programme bringen diese Fähigkeit von Haus aus mit, andere lassen sich nachrüsten. Zu Beginn einer OTR-gesicherten Kommunikation müssen beide Teilnehmer ein gemeinsames Passwort eintippen. Ist dieses Geheimnis bei beiden identisch, wird die Verbindung verschlüsselt und gilt als authentisiert. OTR ist so konzipiert, dass es die Bedingungen eines Vieraugengesprächs nachbildet. Dieses ist vertraulich und authentisch; nach dem Gespräch kann jedoch keiner der Gesprächspartner Inhalte der Unterhaltung beweisen. Diese letzte Eigenschaft eines persönlichen Gesprächs, nämlich die nachträgliche Abstreitbarkeit des Gesagten, erreicht OTR, indem jedes Datenpaket so gestaltet ist, dass im Nachhinein kein Beleg für die Kommunikation entsteht. Mit diesem Verfahren lassen sich Grundprobleme bei Instant Messaging lösen: Verbindungen sind leicht Ende-zu-Ende zu verschlüsseln. Die Authentisierung über ein gemeinsames Geheimnis kann aus bereits bekannten Informationen bestehen, wie z. B. einem Aktenzeichen oder einer Personalnummer. Ein umständliches Schlüsselmanagement entfällt. Gleichzeitig wird klar, dass die Abstreitbarkeit der Kommunikation Instant Messaging

? ***Abstreitbarkeit***

Gespräche unter vier Augen sind der klassische Fall einer „abstreitbaren Kommunikation". Es gibt keine Beweise für den Inhalt des Gesprächs. Im Nachhinein können beide Teilnehmer Gegenteiliges behaupten, beweisen kann es niemand. Gerade dieser Umstand hebt persönliche Gespräche von schriftlicher Kommunikation ab: Sie sind vertraulich, ohne jedoch den Grad der Verbindlichkeit eines Briefes zu erreichen.

Die konsequente Adaption dieses Umstands auf digitale Kommunikation wären abstreitbare Chats. Unterhaltungen ohne Brief und Siegel sind schnell geführt und bieten den Kommunikationspartnern Freiheiten, die eine schriftliche Kommunikation nicht bieten kann. Ebenso wie Telefonate für verbindliches Verwaltungshandeln ungeeignet sind, ist allerdings auch der Chat kein Medium für gerichtsfeste Kommunikation.

auch **faktisch zu einem Ersatz für Telefonate** machen kann – ohne verwertbare Gesprächsprotokolle. OTR-gestützte Chats können also die Schriftform nicht ersetzen.

Was ist zu tun?
Instant Messaging ist im „Auslieferungszustand" für den Behördeneinsatz nicht geeignet. Mangelnde Sicherheit und fehlende Authentisierung sind absolute Ausschlusskriterien. Mithilfe geeigneter technischer Maßnahmen ist ein Behördeneinsatz jedoch denkbar. Der Betrieb eines eigenen Chat-Servers ist die sauberste – und gleichzeitig aufwendigste – Lösung. Verfahren wie OTR können Chatten auf ein ähnliches Sicherheitsniveau wie das Telefonieren heben. Der Austausch sensibler Informationen kommt jedoch auch dann nicht in Betracht.

10.3 E-Mail-Archivierung

Anbieter von Produkten zur E-Mail-Archivierung betonen, dass Organisationen bereits seit 2002 dazu verpflichtet sind, sämtliche steuerrelevanten Daten maschinell auswertbar zur Verfügung stellen zu können.

Mit Verweis auf die Verwaltungsanweisung „**Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen**" (GDPdU) sowie das Handelsgesetzbuch und die Abgabenordnung werden seit geraumer Zeit etliche Produkte zur E-Mail-Archivierung auf den Markt geworfen. Deutsche Betriebe sind hiernach verpflichtet, sämtliche geschäftsrelevanten Daten für zehn Jahre vorzuhalten. Da liegt es natürlich nahe, den gesamten E-Mail-Verkehr zu archivieren und ihn vor ungewolltem Löschen zu schützen. Als Lösung bieten die Hersteller häufig eine „Black Box" ohne Eingriffs- oder Kontrollmöglichkeit für den Kunden an, die an zentraler Stelle in dessen Netz eingebunden wird und jeglichen ein- und ausgehenden E-Mail-Verkehr aufzeichnet.

Diese Archivierungslösungen werben mit einer einfachen Installation, einem hohen Grad an Verfügbarkeit aller E-Mails und garantiertem Schutz vor unbeabsichtigtem Löschen. Unabhängig von der Frage, ob private E-Mail-Nutzung erlaubt ist oder nicht: Nicht jede E-Mail ist geschäftsrelevant. Die Betriebsleitung und die IT-Verantwortlichen müssen sich also Gedanken darüber machen, wie das E-Mail-Archiv **datenschutzgerecht** aufgesetzt wird. Der oder die betriebliche Datenschutzbeauftragte und der Betriebsrat sind mit einzubeziehen, da hier Entscheidungen über Mitarbeiterdaten getroffen werden.

Die erste Frage betrifft die **private E-Mail-Nutzung**. Ist diese erlaubt, müssen technische und organisatorische Maßnahmen getroffen werden, um sie vom geschäftlichen E-Mail-Verkehr zu trennen. Zwei separierte E-Mail-Konten für jeden Beschäftigten sorgen für Klarheit. Natürlich muss jeder im Betrieb per Arbeitsanweisung auf diese Trennung der Nutzung hingewiesen werden. Das E-Mail-Archiv darf dann nur den Verkehr an die und von den geschäftlichen Konten archivieren. Auf diese Weise kann jedoch nicht vollständig verhindert werden, dass personenbezogene Daten von Kunden oder auch von Arbeitnehmern auf dem geschäftlichen Account anfallen.

Es bedarf somit technischer Möglichkeiten, einzelne E-Mails aus dem Archiv zu löschen. Fälschlicherweise können private Daten im Geschäftskonto gesendet oder empfangen worden sein. Ein Kunde hat z. B. nach einer Anfrage oder Kontaktaufnahme das Recht, seine Daten vollständig löschen zu lassen. Diese Löschoption widerspricht aber der Zielsetzung eines vollständigen E-Mail-Archivs. Die IT-Verantwortlichen müssen sich daher die Frage beantworten, ob und wenn ja welcher Einsatz einer **Archivierungslösung vertretbar** ist.

Häufig werden die Black-Box-Lösungen ins Netz der Organisation integriert, wobei aus dem bestehenden Verzeichnisdienst sämtliche Nutzerkonten in das Archiv übernommen werden. Neben den eventuell existierenden privaten Konten sind auf jeden Fall die E-Mail-Konten des **Betriebsrats oder der Gleichstellungsbeauftragten** vom Archiv auszunehmen.

Als zusätzliche Funktion bei der Erstinstallation wird oftmals der automatisierte Import aller Inhalte sämtlicher E-Mail-Konten angeboten. Dabei besteht die Gefahr, dass zu viele Daten in das Archiv übernommen und für Jahre gespeichert werden – womöglich ohne dass die dazugehörigen **Nutzer darüber informiert** wurden. Diese müssen aber vor der Einführung eines E-Mail-Archivs davon in Kenntnis gesetzt werden, um eine Entscheidung treffen zu können, welche Daten ihrer E-Mail-Konten nicht in das Archiv übertragen werden sollen.

Ein Problempunkt von Black-Box-Lösungen ist zudem der **Zugriff Dritter**, z. B. durch Hersteller und Dienstleister. Selbst wenn das E-Mail-Archiv verschlüsselt wird, können noch Daten im Klartext vorliegen: Häufig befinden sich unverschlüsselte Daten in Zwischenspeichern, die eventuell vom Dienstleister direkt abrufbar sind.

Was ist zu tun?
Daten verarbeitende Stellen sollten sich vor der Beschaffung und Einführung eines Systems zur E-Mail-Archivierung mit dem ULD und den zuständigen Wirtschaftsprüfern in Verbindung setzen.

10.4 Bunte Keksmischung

Der Begriff „Cookies“ dürfte inzwischen fast jedem Internetnutzer bekannt sein. Es handelt sich ursprünglich um kleine „Datenkrümel“, die eine Webseite im Browser des Besuchers hinterlegen kann, um den Besucher bei Bedarf zuverlässig wiederzuerkennen.

Sinnvoll ist solch eine Wiedererkennung beim Online-Einkauf, wo der Webserver den Warenkorb des Nutzers über diverse Unterseiten hinweg korrekt zuordnen muss. Weniger im Interesse des Nutzers sind Cookies, die ihn über die Dauer einer Sitzung hinweg und über die Grenzen eines einzelnen Angebots quer durchs Web markieren. Wer ohne Argwohn und ohne manuelle Nachbesserung in der eigenen Browserkonfiguration im Internet unterwegs ist, bleibt womöglich über viele Jahre für bestimmte Anbieter **wiedererkennbar**. Das Nutzerprofil, das in

dieser Zeit gebildet werden kann, lässt leicht Rückschlüsse auf die reale Person dahinter zu.

Der Spuk solcher Langzeit-Cookies ist einfach zu beenden. Moderne Browser, mit Ausnahme von Google Chrome, lassen sich so einstellen, dass alle Cookies beim Schließen des Browsers verschwinden. Eine längerfristige **Protokollierung des Surfverhaltens** über diese Cookies ist dann nicht möglich.

Problematisch sind allerdings neuere Entwicklungen, die sich nicht unmittelbar über die Browserkonfiguration steuern lassen: Neben den konventionellen Cookies haben sich inzwischen sogenannte **Flash-Cookies** etabliert. Der Browserzusatz Flash der Firma Adobe ist nach Angaben des Herstellers auf über 90 % aller PCs installiert und sorgt für die Darstellung von Animationen und Videosequenzen. Zum Speichern von Parametern dient dem Flash-Plugin ein eigenes Speichersystem, die Local Shared Objects (LSO). Diese Dateien können vom Flash-Plugin auf dem Nutzerrechner abgelegt werden. Über den Browser hat der Nutzer darauf jedoch keinen Zugriff, sodass auf vielen Rechnern diese Flash-Cookies unentdeckt bleiben. Hinzu kommt, dass dasselbe Flash-Cookie für alle auf dem System befindlichen Browser gilt, sodass Surfsitzungen mit verschiedenen Browsern miteinander verkettet werden können. Wie normale Cookies können Flash-Cookies durchaus sinnvollen Dingen dienen. Verbreitet ist z. B. das Speichern von Spielständen bei Flash-basierten Online-Spielen. Aber auch banale Dinge wie die Lautstärkeeinstellungen von YouTube-Videos werden mithilfe der Local Shared Objects gespeichert. Löschen lassen sich diese Flash-basierten Cookies nur über Adobes Webseiten. Die wenig intuitive Internetadresse lautet:

www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager07.html

Ähnliche Speichermodelle wie Adobe Flash bieten „Microsoft Silverlight“ und „Java“ von Sun. Auch hier sind die Einstellungen zum Deaktivieren von Cookie-ähnlichen Objekten nicht leicht auffindbar. Microsoft versteckt sein Konfigurationstool „Silverlight.Configuration.exe“ bei Windows-Rechnern im Verzeichnis C:\Programme\Microsoft Silverlight\[Versionsnummer]\. Die Java-Konfiguration javacpl.exe liegt bei solchen Rechnern standardmäßig im Verzeichnis C:\Programme\Java\[Version]\bin\.

Eine dritte Inkarnation der herkömmlichen Cookie-Idee stellt der sogenannte DOM-Storage-Mechanismus (DOM: Document Object Model) dar, der seit Firefox 2 in aktuellen Browsern zu finden ist. DOM Storage erweitert die klassische Cookie-Idee im Kern um eine flexiblere Adressbehandlung und vergrößert den verfügbaren Speicherplatz. Können klassische Cookies gerade mal 4 KB fassen, kann ein DOM Storage Cookie deutlich mehr an Daten speichern, nämlich bis zu 5 MB beim Firefox-Browser und sogar bis zu 10 MB beim Internet Explorer. Der dahinterstehende Gedanke ist ironischerweise sogar datenschutzfördernd: Dienste wie Online-Textverarbeitungen können in solchen **Mega-Cookies** ihre Dokumente ablegen, sodass der Nutzer nicht mehr gezwungen ist, diese auf dem Server des Anbieters zu speichern. Trotzdem bleiben auch hier sämtliche Implikationen konventioneller Cookies in Bezug auf langfristige Verkettbarkeit bestehen. Zudem

mangelt es bislang an Transparenz für den Nutzer: Obwohl solche Mega-Cookies vom Browser erzeugt werden und nicht von externen Programmen wie Flash, tauchen sie nicht in der browserinternen Übersicht der gespeicherten Cookies auf.

Das ULD berät Bürgerinnen und Bürger in Fragen des Selbstdatenschutzes und bezüglich **Maßnahmen gegen unerwünschte Cookies**.

Was ist zu tun?
Solange die Hersteller der diversen Browserzusatzprogramme und Laufzeitumgebungen kein einheitliches Steuermodell für lokale Objekte bieten, müssen Nutzer sich jede Technik separat ansehen und entscheiden, ob und welche Daten auf der Festplatte abgelegt werden dürfen. Nutzerverfolgung über Flash-Cookies ist inzwischen keine Ausnahme mehr, sodass zumindest die Flash-Einstellungen durch den Nutzer überprüft werden sollten.

10.5 Reputationssysteme für Webseiten – fragwürdiges Vertrauen

Mitte des Jahres wurde das ULD darauf hingewiesen, dass der Webreputationsdienst Web of Trust vor dem Internetangebot des Datenschutzzentrums warne.

Der Dienst Web of Trust (WOT) bietet Nutzern die Möglichkeit, Webseiten nach verschiedenen Kriterien zu bewerten und so zu einem „Scorewert“ einzelner Webseiten beizutragen. Nach Installation einer entsprechenden Browsererweiterung wird der Nutzer bei dem Zugriff auf eine Webseite über deren Scorewert informiert. Bei extrem schlechter Bewertung sperrt das Programm den Zugriff auf die fragliche Seite sogar und lässt den Nutzer nur nach einem Bestätigungsklick weitersurfen. Besucher von **www.datenschutzzentrum.de**, die das WOT-Tool einsetzten, bekamen solche Warnhinweise zu sehen.

Bei genauerem Hinsehen entpuppte sich die negative Bewertung als **Fehlinterpretation** zweier WOT-Nutzer – einer hatte dem ULD fälschlicherweise Spam-Mails zugerechnet, der andere hatte dessen Eintrag anscheinend ohne weitere Prüfung kopiert. Da diese beiden die einzigen Bewerter waren, sank der Scorewert der ULD-Seiten in den kritischen Bereich. Zu kritisieren ist das Beschwerdemanagement des finnischen Dienstleisters WOT: Auf E-Mails des ULD wurde nicht geantwortet. Die FAQ der Webseite legen nahe, direkt an die betreffenden Bewerter heranzutreten und selbst positive Eigenbewertungen abzugeben. Das wirft die Frage auf, wie verlässlich WOT-Scorewerte eigentlich sind.

WOT ist nicht der einzige Dienst, der sich im Bereich der **Webseitenbewertung** versucht. Auch Antivirenhersteller wie McAfee und nicht zuletzt Google versuchen, Webseiten nach Gut und Böse zu kategorisieren. Dabei verfolgen die Dienste verschiedene Ansätze. WOT setzt auf die berühmt-berüchtigte Weisheit der Massen und erstellt ein reines Aggregat von Nutzermeinungen. Andere Dienste versuchen, Webseiten mit Suchrobotern zu analysieren und so schädliche Inhalte zu finden.

Alle Systeme kranken an der Schwierigkeit für den Nutzer, sich ein Bild über die Gründe einer bestimmten Bewertung einer Webseite zu machen. Letztlich sind **die genauen Kriterien**, nach denen Webseiten klassifiziert werden, eine Art Betriebsgeheimnis oder, wie bei WOT, willkürlich von den jeweiligen Bewertenden abhängig. Das führt zu dem kuriosen Umstand, dass ein und dieselbe Webseite vom einen Dienst als ungefährlich, vom anderen als Bedrohung für den eigenen Computer klassifiziert wird. Dem Nutzer bleibt kaum mehr, als einem Dienst blind zu vertrauen – und sich dessen Unzulänglichkeiten bewusst zu werden. Die ULD-Webseite ist bei WOT übrigens wieder im grünen Bereich, nachdem mehrere Nutzer gute Bewertungen abgegeben haben.

Was ist zu tun?
Dienste zur Darstellung einer Webseitenreputation könnten hilfreich sein. In der Praxis schaffen es die Dienste jedoch nicht, die notwendige Transparenz herzustellen. Bewertungstools können daher im Surfalltag kaum mehr als einen vagen Hinweis geben.

11 Europa und Internationales

Auf **internationaler Ebene** hat sich das ULD an einer Vielzahl von Aktivitäten beteiligt, die darauf abzielen, das globale Datenschutzniveau zu heben und zu verhindern, dass die lokalen Standards nicht durch internationalen Datenaustausch abgesenkt werden (Tz. 2.3).

Die **Europäische Union** (EU) erlangt zunehmenden Einfluss auf die Datenverarbeitung öffentlicher und nicht öffentlicher Stellen in Schleswig-Holstein. Ein Beispiel hierfür ist die Vorratsdatenspeicherung, die auf einer Richtlinie der Europäischen Gemeinschaften beruht. Es ist daher notwendig, sich mit den Vorhaben schon auseinanderzusetzen, wenn sie in Brüssel beraten werden. Einmal beschlossen, bestehen für die Mitgliedstaaten meist keine oder nur geringe Spielräume.

Auf Ebene der EU gewinnen zwei Institutionen eine zunehmende Bedeutung: **der Europäische Datenschutzbeauftragte (EDSB) und die Artikel-29-Datenschutzgruppe**. Der EDSB hat mit dem Lissabon-Vertrag (Tz. 11.1) zusätzliche Aufgaben erhalten. An erster Stelle ist insofern der Bereich „Justiz und Inneres“ zu nennen. Als Koordinierungsgremium zwischen den nationalen Datenschutzaufsichtsbehörden in der EU wie auch als Instanz bei der Festlegung gemeinsamer Positionen erhält die Artikel-29-Datenschutzgruppe immer mehr Gewicht. Sie geht auf die Regelung des Artikels 29 der Europäischen Datenschutzrichtlinie zurück. Die Gruppe hat inzwischen 168 Arbeitspapiere (Working Paper) vor allem für den nicht öffentlichen Bereich erarbeitet, in denen einheitliche Antworten auf sich EU-weit stellende Fragen gegeben werden.

www.edps.europa.eu/EDPSWEB/edps/site/mySite/lang/de/pid/1
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_de.htm

Nach dem im Dezember 2009 verabschiedeten Stockholmer Programm sind in den nächsten fünf Jahren wichtige **Veränderungen im Datenschutz** zu erwarten. Positiv ist, dass es eine grundlegende Evaluierung des europäischen Datenschutzrechts auf seine Eignung zur Gewährleistung eines angemessenen Datenschutzes und eine Stärkung des technischen Datenschutzes vorsieht. Im Sicherheitsbereich sind aufgrund des Stockholmer Programms allerdings gravierende Eingriffe zu erwarten (Tz. 11.2). Angedacht sind etwa Maßnahmen zur Erfassung und Auswertung von Daten über Ein- und Ausreisen in die und aus der EU. Darin deutet sich die Wiederaufnahme des Vorhabens an, in der EU ein System zur Speicherung und Auswertung von Passenger Name Records (PNR) einzurichten (30. TB, Tz. 11.1). Die Arbeiten an einem entsprechenden Rahmenbeschluss sind zunächst wegen erheblicher Vorbehalte des Europäischen Parlaments gestoppt worden. Es ist zu befürchten, dass dieses Thema erneut aufgegriffen wird.

11.1 Vertrag von Lissabon

Am 1. Dezember 2009 ist der Vertrag von Lissabon in Kraft getreten. Damit sind gewichtige Änderungen für die EU verbunden, die sich auch auf den Datenschutz auswirken.

Mit dem Vertrag von Lissabon wurde die **Grundrechtecharta** der EU rechtsverbindlich. Zudem ist vorgesehen, dass die EU der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) beitritt. Hierfür ist noch ein einstimmiger Beschluss des Rates erforderlich. Damit werden die Grundrechte, die in der EMRK niedergelegt sind, zu allgemeinen, direkt anwendbaren Rechtsgrundsätzen in der EU. Für den Datenschutz bedeutet beides eine gewichtige Stärkung, denn sowohl die Grundrechtecharta der EU als auch die EMRK enthalten ein Recht auf Datenschutz.

Besondere Bedeutung hat der Reformvertrag von Lissabon für die **polizeiliche und justizielle Zusammenarbeit** der Mitgliedstaaten der EU in Strafsachen. Nach dem bisherigen Recht galt für diesen Bereich als der sogenannten dritten Säule ein eigenes Rechtssetzungsverfahren, in dem die Entscheidungen maßgeblich durch den Rat, d. h. durch die Regierungen der Mitgliedstaaten, getroffen wurden. Mitwirkungsmöglichkeiten des Europäischen Parlaments waren beschränkt; es war bei Rechtssetzungsverfahren lediglich anzuhören und hatte keine Entscheidungsbefugnisse. Nach dem Vertrag von Lissabon gilt für die Zusammenarbeit in Strafsachen weitgehend das ordentliche Gesetzgebungsverfahren. Dies unterscheidet sich vom früheren Rechtssetzungsverfahren in der dritten Säule vor allem durch eine stärkere Einbindung des Europäischen Parlaments.

Erweiterte Kompetenzen des Europäischen Parlaments bedeuten eine wesentliche **Stärkung der Demokratie** in der EU. Gerade die polizeiliche und justizielle Zusammenarbeit in Strafsachen wurde vor Inkrafttreten des Vertrags von Lissabon wegen ihres Demokratiedefizits kritisiert. Wie wichtig die Beteiligung des Europäischen Parlaments werden kann, hat sich jüngst beim SWIFT-Abkommen (Tz. 11.3) gezeigt. Das Parlament stand dem Abkommen von Anfang an kritisch gegenüber und hat seine Bedenken in einer Entschließung klar zum Ausdruck gebracht. Nach dem Inkrafttreten des Vertrages von Lissabon hat das Parlament das zuvor vom Rat gebilligte Abkommen abgelehnt.

Durch den Vertrag von Lissabon erhalten auch die **nationalen Parlamente** mehr Mitspracherechte. In Deutschland hat vor allem die Entscheidung des Bundesverfassungsgerichts zur Umsetzung des Vertrags von Lissabon dazu geführt, dass dem Bundestag und dem Bundesrat Mitentscheidungsbefugnisse bei der Änderung der Verträge und mehr Mitspracherechte bei Gesetzgebungsverfahren der Europäischen Union eingeräumt werden.

Was ist zu tun?
Der Vertrag von Lissabon verspricht eine Aufwertung von Grundrechten und Demokratie. Schleswig-Holstein sollte diese Chance nutzen, Entscheidungen in Europa mitzugestalten und auf eine Stärkung des Datenschutzes in Europa hinzuwirken.

11.2 Stockholmer Programm

Die EU hat im Stockholmer Programm die Ziele der Innen- und Sicherheitspolitik der EU zur Entwicklung eines Raumes der Freiheit, der Sicherheit und des Rechts festgelegt. Der Katalog der geplanten Maßnahmen zum Schutz der inneren Sicherheit lässt Zweifel entstehen, ob Datenschutzverbesserungen möglich sein werden.

Das Programm nennt als ausdrückliches Ziel die **Wahrung der persönlichen Freiheitsrechte** und der Privatsphäre über die nationalen Grenzen der Mitgliedstaaten hinweg. Das Datenschutzrecht soll vereinheitlicht und weiterentwickelt und es sollen neue datenschutzfreundliche Technologien zertifiziert und eingesetzt werden. Schlimmes ist aber zu befürchten, wenn zugleich das Abkommen über die Zusammenarbeit mit den Vereinigten Staaten von Amerika als vorbildlich bezeichnet wird.

Eine umfassende Darstellung der **sicherheitspolitischen Ziele** des Stockholmer Programms ist in diesem Zusammenhang nicht möglich; drei wesentliche Ziele sind:

- die Optimierung des Informationsaustausches und eine technische Infrastruktur hierfür mit einem europäischen Informationsmodell,
- die Verstärkung von Europol mit einer intensiveren automatisierten Datenvernetzung, auch zu anderen europäischen Datenbanken und internationalen Systemen,
- die Einführung eines elektronischen Registriersystems für Ein- und Ausreisen in die bzw. aus den Hoheitsgebieten der EU-Mitgliedstaaten mit einem Vorabgenehmigungsverfahren.

Voraussetzung für die technische Optimierung des Informationsaustausches ist eine **Synchronisierung** der bisher getrennten Datenverarbeitungswelten. Europäische und nationale Systeme und Verfahren sollen aufeinander abgestimmt werden, damit technische Unverträglichkeiten kein Hindernis mehr darstellen. Die Vereinheitlichung betrifft kompatible Hard- und Software sowie die von den Sicherheitsbehörden verwendeten Datenmodelle.

Europol soll aufgewertet werden und internationale Funktionen übernehmen, indem es in bestimmten Kriminalitätsbereichen zur zentralen Sammelstelle nationaler Informationen und zum Mittler dieser Daten für andere europäische sowie internationale Datenverarbeitungssysteme wird. Geklärt werden muss, inwieweit dabei die Rohdaten der nationalen Behörden und die Inhalte von Analysen weitergegeben werden sollen. Bei den differenzierten Ansätzen muss neben dem automatisierten Datenaustausch weiterhin die konventionelle Datenübermittlung, etwa durch Verbindungsbeamte, im Blickfeld bleiben.

Das US-amerikanische Vorbild für ein elektronisches **Registriersystem für Ein- und Ausreisen** aus den bzw. in die Hoheitsgebiete der Mitgliedstaaten mit einem

Vorabgenehmigungsverfahren ist bekannt. Ein zentraler Bestandteil ist die datenschutzrechtlich äußerst heikle Übermittlung der Passagierdaten, der Passenger Name Records (PNR). Viele Bürgerinnen und Bürger sehen in dieser anlasslosen Überwachung eine übermäßige Beeinträchtigung ihrer Reisefreiheit und verzichten auf Reisen in die USA (30. TB, Tz. 11.1). Die Effizienz des bestehenden Verfahrens in den Vereinigten Staaten ist bis heute nicht erwiesen. Es werden riesige Datenbestände von Reisenden aufgebaut. Für die Betroffenen ist nicht transparent, zu welchen Zwecken diese genutzt und wie lange die Daten bei welcher Stelle gespeichert werden. Das Stockholmer Programm erwähnt das Registriersystem, ohne sich zur Geeignetheit und Effizienz eines solchen Verfahrens zu äußern.

Die **Konferenz der Datenschutzbeauftragten** des Bundes und der Länder hat sich im Oktober 2009 auf eine Entschließung zu den Datenschutzdefiziten in Europa auch nach dem Stockholmer Programm geeinigt.


www.datenschutz.de/dsb-konferenz/
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_de.htm

Was ist zu tun?
Bei allem berechtigten Interesse an Sicherheit in einem geeinten Europa dürfen die Freiheitsrechte der Bürgerinnen und Bürger nicht unverhältnismäßig eingeschränkt werden.

11.3 Bankdaten für die USA

Die gute Nachricht zuerst: Die US-Behörden haben keinen direkten Zugriff mehr auf die internationalen Banktransaktionsdaten des in Belgien ansässigen Dienstleisters SWIFT. Die schlechte Nachricht: Damit ist der Zugriff von US-Behörden auf die Datensätze keineswegs gestoppt, zumindest nicht nach den Plänen der USA.

Drei Jahre nachdem bekannt wurde, dass regelmäßig Daten aus dem US-amerikanischen Rechenzentrum der SWIFT, der Society for Worldwide Interbank Telecommunications, an US-Finanz- und Sicherheitsbehörden übermittelt wurden (29. TB, Tz. 5.1), hat SWIFT mit dem Ziel der Sicherung des Bankgeheimnisses der Kundinnen und Kunden sein **Spiegelrechenzentrum** von den USA in die Schweiz verlegt. Damit war dem Datenzugriff ein Ende bereitet.

Am 30. November 2009, ein Tag vor Inkrafttreten des Vertrags von Lissabon (Tz. 11.1), hat der Rat der EU den Entwurf für ein **Abkommen mit den USA** gebilligt, das US-Behörden doch wieder die internationalen Zahlungsverkehrsdaten von Banknetzdienstleistern ermöglicht. Bereits im Vorfeld war dieser Plan massiv kritisiert worden, u. a. vom Europäischen Parlament, vom Bundesrat und von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

http://www.bfdi.bund.de/cln_134/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/78.DSK_SWIFT.html?nn=409240

Ungeachtet der vorgetragenen Kritik hatte Deutschland mit einer Stimmenthaltung im EU-Rat den Weg für dieses Abkommen frei gemacht. Das EU-Parlament hat das Abkommen dagegen mehrheitlich abgelehnt, sodass es außer Kraft gesetzt ist. Eine besonnene Entscheidung, denn das Abkommen enthält **gewaltige Datenschutzdefizite**. Ein angemessenes Datenschutzniveau der in die USA übermittelten Daten und ihrer weiteren Verwendung ist nicht gewährleistet. Das ULD hat die Kritikpunkte in einer Stellungnahme zusammengefasst.

- Kernstück des Abkommens ist das vom US-Finanzministerium betriebene **Terrorist Finance Tracking Programme**, ein Analysewerkzeug zum Aufspüren von Terrorismusbezügen und Terrorismusfinanzierung. Hierfür sollen Daten von europäischen Zahlungsdiensteanbietern bereitgestellt werden. Was genau sich hinter dem Terrorist Finance Tracking Programme verbirgt, ist im Abkommen nicht beschrieben; lediglich Data Mining wird ausgeschlossen. Der Nutzen der SWIFT-Daten für dieses Programm ist nicht belegt. Angeblich wurden bisher 1.450 Hinweise aus dem Programm an Sicherheitsbehörden in der EU weitergegeben. Was tatsächlich an sicherheitsrelevanten Erkenntnissen herausgekommen ist, ist nicht überprüfbar dargelegt.
- Unzureichend geregelt ist die **Reichweite des Abkommens**. Es zielt vor allem auf SWIFT als globalen Dienstleister. Doch werden weitere Verfahren betrieben, etwa das innereuropäische Überweisungssystem SEPA, dessen Einbeziehung in den Anwendungsbereich des Abkommens keineswegs ausgeschlossen ist. Wer welche Daten liefern soll, wird nicht im Abkommen selbst, sondern in geheimen Zusatzvereinbarungen festgelegt.
- Ausufernd sind die Voraussetzungen für die Bereitstellung der Daten an das US-Finanzministerium. Es reicht ein Verdacht künftiger terroristischer Straftaten und ein nicht näher definierter Bezug hierzu. Die im Abkommen verwendete **Terrorismusdefinition** knüpft schon an Sachverhalte weit im Vorfeld strafbarer Handlungen an. Die Definition ist so weit gefasst, dass auch legitime und in einer Demokratie selbstverständliche Handlungen wie etwa politische Demonstrationen darunterfallen können.
- Den weitreichenden Informationsmöglichkeiten der US-Behörden stehen wenige, völlig **unzureichende Datenschutzvorkehrungen** gegenüber: Mit den bereitgestellten Daten soll kein Data Mining betrieben werden; sie sollen, sicher gespeichert, nur für Zwecke der Terrorismusbekämpfung genutzt und nach spätestens fünf Jahren gelöscht werden. Aus der Datenanalyse erlangte

Hinweise dürfen mit Behörden in den USA, der EU und Drittstaaten ausgetauscht werden. Voraussetzung ist lediglich das Vorliegen terroristischer Anhaltspunkte. Offen bleibt, ob die Hinweise auch personenbezogene Daten enthalten können. Darüber hinaus gibt es keine weiteren materiellen Datenschutzvorkehrungen. Den Betroffenen werden keine Rechte auf Auskunft, Berichtigung und Löschung der Daten eingeräumt. Eine ausreichende unabhängige Datenschutzkontrolle oder ein wirksamer Rechtsschutz ist nicht vorgesehen.

 www.datenschutzzentrum.de/wirtschaft/swift/091218-stellungnahme.html

Im Abkommen wird angedeutet, dass ein System nach dem Vorbild des US-amerikanischen Terrorist Finance Tracking Programme **auch in der EU** eingeführt werden könne. Das Stockholmer Programm weist in dieselbe Richtung, wenn die Kommission aufgefordert wird, Möglichkeiten zur Aufdeckung der Terrorismusfinanzierung innerhalb Europas zu untersuchen.

Was ist zu tun?
Bei einem zu erwartenden neuen Abkommen sollte Schleswig-Holstein seine Mitwirkung nutzen, damit die USA ohne ein datenschutzrechtlich akzeptables Niveau keine Daten erhalten.

11.4 US Safe Harbor

Das US-Safe-Harbor-Programm soll die europäischen Datenschutzstandards für Übermittlungen von personenbezogenen Daten aus Europa an US-amerikanische Unternehmen sicherstellen. Nach Bekanntwerden von weitreichenden Verstößen gegen Safe Harbor stellt sich die Frage nach dessen Verlässlichkeit.

> **?** ***Safe Harbor***
>
> *(engl. für „sicherer Hafen") ist die Bezeichnung für eine Vereinbarung zwischen Europa und den USA. Verpflichtet sich ein US-Unternehmen auf die Einhaltung der Safe-Harbor-Grundsätze, so wird angenommen, dass ein dem EU-Datenschutzrecht vergleichbarer Standard bei der Verarbeitung personenbezogener Daten besteht.*

Das seit dem Jahr 2000 bestehende US-Safe-Harbor-Programm beruht auf einer Vereinbarung zwischen der Europäischen Kommission und dem Wirtschaftsministerium (Department of Commerce) der Vereinigten Staaten von Amerika (USA). US-Unternehmen, die sich hierauf verpflichten, wollen damit die Vereinbarkeit ihrer Datenverarbeitungsgrundsätze mit den Anforderungen der Europäischen Datenschutzrichtlinie nachweisen. Grundvoraussetzung für jede Übermittlung personenbezogener Daten aus der EU in ein Drittland ist das Bestehen eines **mit EU-Datenschutzrecht vergleichbaren Standards** im Empfängerland. Dies liegt für die USA mangels vergleichbarer Datenschutzgesetze nicht vor. Will ein europäisches Unternehmen Daten in die USA übermitteln, muss es sicherstellen, dass

das empfangende Unternehmen die Daten den europäischen Vorgaben entsprechend behandelt. Dies kann über Standardvertragsklauseln, verbindliche Unternehmensregeln (Binding Corporate Rules), eine Genehmigung der zuständigen Datenschutzbehörde oder eben durch eine Selbstverpflichtung des US-Unternehmens nach den Safe-Harbor-Grundsätzen erfolgen. Dies gilt selbstverständlich auch für schleswig-holsteinische Unternehmen, die Daten in die USA transferieren bzw. einen Datenaustausch z. B. mit Konzernmuttergesellschaften mit Sitz in den USA pflegen.

> **? *Federal Trade Commission (FTC)***
>
> *US-amerikanische Bundeshandelskommission, die zuständig für Verbraucherschutz und Wettbewerbsrecht ist.*

Ob sich europäische Unternehmen in jedem Fall auf die Behauptung einer Mitgliedschaft bei Safe Harbor und auf die Einhaltung der Safe-Harbor-Grundsätze in den USA verlassen können, ist nach der australischen Studie „The US Safe Harbor – Fact or Fiction?“ vom Dezember 2008 mehr als fraglich. Im Mittelpunkt der Kritik europäischer Datenschutzbehörden steht die mangelnde Kontrolle der Unternehmen seitens der zuständigen US-Behörde. Bislang kann ein US-Unternehmen die Mitgliedschaft durch Selbsterklärung erlangen, die sogenannte **Selbstzertifizierung**, und dies dem Department of Commerce mitteilen, um sich auf einer zentralen Liste eintragen zu lassen. Seit März 2009 erhebt das Department of Commerce für die Eintragung erstmalig eine einmalige Gebühr von 200 US-Dollar und eine jährliche Gebühr von 100 US-Dollar. Eine Überprüfung erfolgt nicht. Zuständig für Verstöße gegen Safe Harbor ist in begrenztem Umfang die Federal Trade Commission (FTC). Als für den Verbraucherschutz zuständige Behörde kann sie gegen unfaire und irreführende Praktiken vorgehen. Erstmalig wurden 2009 von der FTC Maßnahmen gegen sechs Unternehmen ergriffen, die fälschlicherweise behauptet hatten, sich nach Safe Harbor selbst zertifiziert zu haben. Eine Überprüfung der Einhaltung der Safe-Harbor-Grundsätze – Informationspflicht, Wahlmöglichkeiten, Weitergabe, Sicherheit, Datenintegrität, Auskunftsrecht und Durchsetzung – ist nicht erfolgt.

> **? *Art. 29 Safe Harbor Contact Group***
>
> *ist eine Untergruppe der sogenannten Artikel-29-Datenschutzgruppe, des Zusammenschlusses der Europäischen Aufsichtsbehörden für den Datenschutz, der Europäischen Kommission und des Europäischen Datenschutzbeauftragten. Benannt nach Artikel 29 der Europäischen Datenschutzrichtlinie, hat die Gruppe die Aufgabe, zu datenschutzrechtlichen Fragestellungen im Zusammenhang mit der Umsetzung und Anwendung der Richtlinie und zum Schutzniveau innerhalb der Gemeinschaft sowie in Drittländern Stellung zu nehmen.*

Das ULD hat 2009 die Aufsichtsbehörden der Bundesländer bei den Beratungen der Art. 29 Safe Harbor Contact Group mit dem Department of Commerce und der FTC vertreten. Es bestehen große Bedenken an der weiteren **Tragfähigkeit des Konzeptes**, wenn das Department of Commerce die Einhaltung der Selbstverpflichtungen der an Safe Harbor teilnehmenden Unternehmen nicht in einem höheren Maße selbst kontrolliert oder entsprechende Kontrollmaßnahmen implementiert. Unternehmen ist zu raten, sich nicht allein auf die Behauptung eines US-Unternehmens, Mitglied bei Safe

Harbor zu sein, zu verlassen. Der Verwendung von Standardvertragsklauseln oder der von einer Datenschutzbehörde genehmigten bindenden Unternehmensrichtlinien (BCR) ist derzeit der Vorzug zu geben.

Was ist zu tun?
Es ist auf effektive und transparente Kontrollmaßnahmen zur Einhaltung der Safe-Harbor-Grundsätze durch die US-amerikanischen Behörden hinzuwirken.

12 Informationsfreiheit

War das Informationsfreiheitsgesetz Schleswig-Holstein vor zehn Jahren noch eine kleine Revolution in der **bundesdeutschen Verwaltungslandschaft**, so hat sich der darin zum Ausdruck kommende Gedanke inzwischen bundesweit etabliert. Im Jahr 2006 trat endlich das Informationsfreiheitsgesetz für die Bundesverwaltung in Kraft. Zuvor und danach haben inzwischen folgende Länder ein Gesetz erhalten: 1998: Brandenburg, 1999: Berlin, 2000: Schleswig-Holstein, 2001: Nordrhein-Westfalen, 2006: Bremen, Mecklenburg-Vorpommern, Saarland, Hamburg, 2007: Thüringen, 2008: Rheinland-Pfalz und Sachsen-Anhalt. Es fehlen noch Baden-Württemberg, Bayern, Hessen, Niedersachsen und Sachsen.

Bewährt haben sich nicht nur die Regelungen zur Erhöhung der Verwaltungstransparenz, sondern auch die Aufgabenzuweisung an die Datenschutzbeauftragten, im Fall eines Konfliktes zwischen Bürgerinnen und Bürgern und der Verwaltung zu vermitteln. Hamburg hatte zunächst keine solche Funktion vorgesehen, dann aber 2009 dem Datenschutzbeauftragten auch die Funktion des **Informationsfreiheitsbeauftragten** zugewiesen. Lediglich Thüringen hat nun ein Gesetz ohne eine entsprechende Vermittlungsinstanz. Der oft innerbehördlich entstehende Konflikt zwischen Offenbarung und Geheimhaltung personenbezogener Daten hat sich bisher immer als lösbar erwiesen; es ist geradezu ein Glücksfall, dass im Streit zwischen Verwaltung und Petenten wegen Datenschutz und Transparenz eine neutrale Instanz moderieren kann, die für beide Themen berufen ist.

Das ULD hatte direkt nach Inkrafttreten des Informationsfreiheitsgesetzes im Jahr 2001 eine Broschüre herausgegeben, in der das neue Gesetz für Bürgerinnen und Bürger wie für die Verwaltung erläutert wurde. Nachdem einige Jahre Erfahrungen gesammelt wurden und im Jahr 2007 das Umweltinformationsgesetz des Landes in Kraft getreten ist (30. TB, Tz. 12.3), war es nötig, die Hinweise zu aktualisieren und zu erweitern. Heraus kam ein **Kommentar zu den Informationsfreiheitsgesetzen** in Schleswig-Holstein mit Erläuterungen zum IFG und zum UIG mit 50 exemplarischen Fällen, Formularen und weiteren Hilfen. Die Broschüre mit 120 Seiten wird vom ULD in gedruckter Form unentgeltlich zugesandt und ist im Internet abrufbar unter:

www.datenschutzzentrum.de/informationsfreiheit/ifg-uig-sh.pdf

In der vergangenen Legislaturperiode hatte die Gruppe des SSW schon vorgeschlagen, die Regelungen des allgemeinen Informationsfreiheitsrechtes des Landes mit der Umsetzung der Umweltinformationsrichtlinie der EU in ein Gesetz zu gießen (LT-Drs. 16/82). Trotz einer positiven Grundhaltung gegenüber dieser Initiative gelang es kurzfristig nicht, ein solches Gesetz zu verabschieden, sodass jetzt ein separates Umweltinformationsgesetz (UIG) gilt. Dies hatte eine Vielzahl von Problemen zur Folge: Welches Gesetz ist anwendbar? Wie sind abweichende Begriffe und Verfahrensregelungen auszulegen? Wer ist zuständig? Wie erhalten die Bürgerinnen und Bürger effektiven Zugang zu den Verwaltungsinformationen?

In der **Koalitionsvereinbarung** 2009 haben sich die Regierungsparteien CDU und FDP auf eine neue Initiative geeinigt: „Zur Verwaltungsvereinfachung und Entbürokratisierung werden wir das Umweltinformationsgesetz und das Informationsfreiheitsgesetz in einem Gesetz zusammenfassen." Diese Initiative, mit der sich Schleswig-Holstein wieder an die Spitze der Weiterentwicklung bei der Informationsfreiheit setzen kann, wird vom ULD unterstützt; wir haben gerne unsere Hilfe angeboten.

Was ist zu tun?
Die Zusammenfassung von IFG und UIG im Land sollte nicht auf die lange Bank geschoben werden.

12.1 Entwurf eines Geodateninfrastrukturgesetzes

Mit dem Gesetz soll der rechtliche Rahmen für den Ausbau und den Betrieb einer Geodateninfrastruktur Schleswig-Holstein als Bestandteil einer nationalen Geodateninfrastruktur geschaffen werden.

Aufgrund europarechtlicher Vorgaben ist Schleswig-Holstein per Gesetz verpflichtet, Geodaten via Internet oder über andere geeignete Telekommunikationsmittel zur Verfügung zu stellen. Geodaten sind alle Daten mit direktem oder indirektem Bezug zu einem bestimmten Standort oder geografischen Gebiet. Hierzu zählen etwa Angaben zu Flur- und Grundstücken, zu Adressen, Hausnummern und Postleitzahlen, zu Gebäudestandorten oder zur Bodennutzung. Zu den Geodaten zählen beispielsweise auch Informationen zur geografischen Verteilung verstärkt auftretender pathologischer Befunde, etwa Allergien. Es sollen **Zugänge über Netzdienste** eingerichtet werden: Mithilfe von Suchdiensten können Geodaten recherchiert werden; Darstellungsdienste ermöglichen eine verbesserte Größendarstellung auf den Benutzeroberflächen und beim Download; Abrufdienste werden bereitgestellt.

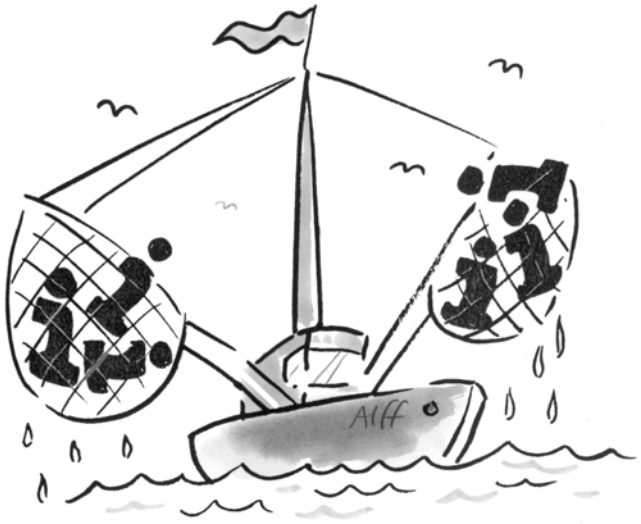
Wenn Geodaten einen Personenbezug aufweisen, muss vor der Eröffnung des Informationszugangs eine **Abwägungsentscheidung** getroffen werden, ob im Einzelfall das öffentliche Interesse an einer Bekanntgabe der Daten gegenüber dem Geheimhaltungsinteresse der betroffenen Personen höher zu bewerten ist. Diese Abwägung würde allerdings einen hohen Verwaltungsaufwand erfordern, wenn jedes Datum einer solchen Einzelprüfung unterworfen würde. Deshalb sollte die Einzelprüfung durch Datenkategorisierungen ersetzt werden, wobei in den Kategorien personenbezogene Geodaten mit unterschiedlicher Sensibilität erfasst werden. Hohe Sensibilität der Daten ist ein Indiz dafür, den Informationszugang zu verweigern. Im Geodateninfrastrukturgesetz Schleswig-Holstein sollte geregelt werden, dass diese Kategorisierung in Absprache mit dem ULD erfolgt.

Was ist zu tun?
Das ULD setzt sich für die Kategorisierung personenbezogener Geodaten ein und unterstützt die Entscheidungsfindung bei der Prüfung eines Informationszugangs.

12.2 Veröffentlichung von Daten der Empfänger von EU-Subventionen

In Schleswig-Holstein werden die Empfänger von Agrarsubventionen angemessen über ihre Datenschutzrechte informiert, die ihnen gegenüber den veröffentlichenden Stellen zustehen.

Mit dem **Agrar- und Fischereifonds-Informationen-Gesetz** wurden die europarechtlichen Vorgaben umgesetzt, wonach im Zusammenhang mit dem Fischereifonds, dem Garantiefonds für die Landwirtschaft und dem Landwirtschaftsfonds für die Entwicklung des ländlichen Raumes gezahlte Subventionen veröffentlicht werden. Zu den Empfängern werden insbesondere folgende Angaben bereitgestellt: Name, Vorname, die Gemeinde, in der der Empfänger wohnt oder eingetragen ist, sowie gegebenenfalls die Postleitzahl, die Höhe der gezahlten Beträge, die im Haushaltsjahr zugeflossen sind, sowie Hinweise zur Währung.



Das ULD unterstützt weiterhin die Forderung des Europäischen Datenschutzbeauftragten, dass die **Widersprüche der Subventionsempfänger** berücksichtigt werden müssen (31. TB, Tz. 12.1). Auf nationaler Ebene wurden vom Bund per Verordnung bisher nur folgende Datenschutzrechte für die Subventionsempfänger vorgesehen: Berichtigung, Sperrung und Löschung von personenbezogenen Informationen. Die Möglichkeit des Widerspruches mit der Folge der Sperrung unter bestimmten Voraussetzungen wird nicht erwähnt.

Das ULD hat das Ministerium für Landwirtschaft, Umwelt und ländliche Räume (MLUR) des Landes bezüglich der Gestaltung der Veröffentlichungen beraten. Nach den vom MLUR erarbeiteten Hinweisen zur Veröffentlichung haben betroffene Personen als Empfänger von Fondsmitteln ein Recht auf Widerspruch, Berichtigung, Sperrung oder Löschung unrichtiger Daten. Diese Rechte können bei den für die jeweilige Zahlung der Mittel zuständigen Stellen der Länder oder des Bundes formlos geltend gemacht werden. Die Empfänger haben ausdrücklich das Recht, schriftlich unter Hinweis auf besondere persönliche Gründe einen **Einwand gegen die Veröffentlichung** zu erheben.

Was ist zu tun?
Im Einzelfall können die Subventionsempfänger gegen die Veröffentlichung ihrer Daten per Einwand vorgehen, wenn das schutzwürdige Interesse des Betroffenen das öffentliche Interesse an der Datenverarbeitung überwiegt. Dies ist von den zuständigen Stellen zu prüfen.

12.3 Der „geheime“ Vertrag

Beim Informationszugang zu Verträgen ist große Sorgfalt auf die Prüfung von Betriebs- oder Geschäftsgeheimnissen zu verwenden. Die pauschale Annahme eines solchen Geheimnisses ohne Prüfung ist nicht möglich.

Eine Bürgerin begehrte gegenüber dem Amt Trave-Land Einsicht in einen zwischen einer amtszugehörigen Gemeinde und einem privaten Unternehmen geschlossenen Vertrag. Die Behörde lehnte den Antrag mit Verweis auf den Schutz von **Betriebs- und Geschäftsgeheimnissen** ab. Derartige Geheimnisse zeichnen sich dadurch aus, dass sie den Gegenstand eines berechtigten wirtschaftlichen Interesses bilden: Kann die Offenlegung der Informationen fremden oder eigenen Wettbewerb schwächen? Geschäftsgeheimnisse können etwa bei Angaben zu Ertragslagen, Rechnungsunterlagen, Kalkulationsunterlagen oder Marktstrategien vorliegen.

Bei Verträgen muss jedoch für jede einzelne Klausel geprüft werden, ob diese Voraussetzungen jeweils vorliegen. Nach Prüfung der konkreten Klauseln gab das ULD der in Anspruch genommenen Behörde mehrere Hinweise, wie und weshalb ein beschränkter Informationszugang zu gewähren ist. Die Behörde ignorierte diese Hinweise mehrfach und nahm **keine Einzelprüfung** vor, sondern verwies immer wieder pauschal darauf, dass der gesamte Vertrag mit seinen Vertragsklauseln Betriebs- und Geschäftsgeheimnisse enthalte. Die Behörde meinte an das Votum des Unternehmens gebunden zu sein, das keine Offenlegung des Vertrags wollte. Das Informationsfreiheitsgesetz sieht aber vor, dass die in Anspruch genommene Behörde eine eigene Prüfung und Abwägungen in jedem Einzelfall vornehmen muss. Wegen der anhaltenden Verweigerung durch die Behörde musste das ULD eine Beanstandung aussprechen.

Was ist zu tun?
Die Behörde muss bei Auskunftsersuchen zu einem Vertrag jede einzelne Klausel prüfen, ob ein Betriebs- oder Geschäftsgeheimnis vorliegt.

12.4 Der offenkundige Vertrag

Dürfen Betriebs- oder Geschäftsgeheimnisse in einem Vertrag nicht offenbart werden, so kommt gegebenenfalls ein beschränkter Informationszugang in Betracht.

Ein Bürger begehrte Einsicht in einen zwischen der Stadt Lübeck und einem Unternehmen geschlossenen Mietvertrag über ein Gebäude. Wieder ging es darum, ob Betriebs- oder Geschäftsgeheimnisse des Unternehmers einer Offenbarung entgegenstehen. Die Behörde nahm nach entsprechender Beratung durch das ULD eine ordnungsgemäße Prüfung der Vertragsklauseln vor. Informationszugang war zu gewähren bezüglich der Angaben zum Mietgegenstand, zur Mietdauer und zu den ohnehin aus den gesetzlichen Vorschriften ableitbaren Haftungsregeln. Angaben zum vereinbarten Mietzins wurden hingegen als Geschäftsgeheimnis

angesehen. Bezüglich dieser Information war auch kein überwiegendes Offenbarungsinteresse der Allgemeinheit erkennbar (29. TB, Tz. 12.4.2). Der Antrag war insoweit abzulehnen. Die Stadt hat die schutzbedürftigen Angaben im Vertragsdokument entsprechend geschwärzt.

Was ist zu tun?
Kommt die Behörde bezüglich einzelner Vertragsklauseln zu dem Ergebnis, dass Betriebs- oder Geschäftsgeheimnisse vorliegen, und besteht insoweit kein Offenbarungsinteresse der Allgemeinheit, so sind entsprechende Angaben zu anonymisieren.

12.5 Lebensgefahr durch Waffenbesitzer?

Ein Antrag nach dem Informationsfreiheitsgesetz auf Bekanntgabe personenbezogener Daten ist im Regelfall abzulehnen, es sei denn, dass die gesetzlich vorgesehenen konkret darzulegenden Ausnahmen greifen.

Der Antragsteller begehrte von der Behörde Auskünfte zum Ausgang eines waffenrechtlichen Verwaltungsverfahrens gegen eine andere Person. Er wollte Einsicht in den gesamten bei der Behörde vorliegenden Vorgang haben und verwies darauf, dass die andere Person möglicherweise im Rahmen einer **nachbarschaftlichen Auseinandersetzung** von der Schusswaffe Gebrauch machen könnte. Die Behörde lehnte den Antrag mit Verweis auf den Schutz personenbezogener Daten ab.

Nach dem IFG kann ein Antrag abgelehnt werden, wenn personenbezogene Informationen offenbart würden, es sei denn, dass die Offenbarung zur Abwehr von **Gefahren für Leben oder Gesundheit** oder sonstiger schwerwiegender Beeinträchtigungen der Rechte Einzelner geboten ist. Eine entsprechende Gefahrenlage muss vom Antragsteller dargelegt werden, d. h., der konkrete Sachverhalt muss so geschildert werden, dass der Schluss auf eine Gefahr für das leibliche Wohl naheliegt. Im erwähnten Fall fehlten solche Darlegungen. Es gab auch keine Anhaltspunkte, dass die andere Person in vergleichbaren Situationen von einer Schusswaffe Gebrauch gemacht oder dies in Aussicht gestellt hatte. Die Behörde hatte den Antrag zu Recht abgelehnt.

Was ist zu tun?
Die Behörde muss prüfen, ob bei dem beantragten Zugang zu personenbezogenen Daten gesetzliche Ausnahmen vorliegen. Der Antragsteller muss hierfür einen hinreichend konkreten Sachverhalt schildern.

12.6 Kein vertraglicher Verzicht auf Informationszugang

Kann eine nach dem Informationsfreiheitsgesetz in Anspruch genommene Stelle die Ablehnung des Antrages mit einem mit dem Antragsteller geschlossenen Vergleich begründen?

Ein Bürger wollte bei einer Behörde in den Vorgang zu einer ordnungsrechtlichen Maßnahme Einsicht nehmen. Die Behörde verwies auf einen mit dem Antragsteller geschlossenen Vergleich. Darin war vereinbart, dass **keine weiteren Ansprüche** im Zusammenhang mit der ordnungsrechtlichen Maßnahme gegenüber der Behörde gestellt werden. Damit habe der Antragsteller auch auf einen Anspruch nach dem Informationsfreiheitsgesetz (IFG) wirksam verzichtet.

Beim Verzicht auf bestehende Ansprüche ist der genaue Erklärungsinhalt relevant, der sich aus dem Zweck der Streitbeilegung und aus der Eigenart der streitigen Rechtsbeziehung ergibt. Der Streit bezog sich auf die **ordnungsrechtliche Maßnahme**, die Streitbeilegung bestand insbesondere darin, dass die Behörde nach Zahlungseingang auf eingeleitete Vollstreckungsmaßnahmen verzichtete und der Bürger in diesem Kontext keine weiteren Ansprüche stellte.

Der Wortlaut des Vergleichs zwingt aber nicht unbedingt zur Annahme, der Bürger habe auf einen gesetzlichen Anspruch nach dem IFG verzichtet. Ansprüche außerhalb des **Erwartungshorizontes** der Streitbeilegung konnten nicht von einer Verzichtserklärung erfasst werden. Die Partner hatten beim Vergleichsabschluss Ansprüche nach dem IFG offensichtlich nicht in ihre Überlegungen einbezogen. Die Voraussetzungen eines Verzichtes wurden von der Behörde, welche die Darlegungs- und Beweislast trägt, nicht ausreichend dargelegt.

Was ist zu tun?
Auf die Vereinbarung eines Verzichtes eines IFG-Anspruchs sollte generell verzichtet werden. Selbst bei Wirksamkeit einer solchen Vereinbarung stehen IFG-Ansprüche grundsätzlich jedermann zu.

12.7 Nicht öffentliche Beratungen in vertraulicher Atmosphäre

Eine Beratung ist nicht allein deshalb „vertraulich“, weil sie in einer nicht öffentlichen Sitzung stattfindet.

Ein Bürger begehrte Informationszugang zum Beratungsprotokoll einer Gemeindevertretersitzung. Die Behörde lehnte den Antrag mit Verweis auf die Nichtöffentlichkeit der Sitzung ab. Nach dem IFG seien **Protokolle vertraulicher Beratungen** geheim zu halten. Tatsächlich kann dem Informationszugang der Schutz eines behördlichen Entscheidungsprozesses entgegenstehen. Ein Antrag ist abzulehnen, soweit und solange die vorzeitige Bekanntgabe von Informationen den Erfolg einer verwaltungsrechtlichen Entscheidung vereiteln würde. Die zitierte Sonderregel für vertrauliche Beratungen ist aber nicht pauschal auf nicht öffentliche Sitzungen anwendbar. Vielmehr ist im Einzelfall zu prüfen, ob der

behördliche Entscheidungsprozess nur durch die Vertraulichkeit der Beratung geschützt werden kann. Maßgebend sind der Beratungsgegenstand und die Schutzinteressen Dritter.

Das Sitzungsprotokoll teilte lediglich mit, dass der Entwurf eines Kaufvertrages über ein Grundstück ausführlich diskutiert wurde. Einzelne Wortmeldungen wurden nicht protokolliert. Ferner enthielt das Protokoll Angaben zur Anzahl der anwesenden Gemeindevertreter, zur Anzahl der Ja- und Nein-Stimmen sowie zu den Stimmenthaltungen und den Beschluss über die Annahme des Vertragsentwurfes. Dieser **Protokollinhalt** unterliegt keiner besonderen Vertraulichkeit. Nach Beratung durch das ULD machte die Behörde das Protokoll dem Antragsteller in Kopie zugänglich.

Was ist zu tun?
Die Behörden müssen anhand des Beratungsgegenstandes und unter Beachtung schutzwürdiger Interessen Dritter prüfen, ob eine Beratung als „vertraulich“ anzusehen ist.

13 DATENSCHUTZAKADEMIE Schleswig-Holstein

2009 wurden in **33 Kursen** 367 Teilnehmerinnen und Teilnehmer in den verschiedensten Bereichen von Datenschutz, Datensicherheit und Informationsfreiheit weitergebildet. Sechs Prüflinge konnten im Dezember 2009 ihr Zertifikat „Systemadministrator mit Datenschutzzertifikat“ entgegennehmen, mit dessen Erwerb nachgewiesen wird, dass sie den Einsatz und Betrieb von IT-Systemen unter datenschutzrechtlichen Aspekten sicher beherrschen. Für die Absolventen bedeutet der Abschluss eine wertvolle Bereicherung ihrer beruflichen Qualifikation.

NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU

Mit dem erstmals für das Jahr 2010 konzipierten

Power-Lehrgang „Datenschutz und Datensicherheit“

bietet die DATENSCHUTZAKADEMIE ein modulares und berufsbegleitendes Qualifikationsmodell an. Systemadministratoren, IT-Revisoren, Datenschutz- und IT-Sicherheitsbeauftragte bekommen in acht Workshops praxisorientiertes Wissen zum technisch-organisatorischen Datenschutz mit dem Schwerpunkt auf Client/Server-Umgebungen unter Windows 2003/2008 vermittelt. Als Abschluss ist die Prüfung zum **Systemadministrator mit Datenschutzzertifikat** möglich.

(Weitere Informationen finden Sie im Jahresprogramm der DSA 2010, Seite 10 – 13.)

NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU

Als Sonderservice bietet die DATENSCHUTZAKADEMIE vor Ort seit Jahren **Inhouse-Schulungen** an, deren Themenschwerpunkte speziell auf die Erfordernisse der Kunden abgestimmt werden. In 19 Sonderkursen wurden weitere 300 Personen geschult. Die Themenvielfalt dieser Kurse bezeichnet die Bandbreite der Anforderungen an die Datenschutzfortbildung:

- Der AK-Technik der deutschen Landesbeauftragten für Datenschutz koordinierte ein mehrtägiges Seminar zum Thema „BSI-Grundschutztools“ in Wiesbaden.
- Die ARGE Kiel hielt drei Einführungslehrgänge in das Sozialdatenschutzrecht ab, die ebenso wie bei der ARGE Dithmarschen den Fokus auf den Umgang mit sensiblen Klientendaten legten.
- Der reguläre Kurs „Führung von Personalakten“ wurde wegen der großen Nachfrage noch einmal als Sonderkurs angeboten und von KOMMA, dem Kompetenzzentrum für Verwaltungsmanagement, in Bordesholm organisiert.

- Auf Initiative der Sparkassenakademie Schleswig-Holstein kamen in Norderstedt zum Seminar „Datenschutz in Kreditinstituten“ Bürgschaftsbankenvertreterinnen und -vertreter aus neun Bundesländern zusammen.
- Neumünster und Brunsbüttel erbaten Fortbildungen im Bereich „Datenschutz im Schulsekretariat“.
- Die Mürwiker Werkstätten in Flensburg erwirkten durch ihre rührige Datenschutzbeauftragte – wie in den vergangenen Jahren – mehrere Veranstaltungen zum Thema „Sozialdatenschutz im Pflegebereich“.
- Novum waren zwei Kurse im ULD für jeweils eine Klasse des neunten Jahrgangs der Realschule Stift. Die anschaulichen Schilderungen von vielen kleinen und großen datenschutzrelevanten Situationen in ihrem alltäglichen Umfeld beeindruckte Schülerinnen und Schüler sowie Lehrkräfte.
- Auch die Technische Universität Harburg möchte die Kurse „Einführung in das Datenschutzrecht“ für IuK-Verantwortliche und für Personendaten verarbeitende Mitarbeiter im kommenden Jahr fortsetzen.
- Weitere Beispiele der Sonderkursthemenvielfalt sind das Seminar „IT-Sicherheit und BSI-Grundschutz für IT-Beauftragte schleswig-holsteinischer Gerichte und Staatsanwaltschaften“ und
- der Kurs „Datenschutz am Arbeitsplatz“ für den Landesbetrieb für Straßenbau und Verkehr Schleswig-Holstein.

NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU

„Betrieblicher Datenschutz – Kompakt“

Der steigenden Nachfrage nach grundlegend ausgebildeten betrieblichen Datenschutzbeauftragten steht jetzt das neue Angebot eines dreitägigen Intensivkurses in der Nordsee Akademie Leck gegenüber.

Vom 13. bis zum 15. Juli 2010

wird die fachkundige Grundlage vor allem für neu bestellte betriebliche Datenschutzbeauftragte gelegt. Dabei werden die rechtlichen Grundlagen, die Gesetzesänderungen, der Aufbau eines betrieblichen Datenschutzmanagements sowie Strukturen des technischen Datenschutzes und Maßnahmen zur Datensicherheit vermittelt.

(Weitere Informationen finden Sie im Jahresprogramm der DSA 2010, Seite 17.)

NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU ∗ NEU

Die seit vielen Jahren angebotenen Grundlagenkurse der DATENSCHUTZ-AKADEMIE machen Schleswig-Holstein zu dem Bundesland mit bester Datenschutzfortbildung:

- **„Datenschutzrecht“ und „Datensicherheitsrecht“ (DR/DT)** befähigen die Datenschutzbeauftragten der schleswig-holsteinischen Behörden nun schon seit 15 Jahren, ihre verantwortungsvolle Aufgabe fachkompetent wahrzunehmen.
- Die **„Einführung Datenschutz im Schulsekretariat“ (ES)**, die in Zusammenarbeit mit KOMMA (Kompetenzzentrum für Verwaltungsmanagement) in Bordesholm stattfindet, wurde wegen des großen Interesses als Workshop im ULD fortgeführt.
- Der Kurs **„Führung von Personalakten“ (PA)** wurde aus demselben Grund ein zweites Mal ausgeschrieben.
- Die Kurse im Sozial- und Medizinbereich bilden ebenfalls seit jeher fundierte Grundlagen des Schulungsbetriebs: **„Datenschutz in der Arztpraxis“ (AR)** und **„Datenschutz im Krankenhaus“ (DK)** verzeichnen nicht zuletzt aufgrund vieler Veränderungen im Rahmen der Gesundheitsreform regen Zuspruch. Der dreitägige Kurs **„Sozialdatenschutzrecht“ (S)**, der ebenso wie andere Mehrtageskurse in der Nordsee Akademie Leck stattfindet, bildet in vielen Fällen die Initialzündung für die Buchung von Sonderkursen, beispielsweise bei ARGEn und in Werkstätten für Menschen mit Behinderungen (siehe oben). Der neu aufgelegte Kurs **„Gesundheitsdaten in Betrieb und Verwaltung“ (GDB)** spricht die Personalverantwortlichen in Betrieben und öffentlichen Verwaltungen ebenso an wie Betriebsärzte und den betriebsärztlichen Dienst der Gesundheitsämter.
- Datenschutz(management) im privatwirtschaftlichen Bereich ist Thema in den Kursen zum Bundesdatenschutzgesetz **(BDSG I & II)**, dem **„Workshop für betriebliche Datenschutzbeauftragte“ (DWBT)** und dem Kurs **„Technischer Datenschutz, Systemdatenschutz“ (SIB)**. Ab 2010 wird in **„Betrieblicher Datenschutz – Kompakt“ (BDK)** eine solide Grundlage für die Fachkunde neu bestellter betrieblicher Datenschutzbeauftragter gelegt (siehe Kasten).
- Das Angebot im Bereich der Technikkurse konnte qualitativ konsolidiert und thematisch erweitert werden. **„IT-Sicherheitsmanagement“ (ITS)** und **„Sicherheitsmanagement auf Basis von IT-Grundschutz“ (ITS-II)** sowie **„Mit dem BSI-Grundschutztool zum IT-Sicherheitskonzept“ (BSI-GST)** befähigen die Absolventen, die Sicherheit von Verfahren oder Geschäftsprozessen und die Verwaltung der IT-Verbünde von Organisationen mithilfe der IT-Grundschutzmethode umzusetzen. Diese Kursinhalte werden zunehmend von öffentlichen Stellen des Landes Schleswig-Holstein nachgefragt. Hinzu kommen 2010 die neuen Kurse **„Datenschutzkontrolle, Sicherheitschecks und Datenschutz-Audits“ (DSD)** sowie **„Dokumentation nach dem Grundschutzstandard des BSI“ (DGB)**.
- Das **Praxisforum (PRAFO)**, ein kostenlos angebotener Beratungsworkshop für behördliche Mitarbeiterinnen und Mitarbeiter, fand 2009 wieder in den Räumen des ULD zu den Themen **„Test & Freigabe“** und **„Dokumentation**

nach LDSG und DSVO“ sowie „**Datenschutzpraxis für die Internetnutzung“** statt. Die 60 Teilnehmer kamen aus verschiedenen Dienststellen schleswig-holsteinischer Behörden.

Wollen Sie wissen, wie Sie sich im Internet sicher bewegen können, was Google alles über Sie weiß, wo Ihre Daten im kommerziellen Adresshandel landen?

In **„Datenschutz im Alltag“**, einem Kurs, der gemeinsam mit der Verbraucherzentrale Schleswig-Holstein durchgeführt wird, bekommen Sie viele Tipps zum Selbstdatenschutz.

(Weitere Informationen finden Sie im Jahresprogramm der DSA 2010, Seite 16.)

Index

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z