SCHLESWIG-HOLSTEINISCHER LANDTAG **Drucksache 15/1700**
15. Wahlperiode 02-04-16

Bericht

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

Tätigkeitsbericht 2002

Tätigkeitsbericht 2002

des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

Berichtszeitraum: 2001, Redaktionsschluss: 20.02.2002
Landtagsdrucksache 15/1700

(24. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz)

Dr. Helmut Bäumler
Leiter des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein, Kiel

Inhaltsverzeichnis **Seite**

1	**Situation des Datenschutzes in Schleswig-Holstein**	**7**
1.1	Bürgernaher Datenschutz	7
1.2	Licht und Schatten bei den Kontrollen	7
1.3	Von der Aufsichtsbehörde zum Innovationszentrum	8
2	**Der Weg in die Informationsgesellschaft**	**10**
2.1	Das Bedürfnis nach Sicherheit – ein Fass ohne Boden?	10
2.2	Datenschutz, der Spaß macht	13
3	**Datenschutz im Landtag**	**17**
	Datenschutzgremium gebildet	17
4	**Datenschutz in der Verwaltung**	**18**
4.1	Kommunalbereich	18
4.1.1	Datenschutzbeauftragte in Kommunen	18
4.1.2	Neues Landesmeldegesetz bringt Vereinfachungen	19
4.1.3	Probleme mit dem Wahlgeheimnis	20
4.1.4	Neustrukturierung der Bauakten	21
4.2	Polizeibereich	22
4.2.1	Überblick	22
4.2.2	Rasterfahndung	22
4.2.3	INPOL-neu: Das Millionengrab?	24
4.2.4	Einsatzleitsystem muss nachgebessert werden	25
4.2.5	Neues Gesetz für polizeilichen Zugriff auf Verbindungsdaten	27
4.2.6	Die Verwertung abgehörter Telefonate	28
4.2.7	Polizeiliche Videoüberwachung	29
4.2.8	Was darf der Rettungsarzt der Polizei mitteilen?	30
4.2.9	EURAS	31
4.2.10	Cyber-Crime Convention	32
4.2.11	Personenbezogene Daten in kriminalpräventiven Räten	33
4.3	Justizverwaltung	33
4.3.1	Zwangsversteigerungsdaten ab ins Internet?	33
4.3.2	Mit dem Scanner durch die Justizregister?	35
4.3.3	Rechte und Pflichten der Betreuer	36
4.3.4	Elektronisches Grundbuch – Wie sicher ist die Unterschrift?	37
4.4	Verfassungsschutz	39
	Mängel bei den behördlichen Geheimschutzbeauftragten	39
4.5	Ausländerbereich	40
4.5.1	Überblick	40
4.5.2	Die Fremden – Testfall für den Überwachungsstaat?	40
4.5.3	Zuwanderungsgesetz – kein Kurswechsel	42

4.6	Wirtschafts- und Verkehrsverwaltung	43
	Straßenmaut – aber bitte mit Datenschutz!	43
4.7	Sozialbereich	44
4.7.1	Überblick	44
4.7.2	Wer ist jetzt eigentlich für die Sozialhilfe zuständig?	44
4.7.3	Wie weit darf die Zusammenarbeit zwischen Arbeitsamt und Sozialamt gehen?	46
4.7.4	Automation bei den Sozialämtern	47
4.7.5	Rundfunkgebührenbefreiung – die dritte	49
4.8	Schutz des Patientengeheimnisses	50
4.8.1	Für die Gesundheitsämter gilt ein neues Gesetz	50
4.8.2	Gesundheitschipkarten	51
4.8.3	Neues EDV-System für die Krankenkassen	52
4.8.4	Outsourcingaktionen bei Krankenkassen – die nächste, bitte?	52
4.8.5	Der Gutachtenauftrag eines schweizerischen Rentenversicherungsträgers	54
4.8.6	Die Arztrechnung von der Privatfirma – Variationen über ein Thema	55
4.8.7	Missbrauch von Patientendaten in Apotheken	56
4.8.8	Aktion „Datenschutz in meiner Arztpraxis“	57
4.8.9	Vorschläge zur Regelung der Genomanalyse	58
4.8.10	Heimlicher Gentest: Ganz der Papi?	60
4.9	Schulbereich	61
	Datensicherheit an vielen Schulen ein Fremdwort	61
4.10	Steuerverwaltung	62
4.10.1	Outsourcing – Die große Freiheit der Steuerverwaltung?	62
4.10.2	Gemeinsame Softwareentwicklung der Steuerbehörden ein Problemfall	64
4.10.3	Datenerhebung zur Zweitwohnungssteuer nicht korrekt	67
4.11	Personaldaten	68
4.11.1	Erörterung von Beurteilungen in „großer Runde“?	68
4.11.2	Diskretion im Beihilfeverfahren	69
5	**Datenschutz bei Gerichten**	**71**
	EUREKA	71
6	**Datenschutz in der Wirtschaft**	**73**
6.1	Was hat das neue Bundesdatenschutzgesetz gebracht?	73
6.2	Auskunfteien	74
6.2.1	Scoring der SCHUFA rechtswidrig	74
6.2.2	Missbräuchliche SCHUFA-Abfrage	76
6.2.3	Bequemlichkeit mit Folgen	77

6.2.4	Auch kleine Sünden bestraft die SCHUFA mit Einträgen nicht unter drei Jahren	78
6.2.5	Eine kleine Erpressung	79
6.2.6	Mängel bei einer Handels- und Wirtschaftsauskunftei	80
6.2.7	Schuldnerpranger im Internet	81
6.3	Banken	82
	Was gibt es zu erben?	82
6.4	Industrie, Handel, Handwerk und freie Berufe	83
6.4.1	Karten- und Datenflut nach Wegfall des Rabattgesetzes	83
6.4.2	Datenschutz mit dem Verwöhnaroma	84
6.4.3	Neugierige Fitnessstudios	85
6.4.4	Vorsicht beim Faxversand	86
6.4.5	Datenschutz im Kündigungsschutzprozess	87
6.5	Neue Zuständigkeit für die Verfolgung von Ordnungswidrigkeiten	89
7	**Systemdatenschutz**	**90**
7.1	Sicheres Surfen und Mailen – die Herausforderung	90
7.2	Landesnetz in Betrieb – noch aber fehlen Sicherheitschecks	92
7.3	Sicherheitskonzept für das Sprachnetz immer noch nicht schlüssig	95
7.4	IKOTECH III – der neue Datenverarbeitungs- und Kommunikationsstandard	97
7.5	Prüfungen automatisierter Verfahren	99
7.5.1	Eine Verwaltung – drei IT-Welten	99
7.5.2	Eine etwas andere Behörde	101
7.5.3	Verwirrende Systemadministration	103
7.5.4	Computer in Kommunen nach wie vor ein Sicherheitsrisiko	104
7.6	Wohin mit den Altakten?	106
8	**Recht und Technik der neuen Medien**	**108**
8.1	E-Government	108
8.2	Protokollierung der gesamten Internet-Kommunikation?	111
8.3	Telekommunikationsüberwachungsverordnung	114
8.4	P3P	116
8.5	Identitätsmanagement	117
8.6	VIS – Fachtagung zu verlässlichen IT-Systemen in Kiel	118
8.7	Neue Vorschriften über den Datenschutz im Internet	119
9	**Modellprojekte zur Weiterentwicklung des Datenschutzes**	**122**
9.1	Virtuelles Datenschutzbüro: Erste Adresse für Datenschutzinfos im Internet	122
9.2	AN.ON	123
9.3	BioTrusT – Biometrische Verfahren im Feldversuch	125
9.4	EU fördert Datenschutzaudit und Gütesiegel in Schleswig-Holstein	128
9.5	Projekt Schul-CD: Datenschutz schülergerecht aufbereitet	129

10	**Gütesiegel und Audit**	**131**
10.1	Der Ablauf der Gütesiegelverfahren	131
10.2	Erste Gutachter akkreditiert	132
10.3	Produktkriterien	133
10.4	Gütesiegel als Vergabekriterium	135
10.5	Produktkriterien als Maßstab bei der Produktentwicklung	136
10.6	Pilotverfahren zum Datenschutzaudit	137
11	**Aus dem IT-Labor**	**140**
11.1	BackUP-Magazin hilft Sicherheitslücken schließen	140
11.2	Schulungs- und Simulationsnetz in Betrieb genommen	141
11.3	Bug oder Feature? Internet Explorer protokolliert Surfverhalten	141
11.4	Neue Browsergeneration bringt nicht nur Vorteile	142
11.5	Mozilla – noch kein Stern am Browserhimmel, aber ein Lichtblick	143
12	**Europa**	**145**
12.1	EUROJUST	145
12.2	Richtlinie über den Datenschutz bei elektronischer Kommunikation: Wohin geht die Reise?	147
13	**Informationsfreiheit**	**149**
13.1	Erfahrungen mit dem Informationsfreiheitsgesetz Schleswig-Holstein	149
13.2	Informationen über das Informationsfreiheitsgesetz sind gefragt	156
13.3	Entwicklung der Informationsfreiheit in Deutschland und in der EU	157
13.4	Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands (AGID)	158
14	**Rückblick**	**160**
14.1	Krankenhausinformationssysteme	160
14.2	Revisionsfähigkeit automatisierter Verfahren	160
14.3	KomFIT macht CeBIT Konkurrenz	160
14.4	Unerbetene Faxwerbung	161
14.5	Sichtschutzfilter bei der Sparkasse	161
14.6	PC-Welt in den Finanzämtern	162
14.7	Gleichstellung der elektronischen Signatur mit der Schriftform im Zivilrecht	162
15	**Beispiele dafür, was die Bürger von unserer Tätigkeit haben**	**163**
16	**DATENSCHUTZAKADEMIE Schleswig-Holstein**	**167**
16.1	Fortbildungsprogramm 2002 der DATENSCHUTZAKADEMIE	167
16.2	Sommerakademie 2002	169
	Beim ULD SH erhältliche Publikationen	**170**
	Index	**171**

1 Situation des Datenschutzes in Schleswig-Holstein

1.1 Bürgernaher Datenschutz

Umfragen zeigen, dass die **Bürgerinnen und Bürger** nach wie vor ein starkes Interesse am Thema Datenschutz haben. Eine Mehrheit von 63 % spricht sich in Schleswig-Holstein dafür aus, dem Datenschutz künftig mehr Bedeutung beizumessen als bisher. Aber wollen sie auch eine Fortsetzung der bisherigen Formen und Methoden des Datenschutzes? Aus vielen Gesprächen und Eingaben wissen wir, dass die Bürger eine effiziente Unterstützung erwarten, wenn sie sich durch Datenverarbeitung ungerecht behandelt fühlen. Sie möchten auch die Gewissheit haben, dass bei den Behörden und Firmen regelmäßig Kontrollen durchgeführt werden. Und sie wünschen brauchbare Tipps und Hinweise zu bekommen, wie sie sich in bestimmten Situationen verhalten sollen und sich insbesondere selbst schützen können. Woran kein Interesse besteht, das ist ein juristischer Kleinkrieg, bürokratisches Gehabe und ein Datenschutz, der auf Verhinderung statt auf Gestaltung gerichtet ist.

Unsere Vorstellungen von einem stärker **marktwirtschaftlichen Datenschutz** kommen dieser Erwartung entgegen. Audit und Gütesiegel (Tz. 10) sind beispielsweise Möglichkeiten, die Bürger selbst (mit)entscheiden zu lassen, wie viel Datenschutz in welcher Qualität sie wünschen. Vor allem bei der jüngeren Generation ist die Tendenz zu beobachten, den Datenschutz nicht in erster Linie als ein schwer erkämpftes Grundrecht zu begreifen, das Behörden und Firmen Tag für Tag aufs Neue abgerungen werden muss, sondern als Teil der Lebensqualität, die sie beanspruchen. Datenschutz, der als selbstverständlicher Service erwartet wird, gehört offenbar für viele bereits heute zum **Lifestyle**.

Wir bemühen uns zudem, unsere Arbeit stärker auf diese Bürgererwartungen auszurichten. Da passte es gut ins Konzept, dass die Dienststelle im vergangenen Jahr auch räumlich näher an die Bürger heranrückte. Sie befindet sich jetzt nicht mehr im Regierungsviertel, sondern bewusst im **Zentrum der Stadt**, mitten in der **Fußgängerzone**. Viele Bürger haben registriert, dass wir damit leichter erreichbar sind. Beim „Tag der offenen Tür“ schauten hunderte persönlich herein und machten sich ein Bild von unseren Serviceangeboten. Die bequeme Erreichbarkeit über elektronische Kommunikationsmittel tut ein Übriges. Längst ist das Informationsangebot im Internet gleichwertig neben die traditionellen Broschüren und Faltblätter getreten. Es ist absehbar, dass der E-Mail-Verkehr mit den Bürgern die traditionelle Briefpost bald überflügelt hat.

1.2 Licht und Schatten bei den Kontrollen

Dass Datenschutz ein selbstverständlicher Service gegenüber Bürgern und Kunden ist und dass sich Schlamperei und Nachlässigkeit bei Fragen der Datensicherheit und der Ordnungsmäßigkeit der Datenverarbeitung bitter rächen können, hat sich allerdings beileibe noch nicht überall herumgesprochen. Viele Behörden, vor-

nehmlich die großen im Lande, verzichten auf die Bestellung von behördlichen Datenschutzbeauftragten, so als seien Spezialkenntnisse auf diesem Gebiet Luxus oder auf wundersame Weise wie von selbst bei ihnen vorhanden.

Die **Ergebnisse** unserer Kontrollen sprechen häufig eine andere Sprache. Elementare Sicherheitsregeln werden nach wie vor verletzt. Manche Behördenchefs meinen offenbar, mit dem Sparen müsse ausgerechnet bei der Datensicherheit angefangen werden. Sie wachen erst auf, wenn man sie bei Kontrollen „erwischt“ oder wenn es zu Datenpannen kommt (Tz. 7.5). Erstaunlicherweise klappt manchmal noch nicht einmal das kleine Einmaleins des sorgsamen Umgangs mit persönlichen Daten. Wie wäre es sonst vorstellbar, dass man in den Müllcontainern mancher Behörden in Schleswig-Holstein immer noch reichlich „Beute“ machen kann (Tz. 7.6).

Immer wieder kann man die Beobachtung machen, dass das Ausblenden der Datenschutzfragen bei der Einführung neuer DV-Projekte am Ende teuer zu stehen kommt. Der Ehrgeiz, den Knopfdruck zum Start der neuen Systeme lieber heute als morgen öffentlich vorführen zu können, endet nicht selten im Katzenjammer über aufwendige **Nachbesserungen** (Tz. 4.2.4, 4.2.9, 7.2 und 7.3). Eine saubere Planung von DV-Projekten vor ihrem Produktionsbeginn gehört leider nach wie vor eher zur Ausnahme.

Das Verführerische des **technisch Machbaren** führt auch an anderen Stellen zu unerklärlicher Bedenkenlosigkeit. Wir haben zwar ein Patientengeheimnis, an das natürlich auch die Apotheken gebunden sind. Aber viele Apotheker verfuhren nach der Devise: „Aber wenn es so bequem und technisch so einfach zu machen ist, über Jahre zu speichern, wer wann welche Medikamente genommen hat, dann machen wir es eben!“ Dass auf diesem Wege ein höchst sensibler Datenbestand aufgebaut wurde, war Nebensache. Man war ja überzeugt, alles geschehe nur zum Besten der Kunden. Nur dass diese gar nichts von ihrem Glück wussten. Auf die Idee, ihre Kunden um Einwilligung zu bitten, mussten die Apotheker erst durch die Datenschutzbeauftragten gebracht werden (Tz. 4.8.7). Andere Beispiele sind Internet-Schuldnerpranger (Tz. 6.2.7) und heimliche Gentests. Es war ja zu erwarten, dass die Tatsache, dass schon ein Haar, das man dem Betroffenen unbemerkt wegnimmt, für eine Genomanalyse reicht, schon bald zu allerlei „Dienstleistungen“ führen würde. Die Entwicklungen in der **Gentechnik** sind so rasant, dass ihre sozialen und kulturellen Auswirkungen kaum überschaubar sind (Tz. 4.8.9). Mag sein, dass es eines Tages üblich wird, heimliche Vaterschaftstests durchzuführen und auch auf andere Weise mittels Gentests in der Privatsphäre anderer herumzuschnüffeln. Der Datenschutz und die jetzige Gesetzeslage stehen dem jedenfalls entgegen (Tz. 4.8.10).

1.3 Von der Aufsichtsbehörde zum Innovationszentrum

An Kontrollaufgaben für die Datenschutzbeauftragten wird es also auch in Zukunft nicht mangeln. Gleichwohl treten die Aspekte der aktiven **Gestaltung der Informationsgesellschaft** immer stärker in den Vordergrund. Wer bei der Entwicklung der Informationstechnik nicht von vornherein den Fuß in der Tür hat,

kann später nur noch schwer etwas verändern. Die „lex informatica“ ist manchmal stärker als das geschriebene Recht. Deshalb wurde der vor Jahren begonnene Weg, den Datenschutz näher an die Entwicklungsprozesse heranzuführen, auch im Berichtsjahr intensiv fortgeführt.

Mehr und mehr zeigt sich, dass die **Modellprojekte** ein wirksamer Hebel sind, um auf die Gestaltung der Technik Einfluss zu bekommen (Tz. 9). Sie ermöglichen es uns, stets die aktuellen technischen Fragestellungen aufzugreifen, das Personal der Dienststelle ständig mit Hochschulabsolventen aufzufrischen und die Kompetenz des Unabhängigen Landeszentrums zu stärken. Längst reichen unsere Kontakte im Rahmen der Modellprojekte weit über die Landes- und Bundesgrenzen hinaus.

Ein anderes Mittel, die Technikentwicklung zu beeinflussen, dürften auf mittlere Sicht die **IT-Gütesiegel** sein. Aus vielen Anfragen aus dem Bereich der Entwickler und Hersteller wissen wir, dass eine Nachfrage nach Datenschutzstandards, die bereits bei der Produktentwicklung berücksichtigt werden können, besteht. Der enorme Aufwand, den es für uns bedeutet hat, die Produktkriterien zu entwickeln (Tz. 10.3), wird sich vermutlich erst in Jahren, dann aber spürbar, bezahlt machen. Leider muss dies alles im Augenblick noch fast im Alleingang erarbeitet werden, weil der Bundesgesetzgeber bei der Novellierung des Bundesdatenschutzgesetzes die Chance verpasst hat, ein bundesweites Verfahren zu etablieren.

Zukunftsinvestitionen sind auch die Aufwendungen für das **IT-Labor** (Tz. 11); die Ergebnisse rechtfertigen aber den Aufwand. So entwickeln sich die Ratgeber aus der Reihe backUP zu richtigen Rennern. Auch die Faltblätter mit Tipps zum sicheren Surfen und die gesamte Beratungstätigkeit gegenüber Behörden, Firmen und Bürgerinnen und Bürgern profitieren von der Möglichkeit, im IT-Labor praktische Tests durchzuführen.

Zu unseren Serviceaufgaben gehört auch die Vermittlung von **Medienkompetenz**. Hier hat sich in neunjähriger Aufbauarbeit die DATENSCHUTZAKADEMIE Schleswig-Holstein einen festen Platz in der Fortbildungslandschaft Schleswig-Holsteins gesichert (Tz. 16). Insgesamt 314 Kurse mit zusammengenommen über 6.700 Teilnehmern sind nicht die Welt, aber in ihrer Wirkung nicht zu unterschätzen, wenn man bedenkt, dass das Schwergewicht der Kurse eindeutig bei der Schulung von Multiplikatoren liegt.

2 Der Weg in die Informationsgesellschaft

2.1 Das Bedürfnis nach Sicherheit – ein Fass ohne Boden?

Alte Reflexe

Eigentlich haben wir schon gedacht, die alten Stereotypen hätten endlich ausgedient. Doch plötzlich, nach dem 11. September, waren sie wieder da. Der Ausgangspunkt war wie häufig in den letzten Jahren: Schlimme Terroranschläge wurden verübt – Anlass hätte auch ein anderes spektakuläres Verbrechen sein können, der Mord an einem Kind etwa –, die Polizei konnte nicht sofort einen Ermittlungserfolg vorweisen, die Medien heizten die Stimmung an und die Politik stand unter Handlungsdruck. In solchen Situationen scheint manchmal nichts besser zu helfen als einen **Sündenbock** zu suchen. Die Trümmer in New York rauchten noch, da war für manche Politiker bereits klar, dass jetzt zuallererst beim Datenschutz ordentlich aufgeräumt werden müsse. So dachte offenbar auch der Bundesinnenminister, als er unmittelbar nach den Terroranschlägen erklärte, jetzt müsse der Datenschutz „etwas tiefer gehängt“ werden. Jeder weiß, dass Anschläge wie die vom 11. September auch bei Null Datenschutz nicht zu verhindern sind (in den USA, in denen die Anschläge verübt und wochenlang vorbereitet wurden, gibt es übrigens im Bereich der Sicherheitsbehörden ohnehin praktisch keinen Datenschutz).

Wer die Entwicklung der Gesetzgebung in Deutschland in den letzten 20 Jahren mit offenen Augen verfolgt hat, der konnte sehen, dass durch viele „Antiterrorgesetze“ der Datenschutz gegenüber den Sicherheitsbehörden Stück für Stück eingeebnet wurde. Nirgendwo sonst ist der Zweckbindungsgrundsatz so massiv durchbrochen wie im Bereich der Strafverfolgung. Wer allerdings nach wie vor den Datenschutz als einen Schuldigen darstellt, geht der Frage aus dem Weg, warum nicht die vielen Gesetzesverschärfungen der letzten Jahre das Maß an Sicherheit gebracht haben, das die Politiker den Bürgern jedes Mal versprochen haben. Der muss auch nicht darlegen, ob die vielen neu geschaffenen Ermittlungsinstrumente, mit denen die Polizei- und Strafverfolgungsgesetze gespickt wurden, tatsächlich geeignet, geschweige denn erforderlich sind. Wer immer nur suggeriert, Polizei und Geheimdiensten seien durch „zu viel Datenschutz“ die Hände gebunden, der lenkt die Aufmerksamkeit des Publikums geschickt von der Frage ab, was die technisch und rechtlich hochgerüsteten Sicherheitsbehörden mit den zusätzlichen Eingriffsbefugnissen der letzten Jahre Positives bewirkt haben.

Wer verteidigt die Grundrechte?

Wo waren in dieser Situation die in einer Demokratie notwendigen Gegenkräfte? Wer trat für die Sache der Grundrechte und der unveräußerlichen Verfassungswerte auch in einer aufgeregten Zeit ein? Von Augenmaß war nach dem 11. September in Deutschland zunächst wenig zu spüren. Stattdessen entwickelte sich geradezu ein Wettlauf um die besten Ideen für die Einschränkung von Grundrechten. Hinter all dem wird ein **Wertewandel** sichtbar, dessen Auswirkungen kaum einzuschätzen sind. Generationen von Juristen und Politikern waren nach den

Erfahrungen mit der Hitlerdiktatur, aufgefrischt durch das DDR-Regime, der Überzeugung, es sei in einer Demokratie wichtig, der Staatsmacht Grenzen aufzuerlegen. Grundrechte, die Strafprozessordnung als ihr „Kleingedrucktes“ und deren Fortsetzung unter den Bedingungen der Informationsgesellschaft, das Datenschutzrecht, wurden als bewusste und gewollte Hindernisse für staatliches, vor allem polizeiliches Handeln begriffen. Der Staat, so der eiserne Konsens der Nachkriegsgeneration, sollte auch um den Preis von Effizienzeinbußen in rechtliche Schranken verwiesen werden.

Was ist davon noch übrig? Allem Anschein nach nicht mehr allzu viel. „Hinderliches“ für die Sicherheitsbehörden ist neuerdings aus der Mode gekommen. Unter den meisten Parteien hat geradezu ein Wettbewerb um die konsequenteste Beseitigung von „**Behinderungen“ der Strafverfolgung oder anderer Bedarfsträger“** begonnen. Alle berufen sich auf die öffentliche Meinung, aber wer versucht eigentlich, die Öffentlichkeit objektiv zu informieren über Ursachen und Wirkungen, über Effektivität und über Spätfolgen? Bekenntnisse zum Rechtsstaat auch in stürmischer Zeit waren – auch in Schleswig-Holstein – nur selten zu hören. Wenn niemand mehr entschlossen für die Grundrechte eintritt, ihr Wert in der öffentlichen Meinung kontinuierlich herabgewürdigt wird, dann schlägt die Stunde derer, die noch einfachere Parolen verbreiten, die die Sache der „behinderungsfreien“, auf Effizienz getrimmten Strafverfolgung noch kompromissloser verfolgen und auf rechtsstaatliche Schnörkel konsequent verzichten wollen. Der Wettlauf um die vollmundigsten Sicherheitsversprechungen nutzt vor allem jenen, die gegen „Behinderungen“ der Strafverfolgung noch skrupelloser polemisieren, als es die etablierten Parteien je wagen würden. Der Wahlerfolg von Law-and-Order-Parteien beruht nicht zuletzt darauf, dass die klarer aussprechen, was sich längst in die Denkweise und Rhetorik auch der anderen Parteien eingeschlichen hat: Rechtsstaat, Grundrechte und Datenschutz gelten als antiquiert. Den Bürgern wird der Eindruck vermittelt, als seien sie letztlich die Ursache für die Kriminalität. Man müsse sie nur gehörig zurückschneiden, dann werde auch die Kriminalität spürbar abnehmen. Darin liegt vielleicht die langfristig problematischste Folge der Debatte nach dem 11. September in Deutschland. Die Grundrechte haben an Unterstützung verloren, Sicherheit ist Trumpf. In einer derartigen Grundstimmung muss ständig mit neuen „Aufräumarbeiten“ unter den Rechtsstaatsprinzipien gerechnet werden.

Was ist denn schon passiert?

Nun mag man einwenden, die bisherige Antiterror-Gesetzgebung nach dem 11. September habe den Rechtsstaat nicht in den Grundfesten erschüttert. In der Tat: Gegenüber dem ursprünglichen Gesetzentwurf und verglichen mit den weitergehenden Vorstellungen einiger Länder im Bundesrat sind dem „Schily-Paket“ manche **Giftzähne gezogen** worden. Die Datenschutzbeauftragten haben mit dazu beigetragen, dass einige der neuen Befugnisse zeitlich begrenzt wurden und dass vor einer etwaigen Verlängerung eine Evaluation stattfinden muss. Trotzdem nagen die neuen Gesetze beharrlich an den Freiheitsrechten. Das Bundeskriminalamt ist wieder einen Schritt weiter auf dem langen Weg, die eigenen Zentralkompetenzen kontinuierlich zulasten der Länderpolizeien zu erweitern. Die Geheimdienste werden immer ungenierter zu Reserve-Strafverfolgungsbehörden

umfunktioniert. Ihr Zugriff auf Banken-, Telekommunikations-, Verkehrs- und andere Daten wurde zwar einstweilen in ein unbequemes Verfahrenskorsett gezwängt. Aber es ist nicht auszuschließen, dass die jeweils dem Präsidenten vorbehaltene Anordnung entsprechender Informationsbeschaffungen schon bald als zu umständlich („Behinderung durch Datenschutz", s. o.) infrage gestellt wird. Jetzt haben die Geheimdienste erst einmal den Fuß in der Tür von Banken, Luftfahrtunternehmen und Telekommunikationsanbietern. Am deutlichsten wirken sich die rechtlichen Veränderungen im **Ausländerbereich** aus. Vom Datenschutz für Ausländer bleibt kaum mehr etwas übrig. Es wird eine regelrechte datenschutzrechtliche Zwei-Klassen-Gesellschaft zementiert. Die Ausländer werden pauschal als kriminalitätsgeneigte Bevölkerungsgruppe angesehen, deren Datenschutzrechte man nach Belieben einschränken kann.

Was kommt als Nächstes?

Obwohl die hoch technisierte Risikogesellschaft mit ihren ökologisch riskanten Großanlagen und den auf unsicherem Boden aufgebauten informationstechnischen Strukturen aus Gründen angreifbar ist, die mit „zu viel" Datenschutz nicht das Geringste zu tun haben und die auch mit noch so perfekten Antiterrorgesetzen nicht aus der Welt zu schaffen sind, wird sich die **Spirale** wohl weiter drehen. Der nächste Terroranschlag, das nächste die Emotionen aufwühlende Verbrechen kommt bestimmt, und dann kann die Suche nach „Hinderlichem" für mehr Sicherheit nach bekanntem Muster weitergehen. Man muss kein Prophet sein, um vorherzusagen, wie das Ganze ablaufen wird: Vermutlich werden als Erstes diejenigen Vorschläge wieder aus der Schublade gezogen, die diesmal nicht durchzusetzen waren; so wie auch Schilys Paket in weiten Teilen abgelehnte Vorschläge aus den letzten Jahren aufwärmte, die mit der Aufklärung von Terroranschlägen wenig zu tun hatten. Aber die Gelegenheit war eben günstig dafür. Die Erfahrungen der letzten Jahre zeigen, dass die Ablehnung einer Gesetzesverschärfung keineswegs den Verzicht auf die dahinter stehenden Absichten bedeuten muss, sondern dass die Entwürfe immer wieder neu eingebracht werden, bis die Situation günstig für ihre Verabschiedung ist.

Diesmal noch abgelehnt, aber ganz oben auf der Wunschliste steht seit Jahren eine **Vorfeldermittlungsbefugnis** für die Polizei, schon vor dem Vorliegen des Anfangsverdachts einer Straftat. Zumeist wird dies als Befugnis zu „Initiativermittlungen" bezeichnet, die es ermöglichen soll, „Kriminalitätsstrukturen" auch ohne Straftatverdacht auszuleuchten. Dann dürfte sicher der Wunsch nach Beseitigung oder Abschwächung der diesmal als Verfahrenshindernis vor allem für die Geheimdienste eingebauten rechtsstaatlichen Prozeduren eine Rolle spielen. Es darf nicht überraschen, wenn bald schon darüber gestöhnt wird, Richtervorbehalte und andere grundrechtssichernde Verfahrensvorschriften seien zu umständlich und müssten verschlankt werden. Schließlich ist damit zu rechnen, dass erneut versucht werden wird, die Internet-Nutzer zu observieren. Die unheimliche Welt des Internets scheint vielen Sicherheitspolitikern ein Dorn im Auge. Der Surfer, das unsichtbare, kaum kontrollierbare Wesen, das in den Augen Einiger stets nur an die Begehung von Straftaten denkt, bedarf dringend der ordnungsbehördlichen Obhut. Die **Protokollierung aller Internet-Aktivitäten** steht deshalb auf der Wunschliste von Sicherheitspolitikern ganz vorne. Mal ist es die Innenminister-

konferenz, mal sind es wie bei der Beratung des Antiterror-Gesetzespaketes im Bundesrat einzelne Bundesländer, mal kommen die Vorstöße aus der Richtung der EU: Immer geht es darum, aufzuzeichnen, wer was wann im Internet getan hat, wofür er sich interessiert hat, was ihm dabei spontan eingefallen ist (man analysiere nur den Klick-Stream), wie er sich ganz allgemein im Netz benommen hat. Was in der realen Welt bislang nicht vorstellbar ist, nämlich das Verhalten der Menschen lückenlos aufzuzeichnen, wird für das Internet ohne Zögern gefordert. Dabei schreibt das geltende Teledienstedatenschutzrecht die Protokollierung von Internet-Aktivitäten nicht vor, sondern verbietet sie sogar ausdrücklich (sic!).

Anstatt zu überlegen, wie die Nutzer endlich gegen das gesetzwidrige Speichern ihres Surfverhaltens durch Provider, Werbeindustrie und windige Datenhaie wirksam geschützt werden können, denkt die Politik offenbar vornehmlich in die andere Richtung. Fast könnte man den Eindruck haben, als warteten einige nur auf eine günstige Gelegenheit, um die **Totalkontrolle der Internet-Nutzer** durchzusetzen. Zwar ist der Traum von ultimativem Recht und Ordnung angesichts der Eigengesetzlichkeiten des offenen, weltumspannenden Internets eben nur ein Traum. Gleichwohl wird dem Publikum suggeriert, man könne durchaus auch im Internet Ordnung und Sicherheit schaffen, wenn nur der Datenschutz ... na ja, Sie wissen schon.

Was ist zu tun?

Die Politik sollte den Bürgern keine uneinlösbaren Sicherheitsversprechungen geben. Stattdessen führt kein Weg an der Erkenntnis vorbei, dass sich leider Kriminalität weder im demokratischen Rechtsstaat noch in einem Polizei- und Geheimdienststaat gänzlich verhindern lässt. Gefragt sind Politiker, die den Mut haben, sich auch in schwierigen Zeiten zum Rechtsstaat und seinen Prinzipien zu bekennen, statt in ziellosem Aktionismus ständig neue Eingriffsgesetze zu beschließen. Notwendig sind Vorschläge zu einer effizienteren Ermittlungsarbeit, die nicht ständig zulasten der Bürgerrechte gehen.

2.2 Datenschutz, der Spaß macht

Sinn und Unsinn von Behinderung

Datenschutz als Schranke für ungezügelte Staats- und insbesondere sicherheitsbehördliche Macht, das macht also auch künftig Sinn. Auf einen Datenschutz, der in keiner Weise im Wege steht, weil er alles erlaubt, könnten wir nämlich von vornherein verzichten. Aber **Beschränkung der Staatsmacht** ist eine Sache, **Erschwerung des Alltagslebens der Menschen** eine ganz andere. Nicht wenige empfinden den Datenschutz in ihrem Berufsleben oder auch bei der privaten Nutzung von Computern manchmal als lästig und umständlich. Das fängt bei Passwörtern an, die man nach bestimmten Regeln bilden, sich merken und regelmäßig wieder ändern muss, und hört keineswegs bei Bildschirmschonern auf, die sich aktivieren, wenn man den Arbeitsplatz für kurze Zeit verlässt. Man könnte und möchte ja so vieles mit dem Computer machen, darf es aber angeblich oder wirklich nicht – aus Datenschutzgründen. Dies wird nur dann akzeptiert, wenn der

daraus folgende Nutzen unmittelbar einsichtig ist. Bei manchen Datenschutzbestimmungen ist dies nur schwer zu vermitteln. Dort, wo es möglich wäre, muss in Zukunft stärker der Versuch dazu gemacht werden. Der Datenschutz als etwas Positives, ja als etwas was man gerne tut, weil man von seiner Sinnhaftigkeit überzeugt ist, muss in der öffentlichen Darstellung viel präsenter werden. Man muss häufiger davon lesen, dass durch einen funktionierenden Datenschutz eine schädigende Nutzung personenbezogener Daten verhindert worden ist. Es dürfen nicht nur die Datenpannen, die Verletzungen des Datenschutzes, die Auswirkungen von Datenschutzvorschriften, die Sinnvolles blockieren oder verkomplizieren, bekannt werden, sondern auch die segensreiche, Schaden verhindernde Wirkung des Datenschutzes, die sich wegen ihrer präventiven Natur bislang zumeist im Verborgenen abspielt.

Kein Blumentopf zu gewinnen mit Datenschutz?

Den meisten Menschen fehlt wahrscheinlich eine Vorstellung davon, wie der Datenschutz tatsächlich für ihr eigenes Leben etwas Positives bewirkt. Dieses Defizit setzt sich fort bei der Wahrnehmung der Tätigkeit der Datenschutzkontrollbehörden. Die Botschaft in ihren Berichten und Verlautbarungen ist immer die Gleiche: Sie haben offenbar nur zu kritisieren und zu beanstanden. Behörden und Firmen halten sich anscheinend durchgängig nicht an die Datenschutzregeln. Positive Resultate von Prüfungen haben nur wenig Platz in den Tätigkeitsberichten oder sie finden in der öffentlichen Wahrnehmung keine Beachtung. So hat sich die Vorstellung herausgebildet, wonach man beim Thema Datenschutz nur verlieren, nicht gewinnen kann. „**Nur nicht unangenehm auffallen**“ ist deshalb die Devise in vielen Behörden und Firmen, denn datenschutzrechtliche Kritik könnte schädlich fürs Image sein. Aber wer möchte stattdessen angenehm auffallen? Was hätte man davon für einen Vorteil? Das deutsche Datenschutzsystem ist auf Positives gar nicht eingestellt, sondern war vom ersten Tag an auf Kritik gebürstet.

Audit und Gütesiegel als Möglichkeiten, positive Datenschutzleistungen sichtbarer zu machen, erobern sich erst ganz langsam einen Platz in diesem Gefüge. Die ersten Erfahrungen mit **Datenschutzaudits** in Schleswig-Holstein zeigen, dass es für Viele eine ungewohnte Erfahrung ist, wenn man mit einem guten Datenschutzangebot auch etwas gewinnen kann, zum Beispiel ein positives Image. Wenn der Eindruck nicht täuscht, dann sind es vornehmlich leistungsstarke Verwaltungsmanager, die auch im Übrigen ein gutes Standing in der Verwaltungslandschaft haben, die mit der Durchführung eines Auditverfahrens beim Thema Datenschutz „klar Schiff“ machen wollen. Wer sich als Dienstleister gegenüber den Bürgerinnen und Bürgern begreift, der will auch beim Datenschutz einen guten Service bieten. Das Audit bietet die Chance, in Sachen Datenschutz Gutes zu tun und darüber auch ausgiebig zu reden.

Ähnlich ist die Situation bezüglich des **Gütesiegels für IT-Produkte**. Welchen Anreiz zu mehr Datenschutz und Datensicherheit bietet das traditionelle Datenschutzsystem für Entwickler und Hersteller von IT-Produkten? Da das Schwergewicht bislang auf der Schaffung von Rechtsvorschriften und bei Kontrollen ihrer konkreten Anwendung lag, war die Ebene der Produktgestaltung weitgehend aus-

geblendet. Prinzipien, wie Datenvermeidung und Datensparsamkeit, Datenschutz durch Technikgestaltung und Unterstützung der Bürger beim Datenselbstschutz, lassen sich aber ohne eine spezifische Ausgestaltung der Informationstechnik nur schwer verwirklichen. Niemand kann erwarten, dass jeder Kunde einzeln ausprobiert, welches IT-Produkt ihn beim Schutz seiner Privatsphäre am besten unterstützt. Notwendig sind stattdessen allgemeine Standards und Instrumente, die dem Nutzer und Konsumenten schnell und „auf den ersten Blick" signalisieren, welche Sorte von IT-Produkt er vor sich hat. IT-Gütesiegel können einen Beitrag dazu leisten, den IT-Markt für die Kunden transparenter zu gestalten. Fast alle könnten damit gewinnen: Die Verbraucher, weil sie die Chance bekommen, beim Kauf von IT-Produkten ihre Interessen besser zur Geltung zu bringen, und die Hersteller, die datenschutzgerechte Produkte anbieten, weil sich ihre Absatzmöglichkeiten verbessern. Einen Nachteil haben allenfalls diejenigen Anbieter, deren Produkte die Voraussetzungen für ein Gütesiegel nicht erfüllen, weil sie den Schutz der Privatsphäre ihrer Kunden nicht unterstützen. Gut so.

Kann Datenschutz wirklich Spaß machen?

Bislang kommt der Datenschutz in der öffentlichen Wahrnehmung eher grau und erdenschwer daher. Wir fragen uns, ob dies nicht auch anders geht. Warum eigentlich nicht? Grundrechtsschutz ist eine wichtige, lohnende Aufgabe, die den Menschen unmittelbar dient. Sie muss nicht immer nur mit bitterer Miene, mit Kritik und Besorgnis angegangen werden. Wenn man damit auch gewinnen, nicht nur verlieren kann, warum sollte Datenschutz keinen **Spaß machen**? Ein Unternehmen, das datenschutzgerechte Produkte mithilfe von Gütesiegeln besser verkaufen kann, sieht den Datenschutz gleich mit ganz anderen Augen. Firmen und Behörden, die per Audit ihren Kunden zu verstehen geben, dass sie beim Thema Datenschutz auf der Höhe der Zeit sind, werden das Vertrauen des Publikums leichter gewinnen.

Und die **Bürgerinnen und Bürger**? Was haben sie davon, wenn andere mit Datenschutz Gewinn machen? Nun, eine Firma oder eine Behörde zu betreten, der per Audit attestiert worden ist, dass sie mit den Daten ihrer Kunden pfleglich umgeht, verbreitet vermutlich ein weitaus besseres Gefühl, als wenn soeben die Kontrollbehörde eine dicke Beanstandung ausgesprochen hat. Surfen im Internet kann Spaß machen, wenn da nicht das mulmige Gefühl wäre, dass man überall Datenspuren hinterlässt, deren weitere Verwendung man nicht in der Hand hat. Könnte man einen vertrauenswürdigen Anonymitätsdienst nutzen, dann würde keine Angst vor neugierigen Geheimdiensten oder ungenierten Datensammlern das Vergnügen trüben. Telefonieren kann eine schöne Sache sein, wenn da nicht manchmal der letzte Rest von Zweifel hochkäme, ob nicht doch jemand mithört. Hätte man Telefone mit eingebauter, sicherer Sprachverschlüsselung, so würde das Telefonieren noch ein bisschen mehr Spaß machen. E-Mail ist wirklich eine feine Sache, mit der man viel Zeit und Geld sparen kann, wenn nur nicht das Internet eine „Post" wäre, die offen ist wie ein Scheunentor. Wie schön, wenn man ein leistungsstarkes, bequem funktionierendes Verschlüsselungsprogramm hätte, das die E-Mail vor fremder Neugier schützt.

Also: Datenschutz kann enorm viel Spaß machen. Es würde unser Leben in vielen Situationen erleichtern, angenehmer und unbeschwerter gestalten, wenn wir uns immer darauf verlassen könnten, dass der **Datenschutz** wirklich **zuverlässig funktioniert**. Es wird Zeit, dass weit mehr Mühe als bisher darauf verwandt wird, deutlich zu machen, dass Behinderung weder Zweck noch Selbstzweck des Datenschutzes ist, sondern dass er den Bürgerinnen und Bürgern die Teilhabe an der Informationsgesellschaft erleichtern soll. Datenschutz als Freund und Helfer in den Untiefen der Informationsgesellschaft – das macht Spaß.

3 Datenschutz im Landtag

Datenschutzgremium gebildet

Mit der Benennung der Mitglieder und der Arbeitsaufnahme des Datenschutzgremiums gibt es nun eine Datenschutzkontrolle des Parlaments

Der Landtag wird wegen seiner legislativen Unabhängigkeit nicht durch eine exekutive Stelle kontrolliert, sondern gemäß seiner Datenschutzordnung durch ein Datenschutzgremium, in dem jede Fraktion durch ein Mitglied vertreten ist. Hiervon ausgenommen sind nur die Fraktionen, die Parlamentarische Kontrollkommission und die G-10-Kommission. In vorangegangenen früheren Tätigkeitsberichten (vgl. 23. TB, Tz. 3) beklagten wir die Zögerlichkeit bei der **institutionellen Umsetzung**. Nun hat sich Einiges getan: Die Mitglieder des Datenschutzgremiums wurden benannt. Die Einführung einer eigenen parlamentarischen Datenschutzeinrichtung ist bundesweit bisher einmalig und richtungsweisend. In den Parlamenten der anderen Länder gibt es teilweise gar keine Datenschutzregelungen, teilweise ist für deren Kontrolle niemand zuständig.

Sicherlich werden im Landtag keine großen Datenmengen verarbeitet. Dafür sind sie aber oft von **hoher Sensibilität**. Dies gilt für die Eingaben beim Petitionsausschuss ebenso wie für die Daten über vertrauliche Gespräche oder über Kontakte im politischen Raum. Bezüglich der Datensicherheit bei der Vernetzung von Landtagsverwaltung und Fraktionen besteht ein hoher Schutzbedarf. Kein Abgeordneter wäre z. B. begeistert, wenn er seine am Computer entwickelten vertraulichen strategischen Überlegungen am nächsten Tag in der Zeitung wiederfände, weil der politische Gegner mitlesen konnte.

Das Datenschutzgremium hat sich umgehend daran gemacht, die nicht mehr aktuelle **Datenschutzordnung** zu überarbeiten. So ist eine Angleichung an das im Jahr 2000 novellierte Landesdatenschutzgesetz erfolgt. Aber auch in technischer Sicht tut sich im Landtag Vieles, was seinen Niederschlag in der Arbeit des neuen Datenschutzgremiums findet. So ist z. B. die Sicherheit der Telekommunikationseinrichtungen etwas, was jeden einzelnen Abgeordneten besonders interessieren dürfte.

4 Datenschutz in der Verwaltung

4.1 Kommunalbereich

4.1.1 Datenschutzbeauftragte in Kommunen

Schleswig-Holsteins Behörden ernennen zunehmend eigene Datenschutzbeauftragte. Eine Umfrage hat gezeigt, dass zwei Drittel aller Kommunen bereits einen behördlichen Datenschutzbeauftragten bestellt haben oder in den nächsten Monaten bestellen werden.

Das neue schleswig-holsteinische Datenschutzgesetz sieht die Bestellung behördlicher Datenschutzbeauftragter zwar nicht zwingend vor. Gleichwohl ist die weit überwiegende Zahl der Kommunen offenbar der Auffassung, es bringe **Vorteile**, einen eigenen Datenschutzbeauftragten zu bestellen. Nach einer Umfrage, die wir Ende 2001 durchgeführt haben, plant lediglich ein Drittel der Kommunen gegenwärtig keine Schritte in diese Richtung. Meistens werden Kostengründe genannt.

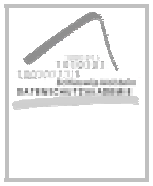
Gerade für kleinere Kommunen kann es sich anbieten, **gemeinsam** mit den Nachbargemeinden einen **behördlichen Beauftragten** zu bestellen. Eine derartige Möglichkeit ist im LDSG ausdrücklich vorgesehen. Wir haben bereits im Laufe dieses Jahres erste Beratungen bei Ämtern und Gemeinden, die die Bestellung eines gemeinsamen Beauftragten planten, durchgeführt. Weitere schleswig-holsteinische Behörden haben ihr Interesse an einer derartigen Vorgehensweise signalisiert.

Soweit Behörden bereits vor In-Kraft-Treten des neuen LDSG einen internen Datenschutzbeauftragten bestellt haben, ist darauf zu achten, dass diese Bestellung den neuen Anforderungen angepasst wird. Ein **Muster einer Bestellung** zur oder zum behördlichen Datenschutzbeauftragten findet sich in den „Tipps und Hinweisen“ des ULD zur Anwendung des neuen Landesdatenschutzgesetzes.

Weitere Hinweise zu diesem Thema gibt es auf unserer Homepage:

www.datenschutzzentrum.de/material/recht/dsleicht/
www.datenschutzzentrum.de/material/themen/bekannt/bestbdsb.htm

Wir planen, die behördlichen Datenschutzbeauftragten bei ihrer Arbeit zu unterstützen und zwar durch:



- Hilfen bei der Gründung von Arbeitskreisen,
- Schaffung eines speziellen Informationsangebotes über unsere Homepage,
- Einrichtung einer Mailingliste,
- Initiierung eines Newsletters,
- Schaffung eines speziellen Fortbildungsangebotes für behördliche Datenschutzbeauftragte und
- Durchführung eines landesweiten Info-Tages.

Was ist zu tun?
Auch diejenigen Behörden, die noch zögern, sollten einen Datenschutzbeauftragten bestellen. Große Städte sollten sich ein Beispiel an den kleinen Kommunen nehmen.

4.1.2 Neues Landesmeldegesetz bringt Vereinfachungen

Der vom Kabinett verabschiedete Entwurf eines Gesetzes zur Änderung des Landesmeldegesetzes soll das Verfahren bei einem Wohnungswechsel deutlich vereinfachen. Gleichzeitig soll durch eine erweiterte Amtsermittlung der Meldebehörden die Fehlerquote in den Melderegistern reduziert werden.

Weshalb muss ein Bürger im Falle eines Umzuges eigentlich bei zwei Meldebehörden vorstellig werden – einmal zur Abmeldung an seinem bisherigen Wohnsitz und ein weiteres Mal zur Anmeldung an seinem neuen Wohnsitz? Der Innenminister ist offenbar wie wir der Auffassung, dass dieses Verfahren einfacher und damit auch **bürgerfreundlicher** gestaltet werden kann.

Im neuen Melderecht soll die Abmeldung bei einem Umzug innerhalb des Landes Schleswig-Holstein nämlich ganz entfallen. Dafür soll die bisherige Kontrollmitteilung durch die Unterrichtung der Wegzugsgemeinde über den Umzug ersetzt werden. Allerdings besteht damit für die Zuzugsgemeinde nicht mehr die Möglichkeit, die Richtigkeit der Angaben des Meldepflichtigen auf der Grundlage einer vorgelegten Abmeldebestätigung zu überprüfen; deshalb wird es in Zukunft möglich sein, im Rahmen eines **automatisierten Abrufverfahrens** direkt auf die Meldedaten der bisherigen Meldebehörde zuzugreifen. Aus datenschutzrechtlicher Sicht wird dadurch die Richtigkeit der gespeicherten Meldedaten verbessert. Gleichzeitig kann mit Ausnahme der neuen Anschrift sowie des Einzugsdatums bereits der vollständige Anmeldevordruck automatisiert ausgefertigt werden. Dem Meldepflichtigen wird das umständliche Ausfüllen von Vordrucken erspart. Er braucht nur noch seine Unterschrift zu leisten. Dies dürfte auch die Warteschlangen in den Meldebehörden deutlich verkürzen.

Mit dem neuen Landesmeldegesetz soll gleichzeitig das **Amtsermittlungsprinzip** gestärkt werden. Ein Abgleich mit den anonymen Statistikdaten aus der Volkszählung hat nämlich gezeigt, dass die Melderegister offensichtlich doch mit erheblichen Fehlerquoten belastet sind. Deshalb sollen die Empfänger von Meldedaten ermächtigt werden, die Meldebehörden zu unterrichten, wenn ihnen Anhaltspunkte für die Unrichtigkeit der übermittelten Daten vorliegen. Anschließend sollen die Meldebehörden diesen Hinweisen nachgehen und die Richtigkeit ihrer Daten von Amts wegen überprüfen und gegebenenfalls berichtigen. Auch gegenüber Finanz- und Sozialämtern soll dieses Verfahren zum Einsatz kommen. Aus datenschutzrechtlicher Sicht bestehen dagegen keine Bedenken, da in den entsprechenden Fällen ausschließlich Meldedaten sowie der Hinweis auf ihre Unrichtigkeit übermittelt werden.

4.1.3 Probleme mit dem Wahlgeheimnis

Wähler müssen darauf vertrauen können, dass ihre Unterstützungsunterschriften für eine Partei nicht der Öffentlichkeit bekannt werden. Verstöße gegen das Wahlgeheimnis verletzen auch das Datenschutzrecht.

Ein nachlässiger Umgang mit personenbezogenen Daten kann für die Betroffenen erhebliche negative Konsequenzen zur Folge haben. Dieses musste ein Mitglied einer kommunalen Wählergemeinschaft erfahren, nachdem es im Rahmen der Vorbereitung zur Landtagswahl eine **Unterstützungsunterschrift** für eine Partei abgegeben hatte. Solche Unterschriften sind notwendig, wenn Parteien, die nicht bereits im Landtag vertreten sind, zur Wahl zugelassen werden wollen.

Die Meldebehörde hat zu prüfen, ob der Betreffende zur Stimmabgabe nach dem geltenden Wahlrecht berechtigt war. Auf der Grundlage der dabei gewonnenen Erkenntnisse informierte ein Mitarbeiter einer Meldebehörde den Bürgermeister der amtsangehörigen Gemeinde, in der der Betroffene politisch engagiert war, über die Unterschriftsleistung für die mit der Wählergemeinschaft konkurrierende Partei. Dieser wiederum nutzte seine **Insiderinformationen** öffentlich im Wahlkampf, mit der Folge, dass der Betroffene die von ihm bekleideten politischen Funktionen in der Wählergemeinschaft niederlegen musste.

Die Nutzung von Unterstützungsunterschriften ist in der Landeswahlordnung restriktiv geregelt. Demnach dürfen Auskünfte über Unterstützungsunterschriften für Wahlvorschläge nur an Behörden, Gerichte und sonstige amtliche Stellen der Bundesrepublik Deutschland und nur unter der Voraussetzung erteilt werden, dass die Auskunft zur Durchführung der Wahl oder eines Wahlprüfungsverfahrens oder zur Aufklärung des Verdachts einer Wahlstraftat erforderlich ist. Angaben darüber, wer für welche Partei eine Unterstützungsunterschrift leistet, unterliegen dem **Wahlgeheimnis**.

Wir haben den Vorgang als erheblichen Verstoß gegen datenschutzrechtliche Bestimmungen beanstandet. Rückgängig zu machen war der Fehler allerdings nicht mehr. Der Behörde blieb nur noch die Möglichkeit, sich beim Betroffenen dafür zu entschuldigen.

Was ist zu tun?
Daten, die dem Wahlgeheimnis unterliegen, erfordern einen besonders sensiblen Umgang durch die zuständigen Mitarbeiter. Behörden müssen durch geeignete Schulungsmaßnahmen die vertrauliche Behandlung von Wahldaten sicherstellen.

4.1.4 Neustrukturierung der Bauakten

Die Führung von Bauakten bereitet manchen Kommunen Probleme. Insbesondere die Trennung der Vorgänge nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen wurde bisher vielerorts nicht realisiert. Ein neuer Organisationserlass des Innenministeriums zur Ausführung der Landesbauordnung sorgt jetzt für Klarheit.

Bisher wurde in der Praxis in den **Bauakten** alles gesammelt, was zu dem betroffenen **Objekt** angefallen war. Dies führte dazu, dass in einer Akte nicht nur Angaben über alle bisherigen Grundstückseigentümer enthalten waren, sondern auch unterschiedliche Sachvorgänge wie z. B.

- bauaufsichtliche Unterlagen,
- abwasserrechtliche Genehmigungen,
- Unterlagen nach der Baumschutzsatzung,
- Bußgeldvorgänge,
- unbegründete Nachbarbeschwerden.

So konnte sich z. B. der aktuelle Eigentümer durch Einsicht in seine Bauakte darüber informieren, welche Streitigkeiten **Voreigentümer** des Grundstücks mit dem Bauamt hatten. Die Gliederung der Vorgänge nach unterschiedlichen Zwecken ist Voraussetzung dafür, um die Datenverarbeitung auf den jeweiligen Zweck zu beschränken. Schließlich wird durch die Trennung der Akten die Möglichkeit dafür verbessert, Unterlagen, die zur rechtmäßigen Aufgabenerfüllung nicht mehr benötigt werden, fristgerecht zu löschen.

Im Wortlaut:
§ 11 Abs. 4 Satz 1 LDSG

Die Datenverarbeitung soll so organisiert sein, dass bei der Verarbeitung, insbesondere der Übermittlung, der Kenntnisnahme im Rahmen der Aufgabenerfüllung und der Einsichtnahme, die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist.

Das Innenministerium hat mit seiner **Neufassung des Organisationserlasses** zur Landesbauordnung nun eindeutige Regelungen zur Bauaktenführung veröffentlicht. Danach sind alle Unterlagen, die zur Dokumentation einer bauaufsichtlichen Entscheidung erforderlich sind, und die Entscheidung selbst sowie gegebenenfalls anschließende Überprüfungsmaßnahmen in einer Akte zusammenzufassen; andere Unterlagen haben in dieser Akte nichts zu suchen. Wird darüber hinaus dem Bauamt ein Eigentümerwechsel bekannt, ist eine neue Akte anzulegen. Da die bis zu diesem Zeitpunkt erteilten Baugenehmigungen auch für und gegen Rechtsnachfolger gelten, sind aus der alten Bauakte die erforderlichen Unterlagen in die neue Bauakte zu übernehmen. Für die Betroffenen ist damit ein Stück mehr Persönlichkeitsrechtsschutz im Bereich der Bauverwaltung verbunden.

Was ist zu tun?
Die Bauämter sollten die Reorganisation ihrer Bauakten nach den Maßgaben des Organisationserlasses ohne Verzug vornehmen. Die Akten müssen spätestens dann umgestellt sein, wenn ihr Inhalt betroffenen Bürgern oder anderen Behörden bekannt gegeben werden soll.

4.2 Polizeibereich

4.2.1 Überblick

In welche Richtung die polizeiliche Datenverarbeitung nach dem einstweiligen Scheitern des Mega-Projektes INPOL-neu (Tz. 4.2.3) gehen wird, lässt sich auch für die schleswig-holsteinischen Verfahren derzeit schwer sagen. Eine Neukonzeptionierung durch die Polizei muss von Anfang an datenschutzrechtlich begleitet werden, damit nicht aufwändige Nachrüstungen erforderlich werden wie etwa beim Einsatzleitstellensystem der Lübecker Polizei (Tz. 4.2.4). Nach den Terroranschlägen des 11. September hat auch in Schleswig-Holstein die Rasterfahndung nach so genannten „Schläfern“ begonnen. Dafür wurde das Landesverwaltungsgesetz um eine entsprechende Rechtsgrundlage ergänzt. Schon tot geglaubte Fahndungskonzepte der Siebzigerjahre erleben damit eine Renaissance. Über Erfolge der Rasterfahndung ist bis zur Fertigstellung dieses Berichts noch nichts bekannt geworden.

4.2.2 Rasterfahndung

Nach den Terroranschlägen des 11. September 2001 beteiligt sich auch die schleswig-holsteinische Polizei an der bundesweit koordinierten Rasterfahndung. Die eigens hierfür im Polizeirecht geschaffene Rechtsgrundlage soll 2005 vom Landtag evaluiert werden.

> ***? Rasterfahndung***
>
> *bedeutet eine polizeiliche Auswertung von Fremddatenbeständen auf Grundlage einer Fahndungshypothese mit daraus abgeleiteten Rasterkriterien. Die Zweckbindung dieser Datenbestände wird durchbrochen. Gegen Personen, die im Raster hängen bleiben, wird anschließend auf Grundlage des Polizeirechts bzw. der StPO weiter ermittelt („Anschlussmaßnahmen“).*

Als 1992 Datenverarbeitungsnormen in das schleswig-holsteinische Polizeirecht eingefügt wurden, verzichtete das Parlament trotz einer im Regierungsentwurf vorgesehenen Regelung bewusst darauf, präventive Rasterfahndungen zuzulassen. Der **grundrechtliche Preis** einer solchen Maßnahme wurde als zu hoch angesehen, denn sie betrifft fast ausschließlich völlig unbescholtene Bürger. Sofern sie in irgendein Kriterienraster passen, auch wenn dieses noch keinen echten Verdacht ergeben muss, werden sie weitergehenden polizeilichen Überprüfungsmaßnahmen unterworfen. Zudem ergaben sich aus den Erfahrungen der Terroristenfahndung in den Siebzigerjahren erhebliche Zweifel an der Effektivität von Rasterfahndung.

Wenige Wochen nach der Novellierung des Landesverwaltungsgesetzes 1992 wurde eine Rechtsgrundlage für Rasterfahndungen im Zusammenhang mit **Strafermittlungsverfahren** in die Strafprozessordnung eingefügt. Diese ist bis heute kaum genutzt worden. Erstaunlicherweise wollten die Staatsanwaltschaften auch angesichts der massiven Straftaten des 11. September nicht auf seiner Grundlage vorgehen. Unter der Koordination des Bundeskriminalamtes (BKA) begann stattdessen eine Rasterfahndung nach „Schläfern", die der Gefahrenabwehr dienen und an der sich auch Schleswig-Holstein beteiligen sollte. Das Polizeirecht wurde daher auf Betreiben des Innenministers bereits einen Monat nach den Anschlägen um eine entsprechende Befugnisgrundlage ergänzt. In einer Stellungnahme haben wir unsere grundsätzlichen Zweifel an der **Eignung** und **Verhältnismäßigkeit** solcher vor allem Unverdächtige betreffenden Maßnahmen dargelegt. Anzuerkennen ist immerhin, dass das schleswig-holsteinische Gesetz hohe grundrechtliche Anforderungen an das Verfahren der Rasterfahndung stellt. Der Innenminister muss dem Landtag jährlich über die Maßnahmen berichten. Die Befugnis läuft Ende 2005 aus; der Landtag wird sich dann mit den Erfahrungen aus der Durchführung von Rasterfahndungen auseinander setzen und darüber entscheiden müssen, ob die bisherigen Resultate eine Verlängerung rechtfertigen.

Im Wortlaut: § 195 a LVwG

1) Die Polizei kann von öffentlichen und nichtöffentlichen Stellen die Übermittlung von personenbezogenen Daten bestimmter Personengruppen aus Dateien zum Zwecke des automatisierten Abgleichs nach fahndungsspezifischen Suchkriterien mit anderen Datenbeständen verlangen, soweit dies erforderlich ist zur Abwehr einer erheblichen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Verhütung von Straftaten erheblicher Bedeutung ... und die Verhütung des Schadens auf andere Weise nicht möglich ist.

2) Die Maßnahme nach Absatz 1 darf nur auf Antrag ... des Leiters des Landeskriminalamtes ... richterlich angeordnet werden. ...

5) Personen, gegen die nach Abschluss einer Maßnahme nach Absatz 1 weitere Maßnahmen durchgeführt werden, sind hierüber durch die Polizei zu unterrichten, sobald dies ohne Gefährdung des Zwecks der weiteren Datennutzung erfolgen kann. ...

6) Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein ist über den Beginn und den Abschluss einer Maßnahme nach Absatz 1 zu unterrichten.

Zwei unserer datenschutzrechtlichen Forderungen wurden bedauerlicherweise nicht umgesetzt: Rasterfahndungen als besonders in die Rechte Unbescholtener eingreifende Maßnahmen sollten nur zur Abwehr einer konkreten Gefahr zulässig sein, wenn also eine gesteigerte Eintrittswahrscheinlichkeit erheblicher Schäden anzunehmen ist. Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, sollten – wie in mehreren anderen Bundesländern – wegen ihrer Sensibilität von vorneherein nicht in einen automatisierten Datenabgleich einbezogen werden können.

Auf der Grundlage von Beschlüssen des Amtsgerichts Kiel, die kurz nach der Verabschiedung des Gesetzes vom Landeskriminalamt beantragt worden waren, begann im November 2001 die Erhebung von Datenbeständen der Meldebehörden, Hochschulen sowie weiterer Stellen durch eine eigens gebildete Projektgruppe des LKA. Entsprechend unserem gesetzlichen Auftrag informieren wir uns fortlaufend über die Durchführung der Rasterfahndung. Zweifel an der Rechtmäßigkeit der bundesweit abgestimmten Vorgehensweise ergeben sich derzeit aufgrund der zentralen Rolle des BKA, das alle von den Ländern erhobenen Datenbestände untereinander abgleicht. Das BKA tritt aber auch selbstständig an weitere Stellen, z. B. Wirtschaftsverbände, heran und ersucht diese um Herausgabe von Datenbeständen „auf freiwilliger Grundlage“ zum Zweck des automatisierten Abgleichs. Da das BKA keine Befugnis besitzt, Rasterfahndungen zur Gefahrenabwehr durchzuführen, könnte es allenfalls von den Länderpolizeien mit der technischen Unterstützung einer bundesweiten Rasterfahndung beauftragt werden. Die Rolle des BKA geht aber weit über eine rein unterstützende Funktion hinaus. Außerdem sind entscheidende Datenbestände, die das BKA in die Rasterfahndung einbezieht, von den Beschlüssen der schleswig-holsteinischen Gerichte nicht gedeckt. Wir haben dem Innenministerium unsere rechtlichen Bedenken gegenüber dem gegenwärtigen Ablaufplan der bundesweiten Rasterfahndung frühzeitig mitgeteilt und um Stellungnahme gebeten.

Was ist zu tun?
Das Innenministerium muss auf eine rechtlich saubere Durchführung der Rasterfahndung auch gegenüber dem BKA dringen.

4.2.3 INPOL-neu: Das Millionengrab?

Die Zukunft des groß angelegten polizeilichen IT-Projekts INPOL-neu steht nach dem gescheiterten Start des Echtbetriebes in den Sternen. Unabhängig davon, in welcher Form das Projekt weitergeführt wird, bleibt seine datenschutzrechtliche Begleitung eine wichtige Aufgabe. Zu hoffen ist allerdings, dass sich die Polizei künftig konstruktiver mit den Vorschlägen der Datenschutzbeauftragten auseinander setzt.

Nach dem Fehlstart im April 2001 wurde das Projekt INPOL-neu einer umfangreichen **Revision** durch einen unabhängigen Gutachter unterworfen. Dessen Fazit lautete, dass die an INPOL-neu gestellten Anforderungen der Polizei an die Grenzen der Machbarkeit gehen und zurzeit zu einer völlig unzureichenden Performance führen würden. Inzwischen wird als Zeitpunkt eines neuen Startversuchs für eine abgespeckte Version Ende 2003 genannt.

Seit 1996 berät eine „Arbeitsgruppe INPOL-neu“ der Datenschutzbeauftragten des Bundes und der Länder, an der wir beteiligt sind, die Projektgruppe beim Bundeskriminalamt. Die nur zum geringen Teil von der Polizei aufgegriffenen datenschutzrechtlichen Verbesserungsvorschläge (vgl. 23. TB, Tz. 4.2.2) müssen bei einem Neuansatz des Projekts endlich zum Tragen kommen. Noch im Sommer 2001 hat die Arbeitsgruppe nämlich zu den Entwürfen einer Reihe von **Errich-**

tungsanordnungen für INPOL-neu Stellung genommen. Dabei haben wir verdeutlicht, dass die geplante Erweiterung des **Kriminalaktennachweises** (KAN) um Fälle unterhalb der im Gesetz vorgesehenen Relevanzschwelle datenschutzrechtlich nicht akzeptabel ist. Das Gleiche gilt für die erweiterte Auslegung der länderübergreifenden Bedeutung von Straftaten. Außerdem sollen in mehreren Dateien **Aufzeichnungen** in Form von Lichtbildern, Tonaufnahmen und Videos von Personen gespeichert werden. Eine derartige, für weitere Technologien zukunftsoffene Aufzeichnungskomponente sollte nach den bisherigen Planungen bereits mit der ersten Zertifizierungsstufe von INPOL-neu eingeführt werden. Offensichtlich war das ganze Projekt bislang überdimensioniert.

Aufgrund der Probleme bei der Realisierung von INPOL-neu ist auch die Frage wieder offen, ob das BKA Daten der Länderpolizeien, die nicht Teil des Informationsverbundes sein dürfen, im Auftrag der Länder verarbeiten wird (vgl. 23. TB, Tz. 4.2.2). Da eine hierzu notwendige Vereinbarung des BKA mit den Länderpolizeien bislang noch nicht abgeschlossen wurde, wird es in Schleswig-Holstein wohl bei der eigenverantwortlichen Datenhaltung bleiben.

***?* Relevanzschwelle**

*Das Bundeskriminalamt unterstützt als Zentralstelle ... die Polizeien des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten mit **länderübergreifender**, **internationaler** oder **erheblicher Bedeutung** (§ 2 Abs. 1 BKA-Gesetz).*

Was ist zu tun?
Der Innenminister sollte auf eine datenschutzgerechte Gestaltung der Neukonzeption des zukünftigen INPOL-Systems hinwirken und den Zeitraum bis zu dessen Realisierung zum Ausbau seiner eigenen Datenhaltung nutzen.

4.2.4 Einsatzleitsystem muss nachgebessert werden

Die Einsatzleitstelle der Polizei in Lübeck verfügt über ein neues Computersystem mit weit reichenden Speicher- und Recherchemöglichkeiten, die deutlich über den datenschutzrechtlich zulässigen Rahmen hinausgehen. Vor dem Hintergrund der geplanten Zentralisierung und Zusammenlegung der Einsatzleitstellen von Polizei und Rettungsdiensten im gesamten Land haben wir mit einer Arbeitsgruppe der Lübecker Polizei die notwendigen nachträglichen Korrekturen erörtert. Deren technische Umsetzung steht noch aus.

Für 2,3 Millionen Mark hat die Lübecker Polizei eine der zurzeit modernsten Einsatzleitstellen in Deutschland erhalten. Kernstück ist das **rechnergesteuerte Einsatzleitsystem (ELS)**, dessen Zweck es ist, das polizeiliche Handeln zu dokumentieren, Informationen für die weitere Sachbearbeitung bereitzustellen und die Aufbereitung von Ermittlungserkenntnissen für operative Einsätze zu ermöglichen. Ein Teil der in dem System gespeicherten Informationen wird von den Betroffenen, z. B. den Inhabern von Geschäften, freiwillig zur Verfügung gestellt und ist daher datenschutzrechtlich unproblematisch.

Sämtliche Einsätze im Bereich der Polizeiinspektion Lübeck werden in Form von elektronischen Einsatzberichten dokumentiert. Neben Einsatzgrund, -zeit und den eingesetzten Kräften werden zahlreiche orts-, aber auch personenbezogene Informationen im ELS erfasst und für die Dauer von drei Jahren gespeichert. Grundsätzlich ist diese Speicherung nur – analog zu den bisherigen papierenen Einsatzberichten – für Zwecke der **Vorgangsdokumentation** zulässig. Problematisch ist deshalb die neuerdings in Lübeck mögliche gezielte Auswertung der Daten aller im Einsatzbericht registrierten Personen (also nicht nur die der Verdächtigen oder Störer, sondern auch die der anderen Anwesenden, Hinweisgeber, Opfer, Zeugen usw.) für Zwecke **künftiger Einsätze**. Da die Informationen in den Einsatzberichten lediglich den allerersten Sachstand wiedergeben, der sich im Verlauf weiterer Ermittlungen ändern kann, ist es problematisch, mit einem möglicherweise nicht mehr zutreffenden polizeilichen „Vorwissen" in neue Einsätze zu gehen. Weil die Einsatzinformationen in der Leitstelle bis auf geringe Ausnahmen **nicht nachgepflegt** werden, würde bei einer solchen Praxis auch gegen das polizeirechtliche Berichtigungsgebot verstoßen.

Wir konnten die Verantwortlichen der Polizeidirektion Süd davon überzeugen, dass eine **undifferenzierte Nutzung** der im ELS gespeicherten personenbezogenen Daten aus Einsätzen über einen Zeitraum von mehr als **drei Jahren** zu operativen Zwecken ohne eine Datenpflege nach dem Landesverwaltungsgesetz **nicht zulässig** ist. Die vorhandenen Funktionalitäten des neuen Systems müssen nachträglich an die rechtlichen Voraussetzungen angepasst werden. Dies ist ein vermeidbarer Mehraufwand, weil dieses Problem bereits während der Projektentwicklung hätte erörtert werden können.

Im Wortlaut: § 196 Abs. 1 LVwG

Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Es ist in geeigneter Weise zu dokumentieren, in welchem Zeitraum und aus welchem Grund die Daten unrichtig waren. Die Daten sind zu ergänzen, wenn der Zweck der Speicherung oder ein berechtigtes Interesse der betroffenen Person dies erfordert.

Für eine operative Nutzung kommen überhaupt nur die Daten von den zum Einsatzzeitpunkt **tatverdächtigen** oder **störenden Personen** in Betracht. Die Daten anderer Personen dürfen außerhalb einer reinen Vorgangsdokumentation und -verwaltung nicht genutzt werden.

Sofern der Tatverdacht sich auf ein Delikt bezieht, das bereits in einem so frühen Ermittlungsstadium die Anfertigung eines Merkblattes für die **Kriminalakte** rechtfertigt, erscheint eine Abrufbarkeit der Daten des Verdächtigen über einen Zeitraum von maximal **sechs Monaten** tragbar. Danach ist von einer ordnungsgemäßen Erfassung in der PED bzw. in INPOL auszugehen.

Darüber hinaus kommt eine sehr kurzfristige, maximal **vierwöchige „Erinnerungsfunktion**" des Systems in Bezug auf Verdächtige und Störer in Betracht, wenn es bei **besonderen Einsatzarten**, die nicht kriminalaktenfähig sind, für die Polizei von Bedeutung ist, dass kurz vorher ein gleichartiger Einsatz stattgefunden hat (z. B. bei häuslicher Gewalt). Es wäre dann nämlich nicht nachzuvollziehen,

warum eine solche Häufung von gleichartigen Einsätzen der Polizei nur deshalb unbekannt wäre, weil in einem größeren Zuständigkeitsbereich jeweils andere Einsatzkräfte ausrücken.

Die Polizeiinspektion Lübeck hat angekündigt, ein **Datenmodell** mit entsprechenden Klassifizierungen nebst Begründungen zur Erforderlichkeit zu erstellen und die technischen Lösungsmöglichkeiten hinsichtlich einer gesetzeskonformen Auswertung des Datenpools zu klären. Die Erörterungen dauern an.

Was ist zu tun?
Am besten ist es, die Rechtmäßigkeit neuer Systeme vor ihrer Inbetriebnahme zu prüfen. Nachträgliche technische Korrekturen sind aufwändig. Der Innenminister muss bei der Ausstattung der künftigen zentralisierten Einsatzleitstellen die Einhaltung der rechtlichen Vorgaben sicherstellen.

4.2.5 Neues Gesetz für polizeilichen Zugriff auf Verbindungsdaten

Der Bund hat ein aus datenschutzrechtlicher Sicht abgewogenes Gesetz zur Regelung der Nutzung von Telekommunikationsverbindungsdaten verabschiedet. Auf sie dürfen Polizei und Staatsanwaltschaft nur mit richterlicher Anordnung im Rahmen der Verfolgung von Straftaten von erheblicher Bedeutung, insbesondere von Katalogtaten nach § 100 a StPO, zugreifen.

Die aus dem Zeitalter der analogen Telekommunikation stammende bisherige Regelung des **Fernmeldeanlagengesetzes** stand seit Jahren in der datenschutzrechtlichen Kritik, weil sie der Fülle und Qualität der im digitalen Zeitalter verfügbaren Verbindungsdaten nicht in verfassungskonformer Weise Rechnung trug. Ihre Geltungsdauer war jedoch vom Bundestag im Zusammenhang mit anderen Gesetzesbeschlüssen im Telekommunikationsrecht mehrfach verlängert worden.

Die Nachfolgeregelung in der Strafprozessordnung nähert die Tatbestandsvoraussetzungen für eine Auskunft über Verbindungsdaten an diejenigen für das Abhören von Inhaltsdaten an. Wesentlich ist, dass Betreiber **nicht zur Aufzeichnung von Verbindungsdaten** vergangener oder künftiger Telekommunikation **verpflichtet** werden, die sie nicht ohnehin für Betriebs- und Abrechnungszwecke rechtmäßigerweise speichern. Insofern bleiben die datensparsamen Regelungen des Telekommunikations- bzw. Telemedienrechts erhalten.

Einer verfassungskonformen Anwendung bedarf die Befugnis zur Auskunftserteilung zur **Zielwahlsuche**, bei der mitgeteilt werden muss, ob von einem Anschluss Verbindungen zu einem Verdächtigen hergestellt worden sind. Falls sich diese Zielwahlsuche auf sämtliche Anschlüsse bezöge, von denen aus eine solche Verbindung hergestellt wurde, wäre ein erheblicher Personenkreis betroffen, ohne dass die Notwendigkeit und Verhältnismäßigkeit einer solchen Anfrageart hinreichend dargetan ist.

Ähnlich problematisch erscheint die nach der Bundesratsbefassung eingefügte Befugnis zur **Funkzellenabfrage**, bei der die richterliche Anordnung nicht die Rufnummer oder sonstige Kennung eines konkreten Anschlusses, sondern lediglich die betreffende Telekommunikation in räumlicher und zeitlicher Hinsicht bezeichnen muss. Auch hier sind in erheblichem Umfang unbeteiligte Dritte von der Übermittlung von Verbindungsdaten innerhalb einer oder mehrerer Funkzellen betroffen.

Die geplante Neuregelung wurde bis 2005 befristet und sieht eine **Evaluation** ihrer Auswirkungen vor. Dieser Ansatz entspricht den Vorstellungen der Datenschutzbeauftragten.

4.2.6 Die Verwertung abgehörter Telefonate

Nach der gegenwärtigen Rechtslage können Informationen aus einer Telefonüberwachung im Rahmen der Strafverfolgung von der Polizei in sehr weitem Umfang für präventiv-polizeiliche Zwecke genutzt und an andere Polizeibehörden übermittelt werden. Durch eine Ergänzung des schleswig-holsteinischen Polizeirechts könnte die Verwendung dieser hochsensiblen Daten zumindest auf die Abwehr erheblicher Gefahren begrenzt werden.

Aus abgehörten Telefonaten im Rahmen eines Drogenermittlungsverfahrens ergab sich für die Polizei als **Zufallsfund** ein Korruptionsverdacht gegen einen Polizeibeamten. Nun entstand die Frage, ob diese Information zur Abwehr der Gefahr, dass der betreffende Beamte weiterhin mit Personen aus kriminellen Kreisen zusammenarbeiten könnte, an dessen Dienstvorgesetzten übermittelt werden durfte.

Nach Einleitung eines Strafermittlungsverfahrens gegen den Polizeibeamten könnte jedenfalls die Staatsanwaltschaft dem Dienstvorgesetzten die Informationen zukommen lassen, die er für eine Entscheidung über gefahrenabwehrende dienstrechtliche Maßnahmen – z. B. eine Umsetzung – benötigt. Unabhängig von der Einleitung eines Strafverfahrens kann jedoch die Polizei nach der Strafprozessordnung (StPO) Informationen aus der Telefonüberwachung „**nach Maßgabe des Polizeirechts**“ nutzen. Wenn das Polizeirecht wie in Schleswig-Holstein keine ausdrücklichen Verwendungsbeschränkungen enthält, dürfen danach auch Daten aus besonderen Grundrechtseingriffen wie der Telefonüberwachung zu allen polizeirechtlichen Zwecken genutzt und an andere Polizeibehörden übermittelt werden. Diese vollständige Öffnung hochsensibler Daten aus Strafverfahren für andere Nutzungszwecke hatten wir gemeinsam mit anderen Datenschutzbeauftragten bereits anlässlich der Novellierung der StPO kritisiert (vgl. 23. TB, Tz. 4.3.1). Verfassungskonform ist allenfalls eine Nutzungs- und Übermittlungsbefugnis zur Abwehr erheblicher Gefahren. Notwendig ist also eine Ergänzung des Polizeirechts, auf das die StPO verweist.

Im **konkreten Fall** bestand nach unserer Auffassung kein Zweifel daran, dass eine Übermittlung an den Dienstvorgesetzten in jedem Fall zulässig war. Ein Korruptionsverdacht gegen Polizeibeamte berührt nämlich die Vertrauenswürdigkeit und Effektivität von Einrichtungen des Rechtsstaates insgesamt.

Was ist zu tun?
Der Landesgesetzgeber sollte die Nutzung von Strafverfahrensdaten zu polizeirechtlichen Zwecken verfassungskonform einschränken.

4.2.7 Polizeiliche Videoüberwachung

Bei der Mitnutzung einer privaten Überwachungsanlage in einer Einkaufspassage durch die Polizei gelten für sie strengere rechtliche Maßstäbe als für den privaten Träger.

Die Polizei sieht gegenwärtig offenbar kein Bedürfnis für eine permanente Videoüberwachung öffentlicher Plätze. Eine Umfrage der Polizei ergab, dass es zurzeit **keine laufende Videoüberwachung** öffentlicher Räume durch die Polizei in Schleswig-Holstein gibt. Eine vor einigen Jahren in Westerland installierte Anlage (vgl. 20. TB, Tz. 4.2.6) ist deaktiviert, da die Voraussetzungen für eine Videobeobachtung weggefallen sind.

Dies schließt natürlich nicht aus, dass sie – zur Wahrnehmung ihres Hausrechts in einzelnen Dienststellen, bei der Verkehrsüberwachung im Falle von Geschwindigkeitsüberschreitungen, bei der Strafverfolgung durch Auswertung von Videomaterial von Banken oder Geschäften oder mit richterlicher Anordnung im Rahmen einer gezielten Observation – von der Videoüberwachung im Einzelfall Gebrauch macht.

Ein Beispiel hierfür ist die gelegentliche polizeiliche Mitnutzung der Videoüberwachungsanlage im **Kieler Sophienhof**, die von der dortigen privaten Grundstücksverwaltung installiert ist. Nach entsprechenden Berichten in der Presse haben wir die Verfahrensweise unter datenschutzrechtlichen Gesichtspunkten geprüft und festgestellt, dass dort mehrere Kameras die Passagen im Innen- und Außenbereich erfassen. Das Bildmaterial wird über einen Zeitraum von drei Tagen hinweg gespeichert, um Straftaten im Nachhinein aufklären zu können. Die Auslegung und Nutzung der Anlage entspricht den Vorschriften des BDSG; allerdings waren die vorgeschriebenen Hinweisschilder, dass eine

Im Wortlaut: § 6b BDSG

Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie
1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.
...
(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

Videoüberwachung stattfindet und wer für sie verantwortlich ist, noch nicht vorhanden. Sie sind zwischenzeitlich angebracht worden.

Der Betreiber des Sophienhofes übermittelt im Falle festgestellter Straftaten ausgedruckte Standbilder – nicht jedoch ganze Videosequenzen – mit der Abbildung der mutmaßlichen Täter zur weiteren Ermittlung an die Polizei. Die **Polizei** selbst nutzt die private Videoüberwachungsanlage im Sophienhof nach eigenen Angaben **lediglich sporadisch** zur unmittelbaren Beobachtung von Personen. Wir haben bei der Prüfung keine Anhaltspunkte dafür gewonnen, dass die Polizei dabei gegen die für sie geltenden, strengeren gesetzlichen Vorschriften des Polizei- und Strafprozessrechts verstößt. Insbesondere sind bislang die von der Anlage ständig gefertigten Aufzeichnungen von der Polizei nicht gezielt ausgewertet worden. Dies ist lediglich bei bevorstehenden schweren Straftaten oder bei einem Anfangsverdacht begangener Straftaten zulässig.

4.2.8 Was darf der Rettungsarzt der Polizei mitteilen?

Ein Verletzter kann sich einer Blutprobe nicht dadurch entziehen, dass er dem Rettungsarzt untersagt, der Polizei den Namen der Klinik zu nennen, in die er eingeliefert wird, weil das Melderecht für das Krankenhaus eine Auskunftspflicht vorsieht. Ob der Unfallarzt eine entsprechende Auskunft erteilt, steht in seinem Ermessen.

Grundsätzlich unterliegt die Tatsache der Behandlung durch einen Arzt bzw. in einer medizinischen Einrichtung der ärztlichen Schweigepflicht, damit das für die medizinische Versorgung unerlässliche **Vertrauensverhältnis zum Patienten** entstehen kann und eine Person es nicht unterlässt, sich in Behandlung zu begeben, weil sie fürchtet, dadurch polizeiliche Ermittlungen gegen sich zu ermöglichen. Hat die Polizei bei einem Unfall jedoch bereits Kenntnis von der Behandlungsbedürftigkeit eines Verletzten und lässt sie ihn per Rettungswagen abtransportieren, bevor eine Blutprobe gesichert werden kann, ist dieser Schutzgedanke nicht mehr relevant, weil die Tatsache der ärztlichen Behandlung für die Polizei kein Geheimnis mehr ist. Hinzu kommt, dass das Melderecht es der Polizei ohnehin erlauben würde, den Ort einer Krankenhausbehandlung zu ermitteln, und damit das Interesse an der Strafverfolgung gegenüber der Geheimhaltung des Aufenthaltsortes höher bewertet. Dies setzt allerdings das „Abklappern“ aller in Betracht kommenden Krankenhäuser voraus.

Allerdings kann ein Arzt zu einer Auskunft auch in der hier dargestellten besonderen Fallgestaltung nicht gezwungen werden, weil sein strafprozessuales Zeugnisverweigerungsrecht auch in Bezug auf Tatsachen besteht, die keine Geheimnisse im Sinne der strafbewehrten Schweigepflicht mehr sind. Da er sein Zeugnisverweigerungsrecht jedoch nicht wahrnehmen **muss**, verfügt der **Arzt** über einen rechtlichen **Spielraum** um zu entscheiden, ob eine Mitteilung an die Polizei über den voraussichtlichen Behandlungsort im konkreten Fall aus seiner Sicht tragbar erscheint. Datenschutzrechtliche Gesichtspunkte stehen einer solchen Mitteilung nicht entgegen.

Was ist zu tun?
Die Rechtslage sollte sowohl im Bereich der Polizei als auch im Bereich der Rettungsdienste transparent gemacht werden, um Missverständnisse am Unfallort auszuschließen.

4.2.9 EURAS

Bei den Bezirkskriminalinspektionen Kiel und Lübeck wurde das EDV-Verfahren EURAS einer datenschutzrechtlichen Überprüfung unterzogen. Gravierende Mängel konnten dabei nicht festgestellt werden.

Bei dem Programm EURAS („Ermittlungshilfe und Rechercheorganisation – ein Auswerte-System“) handelt sich es um ein zur Abwicklung von **komplexen Ermittlungsverfahren** entwickeltes EDV-Verfahren. Die Ermittler erhalten einen schnellen und umfassenden Überblick über alle in dem betreffenden Fall vorhandenen Erkenntnisse und können Verknüpfungen zwischen den Personen und/oder Objekten bzw. Sachen herstellen. Es können auch mehrere verschiedene Ermittlungskomplexe zusammengefasst werden, damit nach einzelnen Begriffen verfahrensübergreifend recherchiert werden kann. EURAS dient auch zur Erschließung von Notizen, Hinweisen und Lichtbildern zu Personen und Sachen sowie zur Verbesserung der Übersicht über sichergestellte Asservate.

Das Verfahren wurde von den geprüften Stellen hauptsächlich zur Auswertung von **Telefonüberwachungen** genutzt. Alle Verfahren waren noch nicht abgeschlossen; die Entscheidung über eine Löschung oder präventive Speicherung von Strafverfahrensdaten stand damit noch nicht an. Beanstandungen ergab die Prüfung zwar nicht. Folgende datenschutzrechtliche Anforderungen sind bei der **künftigen Nutzung** von EURAS zu beachten:

- Bei den einzelnen Dienststellen ist eine Übersicht zu führen, aus der sich die Zugriffsrechte der einzelnen Nutzer in Bezug auf die jeweiligen EURAS-Ermittlungskomplexe ergeben.
- Telefonüberwachungsdaten dürfen nur für diejenigen Nutzer einsehbar sein, die entsprechend der internen Aufgabenzuweisung für die betreffenden Ermittlungen zuständig sind.
- Sämtliche mit EURAS erstellten Gesprächsprotokolle müssen der Staatsanwaltschaft auf Papier zur Verfügung gestellt werden, um entsprechende Benachrichtigungen von Betroffenen einer Telefonüberwachungsmaßnahme zu ermöglichen.
- Nur solche Strafverfahren dürfen zu einem einheitlichen EURAS-Datenbestand zusammengefasst werden, die personell-organisatorische Zusammenhänge aufweisen.
- Nach Abgabe des Verfahrens an die Staatsanwalt muss technisch eine selektive Löschbarkeit nicht mehr erforderlicher Daten nach Weisung der Staatsanwaltschaft möglich sein. Auch beim Einsatz von CD-ROM ist eine entsprechende Verfahrensweise vorzusehen.

- Eine Nutzung von EURAS-Daten zu Zwecken der Gefahrenabwehr oder der Aufklärung zukünftiger Straftaten darf nur erfolgen, wenn die im Landesverwaltungsgesetz genannten engen Voraussetzungen erfüllt sind.
- Die Übermittlung von Lichtbildern aus EURAS an andere Dienststellen ist in der Ermittlungsakte zu dokumentieren.
- Für jedes einzelne EURAS-„Verfahren“ ist eine Errichtungsanordnung zu erstellen. Dabei bietet sich die Verwendung einer an den Einzelkomplex anzupassenden Mustererrichtungsanordnung an.

Was ist zu tun?
Die vorgenannten Punkte sollten in einer Dienstanweisung zu EURAS festgelegt werden.

4.2.10 Cyber-Crime Convention

Der Europarat hat mit Zustimmung Deutschlands den Text der Konvention gegen Datennetzkriminalität, die Cyber-Crime Convention, verabschiedet. Gegenüber dem unzureichenden Entwurf wurden nur geringfügige datenschutzrechtliche Verbesserungen realisiert.

Auf die massive **Kritik von Bürgerrechtlern und Datenschützern** am einseitigen Ansatz des Konventionsentwurfes, die wir im letzten Tätigkeitsbericht (vgl. 23. TB, Tz. 11.2) zusammengefasst hatten, reagierte der Europarat mit der Einfügung eines Artikels, wonach jeder Vertragsstaat für eine angemessene Berücksichtigung von Grundrechten entsprechend internationaler Vereinbarungen und des Verhältnismäßigkeitsgrundsatzes sorgen müsse. Damit wird jedoch lediglich die nationale Verantwortung der Unterzeichnerstaaten für rechtsstaatliche Mindestgarantien unterstrichen, ohne solche Garantien bei den jeweiligen Eingriffsbefugnissen selbst einzubauen.

Nach wie vor kommen Belange der Rechtsstaatlichkeit strafrechtlicher Ermittlungen wie auch datenschutzrechtliche Standards gegenüber den in den Mittelpunkt gestellten Befugnissen der Strafverfolgungsbehörden nach unserer Auffassung zu kurz.

Was ist zu tun?
Bei einer Umsetzung der Konvention in das deutsche Recht müssen die verbliebenen völkerrechtlichen Spielräume zur rechtsstaatlichen Ausgestaltung konsequent genutzt werden.

4.2.11 Personenbezogene Daten in kriminalpräventiven Räten

In Sitzungen der vielerorts entstandenen kriminalpräventiven Räte dürfen Einzelfälle z. B. straffälliger Jugendlicher grundsätzlich nur in anonymisierter oder pseudonymisierter Form besprochen werden. Auch Sozialdaten der Betroffenen müssen geschützt bleiben.

In zahlreichen Städten und Gemeinden Schleswig-Holsteins sind mittlerweile „Runde Tische“ bzw. kriminalpräventive Räte eingerichtet worden, in denen neben kommunalen Einrichtungen und der Polizei auch soziale Organisationen, private Hilfseinrichtungen und Vereine vertreten sind. Sie alle wollen durch eine enge Kooperation insbesondere der Jugenddelinquenz im Bereich von Gewaltdelikten entgegenwirken. Bei diesem sinnvollen Anliegen müssen allerdings, insbesondere bei einer Anwesenheit privater Organisationen, auch datenschutzrechtliche Grenzen der Übermittlung personenbezogener Informationen berücksichtigt werden, die sich für die beteiligten Behörden aus ihren Fachgesetzen (z. B. Strafprozessordnung, Landesverwaltungsgesetz, Sozialgesetzbuchs oder Jugendgerichtsgesetz) ergeben. Am unproblematischsten ist es, Problemfälle in anonymisierter bzw. pseudonymisierter Form zu erörtern. Unter Namensnennung der Betroffenen dürfen Einzelheiten über Straftäter nur so weit am Runden Tisch „ausgebreitet“ werden, wie sie allen Teilnehmern nach den Vorschriften insbesondere des Jugend- und Sozialhilferechts übermittelt werden dürften.

Weitere Hinweise zu diesem Thema können unserer Homepage

www.datenschutzzentrum.de/material/themen/divers/jugpol.htm

entnommen werden.

Was ist zu tun?
Die an „Runden Tischen“ mitwirkenden Behörden müssen auch dort rechtlich korrekt mit personenbezogenen Daten umgehen.

4.3 Justizverwaltung

4.3.1 Zwangsversteigerungsdaten ab ins Internet?

Einige Gerichte wollen im Internet Informationen aus Zwangsversteigerungs- und Insolvenzverfahren veröffentlichen, um Kosten zu sparen und die Wirksamkeit der Veröffentlichung zu erhöhen. Eine Internet-Veröffentlichung belastet die Betroffenen erheblich stärker als herkömmliche Publikationen.

Einige Gerichte in anderen Bundesländern veröffentlichen schon seit längerem die Eröffnungsbeschlüsse aus **Verbraucherinsolvenzverfahren** auf „elektronischen Gerichtstafeln“ im Internet. Teilweise sind die Beschlüsse dort über einen mehrjährigen Zeitraum abrufbar. Das Justizministerium hatte uns daraufhin um Bera-

tung ersucht, ob die Gerichte in Schleswig-Holstein Informationen über Zwangsversteigerungs- und Insolvenzverfahren in das Internet stellen dürften. Wir wiesen auf Folgendes hin: Für einen Schuldner wäre es wirtschaftlich und persönlich fatal, wenn auf unbestimmte Zeit unter seinem Namen in den Suchmaschinen des Internets für Jeden die Tatsache ersichtlich wäre, dass gegen ihn einmal ein Zwangsversteigerungs- oder Verbraucherinsolvenzverfahren lief. Ein wirtschaftlicher Neuanfang wäre wesentlich erschwert, zumal einmal in das Internet eingestellte Daten grundsätzlich nicht mehr rückholbar, d. h. rückstandsfrei löschbar, sind. Privatwirtschaftliche Auskunfteien könnten die Internet-Angebote der Gerichte kopieren und in eigenen Angeboten weit über den Zeitpunkt der offiziellen Veröffentlichung hinaus zur Verfügung stellen. Auch die Entscheidung des Gesetzgebers, dass Insolvenzschuldner nicht in das Schuldnerverzeichnis der Amtsgerichte aufzunehmen sind, ist zu berücksichtigen. Der Bundestag hat inzwischen eine ausdrückliche Rechtsgrundlage für die **Internet-Veröffentlichung** geschaffen, die allerdings noch durch eine Rechtsverordnung konkretisiert werden muss. Das Gesetz verfolgt vor allem den Zweck, Bekanntmachungskosten in örtlichen Zeitungen einzusparen, die über die Gerichtskosten letztlich der Schuldner selbst tragen muss. Die Bedenken der Datenschutzbeauftragten wurden aufgegriffen und im Gesetz festgelegt, dass in der Verordnung Vorkehrungen zur Gewährleistung der Integrität der Daten, der Zuordnung zu ihrem Ursprung und ein Kopierschutz gegenüber Dritten geschaffen werden müssen. Die Erfahrungen mit der Internet-Veröffentlichung von Insolvenzdaten sollen zudem kurzfristig ausgewertet werden. Dabei ist auch darzulegen, ob die beabsichtigten Einsparungen tatsächlich eingetreten sind.

Im Falle von **Zwangsversteigerungen** kann die bessere Zugänglichkeit der Informationen über das betreffende Objekt allerdings dem Schuldner selbst zugute kommen, da auf diese Weise unter Umständen zusätzliche Interessenten angesprochen werden. Das Zwangsversteigerungsgesetz lässt eine auch wiederholte Veröffentlichung bestimmter Informationen in einem anderen Medium als dem örtlichen für Gerichtsbekanntmachungen bestimmten Blatt zu. Um eine langfristige „**Prangerwirkung**“ des Internets gegenüber dem Schuldner zu vermeiden, darf die Inernet-Veröffentlichung jedoch nicht seinen Namen enthalten, der für potenzielle Bietende ohnehin zunächst uninteressant ist. Wenn ein privater Dienstleister (für derzeit vier Amtsgerichte aus Schleswig-Holstein: www.hanmark.de) bei der Internet-Veröffentlichung eingeschaltet wird, liegt eine Auftragsdatenverarbeitung vor. Das beauftragende Gericht darf nur die erforderlichen Daten an den Dienstleister übermitteln und muss im Rahmen einer Vereinbarung sicherstellen, dass die Daten nach der Versteigerung wieder gelöscht werden.

Was ist zu tun?
Das Justizministerium sollte bei der Umsetzung der gesetzlichen Spielräume für Internet-Veröffentlichungen von Daten darauf hinwirken, dass kein „virtueller Schuldenpranger“ für die Betroffenen entsteht.

4.3.2 Mit dem Scanner durch die Justizregister?

Die öffentlichen Register der Justiz sollen der Transparenz bestimmter wirtschaftlicher und gesellschaftlicher Bereiche dienen. Sie werden von Behörden und nicht von privaten Institutionen geführt, damit die Beachtung der Vorschriften über Einsichtnahmen, den räumlichen Erfassungsbereich und über die datenschutzrechtlichen Verpflichtungen der Datenempfänger besser gewährleistet werden kann. Eine Übernahme ganzer Datenbestände durch private Auskunfteien kommt nach der gegenwärtigen Rechtslage nicht in Betracht.

Eine bundesweit organisierte Auskunftei hatte bei einem Amtsgericht beantragt, alle Informationen aus dem **Handels**-, dem **Genossenschafts**-, dem **Partnerschafts**- und dem **Vereinsregister** per Scanner zu übernehmen, soweit sie ohne Darlegung eines berechtigten Interesses einsehbar sind.

Zwar handelt es sich bei den Registern der Justiz grundsätzlich um öffentlich zugängliche Datenbestände. Die Entscheidung jedoch, welchen räumlichen Bereich ein Register abdeckt, welche Anfragemöglichkeiten bestehen und wer automatisierten Zugriff bekommt, ist vom Gesetzgeber getroffen worden und muss daher in staatlicher Hand bleiben. Die bestehenden Register sind bislang dezentral und lassen sich nicht nach einem bestimmten Personennamen durchsuchen. In einem **privaten** „**Parallelregister**“ würden Recherchemöglichkeiten im Gesamtbestand zu einem Namen geschaffen, sodass ersichtlich würde, an welchen Unternehmen und Vereinigungen eine Person in welcher Funktion beteiligt ist. Dies ist bislang vom Gesetzgeber nur beim Schuldnerverzeichnis zugelassen worden. Die Erlaubnis einer weiteren Nutzung wäre datenschutzrechtlich bedenklich.

Allerdings liegen gegenwärtig Gesetzes- bzw. **Verordnungsentwürfe** zur Registerautomation vor, die den erleichterten Zugang Privater zu in Justizregistern gespeicherten Informationen regeln werden. Die zu erwartenden Regelungen würden unterlaufen, wenn an Stelle von Einzelanfragen ganze Datenbestände in die Hand gewerblicher Auskunfteien gegeben würden. Dies haben wir in einer Stellungnahme gegenüber dem Justizministerium dargelegt.

Was ist zu tun?
Die Justiz sollte wachsam gegenüber einer kommerziellen Ausbeutung der ihr anvertrauten Daten sein.

4.3.3 Rechte und Pflichten der Betreuer

Informationen im Zusammenhang mit Betreuungsvorgängen sind sensibel. Betreuer dürfen nur im Rahmen des Erforderlichen bei anderen Behörden über die Betreuten recherchieren. Der Landesrechnungshof darf Betreuungsakten einsehen, wenn es für seine Kontrolltätigkeit erforderlich ist.

Eine **Betreuerin** hatte sich mit der Bitte um Einsichtnahme in die Akte eines mittlerweile eingestellten Strafverfahrens gegen den von ihr Betreuten wegen des Vorwurfs der versuchten Vergewaltigung an die Staatsanwaltschaft gewandt. Darüber hinaus wollte sie wissen, ob weitere Strafverfahren gegen den Betreuten anhängig seien oder waren. Die Staatsanwaltschaft bat uns um Beratung zur Zulässigkeit entsprechender Datenübermittlungen. Einen Anspruch auf Einsichtnahme bzw. Auskünfte hätte die Betreuerin dann gehabt, wenn die ihr vom Gericht übertragenen Aufgabenkreise eine Kenntnis dieser Daten erfordert hätten. Die Betreuerin hätte allerdings darlegen müssen, warum die Daten aus den abgeschlossenen Verfahren für ein anderweitiges Verfahren, insbesondere ein gegenwärtig noch laufendes Strafverfahren, von Bedeutung waren. Ein bloßes Interesse an der Biografie des Betreuten reicht nicht aus. Berechtigt war dagegen die Frage nach anhängigen Strafverfahren gegen den Betreuten, da die Betreuerin gegebenenfalls die Frage prüfen musste, ob ein Verteidiger zu beauftragen war.

Von mehreren Stellen erreichten uns Anfragen, ob Daten über die Betreuer wie auch über die Betreuten im Rahmen einer Prüfung zur Kostenentwicklung im Betreuungswesen an den **Landesrechnungshof** übermittelt werden dürfen. Die Befugnisse des Landesrechnungshofes nach der Landeshaushaltsordnung umfassen auch die Einsichtnahme in Unterlagen mit personenbezogenen Inhalten. Beim Landesrechnungshof unterliegen solche Daten einer strengen Zweckbindung und dürfen nur im erforderlichen Umfang und unter Wahrung technisch-organisatorischer Sicherungen weiterverarbeitet werden. Diese Befugnisse umfassen auch die vorgeschriebenen Meldungen der Betreuer an die Betreuungsbehörden über die Zahl sowie den zeitlichen und finanziellen Umfang der von ihnen geführten Betreuungen. Auch die Betreuungsakten beim Amtsgericht unterfallen diesem Einsichtsrecht. Die Entscheidung darüber, welche Vorgänge an ihn übermittelt werden sollen, trifft der Rechnungshof selbst, weil ansonsten die zu prüfenden Stellen ein faktisches Mitentscheidungsrecht über den Untersuchungsrahmen hätten. Durch präzise Bekanntgabe des Prüfungsthemas muss es der Rechnungshof jedoch z. B. einer Behörde ermöglichen, die Daten, die in keinem sachlichen oder zeitlichen Zusammenhang mit der Anforderung stehen, von den relevanten Unterlagen zu trennen.

4.3.4 Elektronisches Grundbuch – Wie sicher ist die Unterschrift?

Im September des Jahres 2001 wurde das elektronische Grundbuch beim ersten Amtsgericht in Schleswig-Holstein offiziell in Betrieb genommen. Leider gibt es aber noch immer offene Fragen zur Datensicherheit.

Im 23. Tätigkeitsbericht (Tz. 14.1) berichteten wir über den jüngsten Anlauf zur Einführung eines elektronischen Grundbuchs in Schleswig-Holstein, diesmal unter dem Namen **FOLIA** zusammen mit dem Land Baden-Württemberg. Das Grundkonzept dieses Systems ist viel versprechend und berücksichtigt Aspekte der Datensicherheit. Allerdings steckt der Teufel im Detail, nämlich bei der genauen Ausgestaltung der elektronischen Unterschrift. In der Vorschrift, die die Eintragung im elektronischen Grundbuch regelt, heißt es, dass der Urkundsbeamte der Geschäftsstelle der Eintragung den Nachnamen hinzusetzt und beides elektronisch unterschreibt. Übereinstimmend mit dem Standard des Signaturgesetzes für qualifizierte Signaturen wird im Verfahren FOLIA zu diesem Zweck eine Chipkarte an die einzelnen eintragungsberechtigten Mitarbeiter in den Grundbuchämtern ausgegeben, die jeweils mit einer PIN freigeschaltet werden kann. Mithilfe dieser Chipkarte und der PIN, die zu ihrer Aktivierung erforderlich ist, kann eine elektronische Signatur erzeugt werden.

Im Wortlaut:
§ 75 Grundbuchverfügung

Elektronische Unterschrift
Bei dem maschinell geführten Grundbuch soll eine Eintragung nur möglich sein, wenn die für die Führung des Grundbuchs zuständige Person oder, in den Fällen des § 74 Abs. 1 Satz 3, der Urkundsbeamte der Geschäftsstelle der Eintragung ihren oder seinen Nachnamen hinzusetzt und beides elektronisch unterschreibt. Die elektronische Unterschrift soll in einem allgemein als sicher anerkannten automatisierten kryptographischen Verfahren textabhängig und unterzeichnerabhängig hergestellt werden. Die unterschriebene Eintragung und die elektronische Unterschrift werden Bestandteil des maschinell geführten Grundbuchs. Die elektronische Unterschrift soll durch die zuständige Stelle überprüft werden können.

Dieses theoretisch sichere Verfahren ist in der Praxis dadurch „vereinfacht“ worden, dass die PIN bei der Signierchipkarte lediglich wie eine Login-Kennung funktioniert. Zwar muss der Eintragungsberechtigte bei der erstmaligen Verwendung der Chipkarte nach dem Hochfahren des Systems seine PIN eingeben. Nachdem dies erfolgt ist, können allerdings sämtliche folgenden Signiervorgänge ohne weitere Eingabe der PIN vor sich gehen. Es ist dann lediglich erforderlich, der Menüführung zu folgen bzw. „Enter“ zu drücken. Dies eröffnet natürlich **Angriffspunkte für die Sicherheit** des Systems. Zwar sollen die eintragungsberechtigten Grundbuchbeamten angewiesen werden, ihre Chipkarte immer bei sich zu führen. Wird dies allerdings doch einmal unterlassen, so kann jedermann, der Zugang zu den Rechnern hat, mit einer noch im Lesegerät steckenden Chipkarte Eintragungen im elektronischen Grundbuch vornehmen. Diese können im Nachhinein kaum als unrechtmäßig erkannt werden, da sie mit einer Signatur versehen sind, die einem Eintragungsberechtigten zugeordnet war.

Diese Art von Signaturerzeugung wird man nicht als elektronische Unterschrift im Sinne der Vorschrift bezeichnen können. Eine solche wäre nur dann gewährleistet, wenn für jeden Signiervorgang jeweils eine **erneute Eingabe der PIN** gefordert würde. Nur dann wäre die Erklärungshandlung von Aufwand und Maß der geforderten Aktivität mit der herkömmlichen Unterschrift vergleichbar.

Die Einbuße an Sicherheit ist deswegen umso bedenklicher, weil der Verordnungsgeber bei der Führung des automatisierten Grundbuchs ohnehin die Sicherheitsstandards bereits heruntergesetzt hat. Sind im konventionellen Grundbuch immer zwei Personen erforderlich, die unabhängig voneinander einen Eintrag unterzeichnen und damit nach dem **Vieraugenprinzip** für Sicherheit sorgen, so tritt an deren Stelle im automatisierten Grundbuch die oben beschriebene elektronische Unterschrift. Kann diese nun durch einen einfachen Tastaturbefehl ohne die erforderliche Authentifizierung durch Besitz und Wissen in jedem Fall geleistet werden, so wird die Sicherheit des elektronischen Grundbuchs ohne Not herabgesetzt.

Dies kann zu erheblichen Gefährdungen nicht nur für das Datenschutzrecht der Bürger führen. Bekanntlich werden durch Eintragungen im Grundbuch erhebliche Vermögenswerte belegt. Schon eine kurzfristige Unrichtigkeit von Eintragungen könnte von Angreifern ausgenutzt werden und zu einem erheblichen wirtschaftlichen Schaden führen. Dazu kommt, dass das elektronische Grundbuch ebenso wie das papierene den Rechtsschein der Richtigkeit für sich hat. Das bedeutet, dass Eintragungen im Grundbuch zunächst als zutrefffend gelten, bis das Gegenteil bewiesen ist.

Obwohl der Justizverwaltung diese Einwände seit geraumer Zeit bekannt sind, gab es bisher keine Initiative, die Mängel abzustellen. Leider wurde zudem das Verfahren in den **Echtbetrieb** genommen, ohne dass ein durch die Datenschutzverordnung zwingend vorgeschriebenes Sicherheitskonzept vorliegt. Das Justizministerium hat mittlerweile mitgeteilt, dass man im gemeinsamen Entwicklerverbund mit Baden-Württemberg nach einer softwaretechnischen Lösung suchen werde, wegen vorrangiger anderer Arbeiten habe die Sache jedoch keine Priorität. Daher ist mit Ergebnissen wohl nicht vor der zweiten Jahreshälte 2002 zu rechnen. Auch die baldige Übersendung eines Sicherheitskonzeptes wurde vom Justizministerium erneut in Aussicht gestellt.

Was ist zu tun?
Die für die Einführung des elektronischen Grundbuchs Verantwortlichen sollten schnellstmöglich dafür sorgen, dass die elektronische Unterschrift mit der erforderlichen Sicherheit geleistet wird.

4.4 Verfassungsschutz

Mängel bei den behördlichen Geheimschutzbeauftragten

Die bisherige Konzentration der Zuständigkeiten für die Sicherheitsüberprüfung beim Sicherheitsbeauftragten des Landes sollte beibehalten werden. Eine Querschnittsprüfung zeigt, dass es Geheimschutzbeauftragten in den einzelnen Behörden an Ausstattung und Kompetenz mangelt.

> ***? Wer wird sicherheitsüberprüft?***
>
> *Eine sicherheitsempfindliche Tätigkeit übt u. a. aus, wer Zugang zu Verschlusssachen hat oder ihn sich verschaffen kann, die als STRENG GEHEIM, GEHEIM oder VS-VERTRAULICH eingestuft sind.*

Wir haben jahrelang gefordert, die Sicherheitsüberprüfungen im Lande auf eine gesetzliche Grundlage zu stellen. Seit Februar 2001 liegt ein Entwurf eines Landessicherheitsüberprüfungsgesetzes vor. Einige unserer Vorschläge wurden leider nicht berücksichtigt (vgl. 21. TB, Tz. 4.3). Insbesondere ist weiterhin eine Verlagerung der Aufgaben des Sicherheitsbeauftragten auf die örtlichen Geheimschutzbeauftragten beabsichtigt. Vor diesem Hintergrund haben wir im Jahr 2001 eine datenschutzrechtliche Prüfung bei Geheimschutzbeauftragten durchgeführt.

Generell ist seit der Auflösung des Warschauer Pakts Anfang der Neunzigerjahre ein starker Rückgang der Sicherheitsüberprüfungen zu verzeichnen. Es üben nämlich nur noch eine geringe Anzahl von Personen eine sicherheitsempfindliche Tätigkeit entsprechend den Sicherheitsrichtlinien des Landes aus; sie sind in der Regel bis zur Geheimhaltungsstufe „VS-Geheim“ ermächtigt. Bei den Geheimschutzbeauftragten war durchgehend eine **geringe Kenntnis** über den Regelungsgehalt der **Sicherheitsrichtlinien** festzustellen. Selbst deren Existenz war einigen von ihnen nicht bekannt. Eine Information der Geheimschutzbeauftragten über das Ausscheiden von Mitarbeitern aus einem Sicherheitsbereich durch die Personalstelle sowie die fristgerechte Vernichtung der Unterlagen erfolgte nur selten.

Ein korrekter Umgang mit Daten aus Sicherheitsüberprüfungen ist vor allem in den Behörden nicht gewährleistet, in denen Sicherheitsüberprüfungen nur selten zu veranlassen sind und in denen die Funktion des personellen Geheimschutzes lediglich einen geringen Anteil der Aufgaben der jeweiligen Verantwortlichen einnimmt. Die nach den Sicherheitsrichtlinien obligatorischen Schulungen reichen offenbar nicht aus, um in der Fläche eine **rechtskonforme Handhabung** der Unterlagen zu erreichen. Um die Defizite zu beheben, wäre eine bessere Durchstrukturierung des Verfahrens und eine gegenüber dem derzeitigen Stand wesentlich verstärkte Schulung der Geheimschutzbeauftragten erforderlich.

Da bei der Verfassungschutzbehörde und dem **zentralen Sicherheitsbeauftragten** des Landes ein ungleich höherer Datenschutzstandard erreicht ist (vgl. 23. TB, Tz. 4.4.1), erscheint uns eine Dezentralisierung von Geheimschutzaufgaben auf

dem Hintergrund unserer Prüfergebnisse nicht ratsam. Die Aufwendungen für die notwendigen Schulungen sowie für die gebotenen organisatorischen Vorkehrungen wären außerdem enorm. Das Innenministerium wollte dieser Argumentation bislang nicht folgen.

Was ist zu tun?
Das Parlament sollte es bei der bewährten Organisation des Geheimschutzes belassen. Da Sicherheitsüberprüfungen im Zusammenhang mit den Maßnahmen zur Terrorismusbekämpfung sicherlich wieder einen höheren Stellenwert erhalten werden, muss endlich durch eine beschleunigte Fortsetzung des Gesetzgebungsverfahrens eine Rechtsgrundlage hierfür geschaffen werden.

4.5 Ausländerbereich

4.5.1 Überblick

Nach den Terroranschlägen in den USA am 11. September 2001 ist nicht nur im Sicherheitsbereich, sondern auch im Ausländerrecht ein bis dahin ungewohnter politischer Aktionismus zu verzeichnen. Da es sich bei den für die Anschläge verantwortlichen Menschen durchgängig um islamistische Ausländer handelte, meinte man, mit einer Schnellgesetzgebung die offensichtlich bestehenden Defizite bei der Bewertung der Sicherheitslage beheben zu müssen. Dies soll dadurch erreicht werden, dass Ausländerinnen und Ausländer – unabhängig davon, ob sie als **Straftatverdächtige oder gefährliche Personen** aufgefallen sind – in Datenbanken erfasst und überwacht werden. War es z. B. vor den Anschlägen eine Ausnahme, dass Bayern Einbürgerungswillige ohne konkreten Anlass per Regelanfrage vom Landesamt für Verfassungsschutz auf „Verfassungstreue“ überprüfte, so beeilten sich danach alle Länder verfassungsrechtlich problematische derartige Maßnahmen zu ergreifen.

Das lange vorbereitete Zuwanderungsgesetz, mit dem das bisher **als besonderes Polizeirecht** angesehene Ausländergesetz zugunsten eines reinen Aufenthaltsrechtes abgelöst werden sollte, musste plötzlich auch eine Sicherheitsfunktion erfüllen. Dabei ist schon die Grundannahme kritisch zu hinterfragen: Was rechtfertigt es für uns Deutsche anzunehmen, von Ausländern gehe eine so hohe Terrorismusgefahr aus, dass sie mit für Deutsche undenkbaren Maßnahmen zu kontrollieren seien?

4.5.2 Die Fremden – Testfall für den Überwachungsstaat?

Zum Jahresbeginn 2002 trat das Terrorismusbekämpfungsgesetz in Kraft, das **aus verfassungsrechtlicher Sicht** gerade im Hinblick auf seine ausländerbezogenen Vorschriften **schlicht inakzeptabel** ist. Das Grundrecht auf informationelle Selbstbestimmung, der Gleichbehandlungsgrundsatz, das Bestimmtheitsgebot bei gesetzlichen Regelungen und das Asylrecht spielen in diesem Gesetz nicht nur keine Rolle, sondern werden in teilweise grundlegender Weise infrage gestellt.

Im Einzelnen:

- Die fast voraussetzungslose Zulassung der Datenweitergabe von allen Asyl- und Ausländerbehörden an die Ämter für Verfassungsschutz hat – unter Verstoß gegen das Asylgrundrecht des Art. 16a GG – zur Folge, dass die **Begründungen aus Asylanträgen** zu gravierenden Nachteilen für die Flüchtlinge führen können. Die Weitergabe dieser Daten an die Heimatstaaten konnte erst in letzter Minute wenigstens eingeschränkt werden.
- Die Zulassung von verschiedenen **Ausländerausweisen** mit biometrischen Merkmalen auf der Basis einer Rechtsverordnung – nicht eines Gesetzes – läuft darauf hinaus, dass der Probelauf mit elektronischen Ausweisen in Deutschland bei Ausländern durchgeführt werden kann.
- Gegen die Nutzung der **Sprachanalyse** zur Bestimmung einer ungewissen Herkunft ist grundsätzlich wenig einzuwenden. Die Aufbewahrung der Sprachproben in Datenbanken, auf die die Polizei zur Sprecheridentifizierung Zugriff hat, ist dagegen nicht zu rechtfertigen.
- Die **Vorratsdatenspeicherung von Fingerabdrücken** – bisher praktiziert „nur“ bei Flüchtlingen – wird auf weitere Ausländergruppen ausgeweitet und ohne jede Einschränkung für polizeiliche Spurenabgleiche beim BKA vorgehalten.
- Bei Erfüllung bestimmter Gruppenmerkmale von **Visaantragstellern** werden deren Daten mit denen aller Sicherheitsbehörden abgeglichen und dort unter Umständen dauerhaft gespeichert.
- Bei der **Beantragung von Aufenthaltsgenehmigungen** kann eine Regelanfrage bei sämtlichen Polizeibehörden und Geheimdiensten durchgeführt werden.
- Die Möglichkeit einer **Rasterfahndung** mit Daten aus dem Ausländerzentralregister (AZR) wird nicht nur der Polizei, sondern auch allen Geheimdiensten erlaubt, ohne dass eine konkrete Gefahr bestehen müsste.
- Geheimdienste erhalten ungehinderten **Zugriff auf sämtliche AZR-Daten**, sodass sämtliche Ausländer in deren Blickfeld geraten und insofern die Trennung zwischen Verwaltung und Diensten aufgehoben ist.

Der **Bundesrat** meinte, dies sei der Sicherheit vor Ausländerinnen und Ausländern noch nicht genug, weshalb er weitere Eingriffe in deren Grundrechte forderte: Bei der Erteilung unbefristeter Aufenthaltstitel sollte gar eine Pflicht zur Regelanfrage bei den Sicherheitsbehörden eingeführt werden. Und Löschungsfristen z. B. nach Einbürgerungen und bei Visaanträgen sollten nochmals um Jahre hochgesetzt werden, weil dies zur Bekämpfung von Ausländerkriminalität unverzichtbar sei. Dass viele dieser Forderungen schließlich nicht Gesetz wurden, ändert nichts an der Gesamteinschätzung, dass mit diesem Gesetz Ausländer unter Sicherheitsaspekten zu Personen zweiter Klasse gemacht werden, deren Recht auf informationelle Selbstbestimmung zur nahezu beliebigen Disposition steht.

Die Konsequenzen dieser Neuregleungen für die Betroffenen können wegen ihrer Vorbildlosigkeit nur erahnt werden. Es ist absehbar, dass viele Menschen **schuldlos existenziell geschädigt** werden. Von einem Araber, der nach einer Sicherheitsanfrage wegen seiner Nationalität seinen Arbeitsplatz zu verlieren droht, haben wir schon erfahren. Andere Folgen können von der Verweigerung der Visaerteilung und der Einreise über massive polizeiliche Ermittlungsmaßnahmen bis hin zum Risiko der Abschiebung und Ausweisung und der politischen Verfolgung durch den Heimatstaat reichen.

Uns ist nicht erkennbar, wie mit den Regelungen **mehr Sicherheit** geschaffen werden könnte. Eher scheinen sie dazu geeignet, ein Klima von Angst, Abwehr und Aggression zu schüren, das dem Terrorismus förderlich ist.

Was ist zu tun?
Diese überzogene Gesetzgebung sollte so schnell wie möglich korrigiert werden.

4.5.3 Zuwanderungsgesetz – kein Kurswechsel

Zeitgleich mit dem Terrorismusbekämpfungsgesetz wurde im November 2001 von Bundeskabinett der Entwurf eines Zuwanderungsgesetzes beschlossen. Ersteres wurde im Schnelldurchgang durch das Gesetzgebungsverfahren gebracht; das Zuwanderungsgesetz dagegen kommt nicht voran.

Das ursprünglich erklärte Ziel des Zuwanderungsgesetzes war es, das noch als spezielles Polizeigesetz konzipierte Ausländergesetz durch ein modernes **Aufenthaltsrecht** zu ersetzen. Es wurde in einer sich globalisierenden Welt unzeitgemäß angesehen, Ausländern pauschal einen Gefahrenverdacht zuzuschreiben, sie dem gemäß zu behandeln und insbesondere auch informationstechnisch als potenzielle Straftäter zu erfassen.

Anspruch und Wirklichkeit können kaum krasser auseinander gehen als in den Entwürfen des Zuwanderungsgesetzes: Sämtliche vorhandenen und durch das Terrorismusbekämpfungsgesetz **verschärften Datenverarbeitungsbefugnisse** sollen übertragen werden. Durch die Zentralisierung der Ausländerbehörden des Bundes in einem **Bundesamt für Migration und Flüchtlinge** soll überdies eine Stelle geschaffen werden, in der gewaltige Massen an Daten sensibelsten Inhalts zusammengeführt werden sollen. Die Datenbestände des bisherigen Bundesamtes für die Anerkennung politischer Flüchtlinge und des Bundesverwaltungsamtes mit dem Ausländerzentralregister sollen unter einem Dach zusammengeführt werden, ohne dass besondere Abschottungsregelungen vorgesehen wären.

Es werden zwar Anpassungen an das 2001 novellierte Bundesdatenschutzgesetz vorgenommen. In einem Punkt werden die europarechtlichen Vorgaben nicht umgesetzt, indem den Betroffenen das **Widerspruchsrecht** gegen besondere Formen der Datenverarbeitung vorenthalten wird. Damit reiht sich das Zuwanderungsgesetz aus Datenschutzsicht in eine lange Reihe von Gesetzen zur Einschränkung des Datenschutzes für Ausländer ein.

Was ist zu tun?
Bei der weiteren Diskussion des Zuwanderungsgesetzes müssen die eindeutig verfassungswidrigen Entwurfspassagen zurückgenommen werden.

4.6 Wirtschafts- und Verkehrsverwaltung

Straßenmaut – aber bitte mit Datenschutz!

Vom Bundeskabinett wurde ein Gesetzentwurf zur Einführung von „streckenbezogenen Gebühren für die Benutzung von Bundesautobahnen mit schweren Nutzfahrzeugen" beschlossen. Bei dessen technischer Realisierung kann es dazu kommen, dass von einzelnen Verkehrsteilnehmern detailgenaue Bewegungsprofile entstehen.

Schon ab dem Jahr 2003 soll neben der manuellen Erhebung von Gebühren ein automatisches System unter Einsatz von **Mobilfunktechnologie und Satellitennavigation** installiert werden, mit dem streckenbezogene Autobahnbenutzungsgebühren für Lastkraftwagen errechnet werden. Dadurch soll auf stationäre Erfassungseinrichtungen verzichtet werden. Das System ist auch auf den Bereich von Bundesstraßen und auf das Ausland erweiterbar. Dies birgt das Potenzial einer Totalüberwachung des Straßenverkehrs, da feststellbar ist, wer wann wo und wie unterwegs ist.

Sowohl im Interesse einer richtig verstandenen „freien Fahrt für freie Bürger" wie auch der Akzeptanz eines solchen Systems muss es datenschutzgerecht gestaltet werden. In einer Entschließung hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf die dringende Notwendigkeit der Beachtung des Prinzips der **Datensparsamkeit**, der **frühestmöglichen Löschung** und der strikten **Zweckbindung** im Fall des Entstehens von elektronischen Bewegungsprofilen hingewiesen. Vorzugswürdig sind eindeutig Systeme, bei denen Mautgebühren vorab bezahlt werden und bei denen Bewegungsdaten allenfalls beim Zahlungspflichtigen anfallen. Kontrollen, inwieweit der Zahlungspflicht nachgekommen wird, müssen nicht flächendeckend durchgeführt werden, sondern es genügen Stichproben. Das gesamte Verfahren der Gebührenerhebung und -kontrolle muss für die Mautpflichtigen transparent sein.

Weiterhin liegt ein Gesetzentwurf der Bundesregierung vor, der die Erhebung von Mautgebühren an **privat finanzierten Straßenteilen**, z. B. Brücken, Tunneln und Gebirgspässen regeln soll. Auch bei der hierfür zu erlassenden Rechtsverordnung muss darauf geachtet werden, dass über die Finanzierung des Straßenbaus nicht eine Totalüberwachung der Verkehrsteilnehmer entsteht. Insofern ist zu begrüßen, dass das Gesetz die Möglichkeit der anonymen direkten Barbezahlung verpflichtend vorsieht.

Was ist zu tun?
Bei der Straßenmaut muss alles getan werden, damit nicht „Nebenkosten" in Form von Bewegungsprofilen aller Verkehrsteilnehmer entstehen.

4.7 Sozialbereich

4.7.1 Überblick

Während in den vergangenen Jahren Querschnittsprüfungen, Beratungsersuchen und Eingaben unsere Tätigkeit im Bereich „Soziales“ bestimmten, standen 2001 **strukturelle Probleme** im Vordergrund. Es ging im Wesentlichen um das Gesetz zur Verbesserung der Zusammenarbeit zwischen Sozial- und Arbeitsämtern (Tz. 4.7.3) und den Einsatz einer neuen Software bei den Sozialämtern (Tz. 4.7.4). Hinzu kamen „Dauerbrenner“ wie die Frage nach der Sozialhilfezuständigkeit (Tz. 4.7.2) mit dem Problem, ob die Datenbestände der Sozialämter auf einem zentralen Server des Kreissozialamtes verwaltet werden dürfen, ob dem Kreis ein pauschales Einsichtsrecht in die Akten zusteht und ob der Kreis bestimmen kann, dass innerhalb des Kreisgebietes künftig nur noch **eine** Sozialhilfeakte geführt wird. Kontrovers diskutiert werden außerdem immer noch die Voraussetzungen für die **Datenübermittlung an private Arbeitsvermittler**. Unserer im 22. Tätigkeitsbericht dargelegten Rechtsauffassung (Tz. 4.6.4) haben sich aber inzwischen die Kommunalaufsicht des Innenministeriums und das Sozialministerium angeschlossen.

2001 bot gelegentlich auch **Skurriles**. Mit der Amtsverwaltung Stapelholm machten wir im Rahmen einer Beschwerde über einen „Hausbesuch“ bei einer Sozialhilfeempfängerin, der eher einer Hausdurchsuchung gleichkam, Bekanntschaft (zur Zulässigkeit von Hausbesuchen siehe 23. TB, Tz. 4.7.3). Der Amtsvorsteher verweigerte trotz Prüfung und Beanstandung beständig eine Stellungnahme. Auch der Kreis Schleswig-Flensburg als Aufsichtsbehörde konnte sich bislang gegen das kleine Amt nicht durchsetzen.

Wir lernten ein Kreisjugendamt kennen, in dem die neue Chefin für frischen Wind in verstaubten Amtsstuben sorgen wollte und sich prompt einige Sozialarbeiter, besorgt um lieb gewonnene Gewohnheiten, an ihre Schweigepflicht bzw. genauer gesagt an ihr Schweigerecht erinnerten. Der Amtsleitung wurde zu Recht die Kenntnis von Daten über betreute Jugendliche verwehrt. Das kann und darf aber einen Chef nicht hindern zu **kontrollieren**, was seine **Mitarbeiter** den lieben langen Tag so machen. Es bedurfte einiger Gespräche, bis eine Regelung gefunden wurde, die es sowohl den Bediensteten wie auch der Amtsleitung ermöglichte, ihre Arbeit sinnvoll zu verrichten und zugleich den Datenschutz zu beachten.

4.7.2 Wer ist jetzt eigentlich für die Sozialhilfe zuständig?

Sind es nun die Kreissozialämter oder die Sozialämter der Gemeinden, Amtsverwaltungen oder kreisangehörigen Städte, die die Verantwortung für die Datenverarbeitung im Bereich der Sozialhilfegewährung tragen? Der Schleswig-Holsteinische Landkreistag hat seine Position festgelegt. Ob diese Auffassung auch vom Schleswig-Holsteinischen Gemeindetag geteilt wird, ist noch unklar.

Wir erinnern uns: Im letzten Tätigkeitsbericht (Tz. 4.7.5) schilderten wir, dass das Bundessozialhilfegesetz die Kreise und kreisfreien Städte als Träger der Sozialhil-

fe bestimmt. Um Sozialhilfe **bürgernah** zu gewähren, können sie sich der Hilfe der Gemeinden bedienen. Von dieser Möglichkeit haben in Schleswig-Holstein alle Kreise Gebrauch gemacht. Ein Bürger kann den Antrag also vor Ort in seiner Gemeinde stellen, erhält von hier den Bescheid und die Leistung. Lange Wege zum Kreissozialamt entfallen. Aus der Sicht des Bürgers ist folglich die **Gemeinde** Daten verarbeitende und damit **die verantwortliche Stelle** und nicht nur eine „Außenstelle" des Kreissozialamtes. Nach unserer Erfahrung sind die Gemeinden durchaus bereit, diese Verantwortung für die Sozialhilfegewährung und die hierfür erforderliche Datenverarbeitung zu übernehmen.

Genau solche praxisgerechten Lösungen sehen auch die gesetzlichen Bestimmungen vor. So ist den Ausführungsgesetzen der Länder zum Bundessozialhilfegesetz zu entnehmen, dass mit der Übertragung der Aufgaben auf die Gemeinden auch die Verantwortung übertragen wird. Wie im letzten Tätigkeitsbericht dargelegt, ist dies zudem eine datenschutzgerechte Lösung. In **Schleswig-Holstein** gibt es jedoch eine **gesetzliche Besonderheit**. Nach dem Ausführungsgesetz zum Bundessozialhilfegesetz kann ein Kreis bestimmen, dass die Gemeinden zur generellen Aufgabenerfüllung herangezogen werden, **ohne** dass diese gleichfalls die **Verantwortung** hierfür übernehmen. In der Gesetzesbegründung wird ausgeführt, dass hiervon nur „vorwiegend" im Einzelfall Gebrauch zu machen ist.

Die Praxis sieht in Schleswig-Holstein aber anders aus. Zehn von elf **Kreisen** lassen zwar die „Arbeit" von den Gemeinden verrichten, wollen aber selbst **Herr des Verfahrens** bleiben. Nach eingehender Prüfung bestätigte der Schleswig-Holsteinische Landkreistag diese aus seiner Sicht rechtmäßige Vorgehensweise als sinnvoll. Die Form der Heranziehung ist für eine Vielzahl von Fragestellungen von großer **Bedeutung**, u. a. für

- die Weitergabe von Sozialhilfeakten innerhalb des Kreises,
- die Führung einer einzigen Sozialhilfeakte im Kreisgebiet,
- die Einführung von EDV in den Sozialämtern,
- die Kontrolle der Sozialhilfesachbearbeitung,
- die Erteilung von Weisungen durch die Kreise,
- die Zugriffsmöglichkeit der Kreise auf elektronisch geführte Daten in den Kommunen,
- die Gestaltung von Formularen, Bescheiden und Briefbögen und
- die Adressierung datenschutzrechtlicher Beanstandungen durch unsere Dienststelle.

Wir waren zunächst der Auffassung, dass die Gemeinden im Rahmen der Sozialhilfe selbstständig handeln. Nach Auffassung des Schleswig-Holsteinischen Landkreistages obliegt es jedoch allein den Kreissozialämtern, die entsprechenden Festlegungen zu treffen. Die kreisangehörigen Kommunen müssten sich daran halten. Wir wollten wissen: Was sagen die Gemeinden hierzu? Die Stellungnahme des Gemeindetages steht noch aus.

Was ist zu tun?
Ein Sozialhilfeempfänger muss eindeutig erkennen können, ob der Kreis oder die Gemeinde das Sagen hat. Man muss sich entscheiden, wer nun der Herr und damit Verantwortliche des Verfahrens ist, Kreis oder Gemeinde.

4.7.3 Wie weit darf die Zusammenarbeit zwischen Arbeitsamt und Sozialamt gehen?

Durch ein neues Gesetz zur Verbesserung der Zusammenarbeit sollen Sozial- und Arbeitsämter gemeinsam arbeitslosen Leistungsempfängern bessere Unterstützungen bei der Eingliederung ins Arbeitsleben geben können – ein vernünftiger Ansatz, der Synergieeffekte verspricht. Bei der Umsetzung wurde die Praxis vor Ort aber vom Gesetzgeber mit den Problemen allein gelassen. Zusammen mit den beteiligten Stellen erarbeiten wir datenschutzgerechte Lösungen.

Arbeitsverwaltung und Sozialhilfegewährung unterscheiden sich **in wesentlichen Punkten**. Das gilt es zu berücksichtigen, will man die Zusammenarbeit der Ämter verbessern und nicht behindern. Das Sozialamt hat primär die Aufgabe der Sicherstellung des lebensnotwendigen Unterhaltes; das Arbeitsamt hingegen ist für die Arbeitsförderung zuständig. Das örtliche Arbeitsamt unterliegt als Teil der Bundesanstalt für Arbeit der Kontrolle des Bundesarbeitsministers, die Sozialhilfegewährung ist dagegen eine kommunale Selbstverwaltungsaufgabe der Kreise und kreisfreien Städte, die der Aufsicht des Landes unterliegt.

Bundesweit haben sich ca. 30 Arbeits- und Sozialämter zu Modellvorhaben zusammengefunden, drei davon in Schleswig-Holstein. Unter der Bezeichung **MoZART** werden hier Arbeitssuchende beraten und vermittelt. Dies ist eigentlich kein Problem: Man setzt einfach von jedem Amt einige Mitarbeiter gemeinsam in einen Raum. Dann aber kommen die Fragen: Wie erhalten diese Mitarbeiter Kenntnis von Fällen, die sie beraten und vermitteln können? Welche Daten über diese Personen dürfen erhoben werden? Was passiert, wenn sich ein Leistungsempfänger partout nicht beraten und vermitteln lassen will? Wann dürfen personenbezogene Daten an potenzielle Arbeitgeber übermittelt werden? Dürfen Bedienstete des Sozialamtes die Datenbestände des Arbeitsamtes einsehen und umgekehrt? Wo und für wie lange dürfen die Daten des Modellpojektes gespeichert werden? Wem gegenüber sind die Betreiber des Modellprojektes verantwortlich und wer übt die Aufsicht und Kontrolle aus? Darf ein Forschungsinstitut Kenntnis von den personenbezogenen Daten erhalten, um festzustellen, welches Modellprojekt zu einer Verbesserung der Zusammenarbeit geführt hat?

Die Mitarbeiterinnen und Mitarbeiter des Projektes „**Tandem**“, das die Landeshauptstadt Kiel im Rahmen von MoZART betreibt, sind sich der datenschutzrechtlichen Sensibilität ihres Handelns bewusst. Ihr Ziel ist es, gemeinsam mit dem Arbeitssuchenden eine erfolgreiche Beratung und Vermittlung zu erreichen. Um hierfür das nötige Vertrauen gewinnen zu können, bedarf es einer umfassenden **Transparenz** des Verwaltungshandelns. Die Leistungsempfänger werden umfassend über das Modellvorhaben informiert. Einen Zwang zur Teilnahme gibt

es nicht. Erst nach deren **Einwilligung** werden die Daten an die Mitarbeiter des Projektes weitergegeben. Bei der Erstellung eines Arbeitnehmerprofils wird der Arbeitssuchende beteiligt. Ihm ist bekannt, welche Daten von ihm erhoben und weitergegeben werden. Für eine effektive Arbeitsberatung und –vermittlung wird mehr als nur der Name und die Anschrift des Betroffenen benötigt: Schul- und Berufsausbildung, das Einkommen und die Schulden, Probleme in der Ehe oder mit den Kindern, Suchterkrankungen, Vorstrafen sind von Bedeutung. Auf subjektive „negative Daten“ wie z. B. zum Erscheinungsbild („gepflegt“, „sauber“), zur persönlichen Einstellung („unmotiviert“, „kommt ständig zu spät“) oder zum Verhalten des Betroffenen („lügt“, „aggressiv“, „unsicher“) wird bewusst verzichtet, um Stigmatisierungswirkungen zu vermeiden.

Gemeinsam mit dem Betroffenen wird ein **Handlungsplan** erstellt. Dieser wird laufend aktualisiert und dem Arbeitssuchenden in Kopie ausgehändigt. Dritte, z. B. potenzielle Arbeitgeber, erhalten zunächst grundsätzlich nur pseudonymisierte Daten übermittelt. Bekunden sie Interesse an einer Person, wird von dieser eine Einwilligung zur Weitergabe der Daten eingeholt. Bei Tandem selbst werden Daten nur solange gespeichert, wie dies für die Beratung und Vermittlung erforderlich ist. Hat der Betroffene eine Arbeit gefunden, so werden seine Daten nach sechs Monaten gelöscht. Insoweit ist das Projekt vorbildlich.

Leider mussten wir bei unseren weiteren Recherchen feststellen, dass die datenschutzfreundlichen Lösungen weder bei den anderen Projekten im Lande noch in den anderen Ländern selbstverständlich sind. Kritikwürdig ist zudem die **Einbindung aller Projekte** in die größeren Zusammenhänge: So ist es weder fachlich erforderlich noch zulässig, dass die Projektmitarbeiter einen bundesweiten Zugriff auf alle Falldaten der Bundesanstalt für Arbeit (von München bis Flensburg) bzw. auf alle Sozialhilfefälle der jeweiligen Kommune haben. Zum Zwecke der bundesweiten Evaluierung sind außerdem nur anonymisierte Daten zu übermitteln.

Was ist zu tun?
Bei der Durchführung von Modellvorhaben nach dem Gesetz zur Verbesserung der Zusammenarbeit von Arbeitsämtern und Trägern der Sozialhilfe sind von der Praxis Verfahrensweisen zur Sicherung des Sozialdatenschutzes zu entwickeln und umzusetzen, da das Gesetz selbst dafür keine brauchbaren Festlegungen enthält.

4.7.4 Automation bei den Sozialämtern

Bei der Einführung einer neuen Software in Sozialämtern gilt, dass nicht alles, was technisch möglich erscheint, auch fachlich sinnvoll und datenschutzrechtlich zulässig ist.

Die Aufgabe der Sozialhilfegewährung ist vielseitig: Hilfe zum Lebensunterhalt, Hilfe in besonderen Lebenslagen, Hilfe zur Arbeit ... Mal ist es das Land, mal das Kreissozialamt und häufig die Kommune, welche die Hilfen gewährt. Soll sie effektiv, effizient und bürgernah erfolgen, sind nicht nur geschulte Bedienstete,

sondern auch eine kompakte Sozialhilfesoftware nötig. Die Kreissozialämter in Schleswig-Holstein haben deshalb im vergangenen Jahr beschlossen, gemeinsam eine passende Software zu suchen. Unter Beteiligung des Ministeriums für Arbeit, Soziales, Gesundheit und Verbraucherschutz, das auch finanzielle Unterstützung in Aussicht stellte, wurde eine Arbeitsgruppe gebildet, um ein Anforderungsprofil zu definieren. Mit **einheitlicher Software** würde auch die Auswertung zum Zweck der Berichterstattung ans Ministerium vereinfacht.

Nach dem Motto: „Kann es nicht ein wenig mehr sein?“ scheint so mancher Teilnehmer an der Arbeitsgruppe vor Begierde glänzende Augen bekommen zu haben. Sollte die bisher benutzten Programme nur die Sozialhilfe berechnen, so soll nun durch entsprechende **Eingabefelder, Auswertungsprogramme und Schnittstellen** umfassende Personenprofile erstellt werden können. Es wäre danach theoretisch möglich gewesen, per Mausklick festzustellen, ob blonde Frauen eine schlechtere Schulbildung haben oder wie viel Prozent der Hilfeempfänger ungepflegt aussehen oder lügen. Über Schnittstellen hätten solche Daten kreis- und landesweit verglichen oder an dritte Stellen, wie Vermittlungs- und Beratungsgesellschaften übermittelt werden können.

Diese ausgefallenen Wünsche hätte das Verfahren **LÄMMkom**, das von der überwiegenden Zahl der Sozialämter favorisiert wurde, erfüllen können. Von einigen Sozialämtern um Prüfung gebeten, haben wir es im engen Kontakt mit dem Ministerium unter Berücksichtigung des Sozialdatenschutzes bewertet. Hinsichtlich des **Umfangs der dabei möglichen Datenerhebung**, so z. B. zur Erstellung eines Arbeitnehmerprofiles, wurden sich alle Beteiligten einig, dass so genannte negative Merkmale für die Aufgabenerfüllung nicht erforderlich sind und damit deren Erhebung datenschutzrechtlich unzulässig ist. Der Datenkatalog wurde im Einzelnen geprüft. Eine „geprüfte Version“ liegt dem Ministerium vor.

LÄMMkom ist ein flexibles System, in dem Datenfelder vom Anwender frei und eigenverantwortlich definiert werden können. Zur Vermeidung des Einsatzes datenschutzwidriger Versionen haben wir der Firma die **Zertifizierung** ihres Produktes angeraten. So können Käufer sichergehen, ein geprüftes System einzusetzen.

Was ist zu tun?
Vor Einsatz einer neuen komplexen Sozialhilfesoftware muss von den behördlichen Datenschutzbeauftragten eine Vorabkontrolle bezüglich der Vereinbarkeit mit dem Sozialdatenschutz vorgenommen werden. Produkte, deren Vereinbarkeit mit den Vorschriften in einem förmlichen Verfahren festgestellt wurde, sollen vorrangig eingesetzt werden.

4.7.5 Rundfunkgebührenbefreiung – die dritte

In Anträgen zur Befreiung von der Gebührenpflicht dürfen von den Rundfunkanstalten nur die hierfür erforderlichen Daten erhoben werden. In einer Pilotphase wird ein neues Online-Antragsverfahren erprobt.

In den letzten zwei Tätigkeitsberichten (22. TB, Tz. 4.8.3 und 23. TB, Tz. 4.7.6) berichteten wir über das pauschale Misstrauen des NDR gegenüber Studierenden bei der Beantragung der Befreiung von Rundfunkgebühren. Auf „Heller und Pfennig“ sollten diese auf einem **Fragebogen** ihre Ausgaben, z. B. Telefon-, Kabel-, Internet-Gebühren und vieles mehr ausweisen. Derart in die Tiefe gehen noch nicht einmal Sozialämter und Finanzämter, obwohl es bei ihnen um wesentlich mehr Geld geht.

„Angriff ist die beste Verteidigung“ – mag man sich beim NDR gedacht haben, als der bisher nur für Studierende vorgesehene, viel zu detaillierte Fragebogen zur Pflicht für alle Antragstellenden gemacht wurde. Zudem zeigte man sich modern und entwickelte ein **elektronisches Online-Verfahren**, ohne aber auf die Substanz unserer datenschutzrechtlichen Kritik einzugehen. Erst nach einigen gemeinsamen Gesprächen wurde eine Lösung erzielt, die für alle Beteiligten tragbar ist:

Das neue Online-Verfahren wird als **Pilotverfahren** eingeführt. Dabei werden die datenschutzrechtlich bedenklichen (Plausibilitäts-)Daten zunächst im Sozialamt erfragt, im Falle einer Befreiung aber nicht gespeichert. Eine Übermittlung dieser Daten an den NDR erfolgt nur in jenen Zweifelsfällen, in denen der NDR die weitere Bearbeitung der Anträge übernimmt. Verbessert wurden zudem die Einwilligungserklärung und die Sicherheit bei der Datenübermittlung. Bestimmte Datenfelder, z. B. zu alten Anschriften des Antragstellers, wurden gänzlich gestrichen. In der Pilotphase wird statistisch erfasst, wie viele Anträge gestellt, positiv bzw. negativ beschieden und in welchen Fällen die Plausibilitätsdaten tatsächlich für eine Entscheidungsfindung beim NDR benötigt wurden.

Was ist zu tun?
Nach Abschluss der Pilotphase Ende 2002 werden sich alle Beteiligten erneut an einen Tisch setzen und darüber entscheiden müssen, ob das Verfahren zur Befreiung von der Rundfunkgebührenpflicht datenschutzrechtlich weiter verbessert werden kann.

4.8 Schutz des Patientengeheimnisses

4.8.1 Für die Gesundheitsämter gilt ein neues Gesetz

Beim öffentlichen Gesundheitsdienst gibt es endlich gesetzliche Regeln für die Verarbeitung von Gesundheitsdaten. Nach jahrelangem Zögern verabschiedete der Landtag ein Gesundheitsdienstgesetz (GDG).

Das Gesetz verbessert den Schutz der Gesundheitsdaten der Bürgerinnen und Bürger. Sie dürfen nur zweckgebunden verwendet werden. Das **Zweckbindungsprinzip** gilt auch innerhalb der Gesundheitsämter und muss durch entsprechende Abschottungen gewährleistet werden. Die „Kunden“ des Gesundheitsamtes sollen darauf vertrauen können, dass das Beratungsgeheimnis beachtet wird. Eine zweckändernde Nutzung der Daten ist nur dann erlaubt, wenn es um schwere Gefahren für Leben, Gesundheit und Freiheit oder um die Verfolgung von Verbrechen geht.

Deshalb war ein Petent zu Recht erstaunt, als er in der Auseinandersetzung mit seinem Finanzamt über die Anerkennung von medizinisch angezeigten Thermalbadbesuchen als „außergewöhnliche Belastung“ erfahren musste, dass sich die Finanzbeamtin an ihm vorbei ein Bild über den Gesundheitszustand direkt beim Gesundheitsamt verschaffte. Neben dem GDG bleiben die Regelungen des LDSG anwendbar. Dies bedeutet, dass Auskünfte des Gesundheitsamtes an andere Stellen in der Regel der Einwilligung des Betroffenen bedürfen. Dies gilt auch gegenüber dem **Finanzamt**, wenn dieses beispielsweise Rückfragen zu einem mit der Steuererklärung eingereichten amtsärztlichen Attest hat.

Erstmals wird in dem Gesundheitsdienstgesetz auch die **Gesundheitsberichterstattung** als eine spezielle Form medizinischer Statistik vorgesehen. Vorrang hat dabei die Sammlung nicht personenbezogener gesundheitsrelevanter Daten. Auf unseren Vorschlag hin wird bei der Nutzung personenbezogener Patientendaten das Statistikrecht angewandt. Dessen Regelungen gewährleisten aufgrund des Statistikgeheimnisses die Vertraulichkeit der Daten und insbesondere die Abschottung der Statistikaktivitäten von den sonstigen Aufgaben in den Gesundheitsämtern. Die personenbezogenen Merkmale müssen so früh wie möglich von den epidemiologischen Daten getrennt werden. Eine Auskunftspflicht gegenüber Dritten ist ausdrücklich ausgeschlossen.

Was ist zu tun?
Die Regelungen des GDG zwingen nicht zu einer grundlegenden Revision der Datenverarbeitung in den Gesundheitsämtern. Das neue Gesetz sollte aber zum Anlass genommen werden, den Mitarbeitern dieser Ämter ihre besondere Verschwiegenheitspflicht in Erinnerung zu rufen.

4.8.2 Gesundheitschipkarten

Bei der Reformierung des Gesundheitssystems haben nur solche Pläne eine Chance auf Realisierung, die mit dem Patientengeheimnis vereinbar sind.

Die Kostenexplosion und die Vielzahl der „Player" in unserem Gesundheitssystem mit teilweise diametral entgegengesetzten materiellen Interessen führt dazu, dass ein Patentrezept nach dem anderen öffentlich präsentiert wird und nach gehöriger Kritik wieder verschwindet. Viele dieser Rezepte zur Gesundung des Gesundheitswesens basieren auf der Idee der **Datensammlung über Patientinnen und Patienten** und der Hoffnung auf die Automation und Rationalisierung der sehr teuren administrativen Abläufe. Das Hausarztmodell und die integrierten Versorgungskonszepte wurden im Jahr 2000 eingeführt. Der zeitgleich gestartete Versuch der Schaffung von mehr Kostentransparenz scheiterte zunächst am Bundesrat und seitdem am Widerstand der Krankenkassen (vgl. 23. TB, Tz. 4.8.5). Das elektronische Rezept soll Abrechnungsabläufe beschleunigen und die Verschreibungspraxis durchsichtiger machen. Mithilfe einer elektronischen Patientenakte sollen Mehrfachuntersuchungen vermieden werden.

Was bei all diesen Plänen und den Diskussionen in der Regel zu kurz kommt, sind die Interessen der Patienten. Fast alle erörterten Maßnahmen greifen in deren informationelles Selbstbestimmungsrecht ein, in ihre Rechte auf freie Arztwahl und auf Wahrung ihres Patientengeheimnisses. Die **Datenschutzbeauftragten** verstehen sich als Vertreter dieser **Patienteninteressen**.

Eines der oben genannten Projekte ist die von der Bundesgesundheitsministerin geforderte **obligatorische Gesundheitschipkarte**. In die Diskussion eingeführt wurde diese Arzneimittelkarte als Antwort auf einen Medikamentenskandal, doch mutierte sie schnell zu einem umfassenden Pflichtpass, auf dem neben den Identifizierungsangaben und Medikationen auch Notfalldaten, Allergien, Impfungen und viele weitere medizinische Angaben gespeichert werden sollen. Wiederholt mussten wir darauf hinweisen, dass es das ureigene Recht der Patienten ist selbst zu entscheiden, wem sie welche ihrer sensibelsten Daten anvertrauen. Eine Ausgabe an alle Kassenmitglieder verbunden mit einer Vorlagepflicht wäre damit nicht vereinbar. Die Pläne sehen zudem die Schaffung eines zentralen Registers mit den Gesundheitsdaten von 90% der Bevölkerung vor – ein Datenbestand, der gewaltige Begehrlichkeiten auslösen würde. Wir lehnen einen **Patientenausweis** nicht grundsätzlich ab. Doch muss die Freiwilligkeit bei der Verwendung gesichert bleiben.

Was ist zu tun?
Es ist beides zu realisieren: Kosteneinsparungen im Gesundheitswesen und ein effizienter Schutz des Patientengeheimnisses.

4.8.3 Neues EDV-System für die Krankenkassen

Die Krankenkassen sind derzeit dabei, ihre elektronische Datenverarbeitung zu modernisieren. Soll es nicht zu einem Desaster kommen wie bei anderen großen Verwaltungsverfahren, so müssen Datenschutz und Datensicherheit von Anfang an eine zentrale Rolle spielen.

Von Kollegen anderer Bundesländer erfuhren wir von den Plänen der Allgemeinen Ortskrankenkassen, gemeinsam mit dem AOK-Bundesverband und einer „outgesourcten" AOK-Systems GmbH das ca. 20 Jahre alte EDV-System IDVS II durch ein modernes Verfahren mit dem Kürzel SAM (SAP-AOK-Master) zu ersetzen. Aus Datenschutzsicht ist dies sehr zu begrüßen, da das alte Verfahren aktuellen Datenschutznotwendigkeiten, z. B. Protokollierungsanforderungen, nicht gerecht wird (vgl. 23. TB, Tz. 4.8.7). Auch im Hinblick auf die weitgehenden Pläne der Bundesregierung zur Verbesserung der Kostentransparenz im Gesundheitswesen sind neben neuen Auswertungs- auch **neue Schutzmechanismen**, z. B. die Etablierung einer pseudonymisierten Datenverarbeitung, ein absolutes Muss. Das AOK-Projekt erhält eine noch größere Bedeutung dadurch, dass offensichtlich auch andere Kassen erwägen, das EDV-Verfahren zu übernehmen.

Die Etablierung derart großer zentraler Gesundheitsdatenbanken mit vielfältigen Auswertungs- und Nutzungsmöglichkeiten kann nur dann erfolgreich sein, wenn von Anfang an deren Rechtmäßigkeit und hier insbesondere der **Schutz des Patientengeheimnisses integrierter Verfahrensbestandteil** ist. Welches – auch finanzielles – Desaster entstehen kann, wenn Aspekte des Datenschutzes und der Datensicherheit in der Projektphase ignoriert werden, haben wir bei den anderen beiden EDV-Großprojekten – im Bereich der Polizei und der Finanzverwaltung – gesehen. Daher haben die Datenschutzbeauftragten des Bundes und der Länder angeboten, die Planungen von Anfang an zu begleiten. Leider liegt hierzu bisher seitens der Krankenkassen keine positive Resonanz vor.

Was ist zu tun?
Die Projektplaner sollten sich dessen bewusst werden, dass eine ausreichende Integration des Datenschutzes in die neuen Krankenkassensysteme eine Voraussetzung für deren Einführung ist.

4.8.4 Outsourcingaktionen bei Krankenkassen – die nächste, bitte?

Sozialdaten sind keine normalen Daten, deren Verarbeitung so ohne weiteres an Dritte, eventuell gar Private, übertragen werden kann und darf. Diese Erkenntnis muss auch – bei allem Verständnis für Einsparungen – bei den Krankenkassen gelten. Letztlich geht es dabei um die Sicherung des Vertrauens der Kassenmitglieder.

Die Anfrage der AOK, ob die **Rechnungsprüfung** durch eine Kasse in einem anderen Land wahrgenommen werden kann, konnten wir im Hinblick auf die Regelungen zur Auftragsdatenverarbeitung von Leistungsträgern positiv beschei-

den: Es können danach sogar ganze Bereiche der Sachbearbeitung an andere Sozialleistungsträger ausgelagert werden, was einer Funktionsübertragung gleichkommt und keine „Datenverarbeitung im Auftrag“ ist (vgl. 23. TB, Tz. 4.8.7). Werden Rechnungen auf ihre inhaltliche Begründetheit hin überprüft, ist dabei Schriftwechsel nötig und trifft die letztendliche Entscheidung der Auftragnehmer, so müssen aber „**Private**“ ausgeschlossen bleiben. Stehen bei der Prüfung von eingereichten Rechnungen dagegen rein manuelle oder technische Aktivitäten im Vordergrund wie z. B. Erfassung der Daten sowie Feststellung der Plausibilität, so kann dies als Auftragsdatenverarbeitung unter Umständen auch an Private übertragen werden; der Auftraggeber bleibt in diesem Fall voll verantwortlich.

Im Wortlaut:
§ 80 Sozialgesetzbuch X
Verarbeitung von Sozialdaten im Auftrag

(1) Werden Sozialdaten im Auftrag durch andere Stellen verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften verantwortlich. ...

(2) Eine Auftragserteilung für die Verarbeitung und Nutzung von Sozialdaten ist nur zulässig, wenn der Datenschutz beim Auftragnehmer den Anforderungen genügt, die für den Auftraggeber gelten. Der Auftrag ist schriftlich zu erteilen, wobei die Datenverarbeitung und -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Der Auftraggeber ist verpflichtet, erforderlichenfalls Weisungen zur Ergänzung der beim Auftragnehmer vorhandenen technischen und organisatorischen Maßnahmen zu ergreifen. ...

(4) Der Auftragnehmer darf die zur Datenverarbeitung überlassenen Sozialdaten nicht für andere Zwecke verarbeiten und nutzen und nicht länger speichern, als der Auftraggeber schriftlich bestimmt. ...

Verwundert waren wir, als wir davon Kenntnis erhielten, dass die **Durchsetzung von Schadensersatzansprüchen** von Krankenkassen nach Ansicht der Aufsichtsbehörden des Bundes und der Länder auf private Firmen übertragen werden dürfe. Aus datenschutzrechtlichen Gründen können die Kassen natürlich nicht daran gehindert werden, ihnen zustehende finanzielle Forderungen durchzusetzen. Dies kann im Konfliktfall auch die Einschaltung eines Rechtsanwaltes – der selbst einer beruflichen Schweigepflicht unterworfen ist – notwendig machen. Die Übertragung des Inkasso an eine private Firma zum vorgerichtlichen Forderungseinzug und die damit zwangsläufig verbundene Mitteilung von Sozialdaten in zumeist heiklen Einzelfällen hat der Gesetzgeber aber nicht erlaubt. Diese einheitliche Rechtsauffassung der Datenschutzbeauftragten des Bundes und der Länder konnte auch gegenüber den Aufsichtsbehörden durchgesetzt werden.

Was ist zu tun?
Trotz des Kostendrucks muss das Sozialgeheimnis bundesweit nach einheitlichen Maßstäben gegen unzulässige Privatisierungen verteidigt werden.

4.8.5 Der Gutachtenauftrag eines schweizerischen Rentenversicherungsträgers

Wenn aus gesundheitlichen Gründen eine Sozialleistung beantragt wird, benötigt der Sozialleistungsträger in der Regel ärztliche Atteste als Nachweis der Bedürftigkeit. Werden externe Gutachter mit der Prüfung der vorgelegten Atteste beauftragt, so muss der Antragsteller in die Übermittlung seiner Sozialdaten schriftlich einwilligen.

Ein Bundesbürger, der seit Jahren eine kleine Rente aus der Schweiz erhielt, war nicht wenig erstaunt, als er Post von der **Landesversicherungsanstalt Schleswig-Holstein** (LVA) erhielt. Wegen eines „Rentenantrages" solle er Atteste seines behandelnden Arztes an eine ihm nicht bekannte Hamburger Arztpraxis übersenden, damit diese eine umfassende medizinische Begutachtung durchführen könne. Auf seine telefonische Nachfrage bei der LVA, mit der er sonst nichts zu tun hatte, ob hier ein Büroversehen vorläge, erhielt er lapidar die Mitteilung, das werde schon seine Richtigkeit haben. Man wisse nur, dass der **Begutachtungsauftrag** von der LVA Baden-Württemberg käme. Von dort erfuhr er, dass die Schweizer Rentenanstalt die BfA und diese wiederum die LVA Baden-Württemberg um eine kardiologische Untersuchung gebeten hatte. Dies sei ein übliches Verfahren, wenn ein Bundesbürger aus der Schweiz eine Rente bezieht. So werde Bürgernähe sichergestellt. Es ging also nicht um einen neuen Rentenantrag, sondern um die Frage, ob die Rente unverändert weitergezahlt werden konnte.

Im Wortlaut:
§ 88 Sozialgesetzbuch X
Auftrag

(1) Ein Leistungsträger (Auftraggeber) kann ihm obliegende Aufgaben durch einen anderen Leistungsträger oder seinen Verband (Beauftragter) mit dessen Zustimmung wahrnehmen lassen, wenn dies

1. wegen des sachlichen Zusammenhangs der Aufgaben vom Auftraggeber und Beauftragten,
2. zur Durchführung der Aufgaben und
3. im wohl verstandenen Interesse der Betroffenen zweckmäßig ist. ...

(4) Der Auftraggeber hat einen Auftrag für gleich gelagerte Fälle in der für seine amtlichen Veröffentlichungen vorgeschriebenen Weise bekannt zu geben.

Der Petent war zu Recht verärgert. Hatten doch vier Rentenversicherungsträger mit seinen Patientendaten „**Stille Post**" gespielt. Aus einer kardiologischen Untersuchung war dabei eine vollständige medizinische Untersuchung geworden. Wie ein Detektiv musste er den wahren Grund des Schreibens bei diversen Stellen ermitteln. Ohne ihn vorher zu fragen, waren seine Daten an eine Hamburger Arztpraxis übermittelt worden. Besonders ärgerlich war, dass sein eigener Arzt gerade erst eine kardiologische Untersuchung durchgeführt hatte und diese Untersuchungsergebnisse ausreichten – wie sich im Verlaufe unserer Prüfung herausstellte – um die Fragen der Schweizer Rentenanstalt zu beantworten. Eine zusätzliche – schmerzhafte und belastende – Begutachtung war also gar nicht nötig. Hätte man doch nur einmal vorher gefragt!

Die Schuld lag nicht nur bei der LVA Schleswig-Holstein. Auch künftig werden ärztliche Gutachten notwendig sein und Rentenversicherungsträger sich gegenseitig unterstützen. Doch muss dem betroffenen Rentenempfänger genau erläutert werden, warum und auf wessen Ersuchen hin eine Begutachtung durchgeführt werden muss. Wird der **Betroffene aktiv am Verfahren beteiligt**, kann er bereits vorhandene Unterlagen vorlegen, um unnötige Untersuchungen und Kosten zu vermeiden. Die Übermittlung von Daten an einen externen Gutachter bedarf generell der Einwilligung des Betroffenen. In jedem Fall muss dieser über die beabsichtigte Übermittlung seiner Sozialdaten unterrichtet werden, sodass er Gelegenheit hat, der beabsichtigten Datenübermittlung zu widersprechen. Eine Reaktion der LVA Schleswig-Holstein auf unsere Vorschläge für ein praxisnahes und zugleich datenschutzgerechtes Verfahren liegt uns noch nicht vor.

Was ist zu tun?
Sozialverwaltungsverfahren sind bezüglich Zweck, Inhalt und Beteiligte transparent zu gestalten. Bei der Einschaltung externer Gutachter und der damit bedingten Übermittlung von Sozialdaten bedarf es der Einwilligung des Betroffenen, zumindest aber der vorherigen Unterrichtung mit Einräumung eines Widerspruchsmöglichkeit.

4.8.6 Die Arztrechnung von der Privatfirma – Variationen über ein Thema

Medizinische Daten über einen Patienten dürfen an Dienstleister nur übermittelt werden, wenn dieser hierüber zuvor unterrichtet wurde und seine Einwilligung schriftlich erklärt hat.

Im letzten Tätigkeitsbericht (vgl. 23. TB, Tz. 4.8.4) erläuterten wir die Notwendigkeit, dass sich die Ärzte um die Einwilligung ihrer Patienten bemühen, wenn sie eine privatärztliche Verrechnungsstelle bei der Abrechnung einschalten wollen. Eine neue Variante des gleichen Themas: Eine Frau erhielt die **Rechnung eines Taxiunternehmens**, das eine Gewebeprobe von ihr von einem öffentlichen Krankenhaus zu einem externen Labor chauffiert hatte. Die Taxifirma hatte vom Arzt ein Privatrezept mit den auf Rezepten üblichen personenbezogenen Angaben überreicht bekommen, auf dem der Transport an das externe Labor verordnet wurde. Unsere Petentin kannte weder den Auftrag noch das Taxiunternehmen.

Die ärztliche Schweigepflicht verbietet das Offenbaren von Patientengeheimnissen. Bereits die Tatsache, dass sich ein Patient in die Behandlung eines bestimmten Arztes begibt, unterliegt der ärztlichen Schweigepflicht. Die Übergabe eines anonymen verschnürten Päckchens mit der Gewebeprobe allein ist kein Problem. Mit dem Rezept wurden jedoch auch **Behandlungsdaten unzulässig offenbart**. Eine direkte Taxi-Abrechnung mit der Patientin wäre nur mit deren Einwilligung möglich gewesen. Einfacher ist es aber, wenn das Krankenhaus zunächst die Taxi-Kosten übernimmt, um sie danach mit der Patientin abzurechnen. Nach unserer Intervention gegen den Datenschutzverstoß ging das Krankenhaus genau diesen Weg.

Was ist zu tun?
Bevor ein Krankenhaus oder ein Arzt patientenbezogene Leistungen an Dritte vergibt, muss der Patient hierüber aufgeklärt werden und einwilligen. Unproblematisch ist es, wenn das Outsourcing anonym und die Abrechnung über den Auftraggeber erfolgt.

4.8.7 Missbrauch von Patientendaten in Apotheken

Die Überprüfung einer Apotheke führte zur Aufdeckung eines bundesweiten Patientendatenmissbrauchs durch Apotheken und deren Rechenzentren. Auch viele der schleswig-holsteinischen Apotheken waren beteiligt.

Die meisten Apotheken rechnen mit den Krankenkassen heute nicht mehr selbst ab, sondern nehmen hierfür die Angebote von **Apothekenrechenzentren** in Anspruch. Monatlich werden alle angefallenen Rezepte des Abrechnungszeitraumes gebündelt an ein solches Zentrum geschickt, das die Daten nach Krankenkassen sortiert und mit diesen die **Kostenerstattung** abwickelt. Der Apotheker bekommt direkt vom Rechenzentrum – abzüglich einer Bearbeitungsgebühr – einen Betrag überwiesen. So weit, so zulässig, so gut.

Im Wortlaut:
§ 300 Abs. 2 Sozialgesetzbuch V

Die Apotheken ... können zur Erfüllung ihrer Verpflichtungen ... Rechenzentren in Anspruch nehmen. Die Rechenzentren dürfen die Daten für im Sozialgesetzbuch bestimmte Zwecke verarbeiten und nutzen, soweit sie dazu von einer berechtigten Stelle beauftragt worden sind; anonymisierte Daten dürfen auch für andere Zwecke verarbeitet und genutzt werden.

Weil die dabei anfallenden **millionenfachen Patientendaten** auch noch anderweitig Gewinn bringend genutzt werden könnten, haben die unterschiedlichen Rechenzentren Systeme ausgeklügelt, die sich nur wenig unterscheiden: Sämtliche Patientendaten einer Apotheke werden, versehen mit einem Anwenderprogramm, auf CD gebrannt und an die Apotheken zurückverkauft. Diese sind so in der Lage, die Daten ihrer Kundinnen und Kunden auf ihren Computern zu speichern und nach verschiedenen Kriterien zu „**katalogisieren**“. So haben sie den Überblick, ob Frau Meier vor sechs Jahren das Medikament der einen oder der anderen Firma in welcher Menge und von wem verordnet bekam. Sie können „gute Kunden“ durch Aufmerksamkeiten an sich binden. Sie können erkennen, welche Ärzte für welchen Umsatz in ihrer Apotheke sorgen und welche Patienten sie behandeln. Sie können feststellen, welche Patienten eines Straßenteiles zu dem einen oder zu dem anderen Arzt gehen. Eine Auswertung nach speziellen Medikamenten – z. B. Antidepressiva – eröffnet interessante weitere Einsichten. Die am Jahresende auszustellenden kundenbezogenen Zuzahlungsquittungen für Kassenpatienten sind im Anwenderpaket inbegriffen. Und von alledem ahnt der Patient gar nichts.

Verblüfft hat uns, dass zunächst weder vonseiten der Apotheker noch von den Rechenzentren Problembewusstsein gezeigt wurde. Die Letzteren verwiesen da-

rauf, sie hätten doch die Einwilligung der Ersteren. Dass hier **Patienten betroffen** sind und diese Praxis keine rechtliche Grundlage hat, musste erst in zähen Verhandlungen klar gemacht werden. Gemeinsam mit dem Bremer Datenschutzbeauftragten erreichten wir schließlich beim **Norddeutschen Apothekenrechenzentrum (NARZ)** in Bremen, das den größten Teil der Apotheken im Land Schleswig-Holstein unter Vertrag hat, dass die CDs in der bisherigen Fassung nicht mehr vertrieben und die alten Datenscheiben von den Apotheken zurückverlangt werden. Die meisten Apotheken des Landes haben dieser Rückrufaktion auch Folge geleistet.

In Schleswig-Holstein wird es beim NARZ wenigstens nur noch mit der Versichertennummer pseudonymisierte CDs zu kaufen geben. Nach unserer Rechtsauffassung kann die personenbezogene Übermittlung der Patientendaten durch die Apotheken an das Rechenzentrum zwecks Aufbereitung und Rückgabe an sie zur weiteren Nutzung wegen der abschließenden gesetzlichen Regelung im SGB auch nicht durch Patienteneinwilligungen legitimiert werden. Die Rechenzentren dürfen danach die Patientendaten **nur zur Abrechnung** mit den Krankenkassen nutzen.

Was ist zu tun?
Unser Ziel wird es sein, auch bei den anderen für Apotheken in Schleswig-Holstein agierenden Rechenzentren auf die Herausgabe einer datenschutzgerechten CD hinzuwirken.

4.8.8 Aktion „Datenschutz in meiner Arztpraxis“

Einzelanfragen und Beschwerden zum Patientengeheimnis, zur Einsicht in Patientenunterlagen und zur Datensicherheit im medizinischen Bereich veranlassten uns, gemeinsam mit der Ärzte- und der Zahnärztekammer eine breit und langfristig angelegte Aufklärungskampagne mit dem Titel „Datenschutz in meiner Arztpraxis“ zu initiieren.

In einer ersten Phase wurden sämtliche Zahnärzte und Ärzte im Land angeschrieben, über die Aktion unterrichtet und zur aktiven Teilnahme eingeladen. Unter Zuhilfenahme eines mitversandten Leitfadens sollen in einem **Selbstcheck** etwaige Problempunkte in der Praxis ausfindig gemacht werden. Tauchen dabei rechtliche oder technische Fragen auf, so werden diese in einem ausführlichen Text, der im Internet abrufbar ist, beantwortet. Für individuelle Rückfragen stehen unsere Mitarbeiterinnen und Mitarbeiter und die der Kammern zur Verfügung. Über die DATENSCHUTZAKADEMIE werden **Weiterbildungskurse** angeboten.

In einer zweiten Phase werden die Patientinnen und Patienten sowie die Öffentlichkeit angesprochen. Über ein **Informationsfaltblatt** sowie ein **Plakat** können die Ärztinnen und Ärzte den Datenschutz in ihrer Praxis gegenüber ihren Patienten positiv herausstellen. Die Patienten werden über ihre Rechte informiert und eingeladen, sich selbst aktiv an der Aktion zu beteiligen. Dies kann auch darin bestehen, dass sie ihre Arztpraxen unter Datenschutzgesichtspunkten in Augenschein zu nehmen. Weitere Module der Kampagne sind geplant.

Die Gesundheitsministerin hat die Schirmherrschaft übernommen. Die **Aktion** mit den Kammern unter dem Logo „S[ICH]ER“ wird vom Patientenombutsmann e. V. begleitet.

Sämtliche **Informationen zu der Aktion** werden im Internet zum Abruf bereitgestellt. Und wer keinen Internet-Zugang hat, kann sich ein Skript sowie sonstige Aktionsunterlagen gegen einen Unkostenbeitrag vom ULD zusenden lassen.

www.datenschutzzentrum.de/medizin/

Was ist zu tun?
Die Zahnärzte und Ärzte wie die Patientinnen und Patienten sind eingeladen, sich an der Aktion zu beteiligen. So besteht die Chance, dass im Land möglichst viele datenschutzrechtliche Musterpraxen entstehen.

4.8.9 Vorschläge zur Regelung der Genomanalyse

Die Schwerpunkte der Diskussion über die Gentechnik lagen im vergangenen Jahr zweifellos bei der Frage der Stammzellenforschung und der Präimplantationsdiagnostik. Doch wurden auch hinsichtlich der Zulässigkeit von Genanalysen zu medizinischen, wissenschaftlichen oder privaten Zwecken die ersten Weichen gestellt.

Waren vor wenigen Jahren Datenschutzfragen in Bezug auf die Gentechnik eher akademischer Natur, so hat sich dies in jüngster Zeit dramatisch geändert (vgl. 23. TB, Tz. 4.8.2). An den Universitätskrankenhäusern des Landes laufen nicht nur immer mehr genetische Forschungsprojekte, sondern es entstehen auch projektübergreifende **Genproben-Datenbanken**. Auch im rein kommerziellen Sektor gibt es aus Datenschutzsicht Einiges zu tun (Tz. 4.8.10).

Die **besondere Qualität genetischer Daten** ergibt sich aus ihrer weitgehenden Unveränderbarkeit von der Zeugung an. Die informationelle Selbstbestimmung kann nur dadurch wahrgenommen werden, dass über die Befugnis zum Wissen oder über das Nichtwissen entschieden wird. Aus jeder auch noch so geringen Probe von Speichel, Blut, Haut, Haarwurzel oder Sperma lässt sich mit fortschreitendem Wissensstand immer mehr über jeden einzelnen Menschen ableiten. Bekannt werden nicht nur akute, sondern auch latente Eigenschaften, die unter Umständen erst in Jahren und nur mit einer gewissen Wahrscheinlichkeit zum Tragen kommen. Zudem kommt den Daten Aussagekraft auch in Bezug auf nahe Verwandte zu. Eine Verifikation der Richtigkeit der Daten ist dem Betroffenen nicht selbst möglich; vielmehr muss er sich auf wissenschaftliche Untersuchungen verlassen, deren Aussagekraft äußerst umstritten sein kann. Zwar besteht die Sensibilität in besonderem Maße bei Analyseergebnissen aus dem codierenden Bereich des Genoms. Angesichts des Umstands, dass auch aus dem „nichtcodie-

renden Teil“ Wahrscheinlichkeiten abgeleitet werden können, müssen diese Daten grundsätzlich ebenso behandelt werden.

Das Risiko des Verlustes des informationellen Selbstbestimmungsrechts wird dadurch erhöht, dass von uns bei vielen täglichen Verrichtungen unbemerkt Substanzen zurücklassen werden, die mithilfe einer neuen **Genchip-Technik** immer einfacher untersucht werden können. Derartige Chips, mit denen zigtausend Sequenzabgleiche auf einmal vorgenommen werden, können in absehbarer Zeit in Massenproduktion für Kosten im zweistelligen Euro-Bereich hergestellt werden.

Die Notwendigkeit einer gesetzlichen Regelung auf Bundesebene ist inzwischen unter sämtlichen Beteiligten unstreitig. Sowohl eine Enquetekommission des Bundestags wie auch der Ethikbeirat der Bundesregierung haben sich dieser Fragen angenommen. Die Konferenz der Datenschutzbeauftragten hat eine Stellungnahme für die Bundestagsenquetekommission erarbeitet. Mit einem **gesetzesähnlich ausformulierten Text**, soll die Diskussion zielstrebig vorangebracht werden:

www.datenschutzzentrum.de/medizin/genom/
www.datenschutz-berlin.de/doc/de/konf/62/genuntersuchungen.htm

Derzeit dürfen außerhalb der strafprozessualen Befugnisse von staatlichen Stellen genetische Untersuchungen nur ausdrücklich mit Einwilligung der Betroffenen vorgenommen werden. Auch nach einer gesetzlichen Regelung kommt der Einwilligung (**informed consent**) die zentrale Funktion für die Zulassung der Verarbeitung von Gendaten zu. Während bei der datenschutzrechtlichen Einwilligungserklärung generell eine Aussage zu Zweck, verarbeitender Stelle und Datensatz für eine hinreichende Bestimmtheit genügt, sind bei gentechnischen Einwilligungen zusätzliche Anforderungen zu beachten.

Einer einwilligungsbasierten gentechnischen Untersuchung muss eine **Beratung** vorangehen. Diese muss Informationen über die Fragestellung und die Aussagekraft der Untersuchung enthalten sowie Angaben, inwieweit im Fall einer untersuchten Krankheit dieser vorgebeugt oder diese bekämpft werden kann. Der Ablauf der Untersuchung mit Angaben über die beteiligten Stellen über die Aufbewahrung, den Zeitpunkt einer Anonymisierung bzw. Pseudonymisierung sowie die Löschung der Daten bzw. Vernichtung der Proben muss verständlich dargelegt werden. Sowohl unerwartete Ergebnisse wie auch mögliche familiäre, psychische oder auch körperliche Belastungen müssen, so weit dies möglich ist, bekannt gegeben werden. Auf das **Recht zu Wissen**, den Auskunftsanspruch und auf das **Recht auf Nichtwissen** ist hinzuweisen. Die Beratung muss entscheidungsoffen erfolgen. Schließlich muss auf die Freiwilligkeit und die Widerrufbarkeit der Einwilligung hingewiesen werden.

Nach einer erfolgten Untersuchung muss durch ein gestuftes Verfahren der **Informierung** sichergestellt werden, dass die betroffene Person von ihrem Recht auf Wissen bzw. Nichtwissen in differenzierter Form Gebrauch machen kann. Bei der Interpretation des Ergebnisses ist dessen Komplexität und die Wechselwirkung mit Umweltfaktoren und Verhaltensgewohnheiten offen zu legen.

Werden personenbezogene Daten von nahen **Verwandten** gemeinsam mit der zu analysierenden Gewebeprobe erhoben oder werden sie mit der Probe bzw. dem Analyseergebnis zusammengeführt, so muss die Einwilligung auch dieser Personen vorliegen.

Was ist zu tun?
Unter Einbeziehung des Vorschlages der Datenschutzbeauftragten sollte so bald wie möglich ein Gesetz zur gen-informationellen Selbstbestimmung erarbeitet und nach angemessener öffentlicher Diskussion verabschiedet werden.

4.8.10 Heimlicher Gentest: Ganz der Papi?

Die über Internet und nun auch in Apotheken Schleswig-Holsteins erhältlichen genetischen Vaterschaftstests sind nach unserer Auffassung datenschutzrechtlich unzulässig. Es wird Zeit, dass der Gesetzgeber eingreift.

Ein kanadischer Datenschutzkollege wies uns darauf hin, dass „**Papachecks**“ im Internet auch von einer Firma in Schleswig-Holstein angeboten werden. Angegeben sind dort nur Handynummer und Postfach, aber kein Verantwortlicher oder eine Adresse. Diese konnten wir erst nach beharrlichen Recherchen feststellen. Die Unzulässigkeit des Verfahrens liegt für uns auf der Hand.

Das Verfahren läuft so ab: Der vermeintliche Vater sendet eine Materialprobe von sich und seinem „Kuckuckskind“ bei der Firma ein. Dabei kann es sich um eine Speichel-, Blut- oder Haarprobe handeln oder um aus der Windel „entwendeten“ Kot des Babys. Obwohl der Einsender versichert, dass das Material mit Zustimmung der (mit) sorgeberechtigten Mutter entnommen wurde, muss der Firma klar sein, dass dem nur in wenigen Ausnahmefällen so ist. Das ist aus unserer Sicht der Haken an dem ganzen Verfahren. Solange die Firma keine schriftliche Einwilligung vorliegen hat, muss sie davon ausgehen, dass mit dem Test eine **Persönlichkeitsverletzung des Kindes** erfolgt.

Zweifellos hat ein Mann das Recht zu wissen, ob er zu Recht Unterhalt für ein Kind bezahlt. Hierfür ist ein in der Zivilprozessordnung geregeltes Verfahren vorgesehen. Nicht akzeptabel ist aber ein **heimliches Vorgehen**. Damit können massive seelische und familiäre Konsequenzen verbunden sein. Wegen der unzulässigen Probenbeschaffung ist der Gentest datenschutzrechtlich unzulässig. Die Durchsetzung dieses Verbots ist uns als Aufsichtsbehörde aber mangels gesetzlicher Befugnisse nicht möglich.

Weitere Informationen zu diesem Thema unter:

www.datenschutzzentrum.de/material/themen/divers/vatertes.htm

Was ist zu tun?
Der Bundesgesetzgeber ist aufgefordert, durch eine klare Strafnorm sowohl die Auftragserteilung als auch die Durchführung von heimlichen Gentests zu untersagen.

4.9 Schulbereich

Datensicherheit an vielen Schulen ein Fremdwort

Eine Bestandsaufnahme zur Datensicherheit in ca. 250 Schulen ergab, dass es fast überall an Datenschutz- und Datensicherheitsknow-how fehlt.

Klassische Datenschutzprüfungen erlauben einen umfassenden Einblick in die Einzelheiten der Datenverarbeitung einer Behörde. Bewertet werden können aber nur die jeweils vorgefundenen Gegebenheiten, sodass regelmäßig nur wenige Adressaten erreicht werden. Werden allerdings standardisierte Verfahren eingesetzt, so können aus Prüfungsergebnissen auch Rückschlüsse für andere Stellen gezogen werden. Bei Schulen in vier Städten bzw. Kreisen wurde von uns deshalb ein **anderer Prüfansatz** gewählt, der weniger in die Tiefe und mehr in die Breite geht: An über 250 Schulen wurden Fragebogen verschickt, auf denen in einem Ankreuzverfahren Fragen zur Datensicherheit beantwortet werden sollten.

Der **Rücklauf** war grundsätzlich **positiv**. Mit 90 % wurde eine hohe Teilnahmequote erreicht. Soweit dies über Plausibilitätsprüfungen festgestellt werden konnte, wurden wir auch nur selten bewusst „angeschwindelt". Auch datenschutzwidrige Zustände wurden unumwunden zugegeben. Im Bereich der konventionellen Datenverarbeitung wurden überwiegend Defizite festgestellt, die auf Unsicherheiten bezüglich der Aufbewahrungsdauer von Unterlagen zurückzuführen waren.

Im **EDV-Bereich** waren dagegen erhebliche Mängel zu erkennen. Sie resultieren weitgehend daraus, dass bei den Verantwortlichen nicht das notwendige Know-how vorhanden ist. Selbst bezüglich der minimalen Sicherungsmaßnahmen wie Bildschirmschonereinsatz oder ausreichende Passwortgestaltung wurde uns oft Fehlanzeige vermeldet. Es lag weniger an gutem Willen als an fehlender Schulung, Aufklärung bzw. Information. Hieraus haben wir die Konsequenz gezogen, das Bildungsangebot im schulischen Bereich weiter auszubauen, die über Internet verfügbaren Hilfen zu verbessern und das Kultusministerium zu präziseren und **praktikablen Standardvorgaben** zu veranlassen. Hierzu gehört auch die Überarbeitung der sich noch auf das alte LDSG beziehenden Datenschutzverordnung Schule. Eine weitere Verbesserung kann dadurch erreicht werden, die in den Schulen eingesetzten Softwareprodukte schon durch die Hersteller auf ihre Datenschutzfreundlichkeit hin überprüfen und mit einem Gütesiegel versehen zu lassen. Die rechtlichen und organisatorischen Voraussetzungen für das Erlangen solcher Gütesiegel liegen vor (Tz. 10).

Die Methode von **Fragebogen-Querschnittsprüfungen** hat sich mit gewissen Einschränkungen bewährt. So war es wegen des damit verbundenen Aufwands nicht möglich, sämtlichen aus den Fragebögen erkennbaren Mängeln im Einzelfall nachzugehen. Vielmehr war es nötig, standardisierte Ratschläge zu verbreiten. Dies ändert aber nichts an dem Umstand, dass derartige Fragebögen das Problembewusstsein für Datenschutzfragen vor Ort stärken und den Verantwortlichen ein Prüfraster an die Hand geben. In diesem Sinne „bedankten" sich eine ganze Reihe von Schulen für diese Aktion.

Die genauen Ergebnisse der Umfrage können nachgelesen werden unter:

www.datenschutzzentrum.de/material/themen/schule/umfrage.htm

Was ist zu tun?
Die Datenschutzverordnung Schule sollte umgehend aktualisiert werden. Nach Zertifizierung von Schulsoftware sollten nur noch Produkte mit einem Gütesiegel eingesetzt werden. Die EDV- und Datenschutzfortbildung bei Lehrkräften ist weiter zu forcieren.

4.10 Steuerverwaltung

4.10.1 Outsourcing – Die große Freiheit der Steuerverwaltung?

Das Steuergeheimnis wird neben dem Arzt-, dem Brief- und dem Fernmeldegeheimnis seit je her als ein ganz besonders wichtiges Rechtsgut angesehen. Die Finanzbehörden sehen dies offenbar etwas lockerer, wenn es um die Optimierung ihrer Verwaltungsabläufe geht. Die zuständigen Gremien im Bundesrat und Bundestag unterstützen diese Bestrebungen und lehnen klare gesetzliche Regelungen ab.

In mehreren Tätigkeitsberichten haben wir uns mit der Frage befasst, ob das geltende Steuerrecht es den Finanzämtern gestattet, bei der Festsetzung und Erhebung von Steuern **externe Dienstleister** einzusetzen, wenn sich nicht vermeiden lässt, dass diesen bei ihren Tätigkeiten „steuerliche Verhältnisse“ bekannt werden (vgl. 23. TB, Tz. 4.9.1).

In der Vergangenheit wurde von den Steuerverwaltungen und den Datenschutzbeauftragten übereinstimmend die Auffassung vertreten, dass die Ausgestaltung des Steuergeheimnisses in der Abgabenordnung ein **Outsourcing** (früher nannte man es Auftragsdatenverarbeitung) von Verarbeitungsprozessen ausschließt. Die Regelung im Finanzverwaltungsgesetz, nach der, wenn EDV-Anlagen anderer Verwaltungsträger für die Festsetzung und Erhebung von Steuern eingesetzt werden, die zuständige Finanzbehörde fachliche Weisungen zu erteilen hat, wurde nicht als eine „Öffnung“ des Steuergeheimnisses angesehen.

Die ursprünglich strikte Abschottung der Daten der Finanzbehörden gegenüber anderen Verwaltungsbereichen und privaten Stellen unterliegt in den letzten Jahren aufgrund von Kosten- und Praktikabilitätsüberlegungen der Verwaltung einer **zunehmenden Erosion**. Waren es zunächst nur weniger gravierende „lässliche Sünden“ wie z. B. der Druck von Lohnsteuerkarten durch private Stellen oder die kurzzeitige Einschaltung von Datenerfassungsbüros bei der Abwicklung von Arbeitnehmerveranlagungen, so stehen aktuell das Outsourcing von Rechenzentrumsdienstleistungen und die externe Administration von Arbeitsplatzsystemen und Computernetzwerken im Zentrum der Diskussion.

Nachdem auch in Schleswig-Holstein entsprechende Verfahrensweisen beschlossen worden sind (Konzentration der Rechenzentrumsaktivitäten beim Landesamt

für Informationstechnik in Hamburg und Aufbau eines zentralen Druckzentrums in der Datenzentrale), haben wir rechtliche Bedenken wegen der fehlenden Offenbarungsbefugnisse in der Abgabenordnung geltend gemacht (vgl. 22. TB, Tz. 4.9.3). Die wurden zwar vom Finanzministerium nicht geteilt, gleichwohl hat man, um die Rechtsunsicherheit zu beenden, eine **Bundesratsinitiative** gestartet. Das Ziel war, die Regelungen im Finanzverwaltungsgesetz so umzugestalten, dass eine Offenbarung steuerliche Verhältnisse im Rahmen von Auftragsdatenverarbeitungen durch andere Verwaltungsträger zulässig sein sollte.

Dieses „Ansinnen“ wurde durch die Finanzministerien der anderen Länder im Bundesrat und durch das Bundesfinanzministerium mit einer Begründung abgelehnt, die in einem eklatanten Widerspruch zu den vom Bundesverfassungsgericht formulierten Aussagen über den Zweck und die Bedeutung des Steuergeheimnisses steht (vgl. nebenstehender Kasten).

Im Wortlaut:
Zweck und Bedeutung des § 30 Abgabenordnung (AO) nach dem Urteil des Bundesverfassungsgerichts vom 17.07.1984 (BVerfGE 67, 100[139f])

... Diese Vorschrift schützt das Steuergeheimnis als Gegenstück zu den weitgehenden Offenbarungspflichten des Steuerrechts. Sie dient zum einen dem privaten Geheimhaltungsinteresse des Steuerpflichtigen und der anderen zur Auskunftserteilung verpflichteten Personen. Zugleich wird mit ihr der Zweck verfolgt, durch besonderen Schutz des Vertrauens in die Amtsverschwiegenheit die Bereitschaft zur Offenlegung der steuerlich relevanten Sachverhalte zu fördern, um so das Steuerverfahren zu erleichtern, die Steuerquellen vollständig zu erfassen und eine gesetzmäßige, d. h. insbesondere auch gleichmäßige Besteuerung sicherzustellen. Diese im Rechtsstaatsprinzip und im Gleichbehandlungsgebot verankerten öffentlichen Interessen haben einen hohen Rang, der über das nur fiskalische Interesse an der Sicherung des Steueraufkommens hinausgeht.

Ohne auf die offensichtliche Abweichung von der bisher „herrschenden“ Rechtsauffassung einzugehen, wurde behauptet, dass technische Hilfstätigkeiten durch automatisierte Einrichtungen eines anderen Bundeslandes oder anderer Verwaltungsträger generell zulässig seien, weil sie **dem Besteuerungsverfahren „dienen“**. Eine besondere Brisanz steckt in der weitergehenden Begründung: Die von Schleswig-Holstein gewünschte Ergänzung könnte ungewollt den Schluss nahe legen, dass auch in den anderen Fällen der Auftragsverarbeitung von dem Steuergeheimnis unterliegenden Daten eine ausdrückliche gesetzliche Regelung erforderlich sei. Dies geschehe nämlich auch durch nichtöffentliche Stellen. Voraussetzung für die Rechtmäßigkeit in diesen Fällen sei nur, dass die bei der Auftragsdatenverarbeitung eingesetzten Personen durch eine Verpflichtung nach dem Verpflichtungsgesetz Amtsträgern gleichgestellt werden. Konsequenz dieser Argumentation: Private Rechenzentren könnten die gesamten IT-Aktivitäten der Steuerverwaltungen übernehmen, wenn ihre Mitarbeiter eine Unterschrift unter einen etwa 10-zeiligen Vordruck gesetzt haben.

Vollends verwirrend wirkt die Argumentation der Bundesrats- und Bundestagsgremien dadurch, dass sie abschließend feststellen: „Will man dagegen eine besondere gesetzliche Regelung für die Zulässigkeit der Offenbarung von dem Steuergeheimnis unterliegenden Daten in Fällen der Auftragsdatenverarbeitung

schaffen, sollte eine solche Regelung in der einschlägigen Verfahrensordnung, im Anschluss an § 30 Abgabenordnung, erfolgen."

So ganz wohl scheint ihnen also bei ihrer „extremen" Auslegung der derzeit geltenden gesetzlichen Bestimmungen nicht zu sein, denn danach wäre jedwede Änderung der Steuergeheimnisregelungen überflüssig. Dies legt den Schluss nahe, dass es im Augenblick nur darum geht, der Verwaltung den von ihr gewünschten größtmöglichen Handlungsspielraum zu geben, Steuergeheimnis hin, Steuergeheimnis her.

Was ist zu tun?
Im Rahmen der Anpassung der Abgabenordnung an die Vorgaben der EU-Datenschutzrichtlinie müssen in Bezug auf das Outsourcing in der Steuerverwaltung klare Verhältnisse geschaffen werden. Die Landesregierung sollte insoweit aktiv werden. Bis zu einer Entscheidung des Gesetzgebers sollten externen Dienstleistern keine Steuerdaten offenbart werden.

4.10.2 Gemeinsame Softwareentwicklung der Steuerbehörden ein Problemfall

Durch die Gründung eines externen Softwarehauses (FISCUS GmbH) soll versucht werden, die seit Jahren ungelösten Probleme bei der Schaffung eines bundeseinheitlichen automatisierten Steuerfestsetzungs- und Erhebungsverfahrens in den Griff zu bekommen. Nachdem der Fortbestand des Softwarehauses aufgrund einer Entscheidung der Finanzminister-Konferenz nicht mehr infrage steht, ist es dringend erforderlich, die datenschutzrechtlich bedenklichen „Altlasten" in den bisherigen FISCUS-Konzepten zu bereinigen.

Eine Arbeitsgruppe des „Arbeitskreises Steuer" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, an der wir beteiligt sind (vgl. 23. TB, Tz. 4.9.2), hat Kontakt zur FISCUS GmbH geknüpft und erörtert folgende Teilkomplexe:

- Allgemeine Security-Policy des FISCUS-Projektes,
- Zugangs- und Zugriffskonzepte,
- Konzept der „elektronischen Steuerakte" und
- Anforderungen an den Test und die Freigabe von FISCUS-Modulen sowie die künftige Rolle des Bundesfinanzministeriums auf diesem Gebiet (Konsequenzen aus den Erfahrungen mit dem Modul ELSTER).

? *FISCUS*

*Die Abkürzung steht für: „**F**öderales **I**ntegriertes **S**tandardisiertes **C**omputer-**U**nterstütztes **S**teuersystem". Hierbei handelt es sich um ein Projekt der Steuerverwaltungen des Bundes und der Länder zur Vereinheitlichung und arbeitsteiligen Entwicklung von automatisierten Besteuerungsverfahren.*

In der bisherigen **sehr umfassenden Security-Policy** waren die Aussagen zu den grundlegenden rechtlichen Vorgaben, zu den strategischen Zielen ihrer Umsetzung und zu den Anforderungen an die technischen Systeme sowie an die organisatorischen Gegebenheiten in der Praxis verknüpft mit teilweise sehr detaillierten technischen Lösungskonzepten und Handlungsalternativen. Das Konzept enthielt dagegen keine Aussagen zu dem Sicherheitsniveau der bereits praktizierten Verfahrensabläufe (Rahmenbedingungen, in die die FISCUS-Module eingebettet werden), das die Grundlage für das Sicherheitsniveau im Rahmen von FISCUS ist. Da in datenschutzrechtlicher Hinsicht insbesondere die Vertraulichkeitsanforderungen von Bedeutung sind, ist bei allen technischen Lösungen von einem hohen Schutzniveau auszugehen.

Das FISCUS-Konzept geht weiterhin davon aus, dass alle Informationen zu einer bestimmten **steuerlich relevanten Person landesweit zusammengeführt** werden. Obwohl das Steuerrecht vielfältige Bestimmungen enthält, die eine Verknüpfung unterschiedlicher Steuerfälle bedingen (einheitliche und gesonderte Feststellungen, Kontrollmitteilungen, Zusammenveranlagungen) ist eine uneingeschränkte Verknüpfung aller Daten einer Person gleichwohl verfahrensrechtlich nicht unproblematisch. Als „Rollen“, in denen Personen neben ihrer Eigenschaft als Steuerpflichtige in Erscheinung treten können, kommen z. B. Steuerberater, Zustellungsbevollmächtigte, Einzelrechtsnachfolger, Gesamtrechtsnachfolger, Drittschuldner, gesetzliche Vertreter, Kinder, Betreuer, Anzeigenerstatter, Gutachter, sonstige Verfahrensbeteiligte, Zeugen und frühere Miteigentümer in Betracht. Ohne eine abschließende Analyse der rechtlichen Konsequenzen, die sich aus der jeweiligen Rolle ergeben, können Zugriffsregeln nicht definiert werden.

Der Umstand, dass FISCUS zu **elektronischen Steuerakten** führen soll, sagt noch nichts über deren rechtliche Relevanz aus. Offen war bisher die Frage, ob die elektronischen Akten als der authentische Datenbestand angesehen werden sollen oder nur als Arbeitskopien der papierenen Akten. Erst daraus ergibt sich jedoch, welche Daten wie lange im elektronischen Bestand vorgehalten werden müssen. Die Zugriffsregeln für den elektronischen Datenbestand können außerdem umso enger gefasst werden, je mehr Daten nach wie vor in den papierenen Akten verfügbar sind. Keinesfalls dürfen Daten elektronisch gespeichert bleiben, obwohl sie aus dem authentischen papierenen Bestand bereits entfernt sind. Auch insoweit fehlt es zurzeit noch an einer abschließenden Klärung von Rechtsfragen und der Festlegung von systemtechnischen Konsequenzen.

Für die Vergabe von **Zugriffsrechten** ist es zudem erforderlich, die „Rollen“, in denen sich die Mitarbeiter der Steuerverwaltung in dem System bewegen, zu klären. Es dürfte zwischen folgenden „Rollen“ zu unterscheiden sein: Finanzamtsvorsteher, Sachgebietsleiter, Sachbearbeiter, Mitarbeiter, sonstige Assistenzkräfte, Kassenmitarbeiter, Vollstreckungsstellenmitarbeiter, Stundungs- und Erlassstellenmitarbeiter, Betriebsprüfer, Mitarbeiter der Steuerfahndungs- und Strafsachenstellen, Innenrevision, Systemadministration in den Finanzämtern, Mitarbeiter anderer Finanzämter, EDV-Mitarbeiter der Oberfinanzdirektion, Groß- und Konzernbetriebsprüfer, Auszubildende, Referendare und Praktikanten. Von den diesen Rollen zugewiesenden Zuständigkeiten hängen die zu erteilenden Zugriffsberechtigungen ab.

Die Sicherheitslücke in dem vom Bundesland Bayern erstellten und von den anderen Bundesländern genutzten Verfahren „ELSTER“ hat gezeigt, dass gerade bei einer Verbundentwicklung dem **Test und der Freigabe** eine große Bedeutung beikommt. Im Fall des Verfahrens ELSTER war die Sicherheitslücke so tief in der Systemarchitektur verankert, dass sie nur für Internet-Spezialisten erkennbar war. Selbst bei gründlichsten Prüfungen durch Steuerfachleute wäre eine Entdeckung unwahrscheinlich gewesen. Insoweit ist dem Land Bayern wohl kein Vorwurf bezüglich unzureichender Tests zu machen. Problematisch erscheint aber, dass die Steuerverwaltungen der anderen Länder offenbar sehr wenig über die Spezifikationen des Produktes wussten. Obwohl sie ihren Steuerpflichtigen gegenüber die Konsequenzen aus der Sicherheitslücke zu verantworten hatten, wurde in Presseveröffentlichungen auf die „Zuständigkeit“ der Bayerischen Steuerverwaltung verwiesen. Im Ergebnis ist damit versucht worden, die Verantwortung auf das „Softwarehaus“ abzuschieben. Auch bei einem Verbundverfahren wie FISCUS bleiben die jeweiligen Steuerverwaltungen der Länder für dessen Rechtmäßigkeit und Sicherheit verantwortlich. Entwicklungsgremien und die FISCUS-GmbH sind lediglich als Dienstleister anzusehen. Die Korrektheit ihrer Arbeit ist von den Auftraggebern zu prüfen und die Software in jedem Land für den Einsatz freizugeben.

Es ist daher zu begrüßen, dass alle bisherigen Entwicklungen auch unter diesen Gesichtspunkten von der FISCUS-GmbH „**auf den Prüfstand gestellt**“ werden sollen. Zwischen unserer Arbeitsgruppe und der FISCUS-GmbH wurden weitere regelmäßige Kontakte verabredet.

Was ist zu tun?
Die Steuerverwaltungen des Bundes und der Länder sollten sich kurzfristig darüber verständigen, wie im Rahmen der anlaufenden Verbundentwicklung von Software ein Test- und Freigabeverfahren gestaltet werden kann, das der tatsächlichen Verantwortung für die Abwicklung der automatisierten Steuerfestsetzungs- und Erhebungsverfahren Rechnung trägt. Die Gremien der Datenschutzbeauftragten sollten sowohl in der Planungs- und Entwicklungs- als auch in der Prüfphase beteiligt werden.

4.10.3 Datenerhebung zur Zweitwohnungssteuer nicht korrekt

Wenn Kommunen eigene Steuern erheben, sind auch sie an die strengen Regeln der Abgabenordnung gebunden. Bei der Gestaltung von Erklärungsvordrucken zur Zweitwohnungssteuer wurde dies in vielen Fällen nicht beachtet, den Steuerpflichtigen wurden viel zu viele Angaben abverlangt.

> ***Im Wortlaut:***
> ***§ 11 Kommunalabgabengesetz***
>
> *Auf die Festsetzung und Erhebung von kommunalen Abgaben findet das Landesverwaltungsgesetz Anwendung. Im Übrigen ist die Abgabenordnung sinngemäß anzuwenden ...*

Die Zweitwohnungssteuer wird von denjenigen, die sie zu zahlen haben, seit Jahren als ungerecht angesehen. Gerichte wurden angerufen und Satzungen korrigiert. Letztendlich ist aber das Steuerschöpfungsrecht der **Kommunen** auch in Bezug auf die Zweitwohnungen nicht zu bestreiten. Allerdings sind sie insoweit **Finanzbehörden** und müssen sich den strengen Datenerhebungsregelungen der Abgabenordnung und des Landesdatenschutzgesetzes unterwerfen; dies sieht das Kommunalabgabengesetz so vor.

Eine Reihe von Zweitwohnungssteuerpflichtigen monierten diesbezügliche Mängel in den **Erklärungsvordrucken** mehrerer Kommunen. Sie fühlten sich unzureichend über die Rechtsgrundlagen aufgeklärt und kritisierten außerdem den übermäßigen Datenhunger.

In der Tat waren die von den Städten und Gemeinden selbst entwickelten **Vordrucke** und Informationsbriefe gleich in mehrfacher Hinsicht **zu beanstanden**. Abgefragt wurden neben den unbestreitbar erforderlichen Angaben zum Steuerpflichtigen und zur Art der Wohnungsnutzung z. B.

- die Namen und die Anzahl von Angehörigen, die die betreffende Wohnung von wann bis wann aus welchen Gründen genutzt haben,
- eine zeitliche und namentliche Einzelaufstellung von Mietern,
- ob Vermietungsagenturen zu Festmieten oder auf Provisionsbasis eingeschaltet worden waren,
- im Falle des zwischenzeitlichen Verkaufs der Name des Käufers und
- Kopien der Dauermietverträge.

Die Steuerpflichtigen wurden dabei im Unklaren darüber gelassen, zu welchen Auskünften sie verpflichtet waren und welche Angaben und Unterlagen der Erklärung zweckmäßigerweise von vornherein beigelegt werden sollten, um ergänzende Nachfragen zu vermeiden. Es gab also **keine** erkennbare **Unterscheidung** zwischen den **Pflicht**- und den **freiwilligen Angaben**.

Als besonders problematisch erwiesen sich Formulierungen, die von dem Betroffenen als **Drohungen** betrachtet werden mussten, für die allerdings bei genauerem

Hinsehen gar keine Rechtsgrundlage bestand. So wiesen einige Verwaltungen forsch darauf hin, dass sie „ermächtigt“ seien, die Angaben der Steuerpflichtigen bei den zuständigen Finanzämtern mit den dort vorliegenden Einkommenssteuerveranlagungen abzugleichen. Dieses ist objektiv unrichtig, da das Steuergeheimnis derartige Abgleiche unterbindet.

Weiterhin wurden von allen Steuerpflichtigen **Versicherungen an Eides statt** dahin gehend abverlangt, dass die Erklärung richtig und vollständig sei und das man „nach bestem Wissen und Gewissen die reine Wahrheit gesagt und nichts verschwiegen“ habe. Ergänzt wurde diese Passage um den Text der Strafnorm zur falschen Versicherung an Eides statt und Hinweisen auf das Landesverwaltungsgesetz und die Abgabenordnung. Hätten die Verfasser der Vordrucke die von ihnen selbst zitierten Vorschriften gelesen, müsste ihnen ihr Fauxpas aufgefallen sein: Das Landesverwaltungsgesetz und die Abgabenordnung schränken derartig gravierende rechtliche Maßnahmen nämlich auf Fälle ein, in denen „andere Mittel zur Erforschung der Wahrheit nicht vorhanden sind, zu keinem Ergebnis geführt haben oder einen unverhältnismäßigen Aufwand erfordern“. Außerdem muss dies „in den betreffenden Verfahren durch Gesetz oder Verordnung vorgesehen und die Behörden durch Rechtsvorschrift für zuständig erklärt worden sein“. Zusätzlich ist das Verfahren formal bis ins Detail geregelt. Eine Versicherung an Eides statt „en passant“ in einer Steuererklärung ist somit weder zulässig noch rechtswirksam.

Die betreffenden Kommunen haben auf die Beanstandungen einsichtig reagiert und zugesagt, uns ihre neuen Erklärungsvordrucke für das Jahr 2001 bis Anfang 2002 zur Prüfung vorzulegen.

Was ist zu tun?
Erklärungsvordrucke müssen das geltende Recht korrekt widerspiegeln. Bei ihrer Entwicklung und vor ihrem Einsatz in der Praxis müssen sie daher verfahrens- und datenschutzrechtlich geprüft werden.

4.11 Personaldaten

4.11.1 Erörterung von Beurteilungen in „großer Runde“?

Beurteilungsdaten gehören zu den besonders vertraulichen Personalaktendaten. Eine Erörterung der Stärken und Schwächen der Betroffenen ist daher nur im Kreis der zuständigen Beurteiler zulässig. Koordinierungsrunden, an denen alle Erst- und Zweitbeurteiler einer Behörde teilnehmen, dürfen sich nur mit den bei Beurteilungen generell anzulegenden Wertungsmaßstäben befassen.

Wiederholt sind wir darauf aufmerksam gemacht worden, dass im Bereich der Landespolizei Beurteilungen in Besprechungen koordiniert wurden, an denen nicht nur die jeweils zuständigen Erst- und Zweitbeurteiler teilgenommen haben. Nachforschungen bei der Polizei haben ergeben, dass von diesem Verfahren **Spitzenbeamte** des gehobenen Dienstes betroffen waren, deren herausgehobene Funktion bzw. Tätigkeit sich nicht nur im Bereich der betreffenden Polizeidirek-

tion, sondern auch bei allen Inspektionen auswirkte. Nach dem Personalaktenrecht sind Beurteilungsdaten grundsätzlich vertraulich zu behandeln und vor unbefugter Einsicht zu schützen. Unsere Prüfung bezog sich deshalb insbesondere auf die Feststellung der Zuständigkeit der einzelnen an der Koordinierung beteiligten Mitarbeiter.

Unproblematisch war danach die Kenntnisnahme von Beurteilungsdaten durch die Mitarbeiter innerhalb der Personalverwaltung. Dieser Personenkreis hat nach dem Landesbeamtengesetz ein Zugangsrecht zu Personalakten und darf folglich auch Beurteilungen zur Kenntnis erhalten. Zuständig sind natürlich auch die Erst- und Zweitbeurteiler der jeweiligen Mitarbeiter, wobei es gerade zu den Aufgaben des Zweitbeurteilers gehört, eine ausreichende **Koordinierung der Beurteilungen**, d. h. eine gleichmäßige Anwendung der festgelegten Bewertungsmaßstäbe auf die Betroffenen sicherzustellen. Darüber hinaus dürfen aber auch solche Mitarbeiter beteiligt werden, die zwar formell nicht Erst- oder Zweitbeurteiler des Betreffenden sind, gleichwohl aber Beurteilungsbeiträge über den Mitarbeiter abzugeben haben. Bei den betreffenden Beamten hatten eine solche Zuständigkeit die Leiter der Polizeiinspektionen sowie deren Vertreter aufgrund der bereichsübergreifenden Aufgaben der zu Beurteilenden.

Das Innenministerium hat erklärt, das geschilderte gewählte Verfahren nur bei den Spitzenbeamten der jeweiligen Laufbahngruppe anzuwenden. Eine personenbezogene Koordinierung für die Mitarbeiter in anderen „normalen“ Funktionen sei nicht erforderlich und werde daher auch nicht mehr stattfinden.

Was ist zu tun?
Bei der personenbezogenen Koordinierung von Beurteilungen hat der Dienstherr sicherzustellen, dass nur zuständige Beurteiler an Besprechungen teilnehmen. Zuständig sind dabei nur solche Mitarbeiter, die aufgrund ihrer dienstlichen Kenntnisse der Arbeit des zu Beurteilenden einen Beitrag zu dessen Leistungsbewertung erbringen können.

4.11.2 Diskretion im Beihilfeverfahren

Beihilfeanträge für Angehörige können nach gegenwärtiger Rechtslage nur durch den beihilfeberechtigten Beamten selbst gestellt werden. Besonders bei getrennt lebenden Ehegatten kann dies zu Problemen führen, wenn Angehörige ihre Arztrechnungen mit entsprechenden Diagnosedaten offenbaren müssen. Eine Gesetzesinitiative soll jetzt für Abhilfe sorgen.

Immer wieder erhalten wir Anfragen und Eingaben von **Ehefrauen**, die zwar mit Beamten verheiratet sind aber von diesen **getrennt leben**. Diese Frauen müssen Arztrechnungen und Rezepte für sich und ihre Kinder ihrem früheren Partner aushändigen, wenn sie die entstandenen Kosten erstattet erhalten wollen. Trotz langjähriger Bemühungen war an dieser Situation bisher nichts zu ändern, da das Finanzministerium wegen entsprechender Absprachen auf Bund-Länder-Ebene nicht zu einer Gesetzesinitiative für ein eigenes Antragsrecht der Angehörigen bereit war (vgl. 17. TB, Tz. 4.1.1.4).

Im Berichtsjahr unternahm auch die Bürgerbeauftragte für soziale Angelegenheiten des Landes Schleswig-Holstein einen Vorstoß. Daraufhin wurde die Angelegenheit erneut erörtert. Eine Prüfung durch den wissenschaftlichen Dienst des Landtages ergab, dass ein landesgesetzlich begründetes **eigenes Beihilfeantragsrecht** für Angehörige weder gegen das Beamtenrechtsrahmengesetz noch gegen die verfassungsrechtlich geschützten Grundsätze des Berufsbeamtentums verstoßen würde. Inzwischen wurde ein entsprechender Gesetzentwurf in das Parlament eingebracht. Es bleibt zu hoffen, dass getrennt lebende Angehörige bald ohne Offenbarung intimer Gesundheitsdaten ihren Beihilfeanspruch realisieren können.

Was ist zu tun?
Der Landtag sollte die Änderung des Landesbeamtengesetzes zügig zum Abschluss bringen.

5 Datenschutz bei Gerichten

EUREKA

Das Verwaltungsgericht hat ein automatisiertes Verfahren namens EUREKA in den Geschäftsstellen und an den Richterarbeitsplätzen eingeführt. Unter Datenschutzaspekten sind eine Reihe von Verbesserungen notwendig.

Eine Anpassung des bei den ordentlichen Gerichten in Schleswig-Holstein eingesetzten Programms MEGA an die Gegebenheiten der Verwaltungsgerichtsbarkeit kam offenbar nicht infrage. Oberverwaltungsgericht (OVG) und Verwaltungsgericht (VG) übernahmen daher die Software **EUREKA** – zunächst begrenzt auf die Arbeitsplätze beim VG – aus einem anderen Bundesland und wirken an seiner Fortentwicklung in einem Lenkungsausschuss mit, dem sechs weitere Bundesländer angehören. Eine Ausstattung der Arbeitsplätze beim OVG ist für die Zukunft geplant.

EUREKA erledigt die Verwaltung von **Verfahrensstammdaten** und enthält verschiedene **Funktionen**, über die die Adressen von Verfahrensbeteiligten sowie die Rechtsstreitigkeiten, an denen sie beteiligt waren oder sind, aufgerufen werden können. Grundsätzlich gilt das „Kammerprinzip“, wonach die Daten nur innerhalb der Kammer zugänglich sind; einige Listenfunktionen gehen allerdings hierüber hinaus. Über ein Schreibwerk können Dokumente erstellt und ausgedruckt werden. Schließlich bietet EUREKA mehrere Statistikfunktionen an, die Zahl und Arten der Erledigung von Verfahren bis zum einzelnen Berichterstatter ausweisen.

Gemeinsam mit dem OVG, dessen IT-Leitstelle auch für den Bereich des VG zuständig ist, haben wir die verbleibenden **datenschutzrechtlichen Anforderungen** ermittelt:

- Entscheidungen in nicht anonymisierter Form dürfen in kammerweit zugreifbaren Verzeichnissen für maximal fünf Jahre abgelegt werden. Aus unserer Sicht ist eine Verkürzung dieser Frist auf zwei Jahre angezeigt. Erst nach einer Anonymisierung können die Entscheidungen in ein gerichtsweit zugreifbares Verzeichnis verschoben und dort dauerhaft gespeichert werden.
- Die Verfahrensdaten sollten Schritt für Schritt reduziert und nach fünf Jahren gelöscht werden.
- In der gerichtsweit verfügbaren „Streitliste“ sollten nur anhängige Verfahren enthalten sein. Sie sollte nur für den Präsidenten des Gerichts sowie die übrigen Mitglieder des Präsidiums zu Zwecken der Organisation einsehbar sein.
- Die Funktionen der Statistik gehen zwar nicht über die bislang in papierener Form geführten Übersichten hinaus. Sie sollen den Nutzern des Systems gleichwohl transparent gemacht werden, um Befürchtungen hinsichtlich neuer, automatisierter Formen der Leistungskontrolle vorzubeugen.
- Werden Arbeitsstationen längere Zeit nicht genutzt, müssen systemseitig Bildschirmschoner mit Passwortschutz aktiviert werden.

- Diskettenlaufwerke dürfen nur bei Einsatz eines Verschlüsselungsprogramms geöffnet werden. Die Öffnung an einigen Arbeitsplätzen mit der Erlaubnis, nicht personenbezogene Textpassagen zur Weiterbearbeitung am häuslichen Arbeitsplatz auf Diskette zu speichern, stellt eine erhebliche Sicherheitslücke dar.
- Auch die Datensicherheit am häuslichen PC-Arbeitsplatz der Richter steht in der Mitverantwortung der Gerichte. Durch Zurverfügungstellen entsprechender Tools und in Kooperation mit der Personalvertretung der Richter sollte der Datenschutz auch am häuslichen Arbeitsplatz gewährleistet werden.
- Die Verpflichtung zur Protokollierung systemverändernder Zugriffe muss umgesetzt werden.

Da hierdurch Programmänderungen von EUREKA erforderlich werden, müssen die datenschutzrechtlichen Anforderungen in dem zuständigen länderübergreifenden Entscheidungsgremium angemeldet und kurzfristig umgesetzt werden. Es kann nicht angehen, dass die Projektpartner im Rahmen von Gemeinschaftsprojekten mit anderen Bundesländern landesintern jeweils auf die angeblich niedrigeren Datenschutzerfordernisse der anderen Partner verweisen.

Was ist zu tun?
Das OVG sollte die Schwachpunkte des Verfahrens alsbald beheben lassen.

6 Datenschutz in der Wirtschaft

6.1 Was hat das neue Bundesdatenschutzgesetz gebracht?

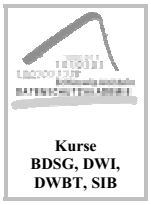
Über zehn Jahre hatte das bisherige Bundesdatenschutzgesetz (BDSG) ohne wesentliche Änderungen Bestand. Angesichts der erheblichen Weiterentwicklung der Technik ist eine umfassende Novellierung dringend erforderlich. Im Rahmen der Anpassung an die Anforderungen der Europäischen Datenschutzrichtlinie von 1995 ist der Gesetzgeber erst wenige kleine Schritte in Richtung Modernisierung des Datenschutzes gegangen.

Die am 23. Mai 2001 in Kraft getretene Novellierung bringt unter anderem folgende **Änderungen** für den nicht öffentlichen Bereich:

- Das Gesetz findet nunmehr grundsätzlich auch bei der **Datenerhebung** (also der Beschaffung von personenbezogenen Daten) Anwendung.
- Die Übermittlung von personenbezogenen Daten in das **Ausland** ist jetzt ausdrücklich geregelt. Für die Weitergabe personenbezogener Daten an Stellen mit Sitz in einem Mitgliedstaat der Europäischen Union oder des Abkommens über den Europäischen Wirtschaftsraum gelten dabei die normalen Datenschutzregelungen des BDSG. Sitzt der Empfänger in einem so genannten Drittstaat, muss dort ein angemessenes Datenschutzniveau gewährleistet sein.
- Nicht öffentliche Stellen werden verpflichtet, bereits bei der Einrichtung von Datenverarbeitungsverfahren auf die **Grundsätze der Datenvermeidung und Datensparsamkeit** zu achten.
- Die **Meldepflicht** für Dateien bei der staatlichen Aufsichtsbehörde wurde zu einer Meldepflicht für automatisierte Verfahren umgestaltet. In vielen Fällen erübrigt sich allerdings die Meldepflicht mit der Bestellung eines betrieblichen Datenschutzbeauftragten.
- **Automatisierte Einzelentscheidungen**, die **Videoüberwachung öffentlich zugänglicher Räume** und die Verwendung von **Chipkarten** sind nur unter besonderen Voraussetzungen zulässig, weil sie erhebliche Risiken für die betroffenen Bürgerinnen und Bürger mit sich bringen.
- Die Verarbeitung personenbezogener Daten mit hohem Gefährdungspotenzial für die Betroffenen, zum Beispiel **Informationen** über den **Gesundheitszustand**, ist an besondere Schutzmechanismen geknüpft. So besteht u. a. eine Verpflichtung zur Durchführung einer Vorabkontrolle.
- Die **Informationsrechte** der von einer Datenverarbeitung betroffenen Bürgerinnen und Bürger sind erheblich gestärkt worden. Schreibt z. B. ein Unternehmen einen Betroffenen direkt zu Werbezwecken an, muss er diesen zugleich darauf hingewiesen werden, dass er ein Recht auf Widerspruch gegen die Datenverarbeitung zu Werbezwecken hat. Die Adresse der verantwortlichen Stelle ist ebenfalls mitzuteilen, damit er dieses Widerspruchsrecht auch geltend machen kann.

- Die **Kompetenzen** der Aufsichtsbehörden sind **erweitert** und präzisiert worden. Insbesondere können Aufsichtsbehörden die Einhaltung der Datenschutzbestimmungen auch ohne einen Anlass überprüfen.

Aufgrund dieser Erweiterungen des Anwendungs- und Aufgabenbereiches ist auch der **Prüfungsaufwand** für uns erheblich **gestiegen**. So waren allein im Berichtszeitraum weit über zweihundert Eingaben und Anfragen von Bürgern und Unternehmen zum Datenschutz in Privatfirmen zu bearbeiten.



Wir haben den Normadressaten auf vielfältige Weise die wesentlichen Inhalte der Gesetzesänderung zu vermitteln versucht. Mit Hilfe der IHK zu Kiel und der Verbände wurden **Informationsveranstaltungen** durchgeführt und **Veröffentlichungen** in Verbandszeitschriften vorgenommen. In Zusammenarbeit mit anderen Aufsichtsbehörden wurden Broschüren entwickelt, die zum Teil auch branchenspezifisch über die Neuerungen informieren. Auch im virtuellen Datenschutzbüro sind Beiträge zum neuen BDSG veröffentlicht. Die DATENSCHUTZAKADEMIE bietet seit dem In-Kraft-Treten der Novelle Kurse über das neue BDSG an.

Eine umfassende **Modernisierung** des Datenschutzrechts ist mit der BDSG-Novellierung 2001 allerdings **nicht gelungen**. Den technischen Datenschutz zukunftsträchtig zu gestalten, bereichsspezifische Regelungen zusammenzuführen und zu vereinfachen, die Voraussetzungen für einen Datenschutz zu schaffen, der auch als Wettbewerbsvorteil zu verstehen ist, diese dringenden Aufgaben schiebt der Bundesgesetzgeber weiter vor sich her.

Was ist zu tun?
Durch Schulungen und Publikationen ist auf die wesentlichen Neuerungen der BDSG-Novellierung aufmerksam zu machen. Ebenso wichtig ist es aber, das BDSG endlich umfassend zu modernisieren.

6.2 Auskunfteien

6.2.1 Scoring der SCHUFA rechtswidrig

Bereits seit längerem haben wir darauf aufmerksam gemacht, dass das Scoring der SCHUFA datenschutzrechtswidrig ist. In einem Zivilprozess hat die SCHUFA dem Kläger gegen das Scoring durch Anerkenntnis Recht gegeben.

Das **Amtsgericht Hamburg** hat die SCHUFA im Rahmen eines Anerkenntnisurteils verurteilt, den Score-Wert des Klägers nicht an ihre Vertragspartner weiter zu geben. Ein Anerkenntnisurteil enthält keine Darstellung des Sachverhaltes und auch keine Urteilsgründe, weil der Beklagte des Verfahrens den prozessual geltend gemachten Anspruch des Klägers anerkennt. Ein solches Urteil erlegt dem Beklagten die gesamten Kosten des Verfahrens auf; es hat nur Wirkung zwischen den beiden streitenden Parteien.

www.datenschutzzentrum.de/faq/schufa.htm
www.datenschutzzentrum.de/material/themen/divers/scoring.htm

Die SCHUFA hat geltend gemacht, das Urteil beinhalte keine richterliche Wertung. Das trifft zwar zu; die SCHUFA muss sich jedoch die Frage gefallen lassen, warum sie einerseits die Auffassung vertritt, das Scoring-Verfahren sei rechtlich einwandfrei, andererseits in einem gerichtlichen Verfahren den zivilprozessualen Anspruch eines Klägers anerkennt. Tatsache ist, dass die SCHUFA beim **Scoring** personenbezogene Daten der Betroffenen mit negativen Kreditinformationen über Dritte verknüpft. Somit stellt dieses Scoring eine Auswertung von Daten dar, welche die Betroffenen nicht selbst beeinflussen können, selbst wenn sie sich im Geschäftsverkehr korrekt verhalten.

Die SCHUFA behauptet, dass der Score-Wert nicht gespeichert, sondern unmittelbar bei der Weitergabe von Daten an die Vertragspartner gebildet werde. Unseres Erachtens führt das erst recht zur **Rechtswidrigkeit des SCHUFA-Scorings**: Weil es für eine solche Datennutzung keine gesetzliche Rechtfertigung gibt, bedürfte sie gemäß § 4 Absatz 1 BDSG der Einwilligung der jeweils Betroffenen.

Der **Score** in seiner derzeitigen Gestaltung ist aber **nicht einwilligungsfähig**. Für eine wirksame Einwilligung ist Voraussetzung, dass die betroffene Person die Tragweite ihrer Entscheidung zu überblicken vermag. Die derzeitige Version der SCHUFA-Erklärung beschreibt jedoch das Scoring mit einem einzigen allgemein gehaltenen Satz, der keine Aussagekraft darüber besitzt, in welchem Umfang personenbezogene Daten ausgewertet werden, um den Score-Wert der jeweils betroffenen Person zu bilden. Mittlerweile erklärt sich die SCHUFA bereit, den Score-Wert zu sperren, wenn Betroffene hierauf bestehen.

Wir haben auch **Score-Wert-Verfahren anderer Auskunfteien** überprüft. Diese lassen sich nicht mit dem Scoring der SCHUFA vergleichen, weil sie sich zumeist auf die Teilnahme von Wirtschaftsunternehmen am Geschäftsverkehr beziehen. Wenn eine natürliche Person als Kaufmann am Wirtschaftsleben teilnimmt, muss sie mit der Veröffentlichung und der Auswertung ihres Verhaltens im Geschäftsverkehr bis zu einem gewissen Grade rechnen. Soweit Unternehmen personenbezogene Daten ihrer Kunden selbst hausintern im Rahmen eines Scorings auswerten, ist dies schon deshalb nicht mit dem Scoring zu vergleichen, weil eine unmittelbare vertragliche Beziehung mit den Betroffenen besteht bzw. bestanden hat.

Was ist zu tun ?
Betroffene, die unsere Bedenken teilen, können ihren Score-Wert bei der SCHUFA sperren lassen.

6.2.2 Missbräuchliche SCHUFA-Abfrage

Seit Jahren wird versucht, ohne Berechtigung an SCHUFA-Daten heranzukommen. Die ständige Ausweitung der Geschäftsfelder der SCHUFA schafft neue Ansatzpunkte für Missbrauchsversuche.

Ein Geschäftsmann bat einen ihm bekannten Steuerberater unter dem Vorwand angeblicher geschäftlicher Kontakte mit dem Betroffenen, für ihn eine **SCHUFA-Abfrage** zu veranlassen. Die SCHUFA beauskunftet nur gegenüber ihren Vertragspartnern oder Betroffenen. Deshalb wandte sich der Steuerberater seinerseits an eine Wohnungsverwaltungsgesellschaft, die dann die erwünschte SCHUFA-Auskunft einholte. Tatsächlich hat es zu keinem Zeitpunkt geschäftliche Beziehungen zwischen dem Geschäftsmann und dem Betroffenen gegeben. Letzterer befürchtete nun, dass die Informationen über seine Kreditwürdigkeit im Bekanntenkreis kursieren.

> ***Im Wortlaut: § 202a Abs. 1 StGB***
>
> *Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder einer Geldstrafe bestraft.*

Der Steuerberater und die Wohnungsverwaltungsgesellschaft haben ihr Fehlverhalten sofort eingeräumt und dem Petenten gegenüber bedauert. Auf unser Betreiben hin hat die Verwaltungsgesellschaft ein neues Reglement geschaffen, das sicherstellen soll, dass künftig SCHUFA-Abfragen nur bei einem berechtigten Interesse erfolgen. Gegen den eigentlichen Veranlasser der SCHUFA-Abfrage wurde vom Betroffenen ein **Strafantrag** wegen Ausspähens von Daten gestellt, da er sich die Daten des Petenten unbefugt verschafft habe.

Der Vorgang zeigt, welche Risiken mit der Ausdehnung des Geschäftsfeldes der SCHUFA auf Unternehmen wie Wohnungsverwaltungsgesellschaften verbunden sein können, die nicht besonderen gesetzlichen Geheimhaltungspflichten unterliegen.

Was ist zu tun?
Gefälligkeitsabfragen, bei denen Dritte bei Auskunfteien kreditrelevante Informationen über Betroffene einholen, ohne hierfür ein berechtigtes Interesse zu haben, sind keine Kavaliersdelikte. Vertragspartner der SCHUFA und anderer Auskunfteien haben solche Anfragen zu unterlassen.

6.2.3 Bequemlichkeit mit Folgen

Das gegenwärtige SCHUFA-Verfahren kann Personenverwechslungen nicht ausschließen. Die Folgen für die Betroffenen können äußerst unangenehm sein.

Mit dem Hinweis auf einen negativen SCHUFA-Eintrag wurde einer Handybesitzerin von ihrem **Mobilfunkanbieter** hartnäckig die Auslandsfreischaltung verweigert, obwohl die Betroffene sich finanziell nichts zu Schulden hatte kommen lassen. Auf unsere Anfrage bei der SCHUFA stellte sich heraus, dass der Grund für die negative Auskunft letztlich auf eine fehlerhafte Zuordnung von Negativdaten zurückzuführen war.

Was war geschehen? Die Mobilfunkkundin hatte im Nachbarort eine Namensvetterin mit identischem Namen und Vornamen. Auch das Geburtsdatum stimmte überein, die Adressen und die Geburtsnamen waren allerdings unterschiedlich. Zu dieser **Namensvetterin** hatte die SCHUFA Negativdaten gespeichert. Als nun bei ihr die wegen der Auslandsfreischaltung übliche Anfrage der Mobilfunkfirma hinsichtlich der Bonität ihrer Kundin einging, fand die Mitarbeiterin im EDV-Bestand nur den mit den Negativmerkmalen behafteten Datensatz der Namensvetterin. Anstatt sich zu vergewissern, ob es sich bei der gespeicherten Person tatsächlich auch um die Person handelte, auf die sich die Anfrage des Mobilfunkanbieters bezog, setzte sie sich über die unterschiedlichen Adressen der beiden Betroffenen hinweg und **unterstellte einen Umzug**. Sie änderte einfach die Adresse der Namensvetterin auf die Adresse der Mobilfunkkundin mit der Folge, dass dieser jetzt die Negativdaten angehängt wurden.

Wir haben die aufgrund der Personenverwechslung fehlerhafte Datenübermittlung an die Mobilfunkfirma beanstandet. Die SCHUFA sprach von einem **Bearbeitungsfehler** ihrer Mitarbeiterin und hat sofort reagiert: durch einen internen Bearbeitungshinweis wurde klar gestellt, dass die beiden betroffenen Personen nicht identisch sind. Das SCHUFA-Verfahren sieht für derartige Konstellationen (identische Namen und Vornamen bei abweichender Anschrift) vor, den Vertragspartner auf die abweichende Anschrift hinzuweisen und um Identitätsprüfung zu bitten. Das reicht nach unserer Auffassung aber nicht aus, denn dadurch wird die Verantwortung lediglich auf den Vertragspartner abgewälzt und eine Personenverwechslung nicht hinreichend sicher ausgeschlossen.

Was ist zu tun?
Die SCHUFA darf die Verantwortung für korrekte Identitätsfeststellungen nicht länger auf ihre Vertragspartner abwälzen, sondern muss durch eigene Maßnahmen (z. B. Einholung von Meldeauskünften oder Rückfrage beim Betroffenen vor der Datenweitergabe) derartige Fehler verhindern.

6.2.4 Auch kleine Sünden bestraft die SCHUFA mit Einträgen nicht unter drei Jahren

Die SCHUFA kennt bei ihren Eintragungen keine Bagatellgrenzen. Da für die Auskunftsempfänger nur die Tatsache einer SCHUFA-Speicherung und nicht deren Hintergrund relevant ist, sind die Folgen in vielen Fällen völlig unverhältnismäßig. So entwickelt sich die SCHUFA immer weiter von dem ursprünglichen Ziel einer angemessenen Kreditsicherung hin zu einer Art Pranger.

Bereits im vergangenen Tätigkeitsbericht haben wir die Praxis der SCHUFA kritisiert, auch geringfügige Verbindlichkeiten an ihre Vertragspartner mitzuteilen (vgl. 23. TB, Tz. 6.4.2). Selbst bei langjährigen, gut funktionierenden Vertragsbeziehungen hat eine solche Mitteilung für die Betroffenen oft unverhältnismäßig schwerwiegende Folgen, wie folgendes Beispiel zeigt:

Vier Jahre lang war eine Petentin eine zuverlässig zahlende Inhaberin eines Festnetzanschlusses. Nach der Trennung von ihrem Lebenspartner wollte sie nun bei demselben **Telekommunikationsunternehmen** dessen Handyvertrag auf sich umschreiben lassen. Doch dabei stieß sie auf einen nachhaltigen Widerstand, den sie sich nicht erklären konnte. Auf ihre wiederholte Nachfrage hin bedeutete das Unternehmen seiner Kundin lediglich, sie genüge nicht den strengen Bonitätskriterien des Hauses, sie solle doch einmal eine SCHUFA-Selbstauskunft einholen. Diese brachte aber nur die Adressdaten der Petentin und die Tatsache der Abfrage durch das Telekommunikationsunternehmen zutage. Noch nicht einmal die Bankverbindung der Petentin war der SCHUFA bekannt.

Schließlich führte unser Tätigwerden zur Aufklärung: Das Unternehmen hatte noch im Jahre 2000 über eine **SCHUFA-Abfrage** erfahren, dass die Petentin 1997 eine Rechnung über sage und schreibe 50 DM nicht beglichen habe. Die Tatsache, dass die eigenen Erfahrungen über das Zahlungsverhalten der Kundin stets positiv waren, zählte da offenbar nicht mehr. Die Petentin hingegen konnte dieses Ergebnis nicht nachvollziehen, weil die SCHUFA-Selbstauskunft den besagten Eintrag jetzt nicht mehr aufwies. Die Petentin erhielt schließlich doch noch die begehrte Umschreibung – und das Telekommunikationsunternehmen von uns eine Beanstandung wegen mangelhafter Beauskunftung. Im Gegenzug versicherte das Unternehmen, künftig seine Beschäftigten durch Schulungsmaßnahmen sensibilisieren zu wollen.

Der Vorgang zeigt, welche Auswirkungen die Nichtbegleichung eines Bagatellbetrages haben kann, wenn er an die SCHUFA gemeldet wird.

Was ist zu tun?
Nach wie vor muss die SCHUFA angehalten werden, für die Speicherung von Negativdaten Bagatellgrenzen einzuführen.

6.2.5 Eine kleine Erpressung

Einige Inkassounternehmen verleihen ihren Mahnschreiben dadurch Nachdruck, dass sie unverhohlen mit einer Meldung an die SCHUFA drohen, falls der Schuldner dem Zahlungsverlangen nicht nachkommt. Derartige Drohungen kommen strafrechtlich relevanten Erpressungen bedenklich nahe.

Ein Petent wollte eine aus seiner Sicht unberechtigte Forderung nicht begleichen. Wenig später fand er in einem **Mahnschreiben** eines **Inkassounternehmens** folgende Formulierung: „Bitte bedenken Sie, dass immer mehr Arbeitgeber die Bonität Ihrer Mitarbeiter über die SCHUFA oder sonstige Auskunfteien überprüfen und Ihr jetziger oder zukünftiger Arbeitgeber eine negative Auskunft als negatives Vertrauensmerkmal werten könnte. Es könnte in dieser Angelegenheit also nicht nur um Ihre private, sondern auch für lange Zeit um Ihre berufliche Zukunft gehen. Handeln Sie daher unverzüglich!“

Grundsätzlich dürfen Vertragspartner der SCHUFA nur solche negativen Informationen über Betroffene an die SCHUFA melden, die objektiv richtig sind. Informationen über gerichtlich festgestellte Zahlungsverpflichtungen werden beispielsweise als solche „harte“ Negativdaten angesehen. Eine **bestrittene Forderung** ist daher nicht meldefähig. Darüber hinaus sind Arbeitgeber nur in Ausnahmefällen dazu berechtigt, über ihre Arbeitnehmer eine SCHUFA-Auskunft einzuholen.

Die **Drohung** mit einer SCHUFA-Meldung war also **irreführend**, weil sie in Aussicht stellte, das Inkassounternehmen werde das Verhalten des Betroffenen der SCHUFA melden. Natürlich ist es nachvollziehbar, dass Inkassobüros auf säumige Schuldner einen gewissen Druck ausüben müssen, damit ausstehende berechtigte Forderungen der ursprünglichen Forderungsinhaber beglichen werden. Das darf jedoch nicht dazu führen, dass sich Vertragspartner eines Unternehmens durch irreführende Formulierungen gezwungen sehen, Zahlungen zu leisten, die sie rechtmäßig verweigert haben. Wir wandten uns deshalb sowohl an den Geschäftsführer des Inkassounternehmens, als auch an den betrieblichen Datenschutzbeauftragten seiner Auftraggeberin und erreichten die Streichung der kritisierten Klausel.

Was ist zu tun?
Die Drohung mit dem SCHUFA-Eintrag ist im Inkassowesen zu einer geläufigen Unsitte geworden. Sie ist jedenfalls dann rechtswidrig, wenn ein Unternehmen mit ihr droht, obwohl tatsächlich keine SCHUFA-Eintragung in Betracht kommt.

6.2.6 Mängel bei einer Handels- und Wirtschaftsauskunftei

Bei der Prüfung der schleswig-holsteinischen Auskunftsstelle einer bundesweit tätigen Handels- und Wirtschaftsauskunftei traten zum Teil erhebliche datenschutzrechtliche Mängel zu Tage.

Die Auskunftei führte neben dem automatisierten Datenbestand auch noch ein **manuelles Archiv** mit personen- bzw. firmenbezogenen Daten, welches seit 1994 nicht mehr gepflegt wurde. Dies hatte zur Folge, dass diese Daten überwiegend veraltet waren; zum Teil waren die Unterlagen 25 Jahre alt. Auf unsere Beanstandung rückte die Auskunftei von ihrer ursprünglichen Absicht ab, die Altdaten noch für weitere fünf Jahre aufzuheben. Die Vernichtung des Papierarchivs soll jetzt **im Jahre 2002** erfolgen.

Nach den gesetzlichen Vorschriften sind die von den Amtsgerichten herausgegebenen Listen über vorzeitige **Löschungen** aus dem **Schuldnerverzeichnis** (so genannte Löschlisten) nach ihrer Auswertung in den Unternehmen unverzüglich zu vernichten. Geschieht dies nicht, so ergibt sich die paradoxe Situation, dass belastende Daten zwar gelöscht werden, aus der Löschliste aber nach wie vor die entsprechenden Informationen rekonstruiert werden können. Die geprüfte Auskunftei hatte die Löschlisten jeweils für drei Jahre aufgehoben und dies mit einer eventuell später einmal eintretenden Beweisnot begründet. Da dies eindeutig gegen die Vorschriften zum Schuldnerverzeichnis verstieß, haben wir die unverzügliche Vernichtung verlangt. Die bisher vorgehaltenen Listen wurden daraufhin in einer Sonderaktion vernichtet; künftig sollen sie sofort nach ihrer Auswertung (d. h. nach ihrer Eingabe in den EDV-Bestand) beseitigt werden. Die Auskunftei war allerdings nur zu einer sofortigen Vernichtung der Löschlisten in Schleswig-Holstein bereit. Wir haben daher die Datenschutzaufsichtsbehörden der übrigen Bundesländer angeschrieben und ein vergleichbares Tätigwerden gegen die dortigen Auskunftsstellen angeregt.

Das Datenschutzrecht verlangt, dass Auskunfteien nur dann personenbezogene Daten an ihre Vertragspartner übermitteln, wenn diese ein **berechtigtes Interesse** an dem Erhalt der Informationen glaubhaft darlegen. Die Auskunfteibranche verwendet dabei regelmäßig standardisierte Begriffe, die man auch als Anfragegründe bezeichnet. Angesichts der Häufigkeit von Anfragen ist das hinzunehmen, wenn die jeweiligen Begriffe ein berechtigtes Interesse hinreichend präzise beschreiben. Die von dieser Auskunftei verwendeten Anfragegründe „**Geschäftsanbahnung**“ und „**Bonitätsprüfung**“ sind nach unserer Ansicht aber zu allgemein und zu vage formuliert. „Geschäftsanbahnung“ sagt nichts über das berechtigte Interesse des Anfragenden aus. Der Begriff „Bonitätsabfrage“ trifft auf alle Anfragekategorien zu, ist also für sich allein genommen nicht aussagekräftig. Zumindest in diesen beiden Kategorien kann das berechtigte Interesse der Empfänger an den Daten nach unserer Auffassung nicht hinreichend glaubhaft dargelegt werden. Der Anfragegrund „Geschäftsanbahnung“ müsste daher im Anfrageschein **präzisiert** werden (z. B. „Geschäftsanbahnung mit Kreditrisiko“). Denkbar wäre auch eine Klarstellung im Vertrag zwischen Auskunftei und Kunde. Die Kategorie „Bonitätsprüfung“ muss mangels Aussagekraft völlig **gestrichen** werden, da eigentlich

jede Anfrage bei einer Auskunftei eine Überprüfung der Bonität des Vertragspartners zum Zweck hat. Die Auskunftei ist jedoch zu einer entsprechenden Änderung ihres Verfahrens insbesondere in Hinblick auf dessen Bundeseinheitlichkeit bislang nicht bereit.

Nach einer Vereinbarung zwischen den obersten Datenschutzaufsichtsbehörden und dem Verband der Handelsauskunfteien sollen die Auskunfteien **das berechtigte Interesse** der Anfragenden in einem bestimmten Promillesatz der erteilten Auskünfte **stichprobenartig überprüfen**. Die Überprüfung der Antwortschreiben der Kunden wurde nicht immer mit der notwendigen Sorgfalt durchgeführt (z. B. fehlende Belege zum Nachweis des berechtigten Interesses). Die fehlenden Überprüfungen des berechtigten Interesses wurden von der Auskunftei noch im Verlauf der Prüfung vervollständigt. Die Auskunftei sagte zu, künftig diesbezüglich mehr Sorgfalt walten zu lassen.

Handelsauskunfteien haben personenbezogene Daten am Ende des fünften Kalenderjahres (BDSG-neu: am Ende des vierten Kalenderjahres) nach ihrer erstmaligen Speicherung daraufhin **zu prüfen**, ob eine länger währende Speicherung erforderlich ist. Diese Prüfung fand bei der kontrollierten Auskunftei faktisch nicht statt. Bestimmte Daten (z. B. Handelsregisternummer, Name, Anschrift, Geburtsdatum) blieben grundsätzlich „ewig“ gespeichert. Es erfolgten in unregelmäßigen Abständen aus Kapazitätsgründen nur „Löschläufe“, für solche Datensätze, bei denen die Betroffenen älter als 80 Jahre waren. Dadurch wurden Daten vorgehalten, die aufgrund ihrer Inaktualität ohnehin nicht ungeprüft beauskunftet werden durften. Wir forderten die Auskunftei auf, künftig dem gesetzlichen Überprüfungsgebot nachzukommen. Die Auskunftei ist dieser Aufforderung bislang unter Hinweis auf ihr „bundeseinheitliches Verfahren“ nicht nachgekommen. Sie ist der Meinung, ihrer gesetzlichen Pflicht dadurch Genüge zu tun, dass sie ältere Datensätze vor einer erneuten Beauskunftung stets nachrecherchiert.

Was ist zu tun?
Wir werden die strittigen Punkte in der Arbeitsgruppe „Handelsauskunfteien“ des „Düsseldorfer Kreises“ zur Diskussion stellen, um eine bundeseinheitliche Lösung herbeizuführen.

6.2.7 Schuldnerpranger im Internet

Die Veröffentlichung der Namen von Schuldnern im Internet zu dem Zweck, sie unter Druck zu setzen, ist rechtswidrig. Ein in Schleswig-Holstein betriebener „Schuldnerpranger“ musste daher seinen Betrieb einstellen.

Ein schleswig-holsteinischer Finanzdienstleister bot im Internet folgenden Service an: Wer Probleme beim Durchsetzen einer gerichtlich bestätigten Forderung hatte, sollte seiner Forderung mit der Drohung der Veröffentlichung im Internet Nachdruck verleihen können. Blieb diese Drohung ohne Resonanz, so sollten Name und Adresse mit einem Hinweis auf dessen Zahlungsunwilligkeit bzw. -fähigkeit **weltweit** elektronisch **veröffentlicht** werden.

Sicherlich sollte jeder seine Schulden bezahlen. Wer eine Forderung aber nicht begleichen kann oder nicht will, z. B. weil er meint, schon gezahlt zu haben oder weil er ihre Berechtigung bestreitet, der darf nicht weltweit an einen **elektronischen Internet-Pranger** gestellt werden. Die Zivilprozessordnung sieht hierfür andere als dieses modern-mittelalterliche Mittel vor. Datenschutzkonforme Bonitätsprüfungen und Verfahren zum Gläubigerschutz gibt es seit Jahren. Das Instrument des Internet-Schuldner-Prangers bietet ein gefährliches Mittel für Selbstjustiz und Rufmord. Der Betrieb des Dienstes wurde wieder vom Netz genommen, nachdem wir rechtliche Konsequenzen wegen des datenschutzwidrigen Angebots angedroht haben.

Wir haben dies durch eine **Pressemitteilung** bekannt gemacht:

www.datenschutzzentrum.de/material/themen/presse/pranger.htm

Dies hatte eine Vielzahl von Hinweisen auf weitere Internet-Dienste mit ähnlichem „Service“ zur Folge. Da diese Unternehmen ausnahmslos ihren Sitz außerhalb von Schleswig-Holstein hatten, haben wir die Adressen der Anbieter an die jeweils zuständigen Aufsichtsbehörden weitergegeben.

In einem vergleichbaren Fall hat das **Oberlandesgericht Rostock** unsere Rechtsauffassung bestätigt und zudem dargelegt, dass die Veröffentlichung von Schuldnerspiegeln im Internet zivilrechtlich selbst dann unzulässig ist, wenn davon ein Gewerbebetrieb betroffen ist. Die Verfassungsbeschwerde des verurteilten Betreibers wurde von dem Bundesverfassungsgericht inzwischen als unzulässig zurückgewiesen.

Was ist zu tun?
Wer derartige Schuldnerpranger im Internet findet, sollte die zuständige Datenschutzaufsichtsbehörde informieren.

6.3 Banken

Was gibt es zu erben?

Informationen über die Vermögensverhältnisse von Verstorbenen dürfen von Geldinstituten nur an Berechtigte herausgegeben werden, die sich mit Erbschein ausweisen.

Nach dem Erbschaftsteuerrecht müssen Kreditinstitute, Versicherungsunternehmen und berufsmäßige Vermögensverwalter nach dem Tod eines Konten- und Depotinhabers die in Verwahrung genommenen Vermögensgegenstände (also Kontenguthaben, fällig werdende Lebensversicherungen usw.) an das zuständige Finanzamt melden. An solchen Informationen haben bisweilen auch andere Interesse. Zwei Eingaben betrafen Banken und Sparkassen, die nach einem Todesfall nicht berechtigten Personen zum Teil umfassend Auskunft über die **Vermögensverhältnisse** des jeweiligen Erblassers gegeben hatten.

Das Bürgerliche Gesetzbuch (BGB) erlaubt eine entsprechende Übermittlung nur an eine Person, die ihre Berechtigung durch einen **Erbschein** ausweist. Im Übrigen ist eine Übermittlung von personenbezogenen Daten an private Dritte im Erbfall grundsätzlich zulässig, wenn dies durch eine andere Rechtsvorschrift erlaubt wird oder wenn eine Vollmacht des Erblassers vorliegt. Die Frage, wer als Erbe in das Vermögen des Erblassers eintritt, ist auch nicht durch ein handgeschriebenes Testament des Verstorbenen nachweisbar. Das ergibt sich bereits daraus, dass ein Testament grundsätzlich jederzeit durch ein späteres, anders lautendes Testament ersetzt werden kann.

Im Wortlaut: § 2365 BGB

Es wird vermutet, dass demjenigen, welcher im Erbschein als Erbe bezeichnet ist, das in dem Erbschein angegebene Erbrecht zustehe und dass er nicht durch andere als die angegebenen Anordnungen beschränkt sei.

Auch das Datenschutzrecht erlaubt nicht die Übermittlung der Vermögensdaten. Nach dem BDSG darf zwar eine Daten verarbeitende Stelle zur Wahrung berechtigter eigener Interessen personenbezogene Informationen übermitteln. Voraussetzung ist jedoch, dass keine Anhaltspunkte dafür bestehen, dass das **schutzwürdige Interesse** des Betroffenen an dem Ausschluss der Übermittlung überwiegt. Ein nicht durch Erbschein ausgewiesener Erbe hat jedoch kein berechtigtes Interesse an der Kenntnisnahme der Vermögensverhältnisse des Erblassers.

Die betroffenen Kreditinstitute haben den Fehler eingeräumt und entsprechende Hinweise an ihre Mitarbeiter weitergegeben.

Was ist zu tun?
Kreditinstitute müssen die Auskunft über die Vermögensverhältnisse eines Verstorbenen von der Vorlage eines Erbscheines abhängig machen.

6.4 Industrie, Handel, Handwerk und freie Berufe

6.4.1 Karten- und Datenflut nach Wegfall des Rabattgesetzes

Nach der Aufhebung des Rabattgesetzes schießen Rabattsparprojekte wie Pilze aus dem Boden. Besonders häufig anzutreffen sind Rabattsparkarten, die eine umfangreiche Sammlung und Auswertung von Kundendaten ermöglichen. Nur zu oft werden die betroffenen Kunden dabei über das Ausmaß der Datenverarbeitung im Unklaren gelassen.

Nach der Aufhebung des Rabattgesetzes sind Rabattsparkarten in Mode gekommen. Durch sie sollen die Konsumenten an ein Unternehmen gebunden werden. **Datenschutzrechtlich** hat diese Idee allerdings einen **Haken**. Während die Kunden Rabattpunkte sammeln, sammeln die Unternehmen nämlich fleißig Kundendaten mit. Viele Rabattkartenbetreiber erheben bereits im Rahmen des Antrages umfangreiche Informationen über den Antragsteller, beispielsweise über das monatliche Haushaltseinkommen sowie seine Kaufgewohnheiten im Internet. Verknüpft mit den Umsatzdaten lassen sich so hübsche **Kundenprofile** erstellen. Möglich ist

auch, die Angaben zu analysieren, um die Kreditwürdigkeit der betroffenen Kunden zu bewerten. Dass das für die Betroffenen erhebliche Auswirkungen haben kann, liegt auf der Hand.

Nur so hat das **Landgericht München** im vergangenen Jahr die Allgemeinen Geschäftsbedingungen für die Payback-Karte als rechtswidrig bezeichnet, weil sie die Antragsteller nicht hinreichend informierten. Als Reaktion hierauf hat der Betreiber dieser Karte immerhin die Transparenz seines Verfahrens verbessert, ohne freilich den Umfang der ausgewerteten personenbezogenen Daten zu verringern. Aufgrund des beschriebenen Risikos und der Rechtsprechung haben wir mehrere Rabattsparkartensysteme eingehend untersucht. Dabei erreichten wir bei allen Betreibern eine erhebliche Verringerung des Umfanges der gespeicherten Daten.

Manchmal geben sich Kartenbetreiber allerdings ziemlich bürokratisch. Eine Kauffrau wollte bei einem Großhandelsunternehmen ihr **Geburtsdatum** nicht angeben. Unser Engagement führte zwar zu einer erheblichen Reduzierung des erhobenen Datensatzes, man wollte aber nach wie vor auf der Angabe des Geburtsdatums bestehen, weil man auf diese Weise die Volljährigkeit der Kauffrau „feststellen“ wollte. Es bedurfte einer gewissen Überzeugungskraft, bis das Unternehmen auf das Geburtsdatum generös verzichtete.

Was ist zu tun?
Verbraucher sollten die Allgemeinen Geschäftsbedingungen von Rabattsparkarten dahingehend genau unter die Lupe nehmen, ob die Datenverarbeitung wirklich verständlich dargestellt wird.

6.4.2 Datenschutz mit dem Verwöhnaroma

In Supermärkten und Kaufhäusern werden an den Kassen manchmal unnötiger Weise personenbezogene Daten erhoben. In einem Fall gab das Unternehmen einen Fehler unumwunden zu und entschuldigte sich bei der Betroffenen mit einem Präsent.

Bei der Kundin eines Supermarktes wurde an der Kasse ein Artikel im Wert von 3,98 DM versehentlich zweimal erfasst. Der Irrtum war schnell erkannt, die Rückzahlung des überzahlten Betrages war ebenfalls kein Problem. Im Gegenzug beharrte die Kassiererin jedoch darauf, dass Name, Anschrift und Telefonnummer der Kundin auf einem so genannten „Retourbon“ eingetragen wurden. Auf Rückfrage der Kundin erklärte die Kassiererin: **„Ich bekomme die Angelegenheit sonst nicht aus der Kasse heraus!“** Die Kundin war mit dieser Aussage nicht zufrieden und wandte sich an uns.

Wir hielten die Erfassung der Kundendaten bei reinen Tipp- oder Erfassungsfehlern an der Kasse mangels Erforderlichkeit der Daten für unzulässig. Im Gegensatz zur Warenrückgabe oder Reklamation (hier könnte sich ja im Nachhinein heraus stellen, dass die zurückgegebene Ware beschädigt ist) ist bei reinen Preis-

erfassungsfehlern mit sofort anschließender Erstattung kein Fall denkbar, der die spätere Kenntnis der Kundendaten erfordern würde. Die Geschäftsleitung der Supermarktkette schloss sich unserer Auffassung an und begründete das Versehen mit Aufgeregtheit und mangelnder Erfahrung einer neuen Kassiererin. Tatsächlich existierte in dem Unternehmen eine interne schriftliche Vereinbarung, die eine Erfassung von Kundendaten **nur bei Rückgabe bzw. Reklamation von Waren** vorschreibt.

Die Firma reagierte galant. Sie leitete den versehentlich ausgefüllten Retourbon an die Kundin zurück und schenkte ihr gleichermaßen als Krönung der ganzen Angelegenheit ein Pfund Kaffee.

Was ist zu tun?
Der Einzelhandel sollte darauf achten, dass die Erhebung von Kundendaten an den Kassen nur in ganz wenigen Ausnahmefällen zulässig ist.

6.4.3 Neugierige Fitnessstudios

Die Informationstechnik hält auch Einzug in die Fitness- und Sportstudios. Manche Kunden fühlen sich allerdings angesichts der Speicherung ihrer Daten ziemlich unwohl.

Für ein Fitnessstudio eines Sportvereins hatte man computerlesbare Mitgliedsausweise eingeführt, um die Tatsache der Mitgliedschaft sowie die unterschiedlichen Zugangsberechtigungen der Mitglieder besser und schneller kontrollieren zu können. Eine aufmerksame Sportlerin wunderte sich aber darüber, dass ihr Ausweis nicht nur beim **Betreten** sondern auch beim **Verlassen** des Studios eingelesen wurde.

Auf unsere Anfrage begründete der Sportverein, die Erfassung der „Kommt"- und „Geht"-Zeiten mit der Erforderlichkeit dieser Daten zur **Analyse individueller Trainingspläne**, einem besonderen Service des Vereins. Die gespeicherten Besuchszeiten seien aber nur der Geschäftsstelle zugänglich. Schriftliche Regelungen für diese Datensammelei in der Vereinssatzung, in den Eintrittserklärungen oder in gesonderten Einwilligungserklärungen lagen nicht vor.

Wir wiesen den Verein auf die grundsätzliche Problematik der Speicherung von Bewegungsmustern (wer hat sich wann wo aufgehalten?) hin und vertraten die Auffassung, dass es für die Speicherung der individuellen Trainingszeiten der Vereinsmitglieder im vorliegenden Fall keine hinreichende Berechtigung gab. Da der Verein auf seinen Service der Analyse individueller Trainingspläne nicht verzichten wollte, wurde eine datenschutzgerechte Lösung gefunden: Künftig wird das Beitrittsformular des Vereins eine optisch hervorgehobene **Einwilligungsklausel** hinsichtlich der Speicherung der fraglichen Daten enthalten. Für die so genannten „Alt-Mitglieder", die noch das alte Beitrittsformular unterzeichnet haben, wird eine gesonderte schriftliche Einwilligung erstellt und im Studio ausgelegt. Wer nicht damit einverstanden ist, wird auch nicht erfasst.

Was ist zu tun?
Fitnessstudios sind bei der Sammlung von Mitgliederdaten an die Vereinssatzung bzw. an die Erforderlichkeit zur Durchführung des Vertragszweckes gebunden. Die Verarbeitung darüber hinaus gehender Daten der Studiobesucher ist grundsätzlich nur mit deren schriftlicher Einwilligung zulässig.

6.4.4 Vorsicht beim Faxversand

Auch Rechtsanwälte müssen die datenschutzrechtlichen Bestimmungen einhalten, selbst wenn dies im täglichen Massengeschäft nicht immer so einfach ist.

Ein Mitarbeiter der Stadtverwaltung Kiel staunte nicht schlecht, als er ein an seinen Arbeitgeber gerichtetes Fax seiner Rechtsanwältin, aus dem sich die Tatsache der **Pfändung seines Gehalts** ergab, im offenen Faxgerät seiner Fachabteilung vorfand. Dass derartige Informationen dem Personalamt der Stadtverwaltung mitzuteilen sind, hätte er ja noch eingesehen. Durch die Versendung des Faxes an **seine eigene Abteilung** befürchtete er jedoch zu Recht Spekulationen über seine finanziellen Verhältnisse innerhalb seines engsten Kollegenkreises und wandte sich an uns.

Die Rechtsanwältin erklärte, der Pfändungs- und Überweisungsbeschluss diene der Befriedigung ihrer eigenen Honorarforderung. Allerdings hätte die in ihrer Kanzlei beschäftigte Mitarbeiterin versehentlich eine **falsche Fax-Nummer** benutzt und außerdem den **Zusatz „Personalamt“** im Anschriftenfeld des Faxes **vergessen**. Die Rechtsanwältin **entschuldigte** sich ausdrücklich und räumte ihren Fehler bzw. das Versehen ihrer Mitarbeiterin unumwunden ein. Eine Wiederholung wollte sie durch verstärkte Kontrolle und Schulung ihrer Mitarbeiterin erreichen.

Der Fall zeigt, dass die Versendung sensitiver Daten als Fax **grundsätzlich problematisch** ist, da in vielen Firmen und Behörden die Faxgeräte oft in mehr oder weniger offen zugänglichen Poststellen aufgestellt sind. Eine unbefugte Kenntnisnahme durch nicht zuständige Mitarbeiter kann bei einem Fax praktisch nie völlig ausgeschlossen werden. Daher ist bei sensitiven Daten im Zweifelsfalle der gute alte Brief immer noch die sicherere Versendeform.

Was ist zu tun?
Nicht nur für Rechtsanwälte gilt die Grundregel: Sensitive Daten gehören nicht auf das Faxgerät, sondern sind im verschlossenen Brief zu versenden!

6.4.5 Datenschutz im Kündigungsschutzprozess

Bei betriebsbedingten Kündigungen wird oft über die korrekte Auswahl der gekündigten Arbeitnehmer durch den Arbeitgeber gestritten. Wenn Arbeitgeber undifferenziert Listen sämtlicher Beschäftigten mit den kündigungsrelevanten Sozialdaten in den Prozess einführen, kann sich das nicht nur für die Betroffenen, sondern auch für den Betriebsfrieden negativ auswirken.

Zur Durchführung betriebsbedingter Kündigungen hat eine Firma eine alphabetische und eine nach Vergleichbarkeitskriterien sortierte **Liste sämtlicher Arbeitnehmer** sowie eine Liste aller gekündigten Beschäftigten erstellt. Alle drei Verzeichnisse beinhalteten zahlreiche sensitive Daten, unter anderem eine etwaige Schwerbehinderteneigenschaft und die Gehaltsstufen. Diese Listen wurden zunächst dem Betriebsrat zur Anhörung übergeben. Im Rahmen der Vorbereitung und der Durchführung des Prozesses übermittelte der Arbeitgeber die Listen an seinen Prozessvertreter, einen Arbeitgeberverband, um die ordnungsgemäße Anhörung des Betriebsrates und die ordnungsgemäße Sozialauswahl nachzuweisen. Der Verband gab die Listen seinerseits ungekürzt an das Arbeitsgericht und an die Prozessbevollmächtigten der gekündigten Kläger weiter, die sie ihren Mandanten zukommen ließen. Nur kurze Zeit später kursierten die Verzeichnisse im ganzen Unternehmen; mit erheblichen **Auswirkungen**:

- Bislang nicht bekannte, weil nicht sichtbare körperliche Behinderungen wurden plötzlich öffentlich.
- Aufgrund eines angeführten Punkteschemas, das die soziale Schutzwürdigkeit der jeweiligen Arbeitnehmer kennzeichnen sollte, wurden Arbeitnehmer damit konfrontiert, dass sie mit einer für sie ungünstigen Punktezahl „die Nächsten“ bei einer folgenden Kündigungswelle sein könnten.
- Die Zugehörigkeit zu verschiedenen Lohn- und Gehaltsgruppen führte zu Gerechtigkeitsdiskussionen im Betrieb.
- Es entstand eine erhebliche Mobbinggefahr. Der gesamte betriebliche Frieden wurde nachhaltig gestört.

Wir haben die Weitergabe der Listen an den Arbeitgeberverband und an die Prozessgegner als **erheblichen Datenschutzverstoß** gerügt. Zwar sind die Interessen der Parteien im Kündigungsschutzprozess zu berücksichtigen; insbesondere muss der gekündigte Arbeitnehmer die korrekte Auswahl nachvollziehen können. Die arbeitsgerichtliche Rechtsprechung verlangt aber nur, dass der Gekündigte die Informationen erhält, die er zur Beurteilung der Rechtmäßigkeit der Kündigung benötigt. Richtig verstanden führt Datenschutz nicht zu einer Schmälerung der Rechtsposition der Beteiligten, sondern zu der Gewährleistung des betrieblichen Friedens. Die Weitergabe an den Betriebsrat war hingegen datenschutzrechtlich nicht zu beanstanden. Aufgrund seiner betrieblichen Mitwirkungspflichten hat er ein berechtigtes Interesse an dem Erhalt der kompletten Listen. Der Schutz der Betroffenen ist dabei durch die besonderen Geheimhaltungspflichten des Betriebsrates hinreichend gesichert.

Unter Berücksichtigung der arbeitsgerichtlichen Rechtsprechung haben wir folgende Empfehlungen für das **Verhalten in Kündigungsschutzprozessen** gegeben:

- Wenn der Arbeitgeber dem Betriebsrat eine vollständige Liste der Beschäftigten zur Verfügung stellt, genügt im Kündigungsschutzprozess zum Beweis der ordnungsgemäßen Anhörung des Betriebsrates regelmäßig eine schriftliche **Empfangsbestätigung des Betriebsratsvorsitzenden**, dass er die vollständige Liste erhalten hat. Hilfsweise kann sich der Arbeitgeber auch auf das Zeugnis des Betriebsratsvorsitzenden stützen. Die Vollständigkeit der Liste lässt sich dabei aus der Anzahl der aufgelisteten Beschäftigten entnehmen. Das besagte Verzeichnis darf den Bereich des Betriebsrates nicht verlassen; es ist nach erfolgter Anhörung entweder zu vernichten oder bei einer erforderlichen weiteren Aufbewahrung vom Betriebsrat unter Verschluss zu halten.
- Im Rahmen des Prozesses muss der Arbeitgeber grundsätzlich keine vollständigen Beschäftigtenlisten an das Gericht übermitteln, es sei denn, dies wird vom **Gericht** ausdrücklich verlangt: Zum einen wird durch eine vollständige Liste nicht die erforderliche Sozialauswahl bewiesen, zum anderen ist sie für die Verteidigung der Rechtsposition des Gekündigten nicht erforderlich. Insbesondere ist nicht einsehbar, warum der Gekündigte über das Gericht die Sozialdaten anderer gekündigter Arbeitnehmer erfahren soll. Der Arbeitgeber darf nur diejenigen Sozialdaten derjenigen Arbeitnehmer preisgeben, die er für mit dem gekündigten Arbeitnehmer vergleichbar hält.
- Macht der Prozessbevollmächtigte des Arbeitnehmers plausibel geltend, dass der Arbeitgeber nicht alle mit ihm vergleichbaren Arbeitnehmer aufgeführt hat, etwa weil er eine bestimmte Gruppe von Arbeitnehmern vergessen hat, kann der Arbeitgeber im Prozess seine **Sozialauswahl „nachbessern“**, indem er die Sozialdaten der Arbeitnehmer der gerügten Kategorie nachreicht, sofern das Gericht dies verlangt.
- Der Prozessbevollmächtigte des Klage führenden Arbeitnehmers sollte seinen Mandanten auf die **Vertraulichkeit** der übermittelten Daten hinweisen.

Sowohl der Arbeitgeber als auch der beteiligte Arbeitgeberverband haben im Rahmen der Gespräche zugesichert, diese Empfehlungen in künftigen Gerichtsverfahren zu beachten, soweit dies von den Arbeitsgerichten akzeptiert wird.

Was ist zu tun?
In Kündigungsschutzprozessen darf der Arbeitgeber nicht komplette Beschäftigtenlisten mit kündigungsrelevanten Sozialdaten an das Arbeitsgericht und damit mittelbar auch an den klagenden Arbeitnehmer übermitteln, es sei denn, das Gericht verlangt dies ausdrücklich aus Beweisgründen. Der Arbeitgeber darf nur die Sozialdaten der Arbeitnehmer preisgeben, die mit dem gekündigten Arbeitnehmer vergleichbar sind.

6.5 Neue Zuständigkeit für die Verfolgung von Ordnungswidrigkeiten

Durch die Änderung der Ordnungswidrigkeiten-Zuständigkeitsverordnung wurde die Aufgabe der Verfolgung von **Ordnungswidrigkeiten nach dem BDSG** dem Vorstand des ULD übertragen. Nach dem Wortlaut des Bußgeldkataloges im BDSG kann damit der Landesbeauftragte für den Datenschutz als Vorstand des ULD gegenüber privatwirtschaftlichen Stellen Bußgeldbescheide bis zu einer Höhe von 250.000 Euro erlassen. Die Verfolgung von Ordnungswidrigkeiten ist in das pflichtgemäße Ermessen der Verwaltungsbehörde gestellt. Die Verhängung von Bußgeldern wurde bislang nur in den Fällen in Betracht gezogen, in denen die verantwortlichen Stellen vorsätzlich Datenschutzverletzungen begangen haben. Werden nach unserer Intervention Maßnahmen ergriffen, die künftigen Verstößen wirksam entgegenwirken, dann ist die Verhängung von Bußgeldern kontraproduktiv bzw. rechtlich nicht geboten.

7 Systemdatenschutz

7.1 Sicheres Surfen und Mailen – die Herausforderung

Würde in der öffentlichen Verwaltung das Wort des Jahres 2001 gewählt werden, käme „E-Government“ sicher in die engste Wahl. Kaum ein anderer Begriff ist in letzter Zeit so häufig benutzt wurden, um die zukünftige Entwicklung der öffentlichen Verwaltung zu umschreiben. Zu selten wird allerdings analysiert, welche Konsequenzen ein E-Government für die Sicherheit der IT-Systeme haben wird.

Unter dem Begriff „E-Government“ werden sehr unterschiedliche Verwaltungsaktivitäten zusammengefasst (vgl. Tz. 8.1), zwei Komponenten sind jedoch (neben der allgemein üblichen, in diesem Zusammenhang aber nicht so bedeutenden Präsentation der Behörden auf einer Homepage) in allen Konzepten auf Bundes-, Landes- und Kommunalebene besonders ausgeprägt. Es sind dies

- die Informationsgewinnung über das Internet und
- die Kommunikation über das Internet.

Kurz gesagt handelt es sich um das **Surfen** im World Wide Web und das **Mailen**. Die dazu erforderlichen hard- und softwaretechnischen Komponenten sind im privaten Bereich und in der Wirtschaft tausendfach erprobt. Warum sollte sich nicht auch die Verwaltung ihrer bedienen? Eine positive Antwort wäre selbstverständlich, gäbe es da nicht einige Haken: Das Internet ist unsicher: Es gibt keinen Netzbetreiber, der für den korrekten Datentransport die Gewähr übernimmt. Alle aus dem Netz empfangenen Daten, selbst die Absender- und Empfängerangaben, können manipuliert sein. Es ist sogar möglich, dass die an das Netz angeschlossenen Rechner zum Angriff gegeneinander genutzt werden, indem z. B. die Funktionsfähigkeit beeinträchtigt oder gespeicherte Daten ausgeforscht werden. Dies sind alles Merkmale, die dem Sicherheitsbedürfnis in einer öffentlichen Verwaltung grundsätzlich diametral entgegenstehen. Warum wird die Internet-Nutzung dann trotzdem so sehr forciert? Es sind die **unschlagbar niedrigen Kosten** für den Datentransport, die die objektiv bestehenden Risiken in einem milderen Licht erscheinen lassen. Die Verlockungen des nahezu kostenlosen Kommunikationszeitalters sind auch für die öffentliche Verwaltung zu groß.

In der Praxis treffen wir auf zwei unterschiedliche Grundansätze bei der Realisierung der Internet-Nutzung zu Verwaltungszwecken:

- den Infrastrukturansatz und
- den Bedarfsdeckungsansatz.

Beim **Infrastrukturansatz** wiederholt sich eine Verfahrensweise, die zu der explosionsartigen Verbreitung der PC geführt hat. Möglichst alle Mitarbeiter werden in die Lage versetzt, die neue Technik über die internen Verwaltungsnetze zu nutzen. Man erhöht die Akzeptanz dadurch, dass man ihnen größtmögliche

Gestaltungsfreiheiten lässt. Das bedeutet, dass mit Ausnahme pornografischer und gewaltverherrlichender Seiten alles „abgesurft“ werden darf. Auch die Informationsgewinnung zu privaten Zwecken wird häufig begrüßt, weil es dem Surftraining dient. Die E-Mail-Adressen sind auf die einzelnen Personen bezogen. Der kollegiale Informationsaustausch und der persönliche Kontakt mit den Bürgerinnen und Bürgern wird ausdrücklich gefördert. Ähnlich wie beim Faxverkehr wird, wo immer es rechtlich vertretbar ist, auf das Vorhandensein von Unterschriften verzichtet, und die Authentizität von E-Mail-Adressen wird unterstellt. Neben der Nutzung einer Standard-Firewall und eines Virenscanners bestehen in der Regel nur organisatorische Sicherheitsmaßnahmen der Gestalt, dass die Mitarbeiter gehalten sind, alle Aktivitäten zu unterlassen, die zu einer Gefährdung des internen Netzes führen könnten. Das gilt insbesondere für das Herunterladen von Programmen aus dem Netz auf die lokalen Rechner und das Öffnen von Anhängen an E-Mails. Bezüglich der möglichen gezielten Angriffe aus dem Netz geht man davon aus, dass normale Verwaltungsbehörden ein für Hacker unattraktives Ziel darstellen.

Eine solche Vorgehensweise halten wir nicht für angemessen und dem Stand der Technik entsprechend. Es ist zu befürchten, dass der Infrastrukturansatz, der letztendlich zu einem **PC-Wildwuchs** geführt hat (der nach kurzer Zeit durch besser zu steuernde Client-Server-Systeme abgelöst werden musste), spätestens dann zu unbefriedigenden Ergebnissen führt, wenn sich das E-Government zu einem Instrument des (rechts)verbindlichen Verwaltungshandelns entwickelt. Dann wird auch ein noch so großes Vertrauen in das Verantwortungsbewusstsein der Mitarbeiter und in deren Wissen um die Risiken als Sicherheitsmaßnahme nicht mehr ausreichen.

Erfolg versprechender ist dagegen der **Bedarfsdeckungsansatz**, den eine Reihe von Verwaltungen in Schleswig-Holstein, allen voran die Kreise Ostholstein und Schleswig-Flensburg, verfolgen. Sie lassen ein „freies Surfen“ im WWW nur von PC aus zu, die nicht in das Verwaltungsnetz integriert sind und auf denen keine personenbezogenen Daten gespeichert werden. Aus dem Verwaltungsnetz heraus ist die Informationsgewinnung auf Websites beschränkt, die für dienstliche Zwecke sinnvoll erscheinen und deren Vertrauenswürdigkeit zuvor von dem betreffenden Fachbereich und der IT-Stelle gemeinsam geprüft worden ist. Ein Herunterladen von Software ist nur über einen speziellen PC in der IT-Stelle möglich. Die für die Fachämter wichtigen Informationsquellen stehen gleichwohl an den betreffenden Arbeitsplätzen zur Verfügung. Der mit PGP verschlüsselte Versand von E-Mails ist als Standard konfiguriert. Ein Verzicht auf die Verschlüsselung wird als zu begründende Ausnahme angesehen. Eingehende E-Mails werden zentral auf Viren untersucht und gegebenenfalls zuvor entschlüsselt. Nur einige „risikoarme“ Attachmentformate werden direkt in das interne Netz übernommen. Alle als risikobehaftet erkennbaren Formate werden durch eine spezielle Software ausgefiltert, „in Quarantäne“ genommen und die Absender und Empfänger über diese Tatsache per E-Mail informiert. Für alle ein- und ausgehenden E-Mails gilt, dass sie in Papierform zu den Akten zu nehmen und zum frühestmöglichen Zeitpunkt im System zu löschen sind.

Diese Maßnahmen machen die Verknüpfung des Verwaltungsnetzes um ein Vielfaches sicherer, als es beim Infrastrukturansatz erreichbar ist. Die Kreise haben, um Restrisiken erkennbar werden zu lassen, ihre Lösungen sogar einem **Penetrationstest** durch ein externes Sicherheitsunternehmen unterworfen. Der Test wurde von beiden erfolgreich bestanden. Der Kreis Ostholstein hat zusätzlich bei uns ein Behördenaudit für diesen Bereich beantragt. Das entsprechende Zertifikat konnte Anfang 2002 erteilt werden (Tz. 10.6).

Ein noch höheres Maß an Flexibilität und Sicherheit lässt sich nach dem derzeitigen Stand der Technik nur durch ein „**virtuelles Netz-Computing“** erreichen. In diesem Fall wird das interne Netz völlig vom Internet getrennt. Alle internetbezogenen Aktivitäten finden auf dem in einer „neutralen Zone“ installierten Netzcomputer statt. Die Ergebnisse werden im internen Netz nur angezeigt (grafisches Interface). Dieses Konzept wird zurzeit in unserer Dienststelle im Rahmen eines Forschungsprojektes erprobt (vgl. 23. TB, Tz. 10.3). Sobald es die „Produktionsreife“ erreicht hat, werden wir es den interessierten Behörden vorstellen und sie bei einer eventuellen Installation unterstützen.

Was ist zu tun?
Die Behörden sollten bei der Informationsgewinnung und der Kommunikation mittels Internet erkennen, dass das unspezifizierte Ausnutzen aller technischen Möglichkeiten und das Vertrauen in den vorsichtigen Umgang ihrer Mitarbeiter mit diesen Gegebenheiten keine ausreichenden Sicherheitsmaßnahmen darstellen. Das Surfen und Mailen muss durch technische und organisatorische Regelungen zu einem sicheren „Verwaltungshandwerkzeug“ gemacht werden, damit die rechtlichen Herausforderungen, die sich aus einem E-Government ergeben, gemeistert werden können. Die Bürger werden ein E-Government ohne Sicherheit mit Sicherheit nicht akzeptieren.

7.2 Landesnetz in Betrieb – noch aber fehlen Sicherheitschecks

Die im letzten Tätigkeitsbericht geäußerten Befürchtungen haben sich bestätigt: Das Landesnetz ist tatsächlich im Laufe des Jahres 2001 in Betrieb genommen worden, noch bevor selbst die vom Innenministerium für erforderlich gehaltenen Sicherheitsmaßnahmen realisiert worden sind und eine offizielle Freigabe erfolgt ist.

Seit mehreren Jahren beraten wir das Innenministerium bei der Ausgestaltung der datenschutzrechtlichen und sicherheitstechnischen Konzepte für das Landesnetz (vgl. 23. TB, Tz. 7.4). Angesichts der **grundlegenden aufbau- und ablauforganisatorischen Veränderungen**, die mit der Schaffung einer verwaltungsübergreifenden, einheitlichen Kommunikationsinfrastruktur dieser Art verbunden sind, bedarf es nämlich sehr genauer Vereinbarungen zwischen den beteiligten Ministerien und detaillierter Vorgaben an die Datenzentrale Schleswig-Holstein und die Deutsche Telekom AG als die externen technischen Dienstleister. Das Innenministerium als Betreiber des Landesnetzes übernimmt nämlich **Verantwortungen** und **Kompetenzen**, die bisher bei den einzelnen Ressorts gelegen haben. Dies

geschieht nun nicht wie in vergleichbaren Fällen durch eine formelle Änderung der Geschäftsverteilung der Landesregierung auf der Grundlage der Landesverfassung. Vielmehr akzeptieren die Ministerien so genannte Rahmen- und Anschlussbedingungen des Innenministeriums, in denen neue Zuständigkeitsabgrenzungen vorgenommen und Verantwortlichkeiten festgelegt werden. Diese werden wiederum spezifiziert in Betriebs- und Sicherheitskonzepten.

Es ist verständlich, dass derartig komplexe und von technischen Spezifikationen abhängige Regelwerke nicht nur am „Grünen Tisch“ entwickelt, sondern vor einer endgültigen Beschlussfassung auch in einem **Pilotbetrieb** auf ihre Wirksamkeit und Vollständigkeit hin überprüft werden. Während dieser Phase, die nur in einem eng begrenzten überschaubaren Umfang sowie unter einer besonderen „Beobachtung“ der beteiligten Stellen ablaufen darf, ist es vertretbar, noch nicht alle an sich erforderlichen Sicherheitsvorkehrungen zu aktivieren. Eine zeitliche Begrenzung und eine genaue Überwachung des Systems im Testbetrieb ist jedoch obligatorisch. Außerdem dürfen die „weißen Flecke“ in den Betriebs- und Sicherheitskonzepten nicht zu groß sein, weil sonst die Sicherheitsrisiken nicht mehr überschaubar sind. Nicht ohne Grund hat der Gesetzgeber den Echteinsatz automatisierter Verfahren von einem geordneten Test- und Freigabeverfahren abhängig gemacht.

Vom Innenministerium hätte man erwarten können, dass der Echtbetrieb eines sicherheitstechnisch so anspruchsvollen Projektes erst nach Festlegung aller Details und nach Abschluss aller Tests erfolgen würde. Bis zum Redaktionsschluss dieses Berichtes hatte jedoch noch niemand auf den berühmten **roten Knopf** gedrückt. Gleichwohl war bereits im Herbst 2001 in der Hauszeitschrift der Datenzentrale Schleswig-Holstein (bemerkenswerter Weise nicht in einer Publikation des Innenministeriums) zu lesen: „Das Projekt Landesnetz ist lange aus der Visionsphase heraus. Gegenwärtig sind bereits über 200 Teilnehmeranschlüsse in Schleswig-Holstein realisiert ... Inzwischen ist beabsichtigt, stufenweise in den folgenden Jahren bis ca. 400 Organisationen anzuschließen.“ Der Innenminister hat dieser Darstellung nicht widersprochen.

Das seit Ende 2001 gültige **Sicherheitskonzept** ist zwar von uns analysiert worden. Etwa ein Drittel der sich daraus ergebenden Fragestellungen wurden aber vom Innenministerium nur mit dem Hinweis auf noch nicht definierte Sicherheitschecks beantwortet bzw. als „offene Punkte“ bezeichnet. Technisch funktioniert das Landesnetz. Ob es allerdings nachweisbar mit der gebotenen Sicherheit funktioniert, können wir noch nicht beurteilen. Es kann gut sein, dass man nach einem genauen Durchleuchten aller technischen Komponenten und Abläufe zu dem Ergebnis kommt, dass das erforderliche und angemessene Sicherheitsniveau erreicht und das verbleibende Restrisiko vertretbar ist. Das im Verhältnis zu anderen IT-Maßnahmen dieser Größenordnung straffe Projektmanagement spricht durchaus dafür. Es kann aber auch sein, dass in den noch offenen Punkten bisher nicht erkannte Sicherheitslücken stecken, und vor allen Dingen, dass sich die revisionsfähige Überwachung des laufenden Betriebes des Landesnetzes als problematisch erweist.

Für eine detaillierte Darstellung der noch nicht aktivierten Sicherheitschecks ist ein der Öffentlichkeit zugänglicher Tätigkeitsbericht sicher nicht der geeignete Ort. Welche Bandbreite die derzeit erörterten Fragestellungen umfassen, mögen daher nur zwei Beispiele verdeutlichen:

- An verschiedenen Stellen des Landesnetzes, insbesondere in den Parametern der Übergaberouter ist hard- und softwaretechnisch festgelegt, welche Kommunikationen für die betreffende Behörde möglich sein sollen. Die Konfiguration dieser Systeme kann nicht von den Teilnehmern selbst vorgenommen werden, sondern erfolgt auf deren Antrag durch die Datenzentrale bzw. die Deutsche Telekom AG als die Dienstleister des Innenministeriums. Es dürfte unbestritten sein, dass bei einem solchen Anweisungs- und Durchführungsprozess auch Fehler passieren. Solange diese dazu führen, dass eine bestimmte Kommunikationsmöglichkeit nicht freigeschaltet worden ist, hält sich das sicherheitstechnische Risiko in Grenzen. Werden aber ungewollte Kommunikationswege freigeschaltet oder **missverständliche bzw. falsche Anweisungen** erteilt, kann dies weit reichende datenschutzrechtliche Folgen haben. Standardmäßig gibt man bei dieser Konstellation daher der anweisenden Stelle einen lesenden Zugriff auf die generierten Parameter mit der Maßgabe, in regelmäßigen Abständen und nach jeder Änderung die Korrektheit der gespeicherten Werte zu überprüfen. Diese Möglichkeit ist im Landesnetz bisher noch nicht vorgesehen. Ursache hierfür sind offenbar technische Probleme.
- Die Sicherheits- und Strafverfolgungsbehörden haben unter bestimmten rechtlichen Voraussetzungen, die z. B. im Telekommunikationsgesetz und im G10-Gesetz definiert sind, einen Anspruch darauf, dass der Inhalt von Kommunikationsvorgängen und die Tatsache, wer wann mit wem kommuniziert hat, aufgezeichnet werden. Die Betreiber von Telekommunikationseinrichtungen haben in ihren technischen Systemen entsprechende **Schnittstellen** einzurichten. Für das Landesnetz ist derzeit noch nicht geklärt, ob die Pflicht zur Einrichtung derartiger Mitschnittmöglichkeiten und zur Duldung von **Abhörmaßnahmen** der Deutschen Telekom AG obliegt, weil sie dem Innenministerium den so genannten Backbone zur Verfügung stellt, oder aber ob der Innenminister selbst aufgrund seiner Betreibereigenschaft als Telekommunikationsanbieter anzusehen ist. Hierbei handelt es sich nicht nur um eine Rechts-, sondern auch um eine Sicherheitsfrage. Wenn nämlich entsprechende technische „Anzapfmöglichkeiten“ vorgehalten werden, muss auch geklärt sein, wie eine missbräuchliche Nutzung wirksam unterbunden werden kann. Hierüber trifft das Sicherheitskonzept noch keine Aussagen.

Vor diesem Hintergrund wird mit dem Innenministerium zu klären sein, wie die Defizite bezüglich der Ordnungsmäßigkeit des Landesnetzes kurzfristig behoben werden können. Es ist unumgänglich, die noch ausstehenden Sicherheitsmaßnahmen kurzfristig zu realisieren und die Version 1.0 des Landesnetzes auch offiziell in Betrieb zu nehmen, damit die Anwender wissen, welche **ergänzenden technischen** und **organisatorischen Voraussetzungen** für eine sichere Kommunikation nach wie vor von ihnen selbst geschaffen werden müssen. Das gilt insbesondere für Verwaltungen mit einem hohen Schutzbedarf, wie z. B. die Polizei, die Staatsanwaltschaft oder die Steuerverwaltung.

Was ist zu tun?
Der Innenminister als Betreiber des Landesnetzes muss nicht nur den Nachweis erbringen, dass es funktioniert, sondern auch, dass es mit der gebotenen Sicherheit funktioniert. Dazu bedarf es der abschließenden Definition aller Sicherheitskomponenten und deren offiziellen Inbetriebnahme.

7.3 Sicherheitskonzept für das Sprachnetz immer noch nicht schlüssig

Auch im dritten Jahr des Betriebes des Sprachnetzes fehlt es noch an einem vom Finanzministerium als dem verantwortlichen Betreiber genehmigten Sicherheitskonzept. Da das Gesamtsystem einschließlich der Administration von der Deutschen Telekom AG als Paket übernommen wurde, ist das Ministerium darauf angewiesen, die ihm vorgelegten Unterlagen zu prüfen. Für die Erarbeitung eigener Konzepte fehlen die personellen Kapazitäten und das Know-how.

Die Besonderheit des Sprachnetzes besteht darin, dass der Betrieb der technischen Systeme und deren Administration auf der Grundlage vertraglicher Vereinbarung durch die Deutsche Telekom AG erfolgt. Das Finanzministerium ist zwar der verantwortliche Betreiber, hält aber wegen dieses **Outsourcings** nicht mehr die erforderliche Fachkompetenz vor, um selbst ein Sicherheitskonzept zu erstellen, und es dem Dienstleister als Vorgabe zu präsentieren (vgl. 23. TB, Tz. 7.3). Es ist darauf angewiesen, die ihm von dem externen Dienstleister vorgelegten Vorschläge für Sicherheitsmaßnahmen zu prüfen, sie zu akzeptieren oder zu verwerfen. Auch im dritten Jahr des Betriebs des Netzes ist dieser Prozess noch nicht abgeschlossen.

Nach einem immerhin einjährigem Verzug liegt nunmehr eine prüffähige Unterlage vor. Sie ist nach unserer Einschätzung (die vom Finanzministerium geteilt wird), noch nicht schlüssig und bedarf vielfältiger **Konkretisierungen**. Dies mögen folgende Beispiele für sicherheitstechnisch signifikante Problembereiche verdeutlichen:

- Es ist der Deutschen Telekom AG erlaubt, zur Erbringung der vertraglichen Leistungen **Subunternehmer** einzusetzen. Von diesem Recht wurde in der Weise Gebrauch gemacht, dass von ihr die „Siemens Business Services GmbH & Co. OHG“ (SBS) mit der Bereitstellung der Telekommunikationsanlagen einschließlich der darin betriebenen Endeinrichtungen und dem dazugehörigenden Service beauftragt worden ist. Die SBS ist Eigentümer der eingesetzten Telekommunikationseinrichtungen und stellt die Hardware, Software und ihre Dienstleistungen der Deutschen Telekom AG zur Verfügung. Allerdings hat die Firma SBS mit der Abteilung ICN der Firma Siemens AG ihrerseits einen weiteren Subunternehmer eingeschaltet, der einen Teil der Aufbau- und Serviceleistungen erbringt. Ein anderer Teil wird von dem „Service der Deutschen Telekom AG“ in Subunternehmerfunktion für die Firma SBS erbracht. Der Subauftraggeber ist also gleichzeitig Subunternehmer seines Subunternehmers. Außerdem ist der Generalauftragnehmer des Finanzministeriums nicht Eigentümer der Hard- und Softwarekomponenten, die den wesentlichen Inhalt des

Auftragsverhältnisses ausmachen. Diese Konstruktion ist so untypisch, dass es sehr detaillierter Einzelregelungen bedarf, um sicherzustellen, dass in rechtlichen Konflikt- und in technisch-organisatorischen Problemfällen die Beherrschbarkeit des Gesamtsystems durch das Finanzministerium gewährleistet ist. Die datenschutzrechtlichen Vorgaben können nur dann als erfüllt angesehen werden, wenn sich das Finanzministerium den vollen Durchgriff auf alle beteiligten externen Dienstleister vorbehält und diesen im Rahmen einer aktiven Revision auch wahrnimmt.

- Das **Customer-Service-Center** (CSC) ist eine Organisationseinheit, die zwar in einem Gebäude der Deutschen Telekom AG untergebracht ist, deren Personal jedoch sowohl von ihr als auch von der Firma SBS gestellt wird. In die praktischen Abläufe sind offenbar außerdem auch Mitarbeiter der Firma Siemens AG eingebunden. Aus den vorgelegten Unterlagen geht nicht hervor, ob es den beteiligten Unternehmen außerdem gestattet ist, bestimmte Aktivitäten auch außerhalb der Räumlichkeiten des CSC abzuwickeln. Wir haben deshalb empfohlen, hierüber eindeutige Vereinbarungen zu treffen. Im Ergebnis muss vom Finanzministerium festgelegt werden, von welchen Orten wer auf welche Datenbestände zugreifen und welche Veränderungen vornehmen kann.

- Die im CSC zwischengespeicherten **Gebührendaten** sind zwar in einer passwortgeschützten Datei abgelegt, das Konzept enthält jedoch keine Aussagen darüber, welche Personen im CSC dieses Passwort kennen und damit Zugriff auf die Datensätze haben. Weiterhin ist unklar, ob nach Abruf der Daten von den einzelnen Telekommunikationsanlagen dort eine „echte“ Löschung erfolgt.

- Die bezüglich der Funktionen „**Voice-Mail**“ und „**Fax-Mail**“ von uns bereits mehrfach gestellte Frage, ob eine Löschung der gespeicherten Daten durch den Angerufenen tatsächlich eine spätere Rekonstruktion ausschließt, ist nach wie vor nicht geklärt. Die Zugriffe auf die Datenbestände sollen zwar passwortgeschützt sein. Da das Passwort allerdings vom CSC vergeben und die Zugriffe von dort überwacht werden sollen, bedarf es einer genauen Darstellung der dort bestehenden „Gewaltenteilung“. Zu klären wäre auch die Frage, wie sich bei Abwesenheit des Angerufenen die Dienststelle bzw. der Vertreter die (dienstlichen) Daten verfügbar machen können.

- Vergleichbare Unklarheiten bestehen nach wie vor bezogen auf das **Rufjournal**. Fakt ist, dass ein erfolgreicher Anruf von außen spurenlos durch das System durchgeleitet wird. Da bei eingeschaltetem Rufjournal jeder **Anrufversuch** registriert wird, entsteht jedoch ein Datenbestand, der sowohl für den Anrufer als auch für den Angerufenen rechtlich relevant werden kann. Besonders verwirrend ist in diesem Zusammenhang die Speicherung des vermeintlichen Namens des Anrufers. Es ist eine reine Fiktion, dass in jedem Fall nur der registrierte Nutzer des Anschlusses einen Anruf tätigt. Bei Anrufen von außen dürfte der Name des Anschlussinhabers ohnhin nicht bekannt sein.

- Das Konzept konstatiert zwar, dass im CSC für einen **Mitarbeiter des Finanzministeriums** ein Arbeitsplatz eingerichtet wird, von dem aus die Einhaltung der Datenschutzbestimmungen kontrolliert werden kann, über den technischen Anschluss dieses Arbeitsplatzes, über die zur Verfügung stehenden Datenbestände, deren Auswertbarkeit, ihre Revisionsfestigkeit usw. enthält das Kon-

zept jedoch keine detaillierten Angaben. Hier wird deutlich, dass die Vorschläge der Deutschen Telekom AG und der Firma SBS um konzeptionelle Vorgaben des Finanzministeriums ergänzt werden müssen. Wenn die gesamte operative Administration der Telekommunikationsanlagen von externen Dienstleistern abgewickelt wird, lässt sich die rechtliche und sicherheitstechnische Korrektheit des praktischen Betriebs nur gewährleisten, wenn die Einhaltung des Sicherheitskonzeptes revisionsfest protokolliert und systematisch überwacht wird. Zurzeit können daher über die Wirksamkeit der geplanten Revision noch keine Aussagen getroffen werden.

Was ist zu tun?
Die vorstehend beschriebenen Defizite müssen zeitnah behoben werden. Notwendig ist ein vom Finanzministerium genehmigtes Pflichtenheft, das die Verfahrensweise für den praktischen Betrieb des Sprachnetzes und die Verantwortlichkeiten des Finanzministeriums, der an das Sprachnetz angeschlossenen Behörden, der Deutschen Telekom AG, der Firma SBS und der anderen externen Dienstleister verbindlich festlegt. Hieran anschließen muss sich die für „gemeinsame Verfahren“ obligatorische Vorabkontrolle.

7.4 IKOTECH III – der neue Datenverarbeitungs- und Kommunikationsstandard

Nach der Inbetriebnahme des Landesnetzes mit den Teilkomplexen Sprach- und Datenkommunikation errichtet die Landesregierung nunmehr die dritte große Säule des Landessystemkonzeptes. Wiederum übernimmt das Innenministerium Funktionen und Verantwortungen, die bisher in den einzelnen Ressorts gelegen haben. Die sich daraus ergebenden aufbau- und ablauforganisatorischen sowie sicherheitstechnischen Konsequenzen bedürfen noch einer sorgfältigen Prüfung.

Die von der IT-Kommission des Landes im Dezember 2001 verabschiedeten „Rahmen- und Anschlussbedingungen für Organisation, Technik und Betrieb von IKOTECH III“ beschreiben folgende Zielrichtungen des Projektes: IKOTECH III soll einerseits dem Aus- und Aufbau einer weitestgehend zentral **administrierbaren Servicelandschaft** und andererseits der Entwicklung moderner, **multimediafähiger Büroarbeitsplätze** dienen. Um diese Arbeitplätze nutzen zu können, ist der Anschluss der betreffenden Landesbehörde an die zentralen IKOTECH III-Services verbindlich. Deshalb gliedert sich das Projekt in die drei Verantwortungsbereiche „Organisation“, „System“ und „Büro“.

Das Innenministerium übernimmt also sowohl eine **Betreiberfunktion** wie beim Landesnetz als auch die Rollen eines Softwarehauses und einer **Serviceeinrichtung**. Die Betreiberfunktion bezieht sich auf die Verwaltung des so genannten Verzeichnisdienstes, ohne den eine ressortübergreifende Kommunikation nicht möglich ist. Softwarehaus ist das Innenministerium insofern, als es den Behörden im Lande Standardkonfigurationen für die einheitlichen Betriebssystemkomponenten nach entsprechenden Tests zum Einsatz anbietet (ohne dass für die Behörden eine Installationspflicht besteht). Wenn einzelne Ressorts oder Behörden sich

mit der eigenständigen Administration ihrer Systeme überfordert fühlen, können sie diese Arbeiten als Service vom Innenministerium erledigen lassen. Das Innenministerium bedient sich in allen drei Fällen der Datenzentrale als externem Dienstleister.

Diese vom Grundsatz zu begrüßende Konstruktion wirft eine Vielzahl sicherheitstechnisch relevanter Fragen auf, die in dem (derzeit noch im Entwurfsstadium befindlichen) **Sicherheitskonzept** beantwortet werden müssen. Einige Beispiele mögen dies verdeutlichen:

- Die neuen Zuständigkeitsregelungen und Verantwortungsabgrenzungen sind im Hinblick auf die unterschiedlichen Kooperationsmöglichkeiten zwischen den Ressorts und dem Innenministerium noch nicht abschließend definiert.
- Von zentraler Bedeutung ist, welche Eingriffsmöglichkeiten des Innenministeriums bzw. der Datenzentrale auf die Administrationsebene der ressorteigenen Systeme sich aus der Administration des zentralen Verzeichnisdienstes ergeben (gegebenenfalls sogar ergeben müssen).
- Es muss allen Beteiligten transparent gemacht werden, welche Systemsteuerungsdaten, Informationen über Zugriffsrechte, Passwörter, Benutzerprofile usw. an welchen Stellen abgelegt und wem zugänglich sind.
- Die Organisation des E-Mail-Verkehrs erscheint im Hinblick auf die Zwischenspeicherungsnotwendigkeiten noch klärungsbedürftig. Das Gleiche gilt für die Protokollierungsmöglichkeiten.
- Der Innenminister sollte seinen „Kunden“ deutlich machen, welche Sicherheitsanforderungen er an seinen externen Dienstleister (Datenzentrale) gestellt hat.
- Generell muss geklärt werden, wer die Betreiber- und Servicefunktion des Innenministeriums und die tatsächlichen Aktivitäten des externen Dienstleisters im Sinne einer Revision wie überwachen kann.

Das von der IT-Kommission ebenfalls im Dezember 2001 verabschiedete IKOTECH III-Einsatzkonzept trifft hierüber noch keine abschließenden Aussagen, sodass dem Sicherheitskonzept eine große Bedeutung beikommt.

Was ist zu tun?
Das Innenministerium sollte das Sicherheitskonzept für das Projekt IKOTECH III zügig erarbeiten und vor der endgültigen Beschlussfassung über die zu realisierenden technischen und organisatorischen Maßnahmen eine gründliche Prüfung durch die beteiligten Ressorts und gegebenenfalls auch durch uns veranlassen. Zumindest der zentrale Verzeichnisdienst ist als ein „gemeinsames automatisiertes Verfahren“ anzusehen, das einer Vorabkontrolle durch den behördlichen Datenschutzbeauftragten oder durch das Unabhängige Landeszentrum für Datenschutz unterliegt.

7.5 Prüfungen automatisierter Verfahren

7.5.1 Eine Verwaltung – drei IT-Welten

In der schleswig-holsteinischen Verwaltung gibt es nur wenige Organisationseinheiten mit mehr als 500 IT-gestützen Arbeitsplätzen. Sie sind in den vergangenen Jahren praktisch alle einer datenschutzrechtlichen und sicherheitstechnischen Überprüfung unterzogen worden. Da die ersten Kontrollen über 20 Jahre zurückliegen, haben wir mit systematischen Wiederholungsprüfungen begonnen.

Als wir uns vor mehr als zwei Jahrzehnten erstmalig mit der automatisierten Datenverarbeitung der **Stadt Neumünster** befasst haben, hatten die Rechner noch die Ausmaße großer Kleiderschränke, sie wurden wegen der immensen Kosten von den Stadtwerken, der Stadtsparkasse und der Stadtverwaltung gemeinsam betrieben, und ihre Funktionalität war auf die von schnellen Schreib- und Rechenmaschinen begrenzt. An den Arbeitsplätzen in den Fachämtern wurden für jeden Verarbeitungsprozess Erfassungsbelege ausgefüllt, die Ergebnisse stellten sich als Berge übergroßer papierener Bescheide und schwer zu handhabender Computerlisten dar. Andererseits war die Stadtverwaltung Neumünster als ein Pionier der automatisierten Datenverarbeitung im Land anzusehen.

Daher war zu erwarten, dass sich die Informationstechnik gerade unter diesen Vorzeichen zu einem umfassenden und homogenen Arbeitsmittel entwickelt hätte. Ersteres war zutreffend: Wir fanden eine Client-Server-Welt vor, die aus über 20 Zentralrechnern, ca. 550 Arbeitsstationen, fünf verschiedenen Betriebssystemen, fünf Datenbanksystemen, zwölf selbst konzipierten sowie aus ca. 40 auf Fremdprodukten basierenden automatisierten Verfahren bestand. Allerdings konnte von einer aufbau- und ablauforganisatorischen Homogenität der Datenverarbeitung keine Rede sein. Vielmehr hatten sich in der Stadtverwaltung **drei** höchst **unterschiedliche IT-Welten** entwickelt:

- eine zentrale IT-Organisation,
- verschiedene fachbereichsbezogene PC-Welten und
- eine von der übrigen Stadtverwaltung abgekoppelte IT-Organisation im Bereich des Beschäftigungsbeauftragten.

Während die Gestaltung und der Betrieb der zentral gesteuerten automatisierten Verfahren nur wenig Anlass zu datenschutzrechtlichen und sicherheitstechnischen Beanstandungen gab (ihre Dokumentation war sogar außergewöhnlich vollständig und übersichtlich), ergab sich für die **PC-Welt** in den einzelnen Fachdiensten ein grundlegend anderes Bild. Es zeigte sich bereits bei punktuellen Überprüfungen, dass ein inhaltlich schlüssiges IT-Konzept im Jahr 1998 viel zu spät in Kraft gesetzt worden war. Bereits vorher hatten sich nämlich in den verschiedenen Organisationseinheiten Verfahrensweisen etabliert, die den Vorgaben dieses Konzeptes teilweise diametral entgegenstanden. Es macht z. B. für die Durchführung von „IT-Projekten“ die Vorgabe, dass eine gründliche Vorplanung bestehend aus einer

Anwendungskonzeption, einem Pflichtenheft sowie der Darstellung von Realisierungsstufen vorzunehmen ist. Wäre dies in allen Fällen geschehen, hätten sich z. B. folgende **Mängel** verhindern lassen:

- Die Verfahrensdokumentationen waren unvollständig, teilweise waren überhaupt keine Freigabeunterlagen vorhanden.
- Gesundheits- und Beurteilungsdaten waren unverschlüsselt auf zentralen Servern abgelegt.
- Die Passwörter wurden unverschlüsselt gepeichert, Passwortwechsel wurden nicht vorgenommen.
- Nicht mehr erforderliche Sozialdaten konnten nicht gelöscht werden, weil in der Software diese Funktion nicht vorgesehen war.
- Seit Jahren erfolgte keine Löschung der nicht mehr benötigten Textdokumente, selbst dann nicht, wenn sie sensible Personal-, Steuer- oder Sozialdaten enthielten.
- Eine Dokumentation der Zugriffsberechtigungen auf die Vielzahl der Datenbestände bestand nicht, hieraus resultierten u. a. zu weit gehende Zugriffsrechte auf Sozialdaten.
- Diese eher technischen Mängel korrespondierten mit organisatorischen Unzulänglichkeiten. So erfolgte selbst im Personalamt die Entsorgung von Schriftstücken mit personenbezogenem Inhalt über die Papierkörbe, weil es an Schreddern fehlte. Das „Informationsbüro“ im Sozialamt ist als „Glaskasten“ gestaltet, sodass man sogar von der Straße aus sehen kann, wer Sozialhilfe in Anspruch nimmt. Außerdem waren die Arbeitsplätze und Wartezonen so beengt, dass bei den Gesprächen zwischen den Mitarbeitern und den Sozialhilfeempfängern viele Menschen zwangsweise mithörten, sodass von einem Sozialgeheimnis nicht die Rede sein konnte.

Bemerkenswert ist allerdings, dass auf Betreiben des zentralen EDV-Dienstes darauf verzichtet worden ist, das interne Netz der Stadtverwaltung mit dem Internet zu verbinden. Aus Sicherheitsgründen findet die **Internet-Kommunikation** nur über unvernetzte PC in den einzelnen Fachbereichen statt. Das gilt jedoch nicht für den auch im Übrigen abgekoppelten Bereich des Beschäftigungsbeauftragten.

Die **technischen** und **organisatorischen Sicherheitsmaßnahmen** in diesem Bereich mussten angesichts der Schutzbedürftigkeit der verarbeiteten Daten als völlig unzureichend angesehen werden. Zu den Aufgaben des Beschäftigungsbeauftragten gehört es nämlich, Arbeitssuchende vorübergehend in Projekten zu beschäftigen, sie zu beraten, bei der Erstellung von Bewerbungsunterlagen zu unterstützen, weiter zu vermitteln und Hilfestellungen in persönlichen Problemsituationen zu geben. Aufgrund dessen werden Informationen über Lebensläufe, Arbeitsverträge, Zeugnisse, berufliche Werdegänge, familiäre Situationen, Gesundheitszustände und „Vermittlungshemmnisse“ gespeichert.

Die dazu erforderlichen Hard- und Softwarekomponenten sowie die Datenbanken wurden überwiegend von befristet beschäftigten oder sonstigen Hilfskräften ohne konkrete konzeptionelle Vorgaben betreut. Eine Koordination mit den anderen Stellen der Verwaltung insbesondere mit dem zentralen EDV-Dienst fand praktisch nicht statt. Es handelte sich im Ergebnis um eine Art „**Training on the Job**".

Dieses Konzept ist unter Sicherheitsgesichtspunkten als gründlich misslungen zu bezeichnen. Die Mängelliste nur in diesem Bereich umfasst immerhin 37 Positionen. Eine detaillierte Darstellung würde dem Umfang dieses Berichtes sprengen und wäre im Hinblick auf die **Reaktion der Stadt** auf unsere Beanstandungen auch nicht zweckdienlich. Sie hat nämlich mit einer außergewöhnlichen Konsequenz reagiert. Ohne die Dinge zu beschönigen, ist die Behebung der Mängel in Angriff genommen worden. Es wurde eine fachdienstübergreifende Arbeitsgruppe gebildet, die entsprechende aufbau- und ablauforganisatorische Änderungen ausarbeiten und umsetzen soll. Weiterhin fanden von uns moderierte Workshops statt, in denen die künftigen (richtigen) Verfahrensweisen mit den Verantwortlichen der einzelnen Bereiche diskutiert wurden. Über den Fortgang der Arbeiten sollen wir informiert werden.

Was ist zu tun?
Die Stadt Neumünster muss die datenschutzrechtlichen und sicherheitstechnischen Mängel zügig beseitigen.

7.5.2 Eine etwas andere Behörde

Die Behörden der Landes- und der Kommunalverwaltung sowie der anderen öffentlichen Stellen befassen sich zu einem weit überwiegenden Teil, teilweise sogar ausschließlich, mit der Verarbeitung personenbezogener Daten. Im Landesamt für Natur- und Umweltschutz spielen personenbezogene Daten nur eine untergeordnete Rolle. Wird der Datenschutz deshalb vernachlässigt?

Obwohl im Landesamt für Natur- und Umweltschutz (LANU) mehr als 300 Arbeitsplätze mit PC ausgerüstet und 15 Zentralrechner installiert sind, war es nicht ganz einfach, die personenbezogenen Datenbestände aufzuspüren. Im Verhältnis zu der Gesamtmenge der überwiegend wissenschaftlichen Daten nehmen sie nur eine untergeordnete Rolle ein. Es handelt sich im Wesentlichen um Personaldaten. Weitere **personenbezogene Datenbestände** fanden sich in den Bereichen der Umwelttoxikologie und des Natur-Umwelt-Informationssystems (NUIS), das sich aus dem landschafts- und dem wasserwirtschaftlichen Informationssystem sowie dem Bodenkataster, dem Abfallüberwachungs- und dem abfallwirtschaftlichen Informationssystem zusammensetzt.

Die einzelnen automatisierten Fachverfahren gaben keinen Grund zu größeren Beanstandungen. Als **problematisch** erwies sich jedoch das **Management** der mit den Bürokommunikationspaketen erzeugten Datenbestände. Mit ihnen wurden im Laufe der Jahre insgesamt ca. 180.000 Dateien mit einem Datenvolumen von ca.

23 Gigabyte erzeugt. Zu 99 % handelt es sich um nicht personenbezogene, wissenschaftliche Daten, für die keine Löschungsnotwendigkeit besteht. Der Rest von einem Prozent mit Personenbezug wurde aber nicht etwa separiert, sondern befindet sich als Einsprengsel in diesem riesigen Datenpool. Eine systematische Löschung der zweifelsfrei nicht mehr erforderlichen Dokumente und Dateien ist also praktisch unmöglich. Seiner Löschungsverpflichtung kann das LANU also nur dann nachkommen, wenn sie zufällig entdeckt werden. Eine Reorganisation der Datenhaltung wurde uns zugesagt.

Auch in einem zweiten Punkt unterscheidet sich die Datenverarbeitung des LANU von der anderer Behörden: Wegen der in vielen Teilbereichen wissenschaftlichen Ausrichtung wird von allen Mitarbeitern eine Informationsgewinnung und eine **Kommunikation über das Internet** erwartet. Dies führt täglich zu vielfältigen Internet-Aktivitäten. Downloads sind zwar nur dem IT-Dezernat gestattet, eingegangene E-Mails sind auf Viren zu überprüfen und ausgehende E-Mails mit personenbezogenem Inhalt sind zu verschlüsseln. Ansonsten sind den Nutzern aber keine Beschränkungen auferlegt, wenn die Internet-Nutzung denn dienstlichen Zwecken dient.

Die bewusste Öffnung des internen Netzes des LANU zum Internet hin warf die Frage auf, ob und mit welchem Aufwand ein Angriff auf die Vertraulichkeit der gespeicherten personenbezogenen Datenbestände erfolgreich sein könnte. Wir haben dies (soweit möglich) mit Wissen des LANU durch **„Angriffe“ von außen** getestet. Dabei stellten wir fest, dass die Einhaltung des Verbotes von Downloads aus dem Internet faktisch nicht zu überprüfen ist. Ob sich die Mitarbeiter an die Anweisung halten oder nicht, musste ebenso unbeantwortet bleiben wie die Frage, ob sie in unzulässiger Weise Kopien vertraulicher Unterlagen in den häuslichen Bereich mitnehmen. Faktisch kann beides technisch nicht überwacht werden.

E-Mail-Angriffe sind grundsätzlich dadurch möglich, dass man bekannte Softwarefehler, die nicht rechtzeitig durch entsprechende Korrekturen (Patches) behoben worden sind, ausnutzt oder dass man schädigenden Code auf den Rechner platziert, wenn die Mitarbeiter unvorsichtig mit E-Mails umgehen. Die von uns gestarteten Angriffe waren nicht erfolgreich. Dies lässt allerdings keine sicheren Rückschlüsse auf die Zukunft zu, weil die Tatsache unserer Überprüfung und der Tests den Mitarbeitern des LANU bekannt war. Man darf unterstellen, dass sie in dieser Zeit besonders vorsichtigt agiert haben.

Im Rahmen der Prüfung stellte sich heraus, dass das LANU eine Firewall der Datenzentrale einsetzt, deren Filterregeln es nicht im Detail kennt. Dies ist ein unbefriedigender Zustand, weil die Datenzentrale offenbar generell nicht bereit ist, ihren Kunden gegenüber dieses „Geheimnis“ zu lüften, angeblich aus Sicherheitsgründen. Wir haben dem Landesamt unsere Unterstützung bei der Lösung dieser Grundsatzfrage im Rahmen der Konzipierung des Landesnetzes (Tz. 7.2 und 7.4) zugesagt.

Was ist zu tun?
Das Landesamt für Natur- und Umweltschutz wird sein Datenmanagement grundlegend reorganisieren müssen. Die Absicherung des Verwaltungsnetzes gegenüber dem Internet wird sich nicht auf Dauer nur auf organisatorische Regelungen stützen lassen.

7.5.3 Verwirrende Systemadministration

Sicherheitstechnische Überprüfungen werden, wenn keine schriftlichen Unterlagen vorgelegt werden können, im Wesentlichen in Form von „Interviews" der beteiligten Mitarbeiter vor Ort durchgeführt. Dabei ergaben sich bisher höchst selten nachträgliche Interpretationsschwierigkeiten. Das Landesamt für Gesundheit und Arbeitssicherheit stellte die Organisation der Systemadministration in ihren Außenstellen nachträglich allerdings ganz anders dar, als wir sie vorgefunden haben.

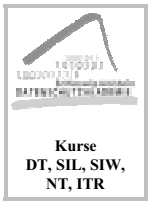
Die Errichtung des Landesamtes für Gesundheit und Arbeitssicherheit erfolgte 1998 im Zusammenhang mit einer Strukturreform der nachgeordneten Behörden in den Geschäftsbereichen mehrerer Ministerien. Es gliedert sich in sieben Dezernate am Standort Kiel und die zwei von uns geprüften unselbstständigen Außenstellen in Itzehoe und Lübeck. Die EDV-Ausstattung war bei der Gründung an allen drei Standorten unterschiedlich. Hieraus resultieren eine Reihe **sicherheitstechnischer Unzulänglichkeiten**, die nach Aussagen des Landesamtes alsbald behoben werden sollen.

Unsere Kritik an unklaren Zuständigkeiten bezüglich der Systemadministration und den daraus resultierenden Sicherheitsrisiken hielt man allerdings nicht für gerechtfertigt, weil aus der Sicht der Behördenleitung die Organisationsstruktur eine ganz andere war, als sie von uns vorgefunden wurde. Selbst offene Diskettenlaufwerke an den Arbeitsplätzen und ein offiziell nicht freigegebener Internet-Zugang der Systemadministratoren, deren Risikopotenzial von den Mitarbeitern „vor Ort" nicht bestritten worden ist, wurden nachträglich gerechtfertigt. Das Landesamt wird sich mit seinen Außenstellen in absehbarer Zeit den IKOTECH-Konventionen anschließen. Die dabei notwendigen **Strukturänderungen** werden dazu führen, dass derartige Diskrepanzen in Zukunft nicht mehr entstehen können.

Was ist zu tun?
Spätestens im Zusammenhang mit der Einführung der IKOTECH-Konventionen muss das Landesamt für Gesundheit und Arbeitssicherheit für eindeutige Verantwortlichkeiten bezüglich der Administration seiner IT-Systeme sorgen und ein verbindliches Sicherheitskonzept aufstellen.

7.5.4 Computer in Kommunen nach wie vor ein Sicherheitsrisiko

Die Überprüfung des Sicherheitsniveaus der informationstechnischen Systeme insbesondere in kleinen und mittleren Kommunalverwaltungen ist längst zur Routine geworden. Die meisten Systemadministratoren freuen sich über unsere Kontrollen, weil sie Hilfestellungen bei der Lösung ihrer Probleme erwarten. Nach wie vor sind viele Risiken hausgemacht, weil von den Mitarbeitern der EDV-Stellen mehr erwartet wird, als sie unter den gegebenen Umständen leisten können.



Kurse
DT, SIL, SIW, NT, ITR

Noch vor wenigen Jahren wäre es undenkbar gewesen, dass Systemadministratoren bei uns anfragen, wann ihre Behörde denn „endlich“ auf dem Prüfungsplan steht, man wolle gerne die selbst noch nicht entdeckten sicherheitstechnischen **Schwachstellen aufgezeigt** bekommen und beheben. Nachdem ein Großteil der für die Informationstechnik in den Kommunen zuständigen Mitarbeiter Kurse an der DATENSCHUTZAKADEMIE Schleswig-Holstein besucht und dort unsere Prüfer kennen gelernt hat, sind derartige Gespräche alltäglich. Höchst selten treffen wir bei Prüfungen auf Administratoren mit einem zu gering ausgeprägten Sicherheitsbewusstsein; die weit überwiegende Zahl von ihnen hat den Ehrgeiz, ein sicheres System vorzuweisen.

Es stellt sich daher wie in den vergangenen Jahren (vgl. 23. TB, Tz. 7.5.2) die Frage, warum unsere Prüfungen dann immer noch zu so **vielen Beanstandungen** führen.

- Warum finden wir Software vor, von der niemand weiß, wozu sie gebraucht wird, und warum gibt es Benutzerkonten, deren Zweck niemand kennt?
- Warum werden externe Dienstleister ohne schriftliche Verträge eingeschaltet und ihre Arbeit nicht kontrolliert?
- Warum kauft man sich eine Firewall ein, ohne sich erläutern zu lassen, welche Angriffe aus dem Internet sie ausfiltert?
- Warum sperrt man das System nicht, wenn mehrfach falsche Passwörter eingegeben worden sind?
- Warum werden Sicherheitskomponenten der Betriebssysteme nicht „eingeschaltet“?
- Warum gibt es keine eindeutig definierten Zugriffsberechtigungen?
- Warum wird überflüssiger „Datenschrott“ über Jahre hinweg nicht gelöscht?
- Warum sind die installierten technischen Systeme, die eingesetzte Software und die gespeicherten Datenbestände so schlecht dokumentiert?
- Warum werden Tests an „lebenden Systemen“ durchgeführt, obwohl man weiß, dass sie auch schief gehen können?

Neben vielen anderen Gründen sind zwei Aspekte augenfällig:

- Das Verwaltungsmanagement überfordert häufig ihre meist nur „nebenbei“ als Administratoren tätigen Mitarbeiter.
- Die externen Dienstleister verhalten sich ihnen gegenüber nicht immer fair.

Der Aufbau und die Administration des laufenden Betriebes von Client-Server-Systemen erfordert ein **umfangreiches Fachwissen**, das ständig auf dem neuesten Stand gehalten werden muss. Die Erlangung dieser Kenntnisse ist zeit- und kostenaufwändig und führt häufig nicht zu unmittelbar zählbaren Erfolgen. Völlig zu Unrecht wird dies zudem als Fortbildung bezeichnet und ist mit dem Merkmal einer freiwilligen Leistung des Arbeitgebers versehen. Die betreffenden Mitarbeiter müssen allzu häufig nachdrücklich um die Genehmigung zur Teilnahme an einem Lehrgang bitten, anstatt dass man sich seitens der Verwaltung um ihre qualifizierte Ausbildung bemüht. Andererseits erwartet man ein mit einem minimalen Aufwand administriertes, perfekt funktionierendes System. Die Bürgermeister und Selbstverwaltungsgremien forcieren einerseits so risikobehaftete Vorhaben wie die Internet-Kommunikation, um beim E-Government ganz vorne dabei zu sein, andererseits werden den Administratoren sehr selten Testsysteme zur Verfügung gestellt, an denen sie ihre theoretischen Kenntnisse und die Wirksamkeit von Sicherheitsmaßnahmen ausprobieren können.

Wenn wir in unseren Kursen der DATENSCHUTZAKADEMIE Schleswig-Holstein demonstrieren, wie einfach es vielfach ist, die korrekte Arbeitsweise der Systeme und die Vertraulichkeit der Daten zu beeinträchtigen, hören wir immer wieder: „**Das müsste sich mein Chef einmal anhören**, dann würde er vielmehr Verständnis für meine Probleme haben“ (vgl. Tz. 7.1).

Auch die **Softwarehäuser** und sonstigen **externen Berater** sind eher an zufriedenen Chefs interessiert als an einem fairen Umgang mit den „nachgeordneten“ Administratoren. Eine problemorientierte Beratung und die handwerklich ordentliche Abwicklung der Aufträge wird nicht selten dem Diktat des kostengünstigsten Angebots untergeordnet. Anders ist nicht zu erklären, dass selbst die Datenzentrale offenbar nicht in der Lage ist, von ihr installierte Systeme vor der Übergabe von Installations- und Testsoftware sowie von nicht mehr benötigten Benutzerkonten zu „befreien“ und Installationspasswörter zu ersetzen. Gleiches gilt für eine sachgerechte Darstellung der Filtermechanismen von Firewalls (vgl. Tz. 7.5.2).

Was ist zu tun?
Im Verwaltungsmanagement muss ein Umdenkungsprozess stattfinden. Eine gut funktionierende Systemadministration ist genau so wichtig wie z. B. die fachlich korrekte Arbeit in der Kämmerei, dem Steuer- und dem Sozialamt. Qualifizierte Mitarbeiter fallen jedoch nicht vom Himmel, sie müssen ausgebildet und gefördert werden.

7.6 Wohin mit den Altakten?

Aus der Presse erfuhren wir, dass in frei zugänglichen, unverschlossenen Müllcontainern eines Krankenhauses Papiere und Unterlagen mit personenbezogenen Patientendaten gefunden worden waren. Bei 50 privaten und öffentlichen Stellen mit besonders sensiblen Datenbeständen führten wir daraufhin unangemeldet Prüfungen durch.

Das Ergebnis war erschreckend. Bei zehn Stellen fanden sich **höchst vertrauliche Unterlagen** in Müllcontainern: Ärztliche Gutachten, medizinische Stellungnahmen, Patientenlisten, Beihilfeanträge und –bescheide, Schriftverkehr über die Hormonbehandlung des Sohnes oder die Psychotherapie der Ehefrau, Sozialhilfebescheide, umfangreiche Listen von Sozialhilfeempfängern, Bußgeldbescheide, Vermerke über Pflegekinder und deren Pflegefamilien, Telefonnotizen über Adoptionswünsche, Provisionsabrechnungen – alles war öffentlich zugänglich.

Mehr als verwundert zeigten sich die verantwortlichen Leiter der betreffenden Stellen. Anhand unserer detaillierten Prüfberichte begab man sich umgehend auf **Fehlersuche**. Dass Unterlagen mit personenbezogenen Daten nicht in den normalen Hausmüll gehören, war allen bekannt. Wie konnte es dennoch zu solchen Schlampereien kommen? Als häufigste Ursache wurde uns individuelles Fehlverhalten einzelner Mitarbeiter genannt. Unkenntnis, mangelnde Sensibilität, Überlastung, Bequemlichkeit und in einem Fall sogar böser Wille waren die Ursachen dafür, dass entgegen bestehender Arbeitsanweisungen Unterlagen nicht datenschutzgerecht entsorgt wurden. Das Fehlen von Aktenvernichtern (Schreddern) und verschließbaren Datensicherheitsbehältern sowie organisatorische Defizite trugen ihr Übriges bei.

Was ist seitdem passiert? Unsere Prüfungsergebnisse wurden den Bediensteten zur Kenntnis gegeben. Arbeitsanweisungen wurden überarbeitet, Informationswege und Arbeitsabläufe optimiert, Aktenvernichter in ausreichender Zahl beschafft, Aufklärungsveranstaltungen und Schulungen der Mitarbeiterinnen und Mitarbeiter (auch der Reinigungskräfte) sowie innerbetriebliche bzw. innerbehördliche Kontrollen durchgeführt. Einige Stellen nahmen die Vorfälle zum Anlass einer umfassenden Sicherheitsprüfung auch in Bezug auf Schließanlagen und Aktenschränke. Insgesamt waren wir überrascht über das positive Echo bei den geprüften Stellen. Es schien ein **„Ruck“ durch die Institutionen** gegangen zu sein.

Ein Bericht für den Sozialausschuss des Landtages über diese Prüfungen und Feststellungen ist in einer anonymisierten Fassung im Internet unter

www.datenschutzzentrum.de/material/themen/pruefbe/papmuell.htm

veröffentlicht.

Was ist zu tun?
Papiere und Unterlagen mit personenbezogenen Daten gehören nicht in den Müll, sondern sind datenschutzgerecht zu entsorgen. Die Regeln hierfür sind allgemein bekannt zu geben und laufend zu kontrollieren. Aktenschredder sollten zum Bürostandard gehören.

8 Recht und Technik der neuen Medien

8.1 E-Government

Immer mehr Verwaltungsbehörden wollen sich auch im Internet für die Bürger öffnen. So nützlich die Online-Präsenz der Verwaltung sein kann, sie darf nicht dazu führen, dass Datenschutzstandards abgebaut oder Bürger zum Einsatz von IT-Verfahren genötigt werden, die sie nicht beherrschen können.

Im privaten Sektor hatten Schlagworte wie „E-Commerce“, „E-Business“, „E-Banking“ oder sogar „E-Culture“ bis vor kurzem einen magischen Klang. Das vorgestellte „E“ verhieß glänzende Geschäfte und den Einsatz modernster Techniken. Es überrascht nicht, dass auch die öffentlichen Verwaltungen ihre Dienstleistungen in diesem Glanz positionieren und dazu an den Modernisierungseffekten teilnehmen wollen, die das Internet verspricht (vgl. Tz. 7.1). Obwohl die korrekte Übersetzung von Verwaltung eigentlich „Administration“ wäre, hat sich für diesen Bereich der Begriff „**E-Government**“ durchgesetzt. Dahinter steht das konkrete Ziel, möglichst viele Dienstleistungen der öffentlichen Verwaltung auch im Internet anzubieten. Auf Bundesebene wurde die ehrgeizige Losung ausgegeben, bis zum Jahr 2005 von 383 Verwaltungsleistungen des Bundes 376 zumindest teilweise online abwickeln zu wollen. Auch im Land Schleswig-Holstein gibt es auf Landesebene und auf kommunaler Ebene entsprechende Vorstellungen.

Schriftform und elektronische Signatur

Allerdings gilt es für die öffentlichen Verwaltungen zusätzliche Hürden zu nehmen, die in dieser Weise für den E-Commerce nicht bestehen. Dazu gehört, dass für eine große Zahl von Verwaltungsleistungen gesetzlich die **Schriftform** vorgeschrieben ist. Zwar stehen Verfahren der qualifizierten elektronischen Signatur (vgl. 23. TB, Tz. 8.8) zur Verfügung, um die Schriftform zu ersetzen. Dazu bedarf es aber zunächst einer Änderung des Verwaltungsverfahrensrechts, in dem ebenso wie im Zivilrecht (Tz. 14.9) eine weitgehende Gleichstellung der Signaturen zur Schriftform angeordnet werden müsste.

Da die Verwaltungsverfahrensgesetze auf Bundes- und Länderebene (in Schleswig-Holstein das Landesverwaltungsgesetz, LVwG) in den wesentlichen Passagen ähnlich sind, kam es zu einer länderübergreifenden Koordination. Im Sommer des Jahres 2001 stellte das Bundesinnenministerium den Entwurf zur **Änderung des Verwaltungsverfahrensgesetzes** und zur Einführung eines elektronischen Verwaltungsaktes im Internet zur öffentlichen Diskussion.

Der Gesetzentwurf beinhaltet die Gefahr, dass die Bürger von den Verwaltungen geradezu **in informationstechnische Verfahren gedrängt** werden könnten, die viele nicht beherrschen. So ist z. B. nicht ausgeschlossen, dass Behörden allein aufgrund der Tatsache, dass ein Bürger eine Anfrage per E-Mail schickt, vermuten dürfen, dass dieser Bürger in der Lage ist, elektronisch signierte Verwaltungsakte zu empfangen und zu verarbeiten. Die daran anschließenden Prozeduren zur Prüfung der Echtheit der Signatur sollen ihm aufgebürdet werden.

Risiken der elektronischen Signatur

Mit der elektronischen Signatur können erhebliche Risiken und Belastungen verbunden sein. Es handelt sich um ein strukturelles Problem, dass die **Signaturen mit der Zeit unsicher** werden. Es kann damit gerechnet werden, dass die Rechnerkapazitäten in den nächsten Jahren weiter zunehmen. Eine Signatur mit einer Schlüssellänge, die heute noch als sicher gilt, muss in einigen Jahren bereits als unsicher eingestuft werden. Aus diesem Grund ist die Geltung der Signaturschlüsselzertifikate für qualifizierte Signaturen auf höchstens fünf Jahre beschränkt. Wird einem Bürger ein Verwaltungsakt in elektronischer Form mit der elektronischen Signatur der Behörde zugestellt, so stellt sich die Frage, was nach Ablauf der Gültigkeit des Signaturschlüssels der Behörde geschehen soll. Handelt es sich um einen begünstigenden Verwaltungsakt, so wird der Bürger im Zweifel ein Interesse daran haben, dass die Beweiskraft des elektronischen Dokuments auch nach einer längeren Zeit erhalten bleibt. Offen ist z. B., ob die Behörde von sich aus verpflichtet ist, eine neue Signatur anzubringen, ob sie den Verwaltungsakt neu erlassen muss oder ob der Bürger seinerseits Mitwirkungspflichten hat.

In diesem Punkt unterscheidet sich die Situation im öffentlichen Bereich von der im privaten Sektor, wo sich gleichberechtigte Rechtssubjekte gegenüberstehen, die darüber entscheiden können, ob sie an Verfahren wie der elektronischen Signatur teilnehmen und die dann jeweils bestimmte Obliegenheiten zu beachten haben. Staatliche Stellen müssen dagegen auf die **Wahrung der Grundrechte** ebenso Wert legen wie auf Bindungen aus dem verfassungsmäßigen Rechts- und Sozialstaatsprinzip. Sie dürfen daher die Bürger mit diesen Problemen nicht alleine lassen. Vielmehr muss für die Bürger eine sichere Infrastruktur zur Verfügung stehen, wenn sie am E-Government teilnehmen sollen.

Unsichere IT-Komponenten als Hemmschuh

Kritische Fragen resultieren daraus, dass die meisten IT-Komponenten, die zum Erzeugen und Prüfen elektronischer Signaturen beim Aussteller und Empfänger von elektronisch signierten Dokumenten eingesetzt werden, nur so sicher sind, wie die zugrunde liegende Software der Betriebssysteme. Auf dieses Problem haben Experten aufmerksam gemacht, denen es gelang, die Sicherheitsmechanismen der elektronischen Signatur zu umgehen. Welche **weit reichenden Folgen** dies haben kann, wird vor allem deutlich im Zusammenhang mit den mittlerweile geschaffenen Beweiserleichterungen im Zivilprozess. Im schlimmsten Fall sieht sich ein Bürger, der auf Betreiben einer Behörde am Signaturverfahren teilnimmt, mit einem elektronischen Dokument konfrontiert, das seine Signatur trägt, die er aber nicht ausgestellt hat. Nur wenn er genau nachweisen kann, dass und wie es Unbefugten gelungen sein kann, durch „Einbruch“ in seinen Rechner seine Signatur zu erzeugen, kann er der Haftung daraus entgehen. Im Hinblick auf diese Gefahren macht die Regulierungsbehörde für Telekommunikation und Post darauf aufmerksam, dass am Verfahren der elektronischen Signatur nur teilnehmen soll, wer über eine sichere IT-Infrastruktur verfügt. Dies trifft auf die allermeisten privaten Anwender in ihrer häuslichen Umgebung aber gerade nicht zu.

Dies und eine Reihe weiterer **Kritikpunkte** am Entwurf zur Änderung des Verwaltungsverfahrensgesetzes zeigen deutlich, dass es wenig Erfolg versprechend ist, durch einen Federstrich des Gesetzgebers auf einen Schlag von den in den Verwaltungen seit Jahrhunderten praktizierten schriftlichen Formen umsteigen zu müssen auf elektronische Verfahrensweisen, die zum Teil unsicher und in ihrer Funktionalität nicht mit den bisher verwandten Verfahren vergleichbar sind.

Weitergehende Pflichten der öffentlichen Verwaltung

Aber auch dort, wo schon nach geltendem Recht Verwaltungsleistungen ohne Einhaltung der Schriftform erbracht werden können, ist Vorsicht bei der Einführung von Komponenten der elektronischen Verwaltung geboten. So ist z. B. die **Beantragung eines Führungszeugnisses** nach dem Wortlaut des Bundeszentralregistergesetzes nicht an die Schriftform gebunden. Allerdings haben die zuständigen Meldebehörden sicherzustellen, dass Antragsteller und Person, für die das Führungszeugnis erteilt wird, übereinstimmen. Dies wird sich online selbst bei Verwendung von elektronischen Signaturen nicht bewältigen lassen, da nicht ausgeschlossen ist, dass jemand die Informationen, die zur Benutzung des privaten Schlüssels benötigt werden, an Unbefugte weitergibt. Das Beispiel zeigt, dass öffentliche Stellen weitergehende Verpflichtungen haben als Private, wenn Leistungen über das Netz angeboten werden.

Schließlich muss der Tendenz begegnet werden, dass unter dem Vorwand eines effektiven E-Government datenschutzrechtliche Standards abgebaut werden. So wurden bereits Äußerungen laut, wonach eine effektive Verwaltung der Daten bei den Behörden im so genannten Back-Office durch das **Zweckbindungsgebot** erschwert bzw. unmöglich gemacht werde. Solche Äußerungen zielen nicht darauf ab, E-Government datenschutzgerecht zu organisieren, sondern stattdessen den Datenschutz in diesem Bereich zurückzuschneiden. Die erheblichen Kosten, die von einigen öffentlichen Stellen, vor allem im kommunalen Bereich, in ihre jeweiligen E-Government-Projekte investiert werden, dürfen nicht dazu führen, dass die Rechte der Bürger schlichtweg vom Tisch gewischt werden.

? Back Office

Back-Office ist der Gegenbegriff zu Front-Office. Nach Konzepten zur Verwaltungsmodernisierung werden im Front-Office die Anliegen und Anträge der Bürger entgegengenommen; es stellt den Kontaktpunkt zwischen Verwaltung und Bürger dar. Dagegen findet im Back-Office die eigentliche Sacharbeit statt, die durch die Anfragen im Front-Office generiert wurde. Hier werden Bescheide erstellt, Auszahlung angeordnet und so weiter. Da diese Betrachtungsweise die Arbeit der Verwaltung nicht nach den einzelnen Verfahren sondern rein funktional erfasst, erscheinen die existierenden rechtlichen Beschränkungen wie des Zweckbindungsgebot als unfunktionale Einschränkungen. Dabei darf aber nicht außer Acht gelassen werden, dass sie zum großen Teil von Verfassungs wegen vorgegeben sind.

Was ist zu tun?
Kommunen und andere öffentliche Stellen des Landes müssen bei der Einführung von Verwaltungsleistungen im Internet immer im Auge behalten, dass sie eine besondere Verantwortung für den Datenschutz der Bürgerinnen und Bürger haben.

8.2 Protokollierung der gesamten Internet-Kommunikation?

Manche Politiker wünschen sich, dass jede Bewegung der Nutzer im Internet protokolliert wird, denn alles kann für eine spätere Strafverfolgung relevant sein. Eine derartige Vollprotokollierung würde jedoch zu riesigen Datenbeständen führen und der illegalen Auswertung Tür und Tor öffnen. Sie wäre verfassungswidrig.

Neben den Millionen rechtstreuen Internet-Nutzern gibt es einige Zeitgenossen, die das Internet auf unterschiedliche Weise für verschiedene Deliktsarten benutzen. Neben der in diesem Zusammenhang häufig zitierten Kinderpornografie spielen vor allem Betrugsfälle und **Hacker-Angriffe** eine Rolle. Ein weiteres Problem besteht darin, dass die Kommunikation in missliebigen Diskussionsforen gestört oder durch technische Eingriffe verhindert wird.

> **?** ***IP-Nummer***
>
> *Die IP-Nummer (oder IP-Adresse; IP steht für Internet Protocol) ist die eindeutige Adresse eines jeden Rechners im weltweiten Internet. Man schreibt sie meist als vier durch Punkte voneinander getrennte Zahlen zwischen 0 und 255. Da Bezeichnungen leichter merkbar sind als Zahlen, sind den IP-Nummern so genannte Domain-Namen zugeordnet. So hat der Webserver, der sich über www.datenschutz.de adressieren lässt, die IP-Nummer 213.178.09.187. Die Zuordnung wird im so genannten Domain Name System (DNS) über bestimmte DNS-Server aufgelöst.*

Liegen Straftaten vor, so können sich die Strafverfolgungsbehörden bei ihren Ermittlungen auf die Daten stützen, die auf den Internet-Rechnern über die jeweiligen Vorfälle gespeichert sind. In der Regel stoßen die Ermittler zunächst auf eine IP-Adresse, die mit der konkreten Tat in Verbindung gebracht werden kann. Die meisten Internet-Nutzer verfügen nicht über eine eigene **IP-Adresse**, sondern sie bekommen jeweils eine für die Dauer der Internet-Nutzung von ihrem Access-Provider zugewiesen. Da die Provider nur über einen begrenzten Pool von IP-Nummern verfügen, werden die Nummern jeweils neu vergeben. Die Ermittlungsbehörden wenden sich daher mit der ihnen bekannten IP-Adresse an den Access-Provider, zu dessen Adresspool die Nummer gehört und bitten um Auskunft darüber, welchem Nutzer diese zum Nutzungszeitraum, der sich in der Regel auch aus dem Log-Protokoll am Server ergibt, zugewiesen war. In der Regel lassen sich auf diese Weise entweder bestimmte angemeldete Nutzer identifzieren, oder es ergeben sich sonstige Anhaltspunkte (wie bei Call-by-Call-Verbindungen Telefonnummern).

Das **Teledienstedatenschutzgesetz** (TDDSG) und der **Mediendienste-Staatsvertrag** verlangen von den Providern, dass diese die Nutzungsdaten unmittelbar nach Abschluss des Nutzungsvorgangs löschen, es sei denn, sie sind für Abrechnungszwecke erforderlich. Zu den personenbezogenen Nutzungsdaten gehört nach Auffassung der Datenschutzbeauftragten auch die jeweils verwendete dynamische IP-Nummer. Die Diensteanbieter bzw. Internet-Provider hätten also die Pflicht, derartige Protokolldaten überhaupt nicht entstehen zu lassen bzw. sie in einer Wiese zu führen, die nicht personenbezogen ist. Dafür würde es ausreichen, den letzten der vier Ziffernblöcke in der IP-Adresse zu löschen. Dies gilt sowohl für den Serverbetreiber, der die Zugriffe z. B. auf Webseiten protokolliert, als auch für den Access-Provider, der ein Logfile darüber führt, welchem Nutzer eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war. Zwar wird vor allem der Access-Provider bestimmte Daten zu Abrechnungszwecken nutzen, dafür können z. B. die Zeiten des Login bzw. die abgerufene Datenmenge relevant sein. Jedoch ist kein Abrechnungsmodell bekannt, bei dem es auf die konkret vergebene IP-Adresse ankommt.

Allerdings werden die Vorschriften von den Providern nur in seltenen Fällen beachtet. Häufig werden technische Gründe oder Gründe der internen Auswertung der IP-Nummern dafür genannt, warum sämtliche Daten über die Nutzung durch einzelne IP-Adressen über einen gewissen Zeitraum gespeichert werden. Stoßen die Strafverfolgungsbehörden auf diese Daten, so können sie darauf zugreifen (vgl. Tz. 4.2.5). Der **Zugriff auf Verbindungsdaten** setzt einen richterlichen Beschluss voraus. Aufgrund der ständigen Verletzung der Datenschutzbestimmungen stehen den Ermittlungsbehörden also umfangreiche Datenpools zur Auswertung zur Verfügung. Jedoch gibt es Initiativen dafür, die Einhaltung der Datenschutzregelungen stärker zu kontrollieren und endlich durchzusetzen. Ein anderer Ansatz besteht darin, den Nutzern **Anonymisierungsdienste** zur Verfügung zu stellen, mit deren Hilfe sie selbst die Verknüpfung zwischen der abgerufenen Ressource im Netz und den Informationen über den Nutzer vermeiden können (vgl. Tz. 9.2).

Angesichts dieser Entwicklungen ist aus Politik und Polizei der Ruf danach laut geworden, eine rechtliche Verpflichtung für die Internet-Provider einzuführen, wonach diese – **im genauen Gegensatz zur gegenwärtigen Rechtslage** – die Daten über die Nutzungen nicht zu löschen, sondern gerade zu speichern hätten. Dabei ist an eine Mindestspeicherfrist von sechs Monaten gedacht. Mit einer derartigen Initiative überraschte die Innenministerkonferenz mit einem Beschluss im Jahr 2000.

Die Datenschutzbeauftragten der Länder haben sich mit großer Mehrheit gegen diese Vorhaben gewandt. Die von der Innenministerkonferenz intendierte Speicherpflicht würde zu umfassenden Datensammlungen führen, in denen das Surf- und Nutzungsverhalten jedes Einzelnen gespeichert bliebe und jedenfalls technisch zu Auswertungen und Profilbildungen für alle möglichen Zwecke bereit stünde. Eine derartige Vorratsdatenspeicherung für unterschiedlichste Zwecke im Bereich der Sicherheitsbehörden wäre nach der Rechtsprechung des Bundesverfassungsgerichts unzulässig. Sie würde einen schwerwiegenden **Eingriff in Kom-**

munikationsgrundrechte beinhalten, weil die einzelnen Kommunikationsvorgänge für staatliche Zwecke aufgehoben würden und zugleich auch das Missbrauchsrisiko bei den privaten Daten speichernden Stellen steigen würde. Im Übrigen ist zu erwarten, dass die Bürger von ihren Grundrechten auf Zugang zu Informationen und zur freien Meinungsäußerung dann zurückhaltender Gebrauch machen, wenn sie damit rechnen müssen, bei entsprechenden Aktivitäten in eine vorsorgliche Protokollierung zu geraten.

Der **Innen- und Rechtsausschuss** des **Schleswig-Holsteinischen Landtages** hatte sich im Januar 2001 nachdrücklich gegen die Einführung einer entsprechenden Speicherverpflichtung für Internet-Serviceprovider ausgesprochen. Der Innenminister hat allerdings mitgeteilt, dass er die Sicht des Ausschusses nicht teilen könne und wies auf die aus polizeilicher und aus seiner Sicht erforderliche Notwendigkeit einer derartigen Datenspeicherung hin.

Im Zuge der Verschärfung der Eingriffsbefugnisse nach den Terroranschlägen in den USA wurden in einem Gesetzentwurf der Länder **Bayern** und **Thüringen** „zur Verbesserung des strafrechtlichen Instrumentariums“ konkrete Vorschläge für Speicherpflichten vorgelegt. Die von den beiden Ländern im Bundesrat eingebrachte Vorlage schlug unter anderem vor, sowohl in das Telekommunikationsgesetz (TKG) als auch in das TDDSG eine Ermächtigung zum Erlass einer Verordnung einzufügen. Dann könnte die Bundesregierung ohne Beteiligung des Parlaments die Details über die Vorratsspeicherung sowohl im Bereich der klassischen Telekommunikation als auch im Internet festlegen. Bisher gibt es in beiden Bereichen nur die Befugnis, Daten, die zu Abrechnungszwecken erforderlich sind, bis zu sechs Monate nach Versendung der Rechnung zu speichern. Das TDDSG enthält genauso wenig eine Speicherpflicht von Verbindungsdaten wie die Telekommunikations-Datenschutzverordnung (TDSV) für den Bereich der herkömmlichen Telekommunikation (zur novellierten TDSV vgl. 23. TB, Tz. 8.5).

Andere Initiativen zur Einführung von Mindestspeicherpflichten finden sich auf internationaler Ebene. So kommt das Thema in der mittlerweile verabschiedeten **Cyber-Crime Convention** vor (Tz. 4.2.10). In die Diskussion um die Cyber-Crime Convention, die ein Abkommen des Europarates ist, hatte sich schon im Januar 2001 die EU-Kommission eingeschaltet und eigene Vorschläge unter dem Titel „Schaffung einer sicheren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität“ vorgelegt. Dort wurde bereits auf die vonseiten der Sicherheitsbehörden dargestellte Notwendigkeit der Speicherung von Verbindungsdaten hingewiesen. Offenbar wird auch innerhalb des Rates der EU darüber diskutiert, bei der Neufassung der Richtlinie über den Datenschutz bei der elektronischen Kommunikation (vgl. Tz. 12.2) Vorschriften über Mindestspeicherpflichten einzufügen oder zumindest die Vorschriften über die sofortige Löschung so aufzuweichen, dass die Richtlinien einer gesetzlichen Mindestspeicherpflicht auf Ebene der mitgliedstaatlichen Gesetze nicht entgegensteht.

Was ist zu tun?
Schleswig-Holstein sollte im Bundesrat darauf hinwirken, dass es bei der derzeitigen Rechtslage bleibt und eine vorsorgliche Speicherverpflichtung nicht eingeführt wird.

8.3 Telekommunikationsüberwachungsverordnung

Im Jahr 2001 hat die Bundesregierung die lange geplante Telekommunikationsüberwachungsverordnung (TKÜV) verabschiedet. Trotz einiger deutlicher Verbesserungen zu früheren Entwürfen bleiben viele Details nach wie vor ungeklärt.

Die TKÜV blickt auf eine lange Entstehungsgeschichte zurück. Ihr Erlass war bereits mit dem Telekommunikationsgesetz (TKG) aus dem Jahr 1996 vorgegeben., wo bestimmt ist, welche Pflichten die Telekommunikationsprovider bei der Mitwirkung an der **Überwachung von Telekommunikation** treffen. Dabei geht es vor allem darum, welches Equipment die Provider vorhalten müssen – wohlgemerkt auf eigene Kosten. Dies war bisher nur für die klassische Telefonie in der Fernmeldeüberwachungsverordnung geregelt. Dieses Regelungswerk war nicht mehr den modernen technischen Erfordernissen angepasst und ließ sich schon gar nicht auf den Bereich Internet anwenden.

Beim Erlass der TKÜV kam es vor allem zum öffentlichen Disput darüber, wie weit **Provider** aus dem Bereich **Internet** zur Mitwirkung und zur vorsorglichen Installation von Überwachungstechnik verpflichtet werden sollten (vgl. 22. TB, Tz. 7.2.2). Die Sicherheitsbehörden waren der Auffassung, dass jedenfalls solche Anbieter, die Dienstleistungen für die Öffentlichkeit erbringen, eine Schnittstelle zur Überwachung einbauen müssten. Dies ist für die herkömmlichen Telekommunikationsunternehmen weder technisch noch wirtschaftlich ein großes Problem, da sie bereits nach geltendem Recht eine Überwachungsschnittstelle zu betreiben haben. Die nun verpflichteten Internet-Provider brachten vor, dass auf sie **erhebliche Kosten** zukämen, sollten diese Pflichten auch für sie flächendeckend gelten. Viele Unternehmen sahen ihre Existenz gefährdet, da die Kosten, die ihnen für staatliche Überwachungsmaßnahmen aufgebürdet würden, in keinem Verhältnis zu ihren wirtschaftlichen Erträgen stünden. Diese Diskussion führte bereits im Jahr 1998 zu einer Zurücknahme des damals veröffentlichten Entwurfs einer TKÜV.

Dem zweiten Entwurf aus dem Jahr 2001 ging es zunächst nicht viel besser. Er wurde von den Vertretern der Provider heftig kritisiert und musste stark überarbeitet werden. Nach den Anschlägen des 11. September 2001 wurde ein **Kompromiss** gefunden. Danach soll die Überwachung in erster Linie auf den klassischen Telekommunikationsleitungen stattfinden, die die meisten Nutzer noch benutzen, um die letzte Meile vom Internet zu ihrem häuslichen Anschluss zu überbrücken.

Wo dies dank neuer Techniken wie **DSL** entfällt, müssen die Provider die Möglichkeit des Abhörens auch auf diesen neuartigen Verbindungen sicherstellen. Sie sind zur Mitwirkung an der Überwachung und zum Einbau entsprechender Gerätschaften verpflichtet. Im Bereich Internet werden außerdem die Diensteanbieter von **E-Mail-Kommunikation** in die Pflicht genommen. Von diesen Pflichten sind allerdings solche Diensteanbieter befreit, die nicht mehr als tausend Nutzer versorgen oder die die Telekommunikationsdienste im Wesentlichen für eigene Zwecke erbringen, wie dies z. B. bei Betrieben und Behörden der Fall ist, die lediglich ihren Mitarbeitern oder Tochterfirmen die Telekommunikation zu privaten Zwecken erlauben. Für mittelgroße Provider mit nicht mehr als zehntausend Nutzern sind Erleichterungen bei grundsätzlicher Verpflichtung vorgesehen.

> **? *DSL***
>
> *DSL steht für „Digital Subscriber Line“, zu Deutsch etwa: digitale Teilnehmeranschlussleitung, und bezeichnet eine Technik zur schnellen Übertragung von digitalen Daten unter Nutzung herkömmlicher Zweidraht-Kupferkabel. Grundsätzlich unterscheidet man symmetrisches SDSL und asymmetrisches ADSL. In Deutschland finden sich typischerweise ADSL-Angebote wie das von der Telekom angebotene TDSL mit Übertragungsraten von bis zu 768 kbit/s downstream und bis zu 128 kbit/s upstream. Der Datenverkehr über TDSL wird anders als der übrige Datenverkehr vom und zum Nutzer nicht über die Vermittlungsstellen gelenkt, sondern noch vor der Vermittlungsstelle abgezweigt und über Hochgeschwindigkeitsdatenleitungen mit dem Internet verbunden. Daher besteht technisch keine Möglichkeit, an der Vermittlungsstelle zu überwachen.*

Was genau die zum Teil verpflichteten **Internet-Dienstleister** technisch vorzuhalten haben, ergibt sich aus der TKÜV selbst noch nicht. Dazu wird eine **technische Richtlinie** erlassen werden, die die Einzelheiten regelt. Erst wenn diese Richtlinie vorliegt, werden die Anbieter Klarheit darüber haben, welche Kosten auf sie zukommen. Für die Nutzer bedeutet die erleichterte Abhörbarkeit, dass die Zugriffe der Strafverfolgungsbehörden auf ihre Kommunikation so wie bereits seit Jahren weiter steigen werden. Dieser Trend wird auf der Grundlage der neuen TKÜV voraussichtlich anhalten.

> **? *Strategische Überwachung***
>
> *Mit der strategischen Überwachung durch den Bundesnachrichtendienst (BND) wird zunächst ungezielt ein größerer Anteil der Telekommunikation zwischen Teilnehmern aus Deutschland und dem Ausland kontrolliert, um daraus dann solche Telekommunikationsvorgänge herauszufiltern, die geheimdienstlich relevant sind. Anders als bei der Überwachung zur Strafverfolgung muss der BND daher keine Rufnummern oder Kennungen angeben, um die zu überwachenden Verbindungen zu identifizieren.*

Kaum war die TKÜV Ende Januar 2002 in Kraft getreten, wurde schon Ergänzungsbedarf für den **Bundesnachrichtendienst** (BND) angemeldet. Der BND durfte in der Vergangenheit die so genannte **strategische Überwachung** der Telekommunikation nur bei solchen Auslandsverbindungen betreiben, die über Satellit hergestellt wurden. Nach einer Änderung im G10-Gesetz aus dem Jahr 2001 hat er nun auch die

Befugnis, in der leitungsgebundenen Telekommunikation abzuhören. Damit die strategische Überwachung in leitungsgebundenen Übertragungswegen umgesetzt werden kann, müssten zunächst entsprechende Schnittstellen eingerichtet werden. Mit entsprechenden Änderungen der soeben verabschiedeten TKÜV soll dafür die rechtliche Grundlage geschaffen werden. Dabei ist vorgesehen, gerade eine Gruppe von Unternehmen zur Mitwirkung zu verpflichten, die bisher kein Überwachungsequipment vorhalten müssen: Die Betreiber von leitungsgebundenen Übertragungswegen, die der gebündelten Übertragung von Telekommunikation für Telekommunikationsbeziehungen dienen. Nach der vorgesehenen Änderung könnten dann bis zu 20 % der Telekommunikationen auf den zu überwachenden Übertragungswegen in Kopie an den BND weitergeleitet werden. Damit sind auch Internet-Backbones mit Auslandsbezug erfasst. Allerdings sind viele Details noch unklar, z. B. die Frage, wie bei der Überwachung des Internet-Verkehrs sichergestellt werden soll, dass nur Telekommunikationen mit Auslandsbezug überwacht werden.

Was ist zu tun?
Die Sicherheitsbehörden sollten die Überwachung der Telekommunikation nicht als Standardinstrument einsetzen, sondern die Verhältnismäßigkeit der Mittel bei jeder einzelnen Maßnahme sorgfältig prüfen.

8.4 P3P

Der Durchbruch für P3P – Platform for Privacy Preferences – scheint da zu sein: Der Standard ist nun „offiziell", die Implementationen sind greifbar, und die Diskussion um notwendige oder sinnvolle Erweiterungen ist entbrannt.

Bereits seit mehreren Jahren berichten wir zur Entwicklung von P3P (vgl. 21. TB, Tz. 7.1.4; 22. TB, Tz. 9.3 und 23. TB, Tz. 8.6), und P3P spielte auch auf den letzten beiden Sommerakademien eine Rolle. Als wir vor vielen Jahren vom **World Wide Web Consortium (W3C)** als Experten eingeladen wurden, uns am Standardisierungsprozess von P3P zu beteiligen, hat keiner ahnen können, wie lange dies dauern würde. Nun sind die Bemühungen fürs Erste erfolgreich zu einem Ergebnis gekommen: P3P hat den Status eines offiziellen W3C-Standards erreicht, auf dem nun weltweit aufgesetzt werden kann. Dies bedeutet, dass Internet-Server ab jetzt ihre Datenschutz-Policies auch maschinenlesbar

? P3P

P3P (Platform for Privacy Preferences) steht für einen Internet-Standard des World Wide Web Consortiums (W3C), bei dem der Nutzer eine Kontrolle über seine Daten erhält, indem er zustimmen oder untersagen kann, dass seine Daten übermittelt werden. Dafür legt er fest, welche personenbezogenen Daten er welchem Anbieter zu welchem Zweck hergeben möchte. Der Anbieter wiederum definiert, welche Daten er benötigt und wie er sie verwenden will. Nur wenn diese beiden Anforderungen von Nutzer und Anbieter im Einklang stehen, werden die Daten übermittelt.

in einheitlichen Formaten bereitstellen können, die in der Software des Nutzers automatisch daraufhin ausgewertet werden können, ob sie mit seinen Wünschen übereinstimmen oder nicht. Die ersten Browser unterstützen mittlerweile P3P zumindest teilweise (Tz. 11.4).

Für **Datenschutzaufsichtsbehörden** bietet P3P eine weitere Möglichkeit, die beabsichtigte Datenverarbeitungspraxis der Internet-Diensteanbieter aus der Ferne auf ihre Datenschutzkonformität abzuklopfen. Ob die Datenverarbeitung allerdings mit der Ankündigung in der Datenschutz-Policy übereinstimmt, lässt sich mit einer reinen Online-Kontrolle in dieser Form nicht herausfinden.

Was ist zu tun?
Nach Fertigstellung der Version 1 von P3P muss daran gearbeitet werden, die Implementierungen im Sinne des Datenschutzes zu gestalten. Datenschützer sollten für Nutzer und Anbieter datenschutzgerechte P3P-Konfigurationen zur Verfügung stellen.

8.5 Identitätsmanagement

Die Informationsgesellschaft hängt eng mit dem Agieren in der digitalen Welt zusammen. Doch was passiert mit unseren digitalen Identitäten, die uns in jener Welt repräsentieren?

Vor allem zwei Probleme sind mit dem Handeln im Internet verbunden: Zum einen fehlt es an **Anonymität**, d. h. jeder kann bei seinen Aktionen beobachtet werden, es lassen sich Nutzerprofile erstellen. Zum anderen ist keine **Authentizität** gegeben, d. h. man hat keine Sicherheit darüber, dass der Kommunikationspartner wirklich der ist, der er vorgibt zu sein, bzw. seine zugesagten Leistungen erfüllt. Identity Theft, das „Ausleihen“ und Missbrauchen von fremden Identitäten, lässt sich zurzeit nicht verhindern. Zwar wird seit einigen Jahren an einer Infrastruktur für elektronische Signaturen (Tz. 8.1) „gebaut“, die das Authentizitätsproblem lösen soll, doch kann dies den Datenschutz der Nutzer beeinträchtigen, wenn stets authentische Datenspuren hinterlassen werden.

? Digitale Identität

Digitale Identitäten repräsentieren Menschen in der elektronischen Welt, z. B. im Internet. Die Ausprägungen können verschieden sein: das Auftreten unter dem echten Namen, die Verwendung von digitalen Signaturen zur Sicherung der Authentizität oder auch nur das unabsichtliche Hinterlassen von Datenspuren – immer sind es digitale Identitäten, die mit den Aktionen der Menschen zusammenhängen. Für ein Mehr an Datenschutz ist wichtig, dass die digitalen Identitäten möglichst wenig miteinander verkettbar sind, d. h. immer ein anderes Aussehen haben.

Die Lösung könnte in einem **datenschutzgerechten Identitätsmanagement** liegen (vgl. 23. TB, Tz. 10.6). Es befähigt den Nutzer, souverän sein Recht auf infor-

mationelle Selbstbestimmung wahrzunehmen, d. h. selbst zu steuern, wem er welche Daten von sich unter welchen Bedingungen offenbart, oder zumindest jederzeit das Wissen darüber zu haben, wie und wo seine Daten gerade verarbeitet werden. Auf der Basis von Anonymitätsdiensten im Netz (Tz. 9.2) kann mit Identitätsmanagern genau eingestellt werden, wann der Nutzer wie anonym oder auch mit welchem Grad an Verbindlichkeit auftritt.

Solche datenschutzgerechten Identitätsmanager gibt es bislang nicht, und es ist auch gar nicht so einfach, sie zu entwickeln, bedeutet es doch, die gesamten Datenschutzrechte digital abzubilden und zu implementieren. Wesentlich sind die **Souveränität des Nutzers** über seine Daten und die Vertrauenswürdigkeit des Systems. Dies bedeutet z. B., dass die Nutzerdaten nicht gezwungenermaßen außerhalb seines Einflussbereichs gespeichert sein dürfen – wie es bei vielen heutigen so genannten „Identity Management Tools" der Fall ist. Außerdem geht es nicht nur um die Verwaltung der Echtdaten, sondern als Mittel gegen die weitgehenden Auswertungsmöglichkeiten in der digitalen Welt muss die Profilbildung durch Verkettung gleicher Datensegmente verhindert werden. Hierfür eignen sich Pseudonyme und zertifizierte Attribute, die als authentische Berechtigungsnachweise dienen können (anonymous credentials). Insgesamt reicht ein kleines Stück Identitätsmanagersoftware beim Nutzer nicht aus, sondern auch Anwendungen und Infrastruktur müssen Identitätsmanagement unterstützen, um das angestrebte Ziel wirklich zu erreichen.

In der Arbeit an datenschutzgerechten Identitätsmanagementsystemen stehen wir noch am Anfang, doch hat inzwischen auch die **Europäische Union** die Wichtigkeit und Brisanz des Themas „Digitale Identität" erkannt, was sich in Workshops und Förderschwerpunkten niederschlägt. Gemeinsam mit Kooperationspartnern aus Wissenschaft und Wirtschaft werden wir in den kommenden Jahren dieses für den künftigen Datenschutz so wichtige Thema bearbeiten. Im virtuellen Datenschutzbüro stehen dafür Foren zur Verfügung:

www.datenschutz.de/foren/identitaetsmanagement/

Was ist zu tun?
Auch wenn das Fernziel des technikgestützten, selbst bestimmten Datenschutzes noch weit weg erscheint, sollte man jetzt schon die Ideen des Identitätsmanagements verfolgen, z. B. bei Nutzersoftware, bei der Gestaltung von Anwendungen oder beim Aufbau der Infrastruktur für elektronische Signaturen.

8.6 VIS – Fachtagung zu verlässlichen IT-Systemen in Kiel

Informatiker treffen Datenschützer – das war die Motivation für uns, die Fachtagung „VIS – Verlässliche IT-Systeme" in Kiel auszurichten.

Alle zwei Jahre findet diese Fachtagung der Gesellschaft für Informatik an wechselnden Orten Deutschlands statt. Zusammen mit der Christian-Albrechts-Universität zu Kiel, die die Räumlichkeiten stellte, haben wir im September 2001 diese Konferenz organisiert, auf der sich mehr als 100 Experten für **Datensicherheit**

und technischen Datenschutz aus Wissenschaft, Wirtschaft und Verwaltung trafen. An drei Tagen bestand die Möglichkeit, sich in Fachvorträgen zu vielerlei Themen zu bilden und in mehreren Workshops mitzudiskutieren. Tutorien am Vortag rundeten das Programm ab. Höhepunkte der VIS-Tagung waren die Podiumsdiskussion zum Thema „Cyber-Crime“ und die Abendveranstaltungen mit Empfängen, auf denen fachliche Themen wie Protection Profiles für Datenschutzprodukte (vgl. 21. TB, Tz. 7.6) bzw. die Auswirkungen der Ereignisse am 11. September 2001 im Vordergrund standen. Auch der Vortrag zur Weiterentwicklung des Datenschutzrechts begeisterte die Techniker und regte zur Diskussion an.

Die Terminwahl gleich im Anschluss an die **Sommerakademie** stellte sich im Nachhinein als nicht ideal heraus, da kaum jemand wirklich die ganze Woche Zeit hatte, um die Kieler Datenschutz- und Datensicherheitsveranstaltungen zu besuchen, zumal weitere parallele Treffen angesetzt waren. So hatten sich die Veranstalter mehr Teilnehmer für die Tutorien, insbesondere aber für das fachlich anspruchsvolle Einführungstutorium zu Privacy Enhancing Technologies, gewünscht, bei dem Datenschützer Informatiker und Informatiker Datenschützer ausbilden sollten. Insgesamt war es eine gelungene Veranstaltung, die in einem Tagungsband und mit mehreren Vortragspräsentationen im Web dokumentiert ist:

www.verlaessliche-it-systeme.de/vis2001/

8.7 Neue Vorschriften über den Datenschutz im Internet

Seit 1997 gelten in Deutschland strenge Regelungen für den Datenschutz im Internet. Die Vorschriften wurden jetzt überarbeitet. Dabei wurden vereinzelte Unstimmigkeiten ausgeräumt, ohne dass insgesamt das Schutzniveau verwässert worden ist.

Der deutsche Gesetzgeber hatte bereits recht frühzeitig erkannt, dass im Internet besondere Gefährdungen für die Privatsphäre der Nutzer drohen. Vor allem gilt es zu verhindern, dass die unterschiedlichen Akteure und Provider im Internet die Möglichkeit erhalten, Profile über Kommunikationsvorgänge, Informations- und Konsumverhalten, Vorlieben und Gewohnheiten der Nutzer anzulegen. Da technisch bedingt jede Kommunikation im Internet Daten erzeugt, sind die Gefährdungen hier größer als bei entsprechenden Vorgängen in der Offline-Welt. Die Regelungen des **Teledienstedatenschutzgesetzes** (TDDSG) aus dem Jahr 1997 waren bereits vorbildlich. Sie untersagten grundsätzlich die Verarbeitung personenbezogener Daten. Ausnahmen sollten nur dann gelten, wenn entweder die Betroffenen ihre Einwilligung gegeben haben oder einzelne, klar umrissene Tatbestände des Gesetzes vorlagen. Von Bedeutung ist dies vor allem für die Nutzungsdaten, die das oben beschriebene Potenzial in sich tragen, das Informations- und Kommunikationsverhalten der Nutzer sehr genau abzubilden. Diese Daten durften bisher lediglich zu Abrechnungszwecken über die Dauer der Nutzung hinaus gespeichert werden. In allen anderen Fällen waren die Nutzungsdaten unmittelbar nach dem Ende des Nutzungsvorganges zu löschen (vgl. 20. TB, Tz. 7.1).

Zum Ende des Jahres 2001 ist nun das Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (EGG) in Kraft getreten. Es handelt sich um ein so genanntes Artikelgesetz, das Änderungen mehrerer Gesetze mit sich bringt. Geändert wird zum einen das Teledienstegesetz (TDG), das 1997 zusammen mit dem TDDSG erstmalig in Kraft getreten ist. Zum anderen wird auch das TDDSG selbst geändert. Die Änderungen im TDG gehen auf die Anforderungen einer europäischen Richtlinie zurück und zielen im Wesentlichen nicht auf datenschutzrechtliche Regelungen. Allerdings ist eine Vorschrift auch unter dem Gesichtspunkt des Datenschutzes interessant, die Informationspflichten festgelegt, die bei so genannten „kommerziellen Kommunikationen" gelten sollen. Erfasst sind davon auch **unverlangte Werbesendungen per E-Mail**, die häufig als Spam bezeichnet werden. Das neue Gesetz legt fest, dass diese Sendungen eindeutig als Werbung erkennbar sein müssen, entsprechendes gilt für ihre Absender bzw. Urheber.

Die **Änderungen** im Teledienstedatenschutzgesetz sollen vor allem einige Unklarheiten beseitigen, die sich bei der Evaluierung des Gesetzes (vgl. 22. TB, Tz. 7.3) ergeben hatten. So wird nun eindeutig festgelegt, dass die Vorschriften für die dienstliche Nutzung des Internets durch Arbeitnehmer nicht gelten. Die Möglichkeit der elektronischen Einwilligung zur Datenverarbeitung wurde in der Weise vereinfacht, dass nun nicht mehr die digitale Signatur erforderlich ist. Diese Anforderung hatte sich als nicht praktikabel erwiesen. Erfreulich ist, dass es bei der grundsätzlichen restriktiven Regelung zur Verarbeitung der Nutzungsdaten geblieben ist. Neu hinzugekommen ist nur ein eng umrissener Tatbestand, wonach Diensteanbieter Daten von Nutzern auch dann verarbeiten dürfen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass versucht wurde, die Dienste zu nutzen, ohne das Entgelt dafür zu entrichten. Eine derartige Missbrauchsklausel fehlte in dem alten Gesetz.

Erfreulich ist weiter, dass die Regelung zu pseudonymen Nutzungsprofilen klarer gefasst und zu Gunsten der Nutzer geändert wurden. Nunmehr ist eindeutig geregelt, dass die Anbieter die Möglichkeit haben, das Verhalten der Nutzer in **Profilen** abzubilden, die aber selbst nicht unmittelbar personenbezogen sein dürfen. Es dürfen also nur Pseudonyme in diesen Profilen verwendet werden; diese dürfen nicht mit den Klardaten über die Person der Betroffenen zusammengeführt werden. Selbst diese lediglich pseudonymisierte Profilbildung hat dann zu unterbleiben, wenn die Nutzer ihr widersprechen. Der Diensteanbieter hat die Nutzer auf das Widerspruchsrecht hinzuweisen. Hervorzuheben ist weiterhin, dass in das neue Gesetz nunmehr Ordnungswidrigkeitstatbestände eingeführt wurden. Damit haben die Datenschutzaufsichtsbehörden erstmalig die Möglichkeit, Bußgelder bis zu 50.000 € zu verhängen.

Wie im 20. Tätigkeitsbericht (vgl. Tz. 7.1) dargelegt, regelt das TDDSG nur einen Teil der Internet-Dienste. Der andere Teil wird von der bisher praktisch gleich lautenden Regelung der Länder, dem **Mediendienste-Staatsvertrag** (MDStV), erfasst. Die Länder arbeiten daran, den MDStV an die geänderten Vorschriften des TDDSG anzupassen. Mit der Novellierung des Staatsvertrages ist noch für das Jahr 2002 zu rechnen, sodass es bald wieder einen weitgehenden Gleichklang der Vorschriften gibt.

Ein Problem besteht nach wie vor dadurch, dass die Datenschutzregelungen für den Internet- und Online-Dienstebereich immer noch von vielen Diensteanbietern **nicht eingehalten** werden. An dieser Stelle kann nur wieder an die Anbieter appelliert werden, einzusehen, dass Geschäftsmodelle im Internet nur dann funktionieren werden, wenn die Nutzer ausreichendes Vertrauen in die Seriosität der Dienste haben. Dazu gehört auch, dass ihre Daten, die sie mehr oder weniger freiwillig bei der Nutzung der Dienste offenbaren, entsprechend den Gesetzen behandelt und nicht missbraucht werden.

Was ist zu tun?
Schleswig-Holstein sollte darauf hinwirken, dass es zügig zu einer Anpassung des Mediendienste-Staatsvertrages an das novellierte Teledienstedatenschutzgesetz kommt.

9 Modellprojekte zur Weiterentwicklung des Datenschutzes

9.1 Virtuelles Datenschutzbüro: Erste Adresse für Datenschutzinfos im Internet

Nachdem Ende 2000 das virtuelle Datenschutzbüro online gegangen war, wurde es im Laufe des Jahres 2001 weiter ausgebaut. Mittlerweile hat es sich zu einer Einstiegsadresse für vielerlei Datenschutzinformationen im Internet gemausert, die über die Grenzen Deutschlands hinaus bekannt ist.

Unter den leicht zu merkenden Webadressen

www.datenschutz.de (deutsch) oder
www.privacyservice.org (international)

finden interessierte Internet-Nutzer das virtuelle Datenschutzbüro (vgl. 23. TB, Tz. 9.1). Dabei handelt es sich um einen **gemeinsamen Service** von Datenschutzinstitutionen, die Informationen rund ums Thema Datenschutz bereitstellen. Das virtuelle Datenschutzbüro wird vom ULD technisch betrieben und mit Förderung durch die Initiative Informationsgesellschaft Schleswig-Holstein weiterentwickelt. Zu dem Service gehört ein Newsticker, ein Presseverteiler, eine Suchmaschine, die Möglichkeit des Mitdiskutierens in Mailinglists zu vielen Bereichen und das Beantworten der zahlreichen Fragen der Nutzer – ob per FAQ (Frequently Asked Questions) oder individuell per E-Mail. Außerdem ist das virtuelle Datenschutzbüro die „Heimat" von einigen Datenschutzprojekten, für die es die Infrastruktur zur Verfügung stellt. Die **Nutzungsstatistik** zeigt einen Basiswert von ca. **3.000 Pageviews pro Tag** an. Natürlich wird das Nutzungsverhalten nicht personenbezogen protokolliert, sondern das virtuelle Datenschutzbüro verhält sich gemäß seiner eigenen Datenschutz-Policy vorbildlich (vgl. 20. TB, Tz. 7.1). Zu keiner Zeit werden vollständige IP-Adressen gespeichert.

> ***? Pageview***
>
> *Die Anzahl der Abrufe von Dateien von einem Webserver (Hits genannt) schließt die Abrufe von Grafik- und anderen Dateien ein. Die Teilmenge der Abrufe speziell der HTML/XML-Seiten wird mit Pageviews bezeichnet. Pageviews sind also ein Maß für die Häufigkeit, dass Webseiten abgerufen werden.*

Im Berichtsjahr wurde das virtuelle Datenschutzbüro auf diversen **Veranstaltungen** vorgestellt. Hervorzuheben ist die Präsentation auf der CeBIT im März 2001 an einem eigenen Stand und in mehreren Vorträgen. Daneben war es auch international gefragt, z. B. auf einem Workshop der EU in Brüssel zu „Privacy Enhancing Technologies", in Wien beim Kongress „Chaos Control" oder bei der europäischen Konferenz der Datenschutzbeauftragten in Athen. Im Rahmen des virtuellen Datenschutzbüros haben sich die Mitarbeiter speziell mit der datenschutzgerechten und möglichst sicheren Gestaltung der Internet-Anbindung beschäftigt (vgl. 23. TB, Tz. 10.3 und 10.4). Hierzu gab es viele Nachfragen, z. B. auf dem BSI-Kongress 2001, auf einem Ulmer Datenschutzkongress, anlässlich unseres Tages der offenen Tür und bei einem Tutoriumsvortrag auf der Fachtagung VIS (Tz. 8.6).

Die am virtuellen Datenschutzbüro beteiligten **Projektpartner** sind zurzeit die Datenschutzbeauftragten des Bundes sowie der meisten Länder in Deutschland, der norddeutschen Bistümer der katholischen Kirche, der Evangelischen Kirche Deutschlands, des Südwestrundfunks, aus der Schweiz, den Niederlanden, der Slowakei, Kanada und Polen. Allerdings liegt der Schwerpunkt im Augenblick auf den deutschsprachigen Inhalten, obwohl vielerlei Informationen bereits mehrsprachig vorliegen. Alle Datenschutzbeauftragten sind zur Mitarbeit eingeladen – das virtuelle Datenschutzbüro lebt durch die Aktiven!

Darüber hinaus haben sich bereits **viele Interessierte** gemeldet, die nicht offizielle Datenschutzinstitutionen repräsentieren, gleichwohl aber Interesse an und oft sehr viel Kompetenz in Datenschutzfragen haben. Seit Ende 2001 arbeiten daher auch solche Kooperationspartner im virtuellen Datenschutzbüro mit.

Das Projekt „Virtuelles Datenschutzbüro“ wird gefördert durch

Initiative Informationsgesellschaft Schleswig-Holstein

Was ist zu tun?
Das virtuelle Datenschutzbüro sollte weiter ausgebaut werden, um eine stets aktuelle und vertrauenswürdige Ansprechstelle für das Thema Datenschutz sein zu können.

9.2 AN.ON

Wer im Internet surft, zieht eine lange Datenspur hinter sich her und macht seinen Weg durchs Netz – wohl in der Regel unbewusst – nachvollziehbar. Um das gesetzlich garantierte Recht auf Anonymität im Internet effektiv durchzusetzen, wurde ein Projekt ins Leben gerufen, dessen Ziel es ist, Anonymität zu gewährleisten.

Bereits im 23. Tätigkeitsbericht (vgl. Tz. 9.2) haben wir über das seit Anfang 2001 vom Bundesministerium für Wirtschaft und Technologie geförderte und in Kooperation des Unabhängigen Landeszentrums für Datenschutz und der Technischen Universität (TU) Dresden laufende Projekt „**AN.ON – Anonymität online**“ berichtet.

Während die Aufgabe der TU Dresden in erster Linie in der technischen Realisierung der anonymen Nutzung des Internets durch die Entwicklung des Anonymitäts-Tools JAP besteht, ist das Unabhängige Landeszentrum für Datenschutz vornehmlich mit der Untersuchung der rechtlichen Randbedingungen des anonymen Surfens betraut.

Der von der TU Dresden entwickelte Prototyp des JAP kann von allen Nutzern kostenlos aus dem Internet heruntergeladen werden. Erste Erfahrungen zeigen, dass der Dienst umfangreich genutzt wird. So wurden schon mehr als **100.000 Programmdownloads** gezählt.

Insbesondere auf der CeBIT 2001 stand AN.ON im Mittelpunkt des Interesses der Besucher unseres Messestandes. Dem Projekt kommt auch deswegen eine besondere Bedeutung zu, weil der Anonymitätsdienst JAP nach Einstellung des Betriebs alternativer Internet-Anonymisierungsdienste (z. B. Freedom Network von Zero-Knowledge, Safeweb) weiterhin nicht kommerziell das anonyme Surfen ermöglicht.

? JAP

Um anonym und unbeobachtbar im Internet zu surfen, kann man das Programm JAP auf seinem Rechner installieren und verwenden. Es sorgt dann dafür, dass alle Aktivitäten, die der Nutzer mit seinem Browser im Web ausführt, über den JAP an spezielle Anonymitätsserver, so genannte Mixe, geleitet werden. Dort werden die Datenpakete verschlüsselt und in eine einheitliche Form gebracht, sodass Internet-Provider oder Beobachter nicht mehr sehen können, wer gerade auf welchen Seiten surft. JAP steht kostenlos als Open-Source-Programm auf der Projektwebseite zur Verfügung.

Obwohl die Gewährleistung einer anonymen Internet-Nutzung nach dem Teledienstedatenschutzgesetz grundsätzlich gesetzlich geboten ist, besteht Klärungsbedarf, wie weit dieses Recht des einzelnen Internet-Nutzers reichen soll. Nachdem der Prototyp des JAP so weit implementiert war, dass er von den Nutzern im Probebetrieb praktisch eingesetzt werden konnte, dauerte es nicht lange, bis die Projektpartner mit den ersten Missbrauchsfällen konfrontiert wurden. Strafverfolgungsbehörden, die wegen des Verdachts unterschiedlicher Delikte (z. B. wegen Computerbetruges, Datenveränderung oder Beleidigung) ermittelten, verlangten, teilweise unter Vorlage der erforderlichen richterlichen Anordnung, Auskunft über die Identität der jeweiligen Nutzer. Da es zum **Wesen des Anonymitätsdienstes** gehört, dass keine Verbindungsdaten gespeichert werden, die eine spätere Identifizierung der Nutzer zulassen, haben wir den Strafverfolgungsbehörden in allen Fällen mitgeteilt, dass die Erteilung derartiger Auskünfte nicht möglich ist.

Im Wortlaut: § 4 Abs. 6 TDDSG

Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren.

Grundsätzlich stellt sich die Frage, wie die vom Gesetzgeber gewollte Gewährleistung des Rechts des Einzelnen auf Anonymität im Internet mit Ansprüchen der Strafverfolgungsbehörden auf Auskunft über die Identität der Nutzer in Einklang zu bringen ist, denn eine Behinderung der Arbeit der Strafverfolgungsbehörden wird mit dem Anonymisierungsdienst nicht bezweckt. Da eine pauschale Vorratsspeicherung von Nutzungsdaten nach geltender Rechtslage unzulässig ist, soll natürlich auch in Zukunft weiterhin auf eine derartige Speicherung verzichtet werden. Nur auf diese Weise kann Gesetzeskonformität

gewährleistet werden. Um allerdings Wiederholungstäter enttarnen zu können, diskutieren wir innerhalb des Projektes den Einbau einer „**Fangschaltungsfunktion**“, die es ermöglichen soll, im Einzelfall einen Täter bei der Begehung künftiger Straftaten zu identifizieren. Bei Vorliegen eines richterlichen Beschlusses könnte auf diese Weise der Weg zur IP-Adresse des Täters zurückverfolgt werden. Der Anonymitätsdienst wäre in der Zeit nicht für andere nutzbar, sodass diese technische Lösung einer Massenüberwachung vorbeugen würde.

Weitergehende Informationen befinden sich im Internet unter:

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

Das Projekt „AN.ON“ wird gefördert durch

Was ist zu tun?
Die Garantien des Teledienstedatenschutzgesetzes für eine anonyme Internet-Nutzung sollen auch weiterhin technisch unterstützt werden.

9.3 BioTrusT – Biometrische Verfahren im Feldversuch

Spätestens seit den Terroranschlägen am 11. September 2001 und den darauf folgenden Versuchen der Gesetzgeber, rechtliche Gegenmaßnahmen zu treffen sind biometrische Verfahren stärker in den Mittelpunkt der öffentlichen Diskussion gerückt: Unter dem Stichwort „Fingerabdruck auf den Personalausweis“ wird immer häufiger über Biometrie, d. h. automatische Verfahren zur Erkennung von Gesichtern, Stimmen, Fingerabdrücken oder auch der Iris des Auges, berichtet und diskutiert.

Im Rahmen des Pilotprojektes BioTrusT beschäftigen wir uns schon seit einigen Jahren mit dieser Thematik. In den letzten Tätigkeitsberichten (vgl. 21. TB, Tz. 7.2; 22. TB, Tz. 8.3 und 23. TB, Tz. 9.3) haben wir über **biometrische Verfahren** berichtet, die körperliche Merkmale einer Person automatisiert auswerten, um sie wieder zu erkennen.

- **Wie funktionieren solche Verfahren?**

Durch Sensoren (z. B. Mikrofone, druckempfindliche Schreibflächen, Spezialsensoren für Fingerabdrücke, Videokameras) werden körperliche Merkmale von Personen automatisiert erfasst bzw. vermessen. Danach werden sie mithilfe eines mathematischen Modells in einen speziellen, kleinen Datensatz umgerechnet und mit bereits früher erfassten und gespeicherten **Referenzdaten** verglichen. Stim-

men sie mit diesen Daten (im Rahmen einer gewissen Schwankungsbreite) überein, so gilt die Person als erkannt. Bei automatisierten Verfahren kann dann eine Aktion wie eine Geldauszahlung, ein Zugriff auf Daten, die Freischaltung einer elektronischen Signatur (vgl. 21. TB, Tz. 7.5; 22. TB, Tz. 8.3 und 23. TB, Tz. 8.8) oder der Zugang zu besonders geschützten Räumen ausgelöst werden.

- **Wie hängen Datenschutz und biometrische Verfahren zusammen?**

> **?** ***Biometrie***
>
> *Biometrie dient u. a. zur automatisierten (Wieder-)Erkennung von Personen. Dazu werden mit Sensoren (etwa Kameras oder Fingerabdrucksensoren) ganz unterschiedliche Körpermerkmale von Menschen wie Gesicht, Fingerabdruck, Stimme, Irismuster, Schrift- oder Tastaturanschlagsdynamik (oder Kombinationen davon) erfasst und mit einem zuvor abgespeicherten Referenzwert verglichen.*

Biometrische Merkmale sind regelmäßig dauerhaft personengebundene Merkmale – die Dauerhaftigkeit dieser Bindung ist gerade der Vorteil gegenüber leicht vergessbaren oder weitergebbaren Passwörtern. Es ist denkbar, dass sich aus biometrischen Daten, insbesondere aus den so genannten „Rohdaten“ (z. B. Bildern von Körperteilen wie Augen, Fingern oder dem Gesicht, aber auch Stimmaufnahmen), schon heute oder auch erst in der Zukunft **zusätzliche Informationen** herauslesen lassen. Dies können etwa Hinweise auf Krankheiten und Stimmungslagen sein: Dass aus Bildern des Gesichts oder Sprachaufnahmen Rückschlüsse auf die ethnische Herkunft gezogen werden können, ist ohnehin einleuchtend. Auch die Verwendung des Augenhintergrundes (Retina) im Bereich der Diagnose (Stichwort Diabetes und Bluthochdruck) ist bekannt, ebenso sind medizinische Wahrscheinlichkeitsaussagen (etwa aus dem Muster der Handlinien über mögliche genetische Defekte) dokumentiert. Inwieweit diese Rückschlüsse automatisiert gezogen werden können und ob die komprimierten Referenzdaten ebenfalls solche Rückschlüsse zulassen und schließlich inwiefern solche Aussagen verlässlich sind, ist noch nicht abschließend geklärt.

Biometrische Daten wären allerdings auch „ideal“ als Personenkennzeichen geeignet, über die zu unterschiedlichen Zwecken Daten unterschiedlicher Herkunft zusammengeführt werden könnten. Dass dies im Hinblick auf den Zweckbindungsgrundsatz verhindert werden muss, liegt auf der Hand.

Üblicherweise werden die biometrischen Daten für einen konkreten Zweck (z. B. zur Zutrittskontrolle) erhoben und müssen daher vor einer unbefugten zweckentfremdenden Auswertung geschützt werden. Eine datenschutzgerechte Gestaltung kann die **Zweckentfremdung** eines zentralen Biometrie-Datenbestandes am besten dadurch verhindern, dass ein solcher Bestand gar nicht erst angelegt wird, sondern die Referenzdaten dezentral – am besten verschlüsselt auf einer Chipkarte o. Ä. – gespeichert werden und so die Verfügungsgewalt des Betroffenen nicht verlassen. Eine heimliche und unbefugte Erhebung bei der Benutzung der Geräte (z. B. durch eine unbefugte Kopie der Datenbestände) muss durch eine sorgfältige Kontrolle der Geräte ausgeschlossen werden.

- **Was ist im letzten Jahr im Projekt BioTrusT passiert?**

Das Pilotprojekt **BioTrusT**, das von der Arbeitsgruppe „Biometrische Identifikationssysteme“ von TeleTrusT e. V. ins Leben gerufen wurde, untersucht seit April 1999 die Einsatzmöglichkeiten von biometrischen Verfahren bei Banken und im Bereich des E-Commerce. Neben dem Verbraucherschutzverband VZBV, einem Forschungsinstitut der Fraunhofer-Gesellschaft und einer sozioökonomischen Begleitforschung durch die Fachhochschule Gießen-Friedberg sowie etlichen Herstellern und verschiedenen Bankinstitutionen sind auch wir beteiligt. Die im Rahmen des Projekts erzielten Ergebnisse bieten wertvolle Erfahrung für die gegenwärtige Diskussion, denn die Funktionsweise biometrischer Verfahren und die datenschutzrechtliche Problematik hängt nicht nur von der Anwendung, sondern auch stark von der Technik ab.

Nach dem Test von Geräten zur Zutrittskontrolle zu Arbeitsgebäuden und Arbeitsräumen wurden Verfahren zum Computerzugang untersucht: Die Eingabe eines Kennwortes zum Log-in oder zur Freischaltung eines Bildschirmschoners wurde durch ein biometrisches Verfahren ersetzt. Getestet wurden dabei auch das Zusammenspiel von solchen Verfahren mit Chipkarten, auf denen die biometrischen Merkmale – unter der Verfügung des Nutzers – gespeichert sind. Dazu waren umfangreiche Anpassungen an den neu geschaffenen **Industriestandard BioAPI** durch die Hersteller notwendig, an dessen Entwicklung Mitglieder von BioTrusT beteiligt sind. Viele Hersteller agieren international. Daher bestimmen Standards und Normen über kurz oder lang die Gestaltung aller biometrischen Systeme. Dies betrifft nicht nur die technische Ausführung und Fragen der Kompatibilität, sondern auch international abgestimmte Kriterienwerke, um die Sicherheit der Geräte zu testen.

Der zunächst gefasste Plan einer Untersuchung von biometrischen Verfahren an **Geldausgabeautomaten** wurde nach einer ausführlichen Studie fallen gelassen: Zwar war die Aufgabe, ein einzelnes Verfahren mit einem Geldautomaten zu koppeln, schnell gelöst. Doch für einen umfassenden Einsatz sind die Anforderungen erheblich höher: Es müssen eine Vielzahl von (vernetzten) Geldautomaten angepasst und die Datenverarbeitung und Software in den Bankrechenzentren (die jede Auszahlung autorisieren) entsprechend umorganisiert werden. Um der zentralen Voraussetzung aus der Sicht des Datenschutzes nachzukommen, die biometrischen Referenzdaten nur auf den Bankkarten der Kunden (und nicht in einem Zentralrechner der Banken) zu speichern, sind außerdem Veränderungen im Ablauf des Bankkartenversandes erforderlich, denn die biometrischen Daten müssen im Beisein der Kunden auf die Karten aufgebracht werden.

Hinzu kommt, dass die biometrischen Verfahren zwar immer besser funktionieren, aber derzeit für einen Einsatz im **breiten Kundenumfeld** (alle Kunden müssten jederzeit ein solches System bedienen können, wenn man auf die Verwendung der PIN verzichten will) nicht robust und einfach genug sind. Auch konnten bisher nicht alle Sicherheitsbedenken für einen (nicht überwachten) Einsatz in der Öffentlichkeit ausgeräumt werden, zumal sofort Haftungsfragen in den Vordergrund rücken.

Unsere Absicht im Rahmen unserer Beteiligung an BioTrusT ist, in einer frühen Phase die **technische Gestaltung der Geräte** und den organisatorischen Ablauf bei ihrer Verwendung kennen zu lernen, gegebenenfalls Problemfelder zu benennen, diesen durch Hinweise und konstruktive Mitarbeit entgegenzuwirken und so für eine **datenschutzgerechte Gestaltung** einzutreten.

www.biotrust.de
www.datenschutzzentrum.de/biometrie/

Das Projekt „Datenschutzgerechte Biometrie“ wird gefördert durch

Bundesministerium für Wirtschaft und Technologie

Was ist zu tun?
Biometrische Verfahren, die im Augenblick in der Öffentlichkeit breit diskutiert werden, müssen schon in der Konzeptionsphase sorgfältig datenschutzrechtlich und technisch überprüft werden.

9.4 EU fördert Datenschutzaudit und Gütesiegel in Schleswig-Holstein

Das Land Schleswig-Holstein begreift ein ausgereiftes Datenschutz- und Datensicherheitskonzept als Wettbewerbs- und Standortvorteil für private Unternehmen und öffentliche Stellen. Im Projekt „Innovative Maßnahmen“ wird diese Erkenntnis umgesetzt.

Der marktwirtschaftliche Ansatz im Datenschutz wird jetzt auch von der Europäischen Union gefördert. Die EU hat im Rahmen des **EU-Programmes „Innovative Maßnahmen“** im Themenbereich „eEuropeRegio: die Informationsgesellschaft im Dienste der regionalen Entwicklung“ beschlossen, die Durchführung von Gütesiegelverfahren für IT-Produkte und datenschutzrechtlich relevanten Dienstleistungen in Schleswig-Holstein sowie die Durchführung von Behördenaudits in den Jahren 2002 und 2003 zu fördern (Tz. 10).

REGION Schleswig-Holstein

Ein Programm des Ministeriums für Wirtschaft, Technologie und Verkehr SH und der Technologiestiftung SH – gefördert von der EU aus den Innovativen Maßnahmen des Europäischen Fonds für regionale Entwicklung (EFRE) der Generaldirektion Regionalpolitik

TSH

Im Rahmen des **Produktaudits** werden Gütesiegel an IT-Produkte vergeben, die den Vorschriften über den Datenschutz und die Datensicherheit entsprechen. Das Projekt sieht vor, dass die Kosten für ausgesuchte Prüfverfahren nur teilweise von interessierten Unternehmen oder Vertriebsfirmen getragen werden müssen. Auf diesem Wege sollen vor allem kleinere und mittlere Unternehmen in Schleswig-Holstein gefördert werden. Wir bringen durch eigene Mitarbeiter und Mitarbeiterinnen rechtlichen und technischen Sachverstand ein und haben nun die Möglichkeit, diesen Sachverstand durch neue Fachkräfte zu verstärken. Mittel- und langfristig wird angestrebt, über das Gütesiegel das Datenschutzniveau von Produkten und damit das Vertrauen in öffentlich-rechtliche und private Datenverarbeitung und Online-Angebote zu steigern.

Das **Datenschutz-Behördenaudit** eröffnet öffentlichen Stellen in Schleswig-Holstein die Möglichkeit, ihr Datenschutzkonzept in einem förmlichen Verfahren auf dauerhafte Übereinstimmung mit den datenschutzrechtlichen Bestimmungen überprüfen zu lassen (Tz. 10.4). Das Projekt sieht vor, dass alle öffentlichen Stellen, in denen geförderte Modellprojekte realisiert werden, standardmäßig ein Datenschutzaudit durchlaufen. So sollen im Ergebnis möglichst nur datenschutzgerechte Verfahren in den Genuss öffentlicher Förderung gelangen.

Beide Projekte sind auf zwei Jahre angelegt. Sie werden dazu beitragen, Datenschutzaudit und Gütesiegel in der Praxis zu verankern.

www.datenschutzzentrum.de/audit/
www.datenschutzzentrum.de/guetesiegel/

Was ist zu tun?
Behörden und Firmen sollten die Chancen der neuen Instrumente Audit und Gütesiegel erkennen und für sich nutzen.

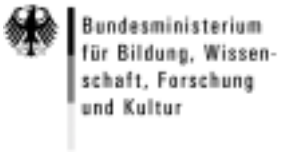
9.5 Projekt Schul-CD: Datenschutz schülergerecht aufbereitet

Mit einer multimedialen CD-ROM soll Schülerinnen und Schülern Medienkompetenz und insbesondere Verständnis und Sensibilität für den Datenschutz im persönlichen, schulischen und beruflichen Alltag vermittelt werden.

Wie schon im vergangenen Tätigkeitsbericht (vgl. 23. TB, Tz. 9.4) dargestellt, entwickeln wir gemeinsam mit einer Firma in Wuppertal und unterstützt durch das Bundesministerium für Bildung, Wissenschaft, Forschung und Kultur eine Schul-CD: Ein kleiner **Datenschutzhelfer** mit Namen Felix soll Schülerinnen und Schüler sowie Lehrkräfte sicher durch den Paragraphendschungel leiten und in verständlicher Art und Weise demonstrieren, wie der Datenschutz das Leben positiv beeinflusst. Er zeigt auf, welch negative Auswirkungen z. B. ein illegaler Datenabgleich auf ein Vorstellungsgespräch haben kann, beschreibt den Einfluss des Datenschutzes auf den Schulalltag oder erklärt gut verständlich, wie Kryptographie funktioniert.

Die CD ist in erster Linie für Berufsschüler und deren Lehrer konzipiert, aber auch für **Schüler an weiterbildenden Schulen** geeignet. Der Inhalt der CD wurde Ende 2001 zwischen den Projektpartnern abschließend festgelegt. Sie soll nach Fertigstellung den Schulen bundesweit noch im Jahr 2002 kostenlos zur Verfügung gestellt werden.

Das Projekt „Schul-CD“ wird gefördert durch



10 Gütesiegel und Audit

Durch die Auszeichnung von IT-Produkten mit einem Gütesiegel will das ULD öffentlichen Stellen und privaten Verbrauchern ermöglichen, den Datenschutz beim Erwerb von IT-Produkten, bei der Teilnahme am E-Commerce und der Bewertung von Standorten als Entscheidungskriterium einzusetzen. Die Vorbereitungen für die praktische Durchführung von Gütesiegelverfahren sind abgeschlossen.

10.1 Der Ablauf der Gütesiegelverfahren

IT-Produkte (Hardware, Software und automatisierte Verfahren) können vom ULD ein Gütesiegel erhalten, wenn sie zur Nutzung durch öffentliche Stellen geeignet und mit den Rechtsvorschriften über den Datenschutz und die Datensicherheit vereinbar sind. Die einzelnen Schritte dieser Produktzertifizierung werden von der **Landesverordnung über ein Datenschutzaudit** (Datenschutzauditverordnung) geregelt, die Ende April 2001 in Kraft getreten ist. Die Datenschutzauditverordnung sieht vor, dass das Gütesiegel vom ULD auf der Basis eines Gutachtens vergeben wird, das von einem beim ULD akkreditierten Gutachter erstellt wurde.

Im Einzelnen läuft die **Erteilung eines Gütesiegels** wie folgt ab:

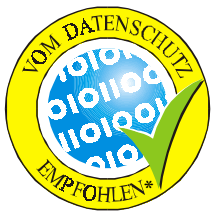
Ein Anbieter, der für sein IT-Produkt ein Gütesiegel erwerben möchte, klärt zunächst die Frage, ob sein **Produkt in öffentlichen Stellen** eingesetzt werden könnte. Nicht erforderlich ist, dass das Produkt bereits dort eingesetzt wird. Eine Nutzung darf jedoch nicht von vornherein ausgeschlossen sein.

Dem Antrag auf Erteilung eines Siegels muss der Anbieter ein Gutachten über sein Produkt beifügen. Für die Erstellung dieser Gutachten **akkreditiert** das ULD in einem gesonderten Verfahren **Gutachter** und **sachverständige Prüfstellen**, die fachlich geeignet, zuverlässig und unabhängig sein müssen. Der interessierte Anbieter sucht sich einen akkreditierten Gutachter oder eine sachverständige Prüfstelle aus und schließt zu privat ausgehandelten Konditionen einen Begutachtungsvertrag ab. Der Gutachter prüft, ob das IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht. Insbesondere prüft der Gutachter die besonderen Eigenschaften des IT-Produkts hinsichtlich

- Datenvermeidung und Datensparsamkeit,
- Datensicherheit und Revisionsfähigkeit und
- Gewährleistung der Rechte der Betroffenen.

Je nach Einsatzbereich unterliegt das Produkt unterschiedlichen rechtlichen Anforderungen an Datenschutz und Datensicherheit. Es muss zunächst geklärt werden, welche rechtlichen Anforderungen bei der Schaffung des Produkts zugrunde gelegt wurden und in welcher Weise der Anbieter diese Anforderungen

technisch umgesetzt hat. Wir haben zu den technischen Kriterien einen **Kriterienkatalog** entwickelt, der nicht nur den Gutachtern als Maßstab und Orientierung dienen soll, sondern auch den Herstellern und Vertriebsfirmen bereits in der Produktentwicklung helfen kann.



Nach erfolgreicher Begutachtung kann der Anbieter den Antrag auf Erteilung des Gütesiegels stellen. Er übersendet mit dem Antrag auch das **Gutachten**, dessen Zusammenfassung im Fall der Siegelvergabe veröffentlicht wird. Wir prüfen das Gutachten auf Schlüssigkeit und Nachvollziehbarkeit und können bei Bedarf auch das Produkt selbst anfordern. Nach erfolgreicher Prüfung vergeben wir das **Gütesiegel** und zwar in der Regel für die Dauer von **zwei Jahren**. Die schnelle Entwicklung im IT-Sektor fordert neben einer zeitlichen Beschränkung der durch die Siegelvergabe ausgesprochenen Empfehlung auch die Möglichkeit, das Siegel bei unverzichtbaren Weiterentwicklungen im rechtlichen oder technischen Anforderungskatalog in der Zwischenzeit wieder entziehen zu können.

Der den Gutachten zugrunde gelegte **Anforderungskatalog** wird jährlich **fortgeschrieben**. Zertifiziert wird ein Produkt daher auf der Grundlage des Kriterienkatalogs des entsprechenden Kalenderjahres. Entwickelt sich das Produkt nicht weiter, wohl aber der Kriterienkatalog, so ist denkbar, dass bei der Rezertifizierung das Siegel nicht erneut vergeben werden kann. Das Produkt erhält eine Nummer und wird mit Nummer und Zusammenfassung der Prüfung in einem **Register veröffentlicht**. Interessierte Kunden können sich so über geeignete Produkte informieren. Das Produkt darf auch mit dem Siegel beworben werden.

Wir haben inzwischen – ausgehend von den Regelungen der Verordnung – die nähere Ausgestaltung des Verfahrens der **Anerkennung der Gutachter** und sachverständigen Prüfstellen entwickelt und auf dieser Grundlage Anfang November 2001 mit der Akkreditierung begonnen.

Die Antragsunterlagen und weitere Informationen zum Verfahren können abgerufen werden unter:

www.datenschutzzentrum.de/guetesiegel/

oder auf dem Postweg angefordert werden.

10.2 Erste Gutachter akkreditiert

Das Verfahren zur Erlangung von Gütesiegeln nach dem schleswig-holsteinischen Datenschutzgesetz sieht vor, dass die dafür notwendigen Gutachten nur von akkreditierten Gutachtern erstellt werden dürfen. Das Verfahren der Akkreditierung ist angelaufen.

Gutachter können akkreditiert werden, wenn die Antragsteller nachweisen, dass sie dem Anforderungsprofil hinsichtlich **Fachkunde**, **Unabhängigkeit** und **Zuver-**

lässigkeit entsprechen. An die Fachkunde der Gutachter und sachverständigen Prüfstellen werden dabei angemessene Anforderungen gestellt, die maßgeblich aus der Notwendigkeit, bei der Erstellung der Gutachten stets auf rechtlichen und technischen Sachverstand zurückgreifen zu können, resultieren. Dieser Sachverstand muss nicht notwendig in einer Person vereint sein. Anerkennungen sind auch beschränkt auf eines dieser Gebiete möglich. Außerdem besteht die Möglichkeit, Gutachten als **Gemeinschaftsgutachten** von Gutachtern oder Prüfstellen, deren fachliche Anerkennungen sich ergänzen, zu erstellen. Den Antragstellern wird die Möglichkeit eröffnet, ihre Kompetenz nicht nur durch formale Bildungsabschlüsse, sondern auch auf sonstige Weise nachzuweisen. Damit wird der Tatsache Rechnung getragen, dass im Bereich der Informationstechnologie hervorragende Fachkompetenz nicht selten auch auf eher unkonventionelle Weise erworben wird.

Die **Unabhängigkeit** der Gutachter und sachverständigen Prüfstellen ist unabdingbare Voraussetzung für die Akkreditierung und wird nicht nur im Rahmen der Anerkennung, sondern auch hinsichtlich des jeweiligen zertifizierten Produkts geprüft. Die Anerkennung wird in der Regel auf Dauer ausgesprochen. Um die Zuverlässigkeit, Unabhängigkeit und Fachkunde dauerhaft zu gewährleisten, unterliegen die anerkannten Gutachter und Prüfstellen jedoch verschiedenen regelmäßigen Meldeverpflichtungen.

10.3 Produktkriterien

Die Erteilung von IT-Gütesiegeln richtet sich nach einem Kriterienkatalog, der jährlich fortgeschrieben wird.

IT-Produkte können ein Gütesiegel erhalten, wenn sie den Rechtsvorschriften über den Datenschutz und die Datensicherheit entsprechen (Tz. 10.1). Was dies genau für ein IT-Produkt bedeutet, kann sich je nach Einsatzbereich unterscheiden. Generell müssen **fünf verschiedene Anforderungsbereiche** beim Prüfen des Produktes berücksichtigt und im Prüfgutachten dokumentiert werden: Recht, Produktbeschreibung, Technik, Organisation und Nutzeradäquanz.

Zunächst wird für das IT-Produkt (Hardware/Software/automatisiertes Verfahren inkl. Produktbeschreibung) aus den einschlägigen Rechtsnormen ein **Anforderungsprofil** abgeleitet, das die Sollvorstellung beschreibt. Anschließend wird auf der Basis der Produktbeschreibung der Istzustand der tatsächlichen Umsetzung im IT-Produkt festgestellt und bewertet. Dabei spielt der Grad der technischen Implementierung von Datenschutz- und Datensicherheitsfunktionalität eine große Rolle: Je besser die Datenschutz- und Datensicherheitsziele durch gut durchdachte und umgesetzte Technik sichergestellt werden und je weniger zusätzliche organisatorische Maßnahmen durch den Anwender notwendig sind, desto besser wird das IT-Produkt bewertet. Insbesondere darf der **Stand der Technik** nicht unterschritten werden. Da in vielen Fällen Technik allein zur Gewährleistung des Datenschutzes nicht ausreicht, müssen die zusätzlich erforderlichen organisatorischen Maßnahmen verständlich beschrieben und einfach mit angemessenem Aufwand

umsetzbar sein. Schließlich spielt auch eine **nutzeradäquate Realisierung** eine Rolle, um etwaige Fehlbedienungen mit Auswirkungen auf den Datenschutz und die Datensicherheit zu vermeiden.

Ein **Kriterienkatalog** auf unserer Homepage

www.datenschutzzentrum.de/guetesiegel/

hilft beim Erstellen des Anforderungsprofils und Bewerten des Produktes. Besonderer Wert wird bei unserem Datenschutzgütesiegel auf die folgenden Produkteigenschaften gelegt:

- **Datenvermeidung und Datensparsamkeit**

Personenbezogene Daten dürfen nur verarbeitet werden, soweit sie erforderlich sind. Dies bedeutet, dass für jedes geprüfte IT-Produkt zu untersuchen ist, inwieweit möglichst weitgehend auf personenbezogene Daten verzichtet wird. Das Maximum an Datenvermeidung ist dann erreicht, wenn bereits im IT-Produkt eine Erhebungsmöglichkeit für personenbezogene Daten verhindert wird. Lässt sich keine Verarbeitung ohne Personenbezug erreichen, muss aus dem Gutachten hervorgehen, warum keine datensparsamere Realisierung (Anonymität, Pseudonymität, frühestmögliches Löschen, Anonymisierung, Pseudonymisierung) gewählt werden konnte. Auch auf etwa anfallende temporäre Dateien muss bei der Prüfung geachtet werden.

- **Datensicherheit und Revisionsfähigkeit**

Um bewerten zu können, inwieweit Datensicherheit von dem IT-Produkt gewährleistet wird, ist klarzustellen, gegen welche Risiken die technischen und organisatorischen Maßnahmen, die beim Einsatz getroffen werden, schützen sollen und welche Risiken verbleiben. Für eine Revisionsfähigkeit ist die verständliche Dokumentation des IT-Produktes in allen Phasen (Erstellung, Installation, Betrieb, Wartung) entscheidend, da anderenfalls keine Nachvollziehbarkeit der Datenverarbeitungsprozesse möglich ist.

- **Gewährleistung der Rechte der Betroffenen**

Die Gewährleistung der Betroffenenrechte wie Auskunft, Löschung, Berichtigung, Sperrung oder Unterrichtung über die Datenverarbeitung sowie über seine Rechte wird heutzutage vielfach auf organisatorischer Ebene abgedeckt. Beim IT-Produkt ist entscheidend, inwieweit dort technisch die Wahrnehmung der Rechte direkt durch die Betroffenen ermöglicht oder sogar gefördert sowie die organisatorische Ebene beim Betreiber zur Gewährleistung der Betroffenenrechte unterstützt wird. Beispielsweise könnten IT-Produkte im Zusammenhang mit dem Internet dem Nutzer anbieten, seinen Anspruch auf Auskunft über seine personenbezogenen Daten unmittelbar über das Netz geltend zu machen – natürlich in einem sicheren Verfahren.

Schließlich besteht die Möglichkeit, unabhängig von allen anderen Produktkriterien zu beschreiben, mit welchen Funktionen oder Konzepten das IT-Produkt besonders datenschutzfördernd wirkt oder **Innovationen** im Datenschutz- oder Datensicherheitsbereich aufweist.

Was ist zu tun?
Hersteller und Vertreiber von IT-Produkten sollten anhand des Kriterienkatalogs prüfen, ob ihr Produkt für ein Gütesiegelverfahren in Betracht kommt.

10.4 Gütesiegel als Vergabekriterium

Gütesiegel sollen der öffentlichen Verwaltung als Entscheidungshilfe bei der Auftragsvergabe dienen. Sobald die ersten Produkte ein Siegel erhalten haben, werden sie im Rahmen der Beschaffung von IT-Produkten zu beachten sein.

Öffentliche Stellen in Schleswig-Holstein sollen die mit dem Gütesiegel ausgezeichneten Produkte bevorzugt beschaffen. Hersteller und Vertriebsfirmen von IT-Produkten unterziehen sich dem Verfahren, da sie sich vom Gütesiegel **Wettbewerbsvorteile** versprechen. Durch die Auszeichnung von IT-Produkten mit einem Gütesiegel kann aber auch der interessierte private Verbraucher den Datenschutz beim Erwerb von IT-Produkten, bei der Teilnahme am E-Commerce und der Bewertung von sonstigen Angeboten als Entscheidungskriterium einzusetzen.

Die Vergabe von Gütesiegeln stellt sich danach als Instrument dar, mit dem der Datenschutz nicht ordnungsrechtlich eingreift, sondern **marktwirtschaftliche Anreize** dafür schafft, dass private Hersteller und Vertriebsfirmen sich bei Konzeption, Entwicklung und Herstellung ihrer Produkte über Inhalt und Bedeutung des Datenschutzes Gedanken machen. Eine gestiegene Verbrauchernachfrage nach solchen Produkten dürfte auf Dauer zu signifikanten Wettbewerbsvorteilen solcher Konkurrenten führen, die sich durch überzeugende Datenschutz- und Datensicherheitslösungen auszeichnen.

Die bevorzugte **Beschaffung** von IT-Produkten mit Gütesiegel durch öffentlichen Stellen ist im Landesdatenschutzgesetz als „Sollvorschrift“ ausgestaltet worden. Das bedeutet für die beschaffende Stelle, dass sie generell die Verpflichtung zur vorrangigen Berücksichtigung dieser Produkte hat, es sei denn, dass zwingende Gründe ein Abweichen rechtfertigen. Die öffentlichen Stellen sind auch an die Regelungen des Vergaberechts gebunden, wonach der Zuschlag auf das wirtschaftlichste Angebot zu erteilen ist. Das wirtschaftlichste Angebot ist aber dasjenige, bei dem das günstigste Verhältnis zwischen der gewünschten Leistung (inklusive der Datenschutzeigenschaft des Produkts) und dem angebotenen Preis erzielt wird.

Bei der Beschaffung von IT-Produkten führt die Sollverpflichtung zur bevorzugten Beschaffung von Produkten mit **datenschutzrechtlichem Gütesiegel** dazu, dass dies ein die Leistungsbeschreibung und auch den Preis beeinflussender Um-

stand und daher von der ausschreibenden Stelle in die Verdingungsunterlagen aufzunehmen ist. Das Gütesiegelverfahren ist zwar nicht kostenneutral und kann daher zu einer anderen Preiskalkulation führen als bei Bietern, deren Produkte kein Siegel führen. Denn die öffentlichen Stellen sind gehalten, vorrangig solche Produkte einzusetzen, die den Vorschriften über Datenschutz und Datensicherheit entsprechen, selbst dann, wenn sie angemessen teurer als nicht datenschutzkonforme Produkte sind. Da ähnliche Bestimmungen inzwischen auch in anderen Ländern bestehen und auch das Bundesdatenschutzgesetz eine entsprechende Vorschrift beinhaltet, werden sich bald datenschutzrechtliche Standards herausbilden, unter die eine öffentliche Stelle bei der Beschaffung von IT-Produkten nicht gehen kann. Die Anerkennung der Gutachter und sachverständigen Prüfstellen setzt keinen Wohn- oder Geschäftssitz im Land Schleswig-Holstein voraus, sondern hängt ausschließlich von Fachkunde, Unabhängigkeit und Zuverlässigkeit ab. Um ein Gütesiegel können sich nicht nur Hersteller und Vertriebsfirmen aus Schleswig-Holstein, sondern auch andere nationale und international tätige Anbieter bewerben.

Was ist zu tun?
Diejenigen, die über die Anschaffung von IT-Produkten zu entscheiden haben, sollten sich zuvor unter

www.datenschutzzentrum.de/guetesiegel/

vergewissern, ob es bereits zertifizierte Produkte gibt.

10.5 Produktkriterien als Maßstab bei der Produktentwicklung

Die Kriterien für die Gütesiegelerteilung sollen nicht nur auf vorhandene IT-Produkte angewandt werden, sondern darüber hinaus die technische Entwicklung positiv beeinflussen.

Mittel- und langfristig erwarten wir die wichtigsten Auswirkungen des Gütesiegels bereits bei der **Entwicklung neuer IT-Produkte**. Denn Hersteller, die bereits im Herstellungsprozess ihres Produktes darauf achten, dass es die vorgegebenen Produktkriterien möglichst gut erfüllt, werden keine Probleme haben, das Gütesiegel zu erhalten. Darüber hinaus wird der Zeitbedarf für eine Prüfung durch Gutachter bei einer guten Vorbereitung und Dokumentation im Sinne der Produktkriterien deutlich geringer, sodass die Kosten für die Beurteilung sinken.

Auch besonders **innovative Ansätze** in den Bereichen Datenschutz und Datensicherheit können sich auszahlen: Zum einen werden sie im Gutachten gesondert herausgestellt (Tz. 10.3). Zum anderen können sie unter bestimmten Umständen als Ausgleich für einzelne Anforderungen herangezogen werden, die lediglich in unzureichender Weise erfüllt sind. Dies ist nur dann möglich, wenn die Gesamtsicht auf das IT-Produkt und seine Datenschutz- und Datensicherheitsfunktionalität positiv ausfällt.

Jede Datenschutzinnovation bedeutet gleichzeitig **Impulse** für die **technische Weiterentwicklung**. Bedingt durch einen fortschreitenden Stand der Technik, aber auch durch Fortschritte im Recht wird so das Erwartungsniveau an Produkte im Laufe der Zeit steigen. Dies bedeutet, dass ein Produkt, das später als ein anderes Produkt begutachtet wird, unter Umständen über zusätzliche Eigenschaften verfügen muss.

Dabei ist aber wichtig, dass Hersteller eine Planungssicherheit haben, was jeweils von ihnen konkret für die Erfüllung der Gütesiegelanforderungen erwartet wird. Ebenso sollen die Anwender und Nutzer wissen, welche Anforderungen bestehen. Wir planen derzeit eine jährliche Zeitschiene: **„Gütesiegel 2002“**, erweiterte Forderungen **„Gütesiegel 2003“**, wiederum erweitert **„Gütesiegel 2004“** usw. Nicht nur die Informationstechnologie, sondern auch das Siegel „lernt“ dazu.

Langfristig soll das Datenschutzgütesiegel dazu führen, dass die IT-Produkte am Markt einen besseren Standard in Sachen Datenschutz und Datensicherheit aufweisen als bisher.

Was ist zu tun?
Entwickler neuer IT-Produkte sollten sich anhand des Kriterienkatalogs für IT-Gütesiegel darüber informieren, was von Datenschutzseite morgen von ihrem Produkt erwartet wird.

10.6 Pilotverfahren zum Datenschutzaudit

Nach Aufnahme der gesetzlichen Regelung über das Datenschutz-Behördenaudit bei öffentlichen Stellen in das novellierte LDSG haben wir im Sommer 2001 mit der Umsetzung des Datenschutzaudits in die Praxis begonnen. Im Rahmen einer Pilotierungsphase werden Auditverfahren bei vier öffentlichen Stellen in Schleswig-Holstein durchgeführt. Ein Pilotprojekt konnte bereits erfolgreich abgeschlossen werden.

Das Datenschutzaudit bildet ein ganz neues Instrument auf dem Gebiet des Datenschutzes. Es tritt neben die klassischen Tätigkeitsfelder der Kontrolle und Beratung, die vom ULD in seiner Funktion als Kontrollorgan bzw. beratende Stelle in Datenschutzfragen wahrgenommen werden. Mit dem Datenschutzaudit soll ein geeignetes Instrument geschaffen werden, um die **Selbstverantwortung** der Behörden für den Datenschutz zu fördern. In erster Linie soll damit die Datenschutzsituation innerhalb einer Behörde verbessert werden.

Das Datenschutzaudit wird in Schleswig-Holstein als **Datenschutz-Behördenaudit** auf der Grundlage des **LDSG** durchgeführt. Öffentlichen Stellen wird die Möglichkeit eingeräumt, ihr Datenschutzkonzept durch das ULD überprüfen und anschließend dessen Ordnungs-

Im Wortlaut: § 43 Abs. 2 LDSG

Öffentliche Stellen können ihr Datenschutzkonzept durch das Unabhängige Landeszentrum für Datenschutz prüfen und beurteilen lassen.

mäßigkeit förmlich bescheinigen zu lassen. Charakteristisch für das Audit ist seine Freiwilligkeit. Gerade durch die freiwillige Teilnahme stärkt die öffentliche Stelle ihre Selbstverantwortung im Bereich von Datenschutz und Datensicherheit. Statt auf etwaige Kontrollen oder gar Beanstandungen zu warten, eröffnet das Audit die Möglichkeit, sich von vornherein positiv mit den Datenschutzfragen zu befassen.

Gegenstand eines Audits können ganz unterschiedliche Verfahren sein. Es kommen einzelne Datenverarbeitungsverfahren, einzelne Teile einer Behörde, d. h. ein einzelnes Amt oder eine Abteilung, oder die gesamte Verarbeitung personenbezogener Daten innerhalb einer öffentlichen Stelle in Betracht.

Grundlage eines jeden Datenschutzaudits ist eine zwischen der zu auditierenden öffentlichen Stelle und dem ULD geschlossene **Vereinbarung**, in der Gegenstand und Ziele des Datenschutzaudits festgelegt werden. Das eigentliche Auditverfahren vollzieht sich im Wesentlichen in den folgenden fünf Schritten:

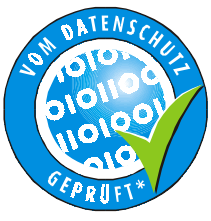
- Bestandsaufnahme,
- Festlegung der Datenschutzziele,
- Einrichtung eines Datenschutzmanagementsystems,
- Begutachtung durch das ULD und
- Verleihung des Datenschutzauditzeichens.

Die Einzelheiten des Auditverfahrens sind in den im März 2001 von uns herausgegebenen **Ausführungsbestimmungen** geregelt. Diese bestimmen den Verfahrensablauf.

Der Text der Ausführungsbestimmungen findet sich im Internet unter:

www.datenschutzzentrum.de/audit/

Den Kernbestandteil des Audits bildet das **Datenschutzmanagementsystem**. Es stellt die interne Organisation der Daten verarbeitenden Stelle im Hinblick auf die Erreichung der Datenschutzziele und die Einhaltung der datenschutzrechtlichen Vorgaben dar. Es ist die Gesamtheit aus Zuständigkeiten, vorgeschriebenen Verhaltensweisen und Abläufen sowie sächlichen Mitteln, die zur Erreichung der Datenschutzziele dienen. Mit dem Datenschutzmanagementsystem soll ein kontinuierlich hohes Datenschutzniveau innerhalb der öffentlichen Stelle sichergestellt werden.



Nach erfolgreichem Abschluss des Auditverfahrens wird der öffentlichen Stelle ein **Datenschutzauditzeichen** verliehen. Der auditierten Stelle wird bescheinigt, dass sie für eine unter Datenschutzgesichtspunkten einwandfreie Datenverarbeitung gesorgt hat. Die öffentliche Stelle kann mit diesem Zeichen werben. In erster Linie wird es sich hier um Werbung um das Vertrauen der Bürgerinnen und Bürger handeln, aber auch im Wettbewerb der öffentlichen Stellen untereinander wird das Auditzeichen sicherlich eine ernst zu nehmende Bedeutung erlangen.

Nach In-Kraft-Treten der Ausführungsbestimmungen im Sommer 2001 haben wir im Rahmen von **vier Pilotprojekten** mit der praktischen Umsetzung begonnen. Beteiligt sind auf kommunaler Ebene der **Kreis Ostholstein**, die **Stadt Norderstedt** und die **Gemeinde Büchen,** auf Landesebene das **Innenministerium des Landes Schleswig-Holstein**. Die Pilotprojekte dienen dem Zweck, auf allen Seiten praktische Erfahrungen mit einem ganz neuen Instrument auf dem Gebiet des Datenschutzes zu sammeln.

Da die vier Pilotprojekte unterschiedliche Verfahren zum Inhalt haben, decken sie die Bandbreite möglicher Auditverfahren ab:

- Das **Innenministerium des Landes Schleswig-Holstein** lässt in seiner Polizeiabteilung ein Auditverfahren für ein geplantes System zur produktorientierten Arbeitszeiterfassung sowie eines dezentralen Schichtdienstmanagements im Bereich der Landespolizei durchführen.
- Die **Stadt Norderstedt** führt ein Auditverfahren für ihr neues automatisiertes Personalverwaltungs- und Informationssystem durch.
- Das Audit der **Gemeinde Büchen** bezieht sich auf die gesamte automatisierte Verarbeitung personenbezogener Daten in der Gemeindeverwaltung Büchen sowie auf das in Büchen laufende Projekt der Einführung des „Virtuellen Rathauses“.

Das erste im Rahmen der Pilotierungsphase erfolgreich durchgeführte Datenschutzaudit betraf das Verfahren des **Kreises Ostholstein** zum Anschluss seines internen Computernetzes an das Internet. Der Kreis Ostholstein arbeitete bereits seit 1999 an einer Konzeption für den **Internet-Anschluss der Kreisverwaltung**. Von Anfang an bestand dabei die Absicht, auch unter datenschutzrechtlichen Aspekten ein korrektes und sicheres Verfahren zu gewährleisten. Die Erstellung eines Sicherheits- und Datenschutzkonzeptes stand im Mittelpunkt der Überlegungen. Ende des vergangenen Jahres legte der Kreis uns die nach den Ausführungsbestimmungen erforderliche Datenschutzerklärung vor. Die Erklärung wurde von uns einer Begutachtung unterzogen. Erstmals in Schleswig-Holstein und in ganz Deutschland wurde im Januar 2002 auf der Grundlage eines Landesdatenschutzgesetzes ein **Datenschutzauditzeichen** verliehen. Darin wird dem Kreis Ostholstein ein überzeugendes datenschutzrechtliches Konzept bestätigt.

Nach Abschluss der übrigen im Rahmen der Pilotprojekte noch kostenlos durchgeführten Auditverfahren im Frühjahr 2002 ist der Weg für alle öffentlichen Stellen eröffnet, sich einem gebührenpflichtigen Datenschutzaudit zu unterziehen. Weitere Informationen zum Audit im Internet:

www.datenschutzzentrum.de/audit/

Was ist zu tun?
Behörden in Schleswig-Holstein sollten die Chance ergreifen und durch die freiwillige Teilnahme an einem Datenschutzaudit zeigen, dass sie im Datenschutz gut sind. Damit können sie um das Vertrauen ihrer Bürgerinnen und Bürger werben.

11 Aus dem IT-Labor

11.1 BackUP-Magazin hilft Sicherheitslücken schließen

Leider wird oft zu wenig darüber nachgedacht, welche Funktionen Mitarbeiter an ihrem Arbeitsplatz-PC tatsächlich benötigen und welche überflüssig sind. Eine zu große Funktionenvielfalt hat zur Folge, dass Computersysteme leichter angegriffen oder manipuliert werden können. Wenn keine technischen Restriktionen vorgenommen werden, ist es z. B. allzu leicht möglich, Passwörter zu cracken, Passwortregeln auszuspionieren oder Daten zu verstecken. Ein neues backUP-Magazin hilft, Sicherheitslücken zu schließen.

Auch das von Wirtschaft und Verwaltung meistgenutzte Betriebssystem Windows NT 4.0 verfügt in der **Standardinstallation** über eine Vielzahl von Funktionen, die einen Benutzer auf dem Arbeitsplatz-PC mit **sicherheitskritischen Administrationsbefugnissen** ausstatten. Die Systeme enthalten nämlich bei der Auslieferung so gut wie keine Voreinstellungen im Hinblick auf die Datensicherheit. Unsicherheit ist so gewissermaßen der „Normalfall“, Datensicherheit muss erst nachträglich aktiviert werden. Wer dieses nicht im ausreichenden Maße tut, serviert seine Daten ungewollt der „Öffentlichkeit“ auf einem silbernen Tablett.

Deshalb haben wir bereits im Jahr 2000 in einem backUP-Magazin grundsätzliche Hilfestellungen gegeben (vgl. 23. TB, Tz. 10.1). Die positive Reaktion der Leser und die Vielzahl der vertiefenden Nachfragen war Anlass zu weiteren Handlungshinweisen. In dem backUP-Magazin **„MS-Windows NT 4.0 Resource Kit und Security Tools“** werden nun spezifische Schwachstellen aufgezeigt und Lösungsansätze beschrieben, die in dem Magazin „MS-Windows NT 4.0 – Sicherheitsmaßnahmen und Restrisiken“ nicht oder nur ansatzweise dargestellt werden konnten.

Dazu gehört auch eine ca. 120 Positionen umfassende **Checkliste**, die den Systemadministratoren einen Vergleich der von ihnen getroffenen technischen und organisatorischen Maßnahmen mit den von uns für erforderlich gehaltenen Mindestsicherheitsstandards ermöglicht.

Schließlich wird das „neue“ **Betriebssystem Windows 2000** in seinen Grundzügen dargestellt, um aufzuzeigen, dass die im Moment getätigten Investitionen in Datensicherheit bei einem Betriebssystemwechsel nicht verfallen, sondern wichtige Grundlagen für notwendige Anpassungen darstellen. Ein Verzeichnis von Internet-Webseiten mit hilfreichen Inhalten rundet das Magazin ab.

Künftige backUP-Magazine werden sich mit den Problemen der neuen Betriebssystemgeneration Windows 2000 und XP befassen.

www.datenschutzzentrum.de/material/themen/edv/backup/

11.2 Schulungs- und Simulationsnetz in Betrieb genommen

Viele sicherheitstechnische Effekte lassen sich im Rahmen von Tests nur prüfen, wenn ein größeres Netz und eine Mehrzahl von Rechnern genutzt wird. Gleiches gilt für die Demonstration von Ursache und Wirkung bei Beratungsgesprächen und Schulungen. Die bisherigen technischen Defizite in diesem Bereich konnten aufgrund der neuen räumlichen Gegebenheiten nach dem Umzug der Dienststelle behoben werden.

Der technische Aufwand, der für die Durchführung von Sicherheitschecks und die **Simulation** von **praxisnahen Konstellationen** betrieben werden muss, steigt mit der Komplexität der von den Daten verarbeitenden Stellen eingesetzten Systeme. Wir können und wollen uns als Kontroll- und Beratungsinstitution von dieser technischen Entwicklung nicht abkoppeln. In der Vergangenheit war es uns allerdings praktisch unmöglich, unsere Erkenntnisse und Lösungsvorschläge zur Behebung von Sicherheitslücken Dritten „live“ zu demonstrieren. Da die geeigneten technischen und räumlichen Voraussetzungen fehlten, blieb es häufig bei der grafischen Darstellung auf Folien und handschriftlichen Schaubildern auf Papier. Diese Defizite konnten nach dem Umzug der Dienststelle in ein neues Domizil behoben werden.

Wir verfügen nunmehr über verschiedene Simulationsmöglichkeiten, da durch eine Wechselplattentechnik auf der gleichen technischen Basis mehrere unterschiedliche Systemkonfigurationen zum Ablauf gebracht werden können. Außerdem ist als Software ein so genanntes **pädagogisches Netz** installiert, das es Teilnehmern an Beratungen und Schulungen ermöglicht, selbst aktiv zu werden, ohne bei fehlerhaften Aktionen Schaden anrichten zu können. In einem technikgestützten Dialog mit anderen Teilnehmern und unseren Mitarbeitern (Aufschalten auf andere Systeme und Darstellung bestimmter Systemzustände) kann die Effektivität der Wissensvermittlung wesentlich erhöht werden.

11.3 Bug oder Feature? Internet Explorer protokolliert Surfverhalten

Wir haben den Internet Explorer der Firma Microsoft einem Test in unserem IT-Labor unterzogen, um den Umgang mit Nutzerdaten beim Surfen zu analysieren. Die Resultate sind durchwachsen.

Der Internet Explorer legt seine temporären Dateien in drei Verzeichnissen ab. Dies sind **„Temporary Internet Files“**, **„Cookies“** und **„History“**. Im ersten Verzeichnis finden sich HTML-Seiten und Grafiken, die dort zwecks schnelleren Zugriffs für weitere Aufrufe vorgehalten werden. Im Cookie-Verzeichnis werden die Cookies abgelegt, die andere Webserver auf dem lokalen PC speichern. History schließlich umfasst die aufgerufenen Seiten mit URL (Webadresse) und Zugriffszeit. Dass es sich bei diesen Daten speziell auf Mehrbenutzersystemen um sensible Informationen handelt, leuchtet ein.

Wir haben den **Browser** daher genauer untersucht. Erstaunlicherweise erlaubt er bis einschließlich Version 5.5 keine vollständige Löschung dieser Informationen. Zum Entfernen der Cookies bietet er keine entsprechende Option, und auch die Buttons zum Löschen von Cache und History versehen nur vordergründig ihren Dienst. Tief in den Systemverzeichnissen befinden sich so genannte Dynamic-Hash-Tables, die als Inhaltsverzeichnis die Aufgabe haben, den Zugriff auf die zwischengespeicherten Daten zu beschleunigen.

Allerdings hat es Microsoft versäumt, Funktionen bereitzustellen, die diese Tabellen bei Bedarf wirklich löschen. Stattdessen werden die entsprechenden Bereiche als „frei" markiert, sodass sie später durch neue Informationen überschrieben werden können. Bis dahin bleiben die alten Inhalte einsehbar. Im Falle der **History** werden die Verlaufsdaten nur an die bestehende Datei angehängt, was zum einen die Datei ständig anwachsen lässt, zum anderen den Zugriff auf vermeintlich gelöschte URLs ermöglicht. Mithilfe eines speziellen Tools von Ward van Wanrooij, das im Internet zur Verfügung steht, ist es möglich, diese URL-Liste einzusehen und als Textdatei abzuspeichern. Dabei kommen alle seit der Installation des Browsers aufgerufenen URLs zum Vorschein, unabhängig davon, ob der Verlauf im Browser gelöscht wurde oder nicht.

Ein **manuelles Löschen** dieser Daten ist ohne tief greifende Fachkenntnisse nicht unmittelbar möglich, da Windows sie als Systemdateien behandelt und insofern Schreibzugriffe unterbindet. Nutzer mit „normalen" Systemkenntnissen können ihre Daten also nicht löschen. Dazu kommen diverse Schutzmechanismen, die es selbst auf Kommandozeilenebene extrem schwer machen, die entsprechenden Dateien zu lokalisieren und zu löschen.

Was ist zu tun?
Benutzer einer Internet Explorer Version bis einschließlich 5.5 sollten ein Update auf die Version 6 vornehmen. Der Einsatz eines alternativen Browsers wie Mozilla, Netscape oder Opera sollte in Erwägung gezogen werden.

11.4 Neue Browsergeneration bringt nicht nur Vorteile

Microsoft und Netscape haben neue Versionen ihrer Browser herausgebracht. Beide warten unter anderem mit verbesserten Sicherheits- und Privacy-Einstellungen auf.

Beide Produkte bieten in der 6er-Version die Möglichkeit, **Cookies** nach bestimmten Regeln zu akzeptieren oder abzulehnen. Hierbei kommt eine erste Teilimplementierung von P3P (Platform for Privacy Preferences) zum Einsatz (Tz. 8.4). P3P sieht vor, dass Privacy-Policies in standardisierter, elektronischer Form vorliegen, sodass Nutzer diese durch ihren Computer auswerten lassen können. Der Internet Explorer wertet bereits in der Standardeinstellung diese Datenschutzrichtlinien aus und lehnt Cookies ab, die vonseiten ohne eine solche Policy stammen. Bei **ersten Tests** wurde deutlich, dass die Standardeinstellung einmal mehr die Privatsphäre nicht optimal schützt. Mit Einführung des neuen Browsers

hatten nämlich auch die werbetreibenden Firmen entsprechende Policies eingeführt, sodass ihre jeweiligen Cookies automatisch akzeptiert wurden – auch die aus Datenschutzsicht bedenklichen persistenten (länger anhaltend gespeicherten) Cookies.

Auch an anderer Stelle hat Microsoft Änderungen vorgenommen. Zwar werden **ActiveX-Steuerelemente** und **Plug-Ins** noch immer standardmäßig und ohne Nachfrage ausgeführt, im Unterschied zur Vorversion ist dieses Verhalten jedoch abgeschaltet, wenn die Sicherheitseinstellungen auf „Hoch“ gesetzt werden.

Netscape setzt mit seinem Navigator ebenfalls auf P3P. Im Unterschied zum Explorer bietet Netscape jedoch von Haus aus eine Einstellung, sämtliche Cookies am Sitzungsende zu löschen. Doch auch hier ist die Standardeinstellung nicht akzeptabel: Mit „Enable All Cookies“ lässt der Browser sämtliche Cookies zu. Justieren von Hand ist also notwendig.

Es zeigt sich, dass die Implementierung verbesserter Sicherheitsstandards an sich noch keine grundsätzliche Verbesserung der persönlichen Sicherheit mit sich bringt. Die **Kompetenz des Nutzers** ist weiterhin gefragt, will er sich nicht auf unzulängliche Standardeinstellungen verlassen.

Was ist zu tun?
Als Benutzer muss man sich mit den Sicherheitheitsfunktionen aktueller Browser ernsthaft auseinander setzen, da auf die Werkseinstellungen kein Verlass ist. Browserhersteller müssen zukünftig der Sicherheit ihrer Produkte einen höheren Stellenwert geben.

11.5 Mozilla – noch kein Stern am Browserhimmel, aber ein Lichtblick

Das Open-Source-Projekt Mozilla hat sich zum Ziel gesetzt, einen Browser zu produzieren, der offiziellen Standards gerecht wird und den Nutzern erlaubt, ihn komplett den eigenen Bedürfnissen anzupassen.

In der bei Redaktionsschluss vorliegenden **Version 0.9.8** lässt sich z. B. die Unterstützung für JavaScript nicht nur komplett an- oder abschalten wie bei anderen Browsern, sondern es können jeweils einzelne Funktionsbereiche wie das Öffnen von Fenstern („Pop-Ups“) sowie der Zugriff per JavaScript auf Cookies abgeschaltet werden.

Neben der Unterstützung von P3P für die Akzeptanz von Cookies bietet Mozilla eine weitere interessante Funktion: So kann das Laden von **Grafiken**, die auf anderen Servern als dem jeweils angewählten liegen, unterbunden werden; ebenso lässt sich der Abruf von Grafiken von bestimmten Servern komplett verhindern.

Da zunehmend so genannte Web-Bugs (winzige, transparente Grafiken, die vom Nutzer nicht wahrgenommen werden) eingesetzt werden, um an Daten über das Nutzerverhalten zu gelangen, wird auch hier ein weitergehender Schutz der Pri-

vatsphäre erlangt. Wie bereits oben angemerkt, ist auch hier die Kenntnisnahme der Nutzer über ihre Möglichkeiten sowie das Anwenden dieser Kenntnisse erforderlich. Auf jeden Fall darf man sich jedoch schon jetzt auf die erste Finalversion des Browsers freuen. Da es sich um ein Open-Source-Projekt handelt, wird es von dem kostenlos erhältlichen Browser wahrscheinlich auch irgendwann eine speziell an Datenschutzanforderungen angepasste Version geben.

12 Europa

12.1 EUROJUST

Für 2002 ist die Einrichtung einer ständigen gemeinsamen Stelle namens EUROJUST zur verbesserten justiziellen Zusammenarbeit innerhalb Europas geplant. Wir haben gemeinsam mit den anderen Datenschutzbeauftragten datenschutzrechtliche Standards für die Ausgestaltung von EUROJUST formuliert.

Auf dem Gipfel in Tampere 1999 hatte der Europäische Rat die Schaffung von EUROJUST als Koordinierungsstelle vor allem für die europäischen Staatsanwaltschaften beschlossen, um im Bereich der schweren organisierten Kriminalität strafrechtliche Ermittlungen europaweit zu unterstützen und die Erledigung von Rechtshilfeersuchen zu vereinfachen. Seit März 2001 arbeitet eine Vorläuferstelle **PRO-EUROJUST** in Brüssel, wo voraussichtlich auch die ständige Stelle ansässig sein wird. EUROJUST soll sowohl mit dem bereits bestehenden Europäischen Justiziellen Netz als auch mit EUROPOL zusammenarbeiten und nach dem Entwurf eines Beschlusses des Rates Befugnisse zur Datenverarbeitung bekommen, die in vielerlei Hinsicht parallel zu EUROPOL verlaufen. Hierin besteht aus unserer Sicht eines der Hauptprobleme der Konzeption von EUROJUST: Eine nachvollziehbare **Zuständigkeitsabgrenzung** dieser Institutionen untereinander ist bislang noch nicht gelungen. EUROPOL ist bereits seit sechs Jahren etabliert und wird sich EUROJUST nicht unterordnen lassen. Zudem bestehen europaweit ganz verschiedene Traditionen, was das Verhältnis der justiziellen zu den polizeilichen Ermittlungsbehörden betrifft. Deshalb ist zu befürchten, dass es häufig zu einer Doppelung der Arbeit und somit auch zu **doppelten Datensammlungen** von EUROPOL und EUROJUST kommen wird. Dies kostet nicht nur Geld, sondern kann auch unangenehme datenschutzrechtliche Folgen haben.

> ***? EUROJUST***
>
> *Koordinierungsstelle für europäische Staatsanwaltschaften und Strafgerichte für die Verfolgung schwerer Straftaten. Jeder Mitgliedstaat entsendet ein nationales Mitglied in das so genannte Kollegium, das von einem Präsidenten geleitet wird. Eine gemeinsame Kontrollinstanz soll die Datenverarbeitung kontrollieren. Die ständige Stelle EUROJUST wird voraussichtlich noch 2002 eingerichtet.*

> ***? EUROPOL***
>
> *Seit 1995 bestehendes Europäisches Polizeiamt (www.europol.eu.int), das polizeiliche Ermittlungen bei schwerer Kriminalität insbesondere durch Informationsaustausch unterstützt. Es unterhält ein Informationssystem und Analysedateien zu speziellen Kriminalitätsformen (vgl. 18. TB, Tz. 4.2.9).*

Die Datenschutzbeauftragten haben in einer gemeinsamen Entschließung vom Oktober 2001 im Wesentlichen folgende **Anforderungen an EUROJUST** formuliert:

- EUROJUST darf nur nach Maßgabe der Erforderlichkeit Daten verarbeiten und grundsätzlich nur dann und mit Zustimmung des Ursprungsstaates an Dritte weiterleiten, wenn dort ein angemessener Datenschutzstandard besteht. Daten von Opfern und Zeugen dürfen nur bei Vorliegen besonderer Voraussetzungen verarbeitet werden.
- Welche Arbeitsdateien eingerichtet werden dürfen, die über Vorgangsverwaltungsdateien hinausgehen, ist im Einzelfall festzulegen.
- Daten sollten bei EUROJUST nicht länger gespeichert werden als in dem jeweils betroffenen Mitgliedstaat mit der kürzesten Löschungsfrist.
- Es muss einen eigenen Auskunftsanspruch Betroffener gegenüber EUROJUST geben.
- Betroffenen ist ein angemessener Rechtsschutz gegenüber EUROJUST zu gewähren.
- Es muss eine unabhängige Gemeinsame Kontrollinstanz geschaffen werden, deren Entscheidungen bindenden Charakter haben.
- Ohne entsprechende Grundlagen im nationalen Recht sind Zugriffe des nationalen Mitglieds bei EUROJUST auf deutsche Register wie das Zentrale Staatsanwaltschaftliche Verfahrensregister oder das Bundeszentralregister wie auch Auskünfte aus Strafverfahren nicht zulässig.

In dem vom Rat der EU grundsätzlich gebilligten Beschluss für die ständige Stelle sind leider **Defizite** hinsichtlich des Umfanges der Datenspeicherung und der Lösch- bzw. Prüffristen **geblieben**. Auch die Möglichkeiten, eine Auskunft zu verweigern, bestehen in weiterem Umfang als z. B. im Rahmen des Schengener Durchführungsübereinkommens oder des EUROPOL-Übereinkommens. Dagegen soll Betroffenen neben der Anrufung der Gemeinsamen Kontrollinstanz auch der Rechtsweg zu den nationalen Gerichten offen stehen. Bedingt durch die Rechtsform eines Ratsbeschlusses können Bundestag und Bundesrat wie bei einer EU-Verordnung noch Einfluss auf die Modalitäten der Umsetzung in das nationale Recht nehmen. Der Gesetzgeber sollte die bestehenden Spielräume zu einer grundrechtsfreundlichen Ausgestaltung von EUROJUST nutzen, damit in Richtung Europa kein Rechtsschutzgefälle für Betroffene entsteht.

Was ist zu tun?
Schleswig-Holstein sollte sich für eine Verbesserung der Rechtsschutzmöglichkeiten im Rahmen von EUROJUST einsetzen.

12.2 Richtlinie über den Datenschutz bei elektronischer Kommunikation: Wohin geht die Reise?

Die Europäische Union plant eine neue Richtlinie, die umfassende Regelungen über den Datenschutz sowohl im klassischen Telekommunikationsbereich als auch für das Internet enthalten soll. Datenschutzrechtliche Rückschritte sind dabei nicht ausgeschlossen.

Im 20. Tätigkeitsbericht (Tz. 9.1) hatten wir darüber berichtet, dass die Europäische Union eine Richtlinie zum Datenschutz bei der Telekommunikation erlassen hatte, die bis 1998 in innerstaatliches Recht umgesetzt werden musste. In Deutschland ist dies spätestens mit dem In-Kraft-Treten der neuen TDSV (vgl. 23. TB, Tz. 8.5) geschehen. Nun verfolgt die Europäische Union das ehrgeizige Ziel, die Datenschutzregelungen für den gesamten Bereich der elektronischen Kommunikation, also sowohl für den herkömmlichen Telekommunikationssektor als auch für das Internet, in einer Richtlinie zusammenzuführen. Dieser Plan ist Teil eines größeren Vorhabens, wonach die unübersichtliche **Regelungslandschaft** im Bereich der elektronischen Medien auf europäischer Ebene **vereinfacht** und **ausgedünnt** werden soll. Ein erster Entwurf wurde Mitte 2000 veröffentlicht und in die Gesetzgebungsmaschinerie der Europäischen Union gegeben.

Der Vorschlag enthielt durchaus **erfreuliche Regelungen**. Für den Telekommunikationsbereich übernahm er im Wesentlichen die bereits bestehenden datenschutzfreundlichen Vorgaben, und dehnte sie auf den Bereich des Internets aus. Damit würde auch auf europäischer Ebene festgelegt, dass beispielsweise **Nutzungsdaten** nur zu Abrechnungszwecken und wenigen anderen, eng umrissenen Zwecken gespeichert werden dürfen. Im Übrigen wären sie ebenso wie nach dem deutschen TDDSG nach Ende der Nutzung zu löschen. In dem Entwurf finden sich auch neuartige Regelungen zu so genannten Location Based Services, also zu Diensten, die darauf basieren, dass der Nutzer mit einem mobilen Handgerät geortet und ihm spezielle Informationen für seinen Standort angeboten werden. Die Nutzung der Standortdaten soll nach dem Richtlinienentwurf von der Zustimmung des Nutzers abhängig sein. Lediglich im Fall von Notrufen soll die Zentrale, bei der die Notrufe auflaufen, den Standort auch ohne Zustimmung des Nutzers sehen.

Weitere Regelungen, die bis zum Schluss umstritten waren, betreffen die Zusendung von unverlangten Informationen. Bislang konnten sich die Mitgliedstaaten nicht darauf einigen, ob insbesondere die Zusendung von unverlangten E-Mails (so genannten **Spaming**) mit einer Opt-In- oder einer Opt-Out-Lösung geregelt werden soll.

> ***? Opt-In***
>
> *Die Einwilligung des Betroffenen muss ausdrücklich erklärt werden.*
>
> ***? Opt-Out***
>
> *Solange der Betroffene nicht widerspricht, dürfen seine Daten verarbeitet werden.*

Daneben waren aber auch **Verschlechterungen des Datenschutzes** in der Diskussion. Die neue Richtlinie wurde nämlich mit einer anderen in Verbindung gebracht, in der es um Straftaten und Strafverfolgungen im Internet geht (Tz. 8.2). Danach soll die Überwachung im Internet verschärft werden. In diesem Zusammenhang wird sogar diskutiert, die **Speicherung von Nutzungsdaten** nicht nur zu erlauben, sondern die Provider zu verpflichten, diese Daten für eventuelle Strafverfolgungszwecke für einen bestimmten Zeitraum zu speichern. So hat der Rat in seinem gemeinsamen Standpunkt vom 21.01.2002 vorgeschlagen, die schon im Kommissionsentwurf enthaltene Vorbehaltsklausel für Belange der öffentlichen Sicherheit und Strafverfolgung zu ergänzen. Danach soll es ausdrücklich auch zulässig sein, durch einzelstaatliches Recht eine Aufbewahrungspflicht für Nutzungsdaten vorzusehen. Allerdings ist die europäische Gesetzgebung damit noch nicht abgeschlossen, sodass noch Änderungen möglich sind. Eine ausdrückliche Pflicht zur Aufbewahrung von Nutzungsdaten muss auf jeden Fall unterbleiben, denn eine Vorratsspeicherung dieses Ausmaßes wäre verfassungsrechtlich nicht zulässig.

Was ist zu tun?
Schleswig-Holstein sollte im Rahmen seiner Einflussmöglichkeiten darauf hinwirken, dass es auf europäischer Ebene nicht zu einer Verwässerung der positiven Vorgaben des neuen Richtlinienentwurfes kommt.

13 Informationsfreiheit

13.1 Erfahrungen mit dem Informationsfreiheitsgesetz Schleswig-Holstein

Nachdem das Informationsfreiheitsgesetz knapp zwei Jahre in Kraft ist, lässt sich eine erste positive Bilanz ziehen: Das Gesetz hat sich unspektakulär einen Platz im schleswig-holsteinischen Rechtssystem gesichert.

Das Informationsfreiheitsgesetz Schleswig-Holstein (IFG-SH) führt wie die entsprechenden Gesetze in Berlin, Brandenburg und Nordrhein-Westfalen eine bislang nicht gekannte Aktenöffentlichkeit in die Verwaltung ein: Es hat einen vom Grundsatz her **verfahrensunabhängigen** und **voraussetzungslosen** Informationszugangsanspruch für alle Bürgerinnen und Bürger gegenüber der Verwaltung geschaffen. Der Grundsatz der beschränkten Aktenöffentlichkeit gilt nicht mehr. Soll ein Akteneinsichtsgesuch ausnahmsweise abgelehnt werden, so muss dies jetzt begründet werden. Hingegen muss derjenige, der Einblick in behördliche Unterlagen nehmen möchte, dies nicht mehr besonders begründen.

So grundlegend diese Neuerung für das deutsche Recht auch sein mag, so **unaufgeregt** ist doch seine **Handhabung** in der bisherigen **Praxis** der schleswig-holsteinischen Landes- und Kommunalbehörden. Obwohl das Gesetz quasi über Nacht eingeführt wurde und es an einer vorherigen öffentlichen Diskussion mangelte, haben die Verwaltungen relativ flexibel auf die ersten Informationsanträge reagiert.

Die uns bekannt gewordenen Informationszugangsbegehren beziehen sich auf nahezu **alle Bereiche der Verwaltung** und waren in der ganz überwiegenden Anzahl gut nachvollziehbar. In den Fällen, in denen kein Anspruch auf Informationszugang bestand, war dies zumeist auf die Nichtanwendbarkeit des Gesetzes oder schlicht darauf zurückzuführen, dass die begehrten Informationen bei der Behörde nicht vorhanden waren. In der Mehrzahl der Fälle konnte indes ein Informationszugang erreicht bzw. – häufig nach Präzisierung des Informationsinteresses des Antragstellers – zwischen dem Informationssuchenden und der Verwaltung **erfolgreich vermittelt** werden. In aller Regel ging es den Informationssuchenden nicht darum, Informationen mit Personenbezug zu erhalten, sodass durch Schwärzung oder Herausnahme bestimmter Aktenteile ein für alle Beteiligten befriedigendes Ergebnis erzielt werden konnte.

Ein **Schwerpunkt** hat sich bislang im öffentlichen **Bauplanungs-** bzw. **-ordnungsrecht** und zunehmend im **Ausschreibungs-** und **Vergaberecht** herausgebildet. Zumeist handelt es sich bei den Antragstellern um Bürgerinnen und Bürger. Aber auch Gemeindevertreter, Mitarbeiter des öffentlichen Dienstes oder private Firmen haben schon entsprechende Anträge auf Informationszugang gestellt. Obwohl das Informationsfreiheitsgesetz grundsätzlich jedermann, d. h. unabhängig davon, wo der Betreffende wohnt oder welcher Nationalität er ist, ein Zugangsrecht gibt, ist die Tendenz zu beobachten, dass die Antragsteller sich häufig im Vorwege einer möglichen eigenen Betroffenheit informieren möchten. So ging es beispielsweise darum, sich rechtzeitig über den Stand eines in der unmittel-

baren Nachbarschaft angesiedelten Planungsvorhabens kundig zu machen. Oder aber man wollte schon einmal vorab Einblick in den kommunalen Erschließungsvertrag nehmen, um abzuschätzen zu können, wie hoch später der Erschließungsbeitrag sein würde. Von steigendem Interesse sind auch diejenigen Fälle, in denen ein Wettbewerbsunternehmen wissen möchte, warum ein öffentlicher Auftrag an ein Konkurrenzunternehmen vergeben worden ist.

Die bisherige Praxis mit dem Informationsfreiheitsgesetz hat insgesamt gezeigt, dass sich die Mehrzahl der Verwaltungen rasch auf die neue Gesetzeslage einzustellen vermocht hat. Offenbar verfügt Schleswig-Holstein über eine **gut entwickelte Informationskultur**, die es den Behörden erleichtert, Informationsbegehren von Bürgern nicht als abzuwehrenden Fremdkörper, sondern als Teil einer demokratischen Informationsordnung zu begreifen, wie die nachfolgende Auswahl interessanter Einzelfälle zeigt:

Interessante Einzelfälle

- **Informationen über die Verwendung von Haushaltsmitteln**

Der **Kreisverband einer Partei** wollte in Erfahrung bringen, warum sowohl auf Kreisebene als auch im Bereich einer kreisfreien Stadt seinen politischen Anliegen auf kommunaler Ebene keine Beachtung geschenkt wurde. Entsprechende Anfragen blieben ebenso unbeantwortet. Dabei ging es sogar um solche, die sich auf den Ansatz von Haushaltsmitteln für politische Fraktionen bezogen. Dafür musste die Partei aus der örtlichen Regionalpresse erfahren, dass sie mit einer Bearbeitungsgebühr von bis zu 4.000 DM zu rechnen habe. Die von uns angeschriebenen Kommunen reagierten rasch und stellten die gewünschten Informationen zur Verfügung. Eine zwischenzeitlich von der Partei beim Verwaltungsgericht Schleswig anhängig gemachte Klage konnte daraufhin für erledigt erklärt werden.

- **Zugang zu Unterschriftenliste**

Ein Landwirt plante die Erweiterung seiner Schweinemästerei. Gegen sein im Außenbereich der Gemeinde geplantes **Bauvorhaben** wandte sich eine Reihe von Bürgern der ca. 150 Einwohner zählenden Gemeinde mithilfe eines Bürgerbegehrens, das mit einer Unterschriftenliste verbunden war. Beide Unterlagen waren dem Bürgermeister der Gemeinde im Rahmen der Gemeindevertretersitzung überreicht worden. Der Antragsteller wandte sich an uns, nachdem sein Antrag auf Zugänglichmachung der Unterschriftenliste von der zuständigen Amtsverwaltung mit der Begründung abgelehnt worden war, dass die Unterschriftenliste bei der Beurteilung seines Bauantrages nach den hierfür einschlägigen Vorschriften des Baugesetzbuches ohne Belang sei. Damit wollte er sich nicht zufrieden geben, da er davon ausging, dass das Bürgerbegehren durchaus von Einfluss auf sein Baugenehmigungsverfahren sei. Da er auf eine rasche Verwirklichung der geplanten Erweiterung seiner Schweinemästerei angewiesen sei, gelte es, sich mit möglichen Einwendungen von betroffenen Nachbarn und Bürgern bereits im Vorfeld zu befassen, um etwaige Rechtsstreitigkeiten von vornherein zu vermeiden.

Das Informationsfreiheitsgesetz stellt besondere Anforderungen an den Informationszugang auf, wenn **Datenschutzrechte Dritter** entgegenstehen. Um die in der Unterschriftenliste enthaltenen Namen zu erfahren, hätte der Antragsteller darlegen müssen, dass er einen Anspruch verfolgt, der sich aus einer konkreten Rechtsbeziehung zu den Unterzeichnern der Unterschriftenliste ergibt. Die von ihm vorgetragenen Umstände waren nicht geeignet, hier ein **rechtliches Interesse** an der Kenntnis der Unterschriftenliste zu begründen. Er war deshalb darauf zu verweisen, dass er bei möglichen nachbarrechtlichen Widersprüchen als Drittbetroffener jederzeit Akteneinsicht beantragen kann, im derzeitigen Stadium des Verfahrens aber nicht nach dem Informationsfreiheitsgesetz.

- **Auskunft über tierschutzrechtliche Maßnahmen**

Tierschützer stellten auf einem **Reiterhof** Mängel bei der Pferdehaltung fest und informierten u. a. den Landrat und das Veterinäramt des Kreises. Nachdem einige Zeit vergangen war, wollten sie wissen, welche aufsichtsbehördlichen Maßnahmen seitens des Kreises getroffen worden waren. Sie erhielten die Antwort, dass der Betrieb von der zuständigen Tierschutzbehörde unter Beteiligung des Amtstierarztes des Kreises regelmäßig überwacht und kontrolliert wurde. Auch seien bereits konkrete Maßnahmen zum Tierschutz erfolgt. Den von den Tierschützern erhobenen Vorwürfen würde auch weiterhin nachgegangen werden. Diese Auskunft genügte den Tierschützern nicht und sie verlangten Akteneinsicht nach dem Informationsfreiheitsgesetz.

Das Gesetz enthält den Grundsatz, dass bei entgegenstehenden Datenschutzrechten Dritter keine Offenbarung der gewünschten Information erfolgen darf. Hiervon kann allerdings dann eine Ausnahme gemacht werden, wenn der Informationssuchende darlegt, dass er in einer konkreten Rechtsbeziehung zu demjenigen, um dessen Daten es geht, steht und keine überwiegenden schutzwürdigen Belange des Betroffenen entgegenstehen. Mittlerweile hatte der Inhaber des Reiterhofes rechtliche Schritte gegen die Tierschützer unternommen und mit Schadensersatzansprüchen gedroht, sollten diese bei ihrer Aussage bleiben, dass auf dem Reiterhof keine artgerechte Tierhaltung stattfinde. Es ließ sich nicht abschließend klären, ob deshalb bereits eine **konkrete Rechtsbeziehung** in dem beschriebenen Sinne vorlag.

Darauf kam es aber nicht an, weil Daten hätten offenbart werden müssen, die einem besonderen **Berufs- oder Amtsgeheimnis** unterliegen. Aufgrund der Tatsache, dass von den Tierärzten des Kreisveterinäramtes sowohl im Rahmen des verwaltungsrechtlichen Verfahrens als auch im Rahmen eines inzwischen bei der zuständigen Staatsanwaltschaft anhängigen Ermittlungsverfahrens tierärztliche Untersuchungen und Begutachtungen durchgeführt worden waren, griffen die Schutzvorschriften des Berufs- und Amtsgeheimnisses. Hierzu gehört auch die Schweigepflicht der Ärzte und der Tierärzte. Der Informationszugang musste daher versagt bleiben.

- **Auftragsvergabe zu Gewässeruntersuchungen**

Ein Petent hatte sich als Betreiber eines Labors für biologische Gewässeruntersuchungen bei der zuständigen Umweltbehörde um Aufträge zu **Gewässeruntersuchungen** bemüht. Seine Nichtberücksichtigung machte ihn stutzig und er begehrte Akteneinsicht um festzustellen, warum jeweils ein Konkurrenzunternehmen mit dem Auftrag betraut worden war. Dies wurde abgelehnt. Nach dem IFG-SH habe der Petent keinen Anspruch auf Akteneinsicht, da dieses durch die speziellere Regelung des Umweltinformationsgesetzes verdrängt werde. Im Übrigen handele es sich bei Auftragsvergaben um fiskalische Tätigkeit, die nicht unter das IFG-SH falle.

Wir haben die Auffassung vertreten, dass das **Informationsfreiheitsgesetz Schleswig-Holstein** auf einen solchen Fall anwendbar ist. Angesichts der in den Akten enthaltenen Angebote der Mitbewerber des Petenten sprach jedoch einiges für das Vorliegen von **Betriebs- bzw. Geschäftsgeheimnissen**. Ein derartiges Geheimnis ist dann anzunehmen, wenn die im Zusammenhang mit einem wirtschaftlichen Geschäftsbetrieb stehende Tatsache nur einem begrenzten Personenkreis zugänglich ist und ein Geheimhaltungsinteresse des Unternehmers sowie ein berechtigtes wirtschaftliches unternehmerisches Interesse besteht. Das Vorliegen eines Betriebs- oder Geschäftsgeheimnisses hindert indes nicht von vornherein die Zugänglichmachung der gewünschten Informationen. Vielmehr muss im Einzelfall eine Abwägung zwischen den schutzwürdigen Belangen des betroffenen Unternehmers und dem Offenbarungsinteresse der Allgemeinheit stattfinden.

Es ging dem Petenten indes nicht um die Kenntnis der hinter den jeweiligen Angeboten stehenden Personen bzw. Firmen, sondern darum, den Gang des Vergabeverfahrens nachzuvollziehen. Wir haben der Umweltbehörde daher geraten, die jeweiligen Angebote so zu **anonymisieren**, dass ein Rückschluss auf personenbezogene Informationen bzw. Betriebsdaten nicht mehr möglich ist. Dem ist die Behörde inzwischen gefolgt.

- **Einsicht in Erschließungsunterlagen**

Verschiedene Grundstückseigentümer in einem Erschließungsgebiet wollten sich schon einmal im Vorwege darüber informieren, welche Kosten für Erschließungsleistungen später auf sie zukommen und zu diesem Zweck den **Erschließungsvertrag** ihrer Gemeinde mit einem großen schleswig-holsteinischen Wohnungsbauunternehmen einsehen. Die Kommune war sich zunächst unsicher, ob damit eine Preisgabe von **Geschäfts- und Betriebsgeheimnissen** verbunden gewesen wäre. Nach Einsicht in den Erschließungsvertrag konnten wir die Bedenken nicht teilen. Unabhängig davon, dass hier lediglich eine einzelne Vertragspassage einschlägiges Zahlenmaterial enthielt, aus dem man aber bei einem derart großen Unternehmen schwerlich Rückschlüsse auf die betriebliche Kalkulation hätte ziehen können, war Folgendes zu berücksichtigen: die **Allgemeinheit** hat ein erhebliches Interesse daran, in welcher Größenordnung sich der für ein Erschließungsunternehmen entstandene umlagefähige Aufwand bewegt, zumal entsprechende Haushaltsansätze bereits in dem öffentlichen Haushaltsplan enthalten sein dürften. Im Ergebnis wurden deshalb die Unterlagen zugänglich gemacht.

- **Einblick in Stellungnahmen der Träger öffentlicher Belange**

Eine schleswig-holsteinische Stadt wollte wissen, ob Bürgerinitiativen Sitzungsvorlagen zu Flächennutzungs- und Landschaftsplänen zur Verfügung gestellt werden müssen. Wir haben dies bejaht, soweit es sich um **Stellungnahmen der Träger öffentlicher Belange** handelt. Zwar muss z. B. im Rahmen eines Bauleitplanverfahrens der Schutz des behördlichen Entscheidungsbildungsprozesses gewährleistet werden. Dieser Schutz gilt indes nicht für alle Arten von Unterlagen. Handelt es sich z. B. um Äußerungen von Trägern öffentlicher Belange, so sind dies – da es sich um extern erstellte Vorlagen handelt, deren inhaltliche Ergebnisse feststehen und von der Behörde nur noch bewertet werden müssen – Unterlagen, die unabhängig vom Stand des jeweiligen Verfahrens zugänglich zu machen sind. Der Kommune wurde geraten, die Stellungnahmen der Träger öffentlicher Belange zugänglich zu machen.

Soweit darüber hinaus auch Einsicht in die Anregungen und Bedenken übriger **Betroffener** begehrt wurde, war hingegen eine Zugänglichmachung der gewünschten Informationen nicht ohne weiteres möglich. Hier hätte die Bürgerinitiative ein rechtliches Interesse, also im Regelfall eine konkrete Rechtsbeziehung zu den Betroffenen, um deren Daten es ging, darlegen müssen, sofern nicht eine Anonymisierung in Betracht kam.

- **Einsicht in Bauscheinakten**

Ein rechtliches Interesse muss auch für den Fall dargelegt werden, dass ein Dritter Einsicht in die **Bauscheinakte** eines Betroffenen nehmen möchte. Derartige Anträge würden mehrfach gestellt. In einem Fall ging es offenbar darum zu erfahren, in welchem Umfang die von einem Nachbarn vorgenommenen Ausgrabungen von der Baubehörde genehmigt worden waren. Sind personenbezogene Daten betroffen, so kann nicht in die gesamte Akte Einblick genommen werden, um festzustellen, was darin enthalten ist, um dann anhand des vorhandenen Inhalts überlegen zu wollen, welche rechtlichen Schritte man gegebenenfalls einleiten möchte. In solchen Fällen ist es immer erforderlich, in einem ersten Schritt – gegebenenfalls unter Zuhilfenahme behördlicher Beratung – anzugeben, in welche Unterlagen konkret Einsicht genommen werden soll. In einem weiteren Schritt ist dann darzulegen, in welcher Rechtsbeziehung man zu den Daten des Betroffenen, um dessen Daten es geht, steht. Generell lässt sich die Aussage treffen, das eine konkrete Rechtsbeziehung in diesem Sinne im Rahmen nachbarschaftlicher Verhältnisse eher gegeben sein wird, während dies bei Außenstehenden wie z. B. einer Bürgerinitiative kaum einmal der Fall ist.

- **Urheberrecht an Bauplänen?**

Bei der Bauordnungsbehörde einer schleswig-holsteinischen Inselgemeinde tauchte die Frage auf, ob sie einem Petenten auch **Kopien** aus einer Bauakte zur Verfügung stellen dürfte. Fraglich war hier insbesondere, ob das **Urheberrecht** des Planverfassers gegen eine Überlassung von Kopien sprach. Nach unserer Auffassung war dies nicht der Fall. Denn zum einen unterliegen die in Bauakten enthal-

tenen Baupläne nicht automatisch dem Urheberrechtsschutz. Dies kann etwa dann der Fall sein, wenn das Bauwerk sich als **Ausdruck individuellen Schaffens** darstellt. Entspricht der Plan eines Wohnhauses hingegen der Darstellung eines üblichen Wohnhauses und zeichnete sich nicht durch besondere gestalterische Elemente aus, wird man nicht von einem dem Urheberrechtsschutz unterliegenden Plan ausgehen können.

Zum anderen ist es aber selbst dann, wenn der Urheberrechtschutz zu bejahen ist, zulässig, Kopien in einer gewissen Anzahl herzustellen (die Rechtsprechung spricht insoweit von bis zu sieben Stück), wenn sie lediglich privat bzw. zur Verfolgung eigener Interessen verwendet werden. Dies kann etwa dann der Fall sein, wenn die kopierten Unterlagen als Grundlage einer Besprechung mit Nachbarn verwendet werden sollen. Einer unsachgemäßen Handhabung der Kopien kann dadurch begegnet werden, das bei ihrer Aushändigung darauf hingewiesen wird, dass die **Daten** nur zu dem Zweck zu verwenden sind, zu dem sie ausgehändigt worden sind.

- **Auskunft über Behördeninformanten?**

Dem Veterinäramt eines Kreises war der **Hinweis** gegeben worden, dass in einem landwirtschaftlichen Betrieb gegen das Tierschutzgesetz verstoßen worden sei. Die Kontrolle durch das zuständige Amt konnte dies zwar nicht bestätigen, es wurden jedoch Verstöße gegen andere Vorschriften aus dem Bereich der Hygiene festgestellt. Der nunmehr von behördlichen Verfügungen betroffene Landwirt verlangte von dem Kreis Auskunft darüber, welche Person den Fall ins Rollen gebracht hatte. Die Kommunalaufsichtsbehörde bat uns um Prüfung, ob der Informationsanspruch berechtigt war.

Der Landwirt konnte sich zunächst wie jedermann auf den Grundsatz des freien Zugangs zu Behördeninformationen nach dem **Informationsfreiheitsgesetz** (IFG-SH) berufen. Daneben stand ihm noch eine weitere Rechtsgrundlage zur Verfügung, da er auch Beteiligter eines Verwaltungsverfahrens war. In diesem Fall gewährt das Landesverwaltungsgesetz einen Anspruch auf Akteneinsicht. Daneben kam weiterhin ein Auskunftsanspruch nach dem Landesdatenschutzgesetz (LDSG) in Betracht. Da der fragliche Informant im Zusammenhang mit den im Verfahren gegen den Landwirt gespeicherten personenbezogenen Daten in der Akte vorkam, war auch der Auskunftsanspruch nach LDSG vom Grundsatz her einschlägig.

Allerdings bestehen all diese Ansprüche nicht uneingeschränkt, vielmehr gelten Begrenzungen, bei deren Vorliegen keine Auskunft gegeben werden darf. Dies ist regelmäßig dann der Fall, wenn Auskunft darüber begehrt wird, welche Person der Behörde einen Hinweis gegeben hat. Hierzu hat die Rechtsprechung ausgeführt, dass staatliche Behörden ihre Aufgaben nur dann erfüllen könnten, wenn sie Hinweise von dritter Seite erhielten und die **Hinweisgeber** sich darauf verlassen könnten, dass ihre Identität nicht offen gelegt werde. Aus diesem Grund besteht regelmäßig kein Anspruch auf Auskunfterteilung über den Namen von Informanten. Anders liegt der Fall nur dann, wenn ausnahmsweise die Interessen des

Behördeninformanten hinter denen des Auskunftssuchenden zurückstehen müssen. Dies ist vor allem dann der Fall, wenn der Informant auf die **Verleumdung** oder **falsche Verdächtigung** des Betroffenen abzielt. Liegen Anhaltspunkte dafür vor, dass der Informant die Behörde wider besseren Wissens und leichtfertig falsch informiert hat, so darf seine Identität dem Auskunftssuchenden mitgeteilt werden. Ist dies nicht der Fall, so hat die Auskunft über den Informanten zu unterbleiben, da anderenfalls die Erfüllung der Aufgaben der Behörde gefährdet würde. Die Anwendung dieser Grundsätze auf den vorliegenden Fall ergab, dass im Ergebnis kein Anspruch auf Mitteilung des Informanten bestand.

- **Zugang zu Unterlagen über ein Straßenbauprojekt**

Ein Bürger einer Großstadt interessierte sich für ein unmittelbar in der Nähe seiner Wohnung geplantes Straßenbauprojekt von zentraler Bedeutung. Die Stadtverwaltung war bereits seit einiger Zeit mit umfangreichen Planungen hinsichtlich der Konzeption und Finanzierung der Anlage befasst. Ein von dem Bürger an die Stadtverwaltung gerichteter Antrag auf Zugang zu „allen Unterlagen des Straßenbauprojektes“ blieb weitgehend unbeantwortet. Der Betroffene wandte sich an uns. Da der Antrag sehr unbestimmt abgefasst war, legten wir ihm zunächst nahe, sein **Informationsinteresse näher darzulegen**. Nachdem klar war, dass es ihm in erster Linie darum ging, die Möglichkeiten für eine alternative Trassenführung auszuloten und zu erfahren, welche Auswirkungen in ökonomischer und ökologischer Sicht das Vorhaben mit sich bringen würde, setzten wir uns mit der Stadtverwaltung in Verbindung. Mehrere Schreiben mit der Bitte um Stellungnahme blieben zunächst unbeantwortet. Schließlich kam es zu einem gemeinsamen Gespräch mit dem Petenten, in dem die gegenseitigen Standpunkte ausgetauscht wurden. Die begehrte Einsichtnahme in die von der Stadt verworfenen Alternativtrassen sowie in ökologische Gutachten lehnte die Stadt unter Berufung auf den **Schutz des behördlichen Entscheidungsbildungsprozesses** rundherum ab.

Wir haben die Stadt darauf hingewiesen, dass es sich dabei im Wesentlichen um extern erstellte Gutachten handelt, bei denen ein Zugangsanspruch unabhängig vom Stand des Verfahrens besteht. Denn derartige extern erstellte Gutachten stehen ihrem Inhalt nach fest und sind nur noch von der Verwaltung zu bewerten. Die Stadt bat sich Bedenkzeit aus. Nachdem wiederum längere Zeit verstrichen war – der Petent wartete nun schon über ein halbes Jahr auf die Entscheidung über seinen Antrag – wandte sich die Stadt an die für sie zuständige Kommunalaufsichtsbehörde. Diese teilte unsere Rechtsauffassung und wies die Stadtverwaltung an, über den Antrag umgehend zu entscheiden. Mittlerweile hat der Petent Einsicht in die begehrten Unterlagen des Straßenbauprojektes erhalten.

- **Streit um die Anwendbarkeit des Gesetzes**

In einer Großstadt wurde im Bereich des örtlichen Universitätsklinikums eine Baumaßnahme auf technischem Gebiet ausgeschrieben und nach Durchführung des **Vergabeverfahrens** an ein Unternehmen vergeben. Eine Konkurrenzfirma wollte sich davon überzeugen, ob dieses Unternehmen tatsächlich das wirtschaftlichste Angebot abgegeben hatte. Die mit der Auftragsvergabe betraute Landes-

anstalt verweigerte die beantragte Akteneinsicht mit der Begründung, das Informationsfreiheitsgesetz sei auf fiskalische Betätigungen der öffentlichen Hand nicht anwendbar. Im Übrigen unterfalle sie ihrer Rechtsform nach bereits nicht dem Anwendungsbereich des Gesetzes.

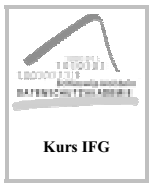
Mit dieser Entscheidung wollte sich das Unternehmen nicht zufrieden geben und wandte sich an uns. Dass das IFG-SH die rechtsfähigen **Anstalten des öffentlichen Rechts** nicht ausdrücklich erwähnt, ist ganz offensichtlich auf ein Versehen im Gesetzgebungsverfahren zurückzuführen: Warum ausgerechnet Anstalten und Stiftungen des öffentlichen Rechts vom Anwendungsbereich ausgeschlossen sein sollen, wenn der Gesetzgeber auf der anderen Seite ausdrücklich sonstige Körperschaften des öffentlichen Rechts angeführt hat, ist nicht nachvollziehbar. Hier sollte anlässlich einer Gesetzesnovellierung eine Klarstellung erfolgen.

Auch kann es für die Anwendung des Gesetzes nicht darauf ankommen, dass die Behörde hier **fiskalisch** gehandelt hat. Zunehmend spielt sich behördliches Handeln auch außerhalb der klassischen Handlungsformen des öffentlichen Rechts ab. Man denke dabei nur an das beliebte Outsourcen von Aufgaben. Wollte man das IFG-SH nur auf die klassischen Betätigungsformen der Behörden beschränken, würde man damit dem gesetzlichen Grundanliegen nach mehr Transparenz in der Verwaltung nicht gerecht. Das Transparenzgebot ist gerade bei Vergabeverfahren von großer Wichtigkeit.

Zu prüfen wäre allenfalls gewesen, ob das betroffene Unternehmen für sich den Schutz seiner **Geschäfts- und Betriebsgeheimnisse** in Anspruch nehmen konnte. Der Fall ist strittig geblieben, weil sich die Landesanstalt unserer Argumentation nicht anschließen wollte. Eine verwaltungsgerichtliche Klage ist **nicht** erhoben worden.

Was ist zu tun?
Die Bürgerinnen und Bürger sollten auch weiterhin ihre gesetzlichen Informationsrechte in Anspruch nehmen. Den Behörden steht es gut an, ihre Informationspflichten als Bürgerservice zu begreifen.

13.2 Informationen über das Informationsfreiheitsgesetz sind gefragt



Neben einer Vielzahl mündlicher und schriftlicher Anfragen zu Einzelfällen war eine spürbare Nachfrage nach **Schulungen** auf dem Gebiet der Informationsfreiheit zu beobachten. Außerhalb der regulären Kurse zum Informationsfreiheitsgesetz an der DATENSCHUTZAKADEMIE Schleswig-Holstein buchten einige Verwaltungen so genannte **Inhouse-Veranstaltungen**, die im Rahmen der DATENSCHUTZAKADEMIE Schleswig-Holstein vor Ort durchgeführt werden. Sie sind eine sinnvolle Alternative für den Fall, dass sich innerhalb der jeweiligen Verwaltung bzw. in Verwaltungen mehrerer Nachbarkommunen genügend interessierte Mitarbeiter finden. Veranstaltungen vor Ort als Inhouse-Seminare sind auch weiterhin möglich. Unsere Informationsmaterialien, insbesondere unsere Anwendungshinweise zum IFG-SH, werden rege nachgefragt. Interesse daran besteht offenbar weit über die Grenzen Schleswig-Holsteins hinaus.

Umfangreiche Materialien zum Thema Informationsfreiheit haben wir auf unserer Homepage zur Verfügung gestellt:

www.datenschutzzentrum.de/informationsfreiheit/

13.3 Entwicklung der Informationsfreiheit in Deutschland und in der EU

Im Mai 2001 verabschiedete das Europäische Parlament eine Verordnung über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission. Damit hat jetzt jede natürliche oder juristische Person mit Wohnsitz oder Sitz in einem Mitgliedsstaat das grundsätzliche Recht auf freien Zugang zu Dokumenten der Organe der EU.

> ***Im Wortlaut:***
> ***Art. 2 Abs. 1 Verordnung (EG) Nr. 1049/2001***
>
> *Jeder Unionsbürger sowie jede natürliche oder juristische Person mit Wohnsitz oder Sitz in einem Mitgliedstaat hat vorbehaltlich der in dieser Verordnung festgelegten Grundsätze, Bedingungen und Einschränkungen ein Recht auf Zugang zu Dokumenten der Organe.*

Grundlage des Informationsfreiheitsrechts ist, dass jedes Organ der EU ein **Register** über die bei ihm vorhandenen Dokumente **öffentlich zugänglich** machen muss, um eine wirksame Ausübung des Informationszugangsrechts durch die Bürger zu ermöglichen. Das Register soll für jedermann über das Internet abrufbar sein. Damit geht die Verordnung über das hinaus, was bislang Gegenstand der in den Bundesländern Berlin, Brandenburg, Schleswig-Holstein und Nordrhein-Westfalen geltenden Informationsfreiheitsgesetze ist: Während dort vorwiegend auf die in den jeweiligen Behörden vorhandenen Informationen abgestellt und nur in Einzelfällen auf eine aktive Zugänglichmachung der Informationen durch das Internet verwiesen wird, wird in der Verordnung unabhängig von einer Antragstellung die Veröffentlichung über das **Internet** vorangetrieben. Diese Regelung hat noch einen weiteren positiven Effekt: Durch sie kann der Bürger erfahren, welche Dokumente überhaupt bei den einzelnen Organen auf EU-Ebene vorhanden sind. Dies ist angesichts der auf EU-Ebene vorhandenen Vielfalt sicherlich ein großer Pluspunkt.

Positiv fallen ebenfalls zwei weitere Aspekte ins Gewicht: Zum einen sieht die Verordnung für die Bearbeitung von Informationszugangsanträgen – wie das IFG-SH übrigens auch – eine **unverzügliche** Bearbeitung vor; spätestens binnen 15 Tagen ergeht eine positive oder negative Entscheidung. Im Falle einer ablehnenden Entscheidung hat der Antragsteller dann die Möglichkeit, einen so genannten Zweitantrag, also eine Art Widerspruch, an das betreffende Organ zu richten und um Überprüfung seines Standpunkts zu ersuchen. Über diesen Zweitantrag muss ebenfalls unverzüglich, spätestens aber binnen 15 Arbeitstagen entschieden werden. Konsequenterweise muss das Organ im Falle einer vollständigen oder teilweisen Ablehnung des Zuganges den Antragsteller über mögliche Rechtsbehelfe unterrichten.

Mit der Regelung, dass vom Antragsteller lediglich Kostenersatz für die Anfertigung von **Kopien ab 20 DIN-A4-Seiten** verlangt werden kann und Gebühren nicht erhoben werden, geht die Verordnung über die Forderungen des Europäischen Gerichtshofs in seiner Entscheidung über die Angemessenheit von Gebühren hinaus.

Ob sich die Verordnung in der täglichen Anwendungspraxis angesichts der recht unscharf formulierten Ausnahmetatbestände der **öffentlichen** und **privaten Belange** – hierunter fallen etwa der Schutz der öffentlichen Sicherheit, der Schutz von Gerichtsverfahren und der Rechtsberatung oder auch der Schutz der Privatsphäre und der Integrität des Einzelnen – bewähren wird, bleibt abzuwarten. Hier muss gegebenenfalls nach einer gewissen Zeit nachgebessert werden.

Auch angesichts der Regelung, dass ein aus einem Mitgliedsstaat stammendes Dokument nicht ohne weiteres ohne die vorherige **Zustimmung** dieses **Mitgliedstaates** verbreitet werden darf, kann es zu Schwierigkeiten kommen. Denkbar wäre z. B. der Fall, dass man, um an ein Dokument aus Deutschland zu gelangen, den Weg über Schweden wählt, in dem es bekanntlich bereits seit dem Jahre 1766 das Recht auf freie Akteneinsicht gibt. Hier wird man im Einzelnen ermitteln müssen, ob es auf die jeweilige Verfügungsgewalt oder auf den Verfasser des Dokumentes ankommt. Bei einem originär europäischen Dokument, also beispielsweise zu Enfopol, sind jedenfalls die europäischen Organe zuständig.

In der Gesamtschau lässt sich bereits heute das Fazit ziehen, dass der Zugang zu behördlichen Entscheidungen und Unterlagen der EU-Organe hoffentlich **Signalwirkung** für den Bundesgesetzgeber hat. Während auf Landesebene mit Nordrhein-Westfalen inzwischen ein weiteres Land über ein Informationsfreiheitsgesetz verfügt, kommt der Bundesgesetzgeber nicht voran. Angesichts der Untätigkeit auf Bundesebene verstärkt sich der Eindruck, dass der Gesetzgeber sein Gesetzesanliegen, das bereits seit 1998 Grundlage des Koalitionsvertrages auf Bundesebene ist, nicht mehr mit hinreichendem Nachdruck verfolgt.

Was ist zu tun?
Die Bürger sind eingeladen, ihre neuen Informationsrechte gegenüber den Organen der EU wahrzunehmen. Der Bund ist aufgefordert, sein angekündigtes Informationsfreiheitsgesetz zügig zu verabschieden.

13.4 Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands (AGID)

Die Informationszugangsbeauftragten von Brandenburg, Berlin, Schleswig-Holstein und Nordrhein-Westfalen haben sich zur Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands (AGID) zusammengeschlossen.

Die Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands (AGID) wurde Ende August 2000 **in Kiel gegründet**, um sich über die datenschutzrechtlichen Bezüge hinaus mit allgemeinen und speziellen Fragen des Informationszugangs zu befassen. Ihr gehören die Informationsbeauftragten der Bundesländer Branden-

burg, Berlin, Nordrhein-Westfalen und Schleswig-Holstein an. Sie tagt zweimal im Jahr. Der Vorsitz wechselt halbjährlich. Im Berichtszeitraum führten Berlin und Schleswig-Holstein den Vorsitz. Ab dem 1. Februar 2002 ist der Vorsitz auf Nordrhein-Westfalen übergegangen, in dem es seit Anfang 2002 ebenfalls ein Informationsfreiheitsgesetz gibt.

Auch im Berichtszeitraum hat sich die Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands AGID wiederum in Berlin und Kiel getroffen, um über Fragen des Informationszuganges zu diskutieren. Dabei ging es neben dem **Erfahrungsaustausch** über die Gesetzespraxis in den beteiligten Ländern im Kern um die Entwicklung der Informationsfreiheit auf europäischer und auf Bundesebene. Begrüßt wurde das In-Kraft-Treten der Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission, wonach jetzt jede natürliche oder juristische Person mit Wohnsitz oder Sitz in einem Mitgliedsstaat das grundsätzliche Recht auf freien Zugang zu Dokumenten der Organe der EU hat.

Die Informationsbeauftragten halten es gerade vor dem Hintergrund dieser positiven Entwicklung auf europäischer Ebene (Tz. 13.3) für dringend geboten, dass der **Bundesgesetzgeber** sein bereits 1998 im Rahmen des Koalitionsvertrages angekündigtes Gesetzesvorhaben zügig in die Tat umsetzt. Die bisherigen Bemühungen zur Umsetzung der Ankündigung im Koalitionsvertrag lassen den Eindruck entstehen, als könnte das Vorhaben stillschweigend in der Schublade verschwinden. Mit der Realisierung des Informationsfreiheitsgesetzes auf Bundesebene hat es die Bundesregierung in der Hand, ein wichtiges Signal zu setzen: Die freiheitliche Demokratie braucht zu ihrem Funktionieren nicht nur wirksamen Schutz vor äußerer und innerer Bedrohung. Ebenso bedarf es gerade jetzt der Stärkung der Bürgerrechte. Nur so kann eine für das Bestehen des Rechtsstaates unabdingbare Balance zwischen staatlichen Eingriffsbefugnissen und grundrechtlich gewährleisteter Wahrnehmung der Bürgerrechte erreicht werden. Wenn die Bundesregierung auf diese Fragen nur einen geringen Bruchteil der Energie verwenden würde, die nach dem 11. September 2001 für die Verschärfung der Sicherheitsgesetze aufgebracht wurde, wäre eine Verabschiedung des Bundesinformationsfreiheitsgesetzes noch in dieser Legislaturperiode möglich.

14 Rückblick

14.1 Krankenhausinformationssysteme

In den vergangenen Jahren haben wir eine größere Anzahl von öffentlichen Krankenhäusern einer sicherheitstechnischen Überprüfung unterzogen. In praktisch allen Fällen stellten wir Sicherheitsprobleme mit den im Einsatz befindlichen Krankenhausinformationssystemen fest. Häufig konnten wir auch erkennen, dass die beabsichtigte Fortentwicklung der automatisierten Datenverarbeitung im medizinischen und im Abrechnungsbereich mit einer hohen Wahrscheinlichkeit zu Defiziten bei der Gestaltung von Zugriffsrechten, der Synchronisation zwischen den papierenen und den elektronischen Datenbeständen, bei der Administration der Systeme und Datenbestände und vor allen Dingen bei der Überwachung der ordnungsgemäßen Anwendung der automatisierten Verfahren führen würde. Die Probleme haben wir vor zwei Jahren (vgl. 22. TB, Tz. 6.5) ausführlich dargestellt in der Erwartung, dass die Verantwortlichen sich mit uns an einen Tisch setzen würden, um gemeinsame Lösungsmöglichkeiten zu erarbeiten. Obwohl uns die Notwendigkeit einer derartigen Vorgehensweise immer wieder in Gesprächen bestätigt wird, hat bisher kein geprüftes Krankenhaus die Initiative ergriffen. Es ist also bei Lippenbekenntnissen geblieben, man laviert weiter, die Hersteller von Software und die Anbieter von Konzepten werden nicht mit konkreten Forderungen konfrontiert. Uns bleibt nur, durch regelmäßige Prüfungen (in diesem Fall ausdrücklich im übertragenen Sinne) immer wieder den Finger in die Wunden zu legen.

14.2 Revisionsfähigkeit automatisierter Verfahren

Die Fortschritte in der Leistungsfähigkeit von IT-Systemen sind nach wie vor rasant. Die automatisierten Verfahren werden im gleichen Maße komplexer. Diese Entwicklung hat uns bereits im Jahr 1998 veranlasst anzumahnen, dass das verfassungsrechtlich begründete Prinzip der Revisionsfähigkeit des Verwaltungshandelns auch im Zeitalter vernetzter Informationssysteme seine Gültigkeit behalten hat (vgl. 20. TB, Tz. 6.6). Wer die Aussagen dieses Berichtes zu den diesbezüglichen Problemen z. B. im Sprach- und Datennetz (Tz. 7.2 und 7.3) mit unseren immerhin vier Jahre alten Forderungen und Vorschlägen vergleicht und berücksichtigt, dass die Grundsätze ordnungsgemäßer Datenverarbeitung in der Datenschutzverordnung immerhin auch schon vor acht Jahren festgelegt worden sind, muss zu dem Schluss kommen, dass die Verwaltung in diesem Punkt nicht dazugelernt hat. Sie versucht, weiter von der Hand in den Mund zu leben und immer nur die Sicherheitslöcher zu stopfen, die aktuell auftauchen.

14.3 KomFIT macht CeBIT Konkurrenz

Über die Gründung von KomFIT hatten wir mehrfach berichtet (vgl. 20. TB, Tz. 6.2; 22. TB, Tz. 12.5). Seit einigen Jahren veranstaltet die Arbeitsgemeinschaft der Kommunalen Landesverbände über ihre gemeinsame Einrichtung

KomFIT einen zentralen Informationstag zum Thema Informationstechnik. Dieses Ereignis, das im Jahr 2001 in Neumünster stattfand, hat sich aus kleinen Anfängen zu einem veritablen Kongress entwickelt. Die geschickte Auswahl von Ausstellern und Vortragenden und die strikte Konzentration auf die im kommunalen Bereich vorrangigen Fragestellungen führte zu einem außergewöhnlich hohen Informationsgehalt. Die aus unserer Sicht besonders wichtige Praxisnähe der Themen initiierte auch bezüglich der datenschutzrechtlich und sicherheitstechnisch bedeutsamen Aspekte intensive Diskussionen und Erörterungen „am Rande“. Wie in den vergangenen Jahren haben wir uns gerne durch die Entsendung von Referenten beteiligt und die Präsentationen und Vorträge besucht. Zusammenfassend ist festzustellen, dass die Führungskräfte und die Verwaltungspraktiker im IT-Bereich eher auf einen CeBIT-Besuch verzichten sollten, als diese KomFIT-Veranstaltung zu versäumen.

14.4 Unerbetene Faxwerbung

Auch im Berichtszeitraum erreichten uns wieder zahlreiche Beschwerden gegen die Zusendung unerbetener und nach der Rechtsprechung auch unerlaubter Faxwerbung durch zumeist ausländische Unternehmen. Inzwischen reift die Erkenntnis, dass es den werbenden Firmen vordergründig gar nicht um den Verkauf von Produkten oder Dienstleistungen geht. Die Empfänger der Werbefaxe sollen vielmehr dazu angehalten werden, gebührenintensive 0190-er Anschlüsse (bis zu 3,63 DM pro Minute!) anzurufen oder dort hin zu faxen, entweder um eine Bestellung aufzugeben, an einer Meinungsumfrage teilzunehmen oder um von ihrem Widerspruchsrecht Gebrauch zu machen. Wegen der fehlenden Zuständigkeit können wir in den meisten Fällen nicht direkt helfen und die Petenten lediglich an andere Ansprechpartner oder Institutionen (wie z. B. die Verbraucherschutzverbände, ausländische Datenschutzkontrollbehörden bzw. Beschwerdestellen oder den Verbraucherservice der Regulierungsbehörde für Telekommunikation und Post) verweisen. Insbesondere der zuletzt aufgeführte Weg verspricht in Zukunft vielleicht Erfolg, da nach unserer Auffassung der von den betroffenen Firmen nachhaltig betriebene Missbrauch der 0190-er Nummern letztendlich wohl nur mit dem Mittel des Lizenzentzuges gestoppt werden kann.

14.5 Sichtschutzfilter bei der Sparkasse

Im letzten Tätigkeitsbericht haben wir darauf hingewiesen, dass immer noch nicht alle Sparkassen im Lande moderne Selbstbedienungsterminals mit Sichtschutzfiltern einsetzen (vgl. 23. TB, Tz. 6.3.5). Nur diese neue Technik erfüllt jedoch die datenschutzrechtlichen Anforderungen an die gebotene Diskretion. Im Berichtszeitraum hat uns eine große Sparkasse aus dem Kieler Raum mitgeteilt, dass der Austausch veralteter Terminals gegen neue Geräte in ihrem Hause nunmehr abgeschlossen sei und künftig nur noch Terminals mit Sichtschutzfiltern im Einsatz seien.

14.6 PC-Welt in den Finanzämtern

Erst waren es die umfangreichen Gesetzesänderungen durch die Steuerreform, dann das Jahr-2000-Problem, dann die Euro-Umstellung, immer wieder wurden von der Oberfinanzdirektion „wichtige“ Gründe genannt, die sie daran hinderten, ein schlüssiges Konzept für die aufbau- und ablauforganisatorischen sowie die sicherheitstechnischen Rahmenbedingungen des PC-Einsatzes in den Finanzämtern vorzulegen (vgl. 23. TB, Tz. 4.9.3). Trotz vieler Planungen und Abstimmungsgespräche ist im Ergebnis bisher nichts passiert. Es ist zu vermuten, dass die von uns bereits vor Jahren festgestellten Defizite nach wie vor bestehen. Wir werden uns hierüber demnächst durch erneute Prüfungen Gewissheit verschaffen.

14.7 Gleichstellung der elektronischen Signatur mit der Schriftform im Zivilrecht

Im 23. Tätigkeitsbericht hatten wir unter Tz. 8.8 darüber berichtet, dass das Signaturgesetz, das die elektronische Signatur regelt, verabschiedet wurde. Zwischenzeitlich wurden auf Bundesebene auch Änderungen des bürgerlichen Gesetzbuches vorgenommen, mit denen qualifizierte elektronische Signaturen nach dem Signaturgesetz mit herkömmlichen Unterschriften rechtlich gleichgestellt werden. In vielen Fällen, in denen gesetzlich die Schriftform vorgeschrieben ist, genügt es, wenn die Erklärungen mit einer elektronischen Signatur versehen sind. Durch eine Beweiserleichterung in der Zivilprozessordnung wird vermutet, dass ein solcher Art signiertes elektronisches Dokument eine Erklärung enthält, die von der Person stammt, der der dazugehörige öffentliche Schlüssel zugeordnet ist. Damit sollen elektronische Geschäftsschlüssel – vor allem im Internet – erleichtert werden.

15 Beispiele dafür, was die Bürger von unserer Tätigkeit haben

1. *Ein Finanzdienstleister bot im Internet einen Service an, bei dem Schuldner gespeichert werden konnten. Den Betroffenen drohte eine moderne Version des Schuldenprangers mit weltweitem Zugriff. Auf unsere Initiative hin wurde dieser „Service“ eingestellt.*

2. *Bei Rabattsparkarten werden in der Regel zu viele personenbezogene Daten der Verbraucher erhoben. Dadurch entsteht die Gefahr detaillierter Kundenprofile. In allen geprüften Fällen haben wir eine erhebliche Reduktion der gespeicherten Datensätze durchgesetzt.*

3. *Das seit August 2001 geltende Lebenspartnerschaftsgesetz schafft für gleichgeschlechtliche Paare die Möglichkeit, eine „Eingetragene Lebenspartnerschaft“ registrieren zu lassen. Die für Schleswig-Holstein vorgeschlagene Regelung zu Auskünften aus den dem Heiratsbuch nachgebildeten Lebenspartnerschaftsbuch enthielt eine Formulierung, die zu unverantwortlichen Auskünften über sensible Sachverhalte geführt hätte. Wir konnten erreichen, dass der Text durch eine den Anforderungen an eine bereichsspezifische Datenschutzvorschrift entsprechende Formulierung ersetzt wurde.*

4. *Ein in Schleswig-Holstein ansässiger Access-Provider eröffnete gemeinsam mit dem Deutschen Forschungsnetz (DFN) speziell für Studenten eine günstige Zugangsmöglichkeit ins Internet. Die im Gegenzug von den Studenten verlangten Daten waren vom Umfang und der Sensibilität her weit überzogen. Wir konnten den Provider davon überzeugen, auf eine Reihe von Angaben zu verzichten, die Freiwilligkeit von Angaben erkennbar zu machen sowie das Angebot insgesamt datenschutzgerecht zu organisieren.*

5. *Das Menschenrechtsbüro der Scientology Kirche e. V. war mit dem Umfang der Informationen, die ihm der Sektenbeauftragte des Landes zugänglich machen wollte, nicht einverstanden. Ein zeitaufwändiger Prozess drohte. Durch unser Tätigwerden konnten wir ein für beide Seiten akzeptables Ergebnis erreichen, sodass sich die eingereichte Verwaltungsklage erledigte.*

6. *Bislang waren Bauakten nach Objekten gegliedert. Jeder neue Besitzer eines Hauses konnte per Akteneinsicht unter Umständen private Angelegenheiten der Voreigentümer in Erfahrung bringen. Auf unseren Vorschlag regelte der Innenminister per Erlass die Ordnung der Bauakten datenschutzgerecht.*

7. *Ein modernes Einsatzleitsystem der Polizei in Lübeck erlaubte umfangreiche Datenbankrecherchen. Dadurch wäre es möglich gewesen, Daten über Bürger unter Umgehung des Polizeirechts zu nutzen. Nach unserer Intervention wird das Einsatzleitsystem datenschutzgerecht nachgebessert.*

8. *In einem Einkaufszentrum in Kiel wurden die Kunden ohne den vorgeschriebenen Hinweis überwacht. Dadurch konnte es zur heimlichen Beobachtung kommen. Nach unserer Kontrolle wurden die notwendigen Hinweisschilder nachgerüstet.*

9. *Die Polizei speichert sensible Daten aus Telefonabhörmaßnahmen in EURAS. Die technischen Optionen des Systems hätten zu einer rechtswidrigen Nutzung der Daten führen können. Nunmehr wird die datenschutzrechtlich zulässige Nutzung von EURAS in einer Reihe von Punkten festgeschrieben.*

10. *Private Auskunfteien wollten justizielle Register automatisiert übernehmen. Die Zweckbindung der Daten wäre nicht mehr zu gewährleisten gewesen. Wir haben dem Justizministerium geraten, die Daten nicht herauszugeben.*

11. *Bei der Zusammenarbeit von Arbeits- und Sozialämtern war ein umfangreicher Datenaustausch vorgesehen. Ohne Erforderlichkeit sollten sensible Sozialdaten sogar bundesweit zum Zugriff bereitgestellt werden. Wir konnten erreichen, dass der Zugriff auf das erforderliche Maß begrenzt wurde.*

12. *Eine neue Standardsoftware für Sozialämter sah umfangreiche Auswertungsprogramme vor. Sozialhilfeempfänger hätten mit ihrer Hilfe unter vielfältigen Gesichtspunkten „gerastert" werden können. Nach unserer Intervention wurde das Programm unter dem Aspekt der Erforderlichkeit „abgespeckt".*

13. *Bei der Prüfung von Rundfunkgebührenbefreiungen sollten detaillierte Fragebögen eingesetzt werden. Sie hätten für eine vergleichsweise geringe Gebührenbefreiung weit reichende Angaben verlangt. Nach Gesprächen mit dem NDR wurden Datenfelder gestrichen und die Abläufe so organisiert, dass ein Datenmissbrauch nur noch schwer möglich ist.*

14. *Apotheken erhielten von ihren Rechenzentren CDs mit „Kundendaten", ohne dass diese etwas davon ahnten. Auf diese Weise hätten sie über Jahre hinweg nachvollziehen können, wer wann welche Medikamente gekauft hatte. Nach unserer Intervention soll dies nur noch mit Einwilligung der Betroffenen geschehen..*

15. *Bei der Koordination von Beurteilungen kam es immer wieder vor, dass einzelne Noten in „Großer Runde" erörtert wurden. Wir konnten den Innenminister davon überzeugen, dass dies allenfalls bei Spitzenbeamten erforderlich sein kann und dass im Übrigen nur Erst- und Zweitbeurteiler Kenntnis von der Note haben dürfen.*

16. *Das neue Computersystem EUREKA der Verwaltungsgerichte war datenschutzrechtlich nicht ausgereift. Dadurch wäre es z. B. einem unnötig großen Personenkreis im Gericht über einen langen Zeitraum möglich gewesen, nachzuvollziehen, wer wann gegen wen und warum einen Prozess geführt hat. Gemeinsam mit dem OVG konnten wir eine ganze Reihe von datenschutzrechtlichen Verbesserungen von EUREKA erreichen.*

17. *Ein Inkassounternehmen „drohte“ säumigen Schuldnern mit einer SCHUFA-Eintragung. Dadurch konnte es aus Furcht vor weiteren „Scherereien“ auch zu begründeten Zahlungen kommen. Wir konnten erreichen, dass das Inkassounternehmen die entsprechende Passage aus seinen Unterlagen strich.*

18. *Eine Handels- und Wirtschaftsauskunftei bewahrte „Löschlisten“ aus dem Schuldnerverzeichnis auch nach der Löschung noch auf. Dadurch konnte es dazu kommen, dass die Wirkung der Löschung verpuffte, da die Speicherung immer noch aus der „Löschliste“ ersichtlich war. Nach unserer Beanstandung mussten die Löschlisten in den Reißwolf.*

19. *Das Verfahren der Warnung von Behörden vor Auftragssperren war bislang ungeregelt. Dies konnte dazu führen, dass ein Unternehmen schon bei einem ersten Verdacht auf Unregelmäßigkeiten auf die Warnliste kam, sodass nahezu irreparable Schäden eintreten konnten, auch wenn an dem Verdacht im Nachhinein nichts „dran“ war. Nach unserer Intervention werden Warnlisten nur noch nach einem korrekt geregelten Verfahren herausgegeben.*

20. *Sensible Information in Altakten landeten bei einigen Behörden im öffentlich zugänglichen Müllcontainer. Spielende Kinder, neugierige Passanten oder recherchierende Journalisten konnten so z. B. Kenntnis von Medizin- und Sozialdaten bekommen. Nach unserer Kontrolle wurden die Verfahrensabläufe in vielen Behörden optimiert und so das Risiko einer unsachgemäßen Müllentsorgung verringert.*

21. *Viele Internet-Provider halten sich nicht an ihre gesetzlichen Pflichten, Nutzungsdaten im Internet sofort zu löschen. Dadurch können die Interessen von Internet-Surfern ausgewertet und zum Nachteil des Betroffenen genutzt werden. Mit unserem Anonymitätsservice AN.ON packen wir das Übel an der Wurzel: Die Nutzer können anonym surfen und so ihre gesetzlichen Rechte selbst durchsetzen.*

22. *Nicht selten sind Bürger und Verwaltung über den Umfang der Rechte nach dem Informationsfreiheitsgesetz unterschiedlicher Meinung. Bei verhärteten Fronten drohen kostspielige Prozesse. Wir könnten durch unsere Vermittlung in den meisten Fällen ein für beide Seiten akzeptables Resultat erreichen.*

23. *Eine Staatsanwaltschaft hat einer Wohnsitzgemeinde eine Benachrichtigung für das Wählerverzeichnis übersandt, aus der über die Tatsache der Verurteilung und die Dauer der Aberkennung des aktiven oder passiven Wahlrechts hinaus weitere belastende Informationen ersichtlich waren. Aufgrund unserer Anfrage entwickelte die Staatsanwaltschaft ein neues Formular, das die Mitteilungen des Wählerverzeichnisses auf den zulässigen Datenumfang beschränkt.*

24. Bei Zeugenladungen wurde häufig der Name des Opfers mitversandt. Dritte, z. B. der Arbeitgeber des Zeugen, konnten so erfahren, wer Opfer welcher Straftat geworden war. Auf unseren Vorschlag hat das Innenministerium die Polizeibehörden angehalten, den Opfernamen künftig nicht mehr auf Zeugenladungen anzugeben.

25. Mehrere Kommunen haben von Bürgern, die zur Zahlung von Zweitwohnungssteuer herangezogen wurden, zu viele Daten erhoben. Unzulässigerweise wurden sie zudem in allen Fällen zur Abgabe Eidesstattlicher Versicherungen gezwungen. Aufgrund von Beanstandungen wird den Betroffenen künftig deutlich dargestellt, welche Angaben in jedem Fall zu machen sind, und wann es zweckmäßig ist, ergänzende Erläuterungen zu geben, um Rückfragen oder gar fehlerhafte Steuerfestsetzungen zu vermeiden.

26. Die Landesbezirkskassen wiesen bisher Behördenmitarbeiter an, bei der Feststellungsbescheinigung auf Kassenanweisungen an die Landesbezirkskasse ihre Vergütungsgruppe anzugeben. Eine Erforderlichkeit für diese Angabe war nicht erkennbar. Auf unsere Anregung hat das Finanzministerium das Verfahren in unserem Sinne geändert.

27. Zwei Kreditinstitute gaben umfassend Auskünfte über die Vermögensverhältnisse von Verstorbenen an nicht erbberechtigte Verwandte weiter und begründeten so die Gefahr von Erbstreitigkeiten. Wir konnten beide Institute davon überzeugen, solche Auskünfte nur noch Erbscheininhabern zu erteilen.

16 DATENSCHUTZAKADEMIE Schleswig-Holstein

16.1 Fortbildungsprogramm 2002 der DATENSCHUTZAKADEMIE

Im Jahr 2001 hat die DATENSCHUTZAKADEMIE Schleswig-Holstein in 52 Kursen und 30 Inhouse-Seminaren insgesamt 1.284 Teilnehmer in Datenschutzfragen geschult. Sie finanziert sich ausschließlich aus den Kursbeiträgen. Das neue Jahresprogramm 2002 der DATENSCHUTZAKADEMIE stützt sich auf die bewährte Fortbildungsarbeit, die sich auch im neunten Jahr ihres Bestehens an den Kundenbedürfnissen orientiert. Neu aufgenommen wurden 2002 die Kurse:

- Datenschutz in der Arztpraxis (AR)
- Workshop für betriebliche Datenschutzbeauftragte (DWBT)

Von der Möglichkeit der zusätzlich zum Jahresprogramm angebotenen Inhouse-Seminare, die bei den Behörden und in den Firmen vor Ort durchgeführt werden können, wird zunehmend Gebrauch gemacht. Bei diesen Kursen kann das Fortbildungsprogramm auf die Fragen der Teilnehmer vor Ort direkt zugeschnitten werden.

Das Unabhängige Landeszentrum für Datenschutz verfügt zur Durchführung von Technikkursen – ebenso wie der Projektpartner Nordsee Akademie in Leck – in den Mitte letzten Jahres bezogenen neuen Räumlichkeiten über einen modernen PC-Schulungsraum mit 12 miteinander vernetzten Computerarbeitsplätzen. Hierin ist die praktische IT-Schulung der Teilnehmer unter Supervision des Kursleiters möglich. Der Raum kann auch zu besonderen Konditionen an andere Fortbildungseinrichtungen vermietet werden.

Das Jahresprogramm 2002 der DATENSCHUTZAKADEMIE Schleswig-Holstein mit näheren Informationen zu den Veranstaltungen und Anmeldeformularen kann kostenlos angefordert werden.

Schleswig-Holstein
DATENSCHUTZAKADEMIE

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstr. 98, 24103 Kiel
Fax: 0431/988-1223
E-Mail: akademie@datenschutzzentrum.de

Das Programm ist auch auf unserer Homepage im Internet verfügbar:

www.datenschutzzentrum.de/akademie/

Veranstaltungsübersicht 2002 für die Kurse der DATENSCHUTZAKADEMIE Schleswig-Holstein			
JANUAR:	Datenschutz in der Arztpraxis	AR 1	24.01.2002
FEBRUAR:	Landesdatenschutzgesetz 2000	R 11	26.02.2002
	Systemdatenschutz nach LDSG 2000	T 11	27.02.2002
MÄRZ:	Datenschutz in der Arztpraxis	AR 2	06.03.2002
	Behördliche Datenschutzbeauftragte Recht	DR 3	11. - 12.03.2002
	Datensicherheitsrecht, Prüfung und Bewertung von Sicherheitsmaßnahmen durch behördliche Datenschutzbeauftragte	DT 3	13. - 15.03.2002
	Das neue Bundesdatenschutzgesetz	BDSG 3	19.03.2002
	Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung im Anwendungsbereich des BDSG	SIB 2	20.03.2002
	Informationsfreiheitsgesetz Schleswig-Holstein	IFG 4	21.03.2002
	Datenschutz an der Schule	L 30	21.03.2002
APRIL:	Windows NT Sicherheit I	NT-I 3	16. - 19.04.2002
MAI:	Schutz von Personaldaten	P 10	06. - 07.05.2002
	Einstieg in das Datenschutzrecht	E 12	08.05.2002
	Datenschutz in der Arztpraxis	AR 3	14.05.2002
	Datenschutz in der Wirtschaft – Schwerpunkte der Datenschutzaufsicht in Schleswig-Holstein	DWI 2	15.05.2002
	Workshop für behördliche Datenschutzbeauftragte	DW 6	29.05.2002
JUNI:	Einführung Datenschutz im Schulsekretariat	ES 11	05.06.2002
	Landesdatenschutzgesetz 2000	R 12	06.06.2002
	Systemdatenschutz nach LDSG 2000	T 12	07.06.2002
	Windows NT Sicherheit II	NT-II 3	11. - 14.06.2002
	Behördliche Datenschutzbeauftragte nach LDSG 2000	BDSB 9	19.06.2002
	Informationsfreiheitsgesetz Schleswig-Holstein	IFG 5	26.06.2002
SEPTEMBER:	Führung von Personalakten	PA 10	09. – 10.09.2002
	IT-Revision	ITR 2	11.09.2002
	Einführung Datenschutz im Schulsekretariat	ES 12	11.09.2002
	Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung im Anwendungsbereich des LDSG	SIL 2	12.09.2002
	Behördliche Datenschutzbeauftragte Recht	DR 4	23. - 24.09.2002
	Datensicherheitsrecht, Prüfung und Bewertung von Sicherheitsmaßnahmen durch behördliche Datenschutzbeauftragte	DT 4	25. - 27.09.2002

OKTOBER:	Das neue Bundesdatenschutz7gesetz	BDSG 4	08.10.2002
	Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung im Anwendungsbereich des BDSG	SIB 3	09.10.2002
	Personaldatenverarbeitung im Rahmen des Mitbestimmungsrechts	PR 6	09.10.2002
	Datenschutz bei der Internet-Nutzung	NET 5	08 - 09.10.2002
	Technik und Recht von Firewalls	FW 9	10.10.2002
NOVEMBER:	Windows NT Sicherheit I	NT-I 4	05. - 08.11.2002
	Behördliche Datenschutzbeauftragte nach LDSG	BDSB	06.11.2002
	Workshop zur Datensicherheit	SIW 8	20. - 22.11.2002
	Informationsfreiheitsgesetz Schleswig-Holstein	IFG 6	26.11.2002
	Workshop für betriebliche Datenschutzbeauftragte	DWBT	27.11.2002
	Datenschutz an der Schule	L 31	28.11.2002
DEZEMBER:	Einstieg in das Datenschutzrecht	E 13	04.12.2002
	Workshop für behördliche Datenschutzbeauftragte	DW 7	05.12.2002
	Technischer Datenschutz an Schulen	LT 7	09.12.2002
	Windows NT Sicherheit II	NT-II 4	10. - 13.12.2002

16.2 Sommerakademie 2002

Die Sommerakademie 2002 findet am **26. August 2002** im **Kieler Schloss** statt.

Das Thema lautet: **„Unser Recht auf Anonymität“**.

Information und Anmeldung beim
Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstraße 98 / 24103 Kiel
Telefon: 0431/988-1200 / Telefax: 0431/988-1223
E-Mail: mail@datenschutzzentrum.de

Die aktuellsten Informationen zur Sommerakademie 2002 werden bekannt gegeben unter:

www.datenschutzzentrum.de/somak/somak02/somak02.htm

Beim **ULD SH** erhältliche Publikationen:

Neues Datenschutzrecht in Schleswig-Holstein
Text des Landesdatenschutzgesetzes, der Datenschutzverordnung, des Informationsfreiheitsgesetzes, der Regelungen zum Datenschutzaudit und Datenschutzgütesiegel und des Bundesdatenschutzgesetzes

Tätigkeitsbericht
des letzten Jahres als Landtagsdrucksache

Faltblätter
Safer Surfen!: Verschlüsseln – Ich?
Safer Surfen!: Selbst sicher(n)!
Safer Surfen!: Ich bin drin! ... Und meine Daten?
Datenschutz im Melderecht ... und was Sie persönlich davon haben
Virtuelles Datenschutzbüro – Virtual Privacy Office
Sicherheit durch Anonymität – Security by Anonymity
Datenschutzgerechte Biometrie – Privacy-compliant Biometrics
Das Informationsfreiheitsgesetz Schleswig-Holstein
Datenschutz-Audit und Datenschutz-Gütesiegel

Broschüren
backUP-Magazin für IT-Sicherheit (Reihe)
Datenschutz leicht gemacht – Praxistipps zum Datenschutzrecht (Reihe)
Sich wohl fühlen in der Informationsgesellschaft – Das ULD stellt sich vor

Diverse Aufkleber
Der Mensch ist mehr als Null und Eins, Virtuelles Datenschutzbüro,
Aufkleber zum Thema E-Mail-Verschlüsselung

DATENSCHUTZAKADEMIE Schleswig-Holstein
Jahresprogramm 2002

Schleswig-holsteinische Datenschutzinformationen im Internet
Datenschutzinformationen aus Schleswig-Holstein sind natürlich auch im weltweiten Datennetz zugänglich: **http://www.datenschutzzentrum.de** (Homepage des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein). Auf der optisch neu gestalteten und inhaltlich neu strukturierten Website finden Sie Publikationen des Unabhängigen Landeszentrums für Datenschutz sowie umfangreiche Informationen zum Thema „Datenschutz“ und das Fortbildungsangebot der DATENSCHUTZAKADEMIE Schleswig-Holstein. Weiterhin ist dort der öffentliche Schlüssel des Unabhängigen Landeszentrums für Datenschutz erhältlich.

Datenschutz auf CD-ROM
Wie jedes Jahr bringen wir eine CD-ROM mit dem Inhalt des Tätigkeitsberichtes und der zum Zeitpunkt der Veröffentlichung dieses Berichtes auf der Homepage bereitstehenden Informationen heraus. Für Benutzer, die über kein eigenes Programm verfügen, um die internetgerechten Dateien anzuschauen, wird ein einfacher Offline-Browser mitgeliefert. Die CD-ROM kann beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein kostenlos angefordert werden.

Index

A

Abhörmaßnahmen **28**, **94**
Abrufverfahren
automatisiertes **19**
Akkreditierung von Gutachtern **132**
Akten **106**, **149**
Akteneinsicht **149**, **151**, **163**
Akteneinsichtsrecht **44**
AN.ON (Anonymität online) **123**
Anonymität **15**, **117**
im Internet **112**, **123**
Antiterrorgesetzgebung **10**
AOK **52**
Apotheken **8**, **56**, **60**, **164**
Arbeitgeber **87**
Arbeitnehmerdaten **87**
Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands (AGID) **158**
Arbeitsverwaltung **46**
Arztpraxen **57**
Auftragsdatenverarbeitung **52**, **63**
Auskunfteien **35**, **74**, **76**, **80**, **164**, **165**
Ausländer **40**, **41**, **42**
Ausländergesetz **40**, **42**
Ausländerzentralregister (AZR) **41**
Authentizität **38**, **117**
automatisierte Datenverarbeitung **71**
automatisierte Verfahren **99**
automatisiertes Abrufverfahren **19**

B

backUP-Magazin **9**, **140**
Banken **82**, **161**, **166**
Bauakten **21**
Bauwesen **153**
Behördenaudit **92**
Beihilfe **69**
Betreuung **36**
Bewegungsprofil **43**
Biometrie **41**, **125**
BioTrusT **125**
Browser **142**, **143**
Bundesdatenschutzgesetz
Novellierung 2001 **73**
Bundeskriminalamt (BKA) **23**
Bundesnachrichtendienst **115**

C

Chipkarte **51**, **127**
Computerkriminalität **113**
Cookies **142**
Customer-Service-Center **96**
Cyber-Crime Convention **32**, **113**

D

Datenabgleich **23**
Datenerhebung **48**, **67**, **73**, **85**
DATENSCHUTZAKADEMIE Schleswig-Holstein **9**, **74**, **105**, **156**, **167**
Datenschutzaudit **7**, **14**, **128**, **137**
Datenschutzauditverordnung **131**
Datenschutzbeauftragter
behördlicher **18**
Datenschutzkonzept **137**, **139**
Datenschutzmanagement **138**
Datenschutzordnung **17**
Datenschutzregelung für das Parlament **17**
Datensicherheit **7**, **8**, **14**, **52**, **57**, **61**, **131**, **134**, **140**
Datensparsamkeit **14**, **43**, **73**, **131**, **134**
Datenspeicherung **81**
Datenübermittlung **28**, **33**, **36**, **41**, **44**, **54**, **57**, **73**, **83**, **87**
Datenvermeidung **14**, **73**, **131**, **134**
Dienstleister
externer **62**, **95**, **98**, **105**
digitale Signatur **120**
DSL (Digital Subscriber Line) **115**
Düsseldorfer Kreis **81**

E

E-Commerce **127**
EDV-Verfahren
Test und Freigabe **66**, **93**
E-Government **90**, **108**
Einsatzleitsystem **25**
Einwilligung **49**, **50**, **55**, **57**, **59**, **75**, **85**
elektronische **120**
elektronische Kommunikation **147**

elektronische Signatur **37**, **108**, **118**, **162**
elektronische Steuerakten **65**
elektronischer Ausweis **41**
elektronisches Grundbuch **37**
E-Mail **91**, **102**, **115**
  Werbesendungen **120**
Errichtungsanordnung **32**
EU-Datenschutzrichtlinie **64**
EURAS („Ermittlungshilfe und Recherche-organisation – ein Auswerte-System“) **31**, **164**
EUREKA **71**, **164**
EUROJUST **145**
Europa **145**
Europäische Datenschutzrichtlinie **73**
Europäische Union **118**, **147**, **157**
EUROPOL **145**

F

Faxverkehr **86**
Faxwerbung **161**
Finanzamt **62**, **162**
Fingerabdrücke **41**
FISCUS (Föderales Integriertes Standardisiertes Computer-Unterstütztes Steuersystem) **64**

G

Gebührendaten **96**
Geheimschutzbeauftragter **39**
Genomanalyse **8**, **58**
Gentechnik **8**, **58**
Gentest **60**
Gericht **33**, **71**
Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (EGG) **120**
Gesetz zur Verbesserung der Zusammenarbeit zwischen Sozial- und Arbeitsämtern **44**, **46**
Gesundheitsamt **50**
Gesundheitsdienstgesetz (GDG) **50**
Gesundheitswesen **51**
Gutachtenauftrag **54**
Gutachter **132**
Gütesiegel **7, 9, 14, 62, 128, 131, 133, 135, 136**

H

Handel **83**, **84**

I

Identitätsmanagement **117**
IKOTECH III **97**
Industrie **83**
informationelles Selbstbestimmungsrecht **40**, **58**
Informationsfreiheitsgesetz **149**, **151**, **156**, **157**, **165**
Informationsgesellschaft **10**
INPOL-neu **22**, **24**
Insolvenzverfahren **33**
Internet **12**, **33**, **81**, **90**, **108**, **111**, **114**, **116**, **117**, **119**, **122**, **123**, **147**, **157**, **163**
  Anonymität **112**, **123**
  Veröffentlichung im **81**
Internet Explorer **141**, **142**
Internet-Kommunikation **100**, **102**, **111**
IP-Nummer **111**
IT-Kommission **97**
IT-Labor **9**, **140**, **141**
IT-Produkte **131**, **133**, **134**, **135**, **136**

J

JAP **124**
JavaScript **143**
Justiz **33**, **35**, **38**
Justizregister **35**

K

KomFIT **160**
Kommunalverwaltung **18**, **67**, **104**, **139**, **150**
Krankenhäuser **160**
Krankenkassen **52**, **53**
Kriminalakten **25**
kriminalpräventive Räte **33**
Kundendaten **85**
Kündigungsschutzprozess **88**

L

Landesbauordnung **21**
Landesmeldegesetz **19**
Landesnetz **92**, **97**
Landesrechnungshof **36**

Landessystemkonzept **97**
Landesverwaltungsgesetz **23**

M

Mediendienste-Staatsvertrag (MDStV) **112**, **120**
Meldedaten **19**
Melderegister **19**
Meldewesen **30**
Modellprojekte **9**
  AN.ON (Anonymität online) **123**
  BioTrusT **125**
  Datenschutzaudit und Gütesiegel **128**
  Schul-CD **129**
  Virtuelles Datenschutzbüro **122**
Mozilla **143**

N

NDR **49**, **164**
neue Medien **108**
novelliertes LDSG **137**
Nutzerdaten **118**, **119**, **120**, **124**, **141**, **147**

O

Ordnungswidrigkeit **89**
organisierte Kriminalität **145**
Outsourcing **52**, **56**, **62**, **95**

P

P3P (Platform for Privacy Preferences) **116**, **142**
Pageview **122**
Parlament
  Datenschutzregelung für das **17**
Patienten **30**, **55**, **57**
Patientenakte **51**
Patientendaten **50**, **54**, **56**
Patientengeheimnis **8**, **50**, **52**, **55**, **57**
Personalaktendaten **68**
Personaldaten **68**
Persönlichkeitsrecht **60**
Polizei **22**, **24**, **25**, **28**, **29**, **30**, **163**, **164**, **166**
privatärztliche Verrechnungsstelle **55**
Protokollierung **12**, **111**
Provider **111**, **114**, **119**, **148**, **163**, **165**
Prüfungsmaßnahmen des Landesdaten-schutzbeauftragten
  Bezirkskriminalinspektion Kiel **31**
  Bezirkskriminalinspektion Lübeck **31**
  Entsorgung von Altakten **106**
  EURAS **31**
  Geheimschutzbeauftragte **39**
  Kieler Sophienhof **29**
  Kommunalbereich **104**
  Landesamt für Gesundheit und Arbeits-sicherheit **103**
  Landesamt für Natur- und Umweltschutz **101**
  Schulen **61**
  Stadt Neumünster **99**
Pseudonymisierung **52**
Publikationen
  des Landesbeauftragten für den Datenschutz **170**

R

Rabattsparkarte **83**, **163**
Rasterfahndung **22**, **41**
Revisionsfähigkeit **131**, **134**, **160**
Richtlinie über den Datenschutz bei elektronischer Kommunikation **147**
Rundfunk **49**, **164**

S

SCHUFA **74**, **76**, **77**, **78**, **79**, **165**
Schul-CD **129**
Schuldnerverzeichnis **80**, **165**
Schule **61**, **129**
Schulungs- und Simulationsnetz **141**
Schweigepflicht **30**, **55**, **151**
Scoring-Verfahren **75**
Sekten **163**
Sicherheitskonzept **93**, **95**, **98**
Sicherheitsüberprüfung **39**
Sicherheitsüberprüfungsgesetz **39**
Signatur
  digitale **120**
  elektronische **37**, **108**, **118**, **162**
Sommerakademie **119**
Sozialamt **44**, **46**, **47**, **164**
Sozialbereich **44**
Sozialdaten **33**, **52**, **53**, **54**, **87**, **164**
Sozialdatenschutz **47**, **48**
Sozialgeheimnis **53**
Sozialhilfe **44**
Sprachnetz **95**
Steuergeheimnis **62**
Steuerverwaltung **62**, **64**

Strafverfahren **28**, **31**
Strafverfolgung **10**, **28**, **148**
Straßenmaut **43**
Studentendaten **49**
Surfen **90**, **141**
Systemadministration **103**, **105**
Systemdatenschutz **90**

T

Technik **43**
Teledienstedatenschutzgesetz (TDDSG) **112**, **119**, **120**, **124**, **147**
Teledienstegesetz (TDG) **120**
Telekom **95**
Telekommunikation **27**, **113**, **114**, **147**
Telekommunikations-Datenschutz-verordnung (TDSV) **113**, **147**
Telekommunikationsgesetz (TKG) **113**, **114**
Telekommunikationsüberwachungs-verordnung **114**
Terrorismusbekämpfungsgesetz **40**, **42**
Test und Freigabe von EDV-Verfahren **66**, **93**

V

Verbindungsdaten **27**, **112**
Vereinsdaten **86**
Verfahren
automatisierte **99**
Verfassungsschutz **39**, **41**
Verkehr **43**
Vernichtung **106**
Veröffentlichung **34**
im Internet **81**
Verwaltungsverfahrensgesetz **110**
Videoüberwachung **29**
Virtuelles Datenschutzbüro **118**, **122**
VIS (Verlässliche IT-Systeme) – Fachtagung **118**
Vorabkontrolle **48**, **73**, **98**
Vorgangsverwaltung Polizei **26**

W

Wahlgeheimnis **20**
Werbesendungen per E-Mail **120**
Widerspruchsrecht **42**
Wirtschaft **43**, **73**

Z

zentrale Gesundheitsdatenbank **52**
Zeugnisverweigerungsrecht **30**
Zuwanderungsgesetz **42**
Zwangsversteigerungsverfahren **33**
Zweckbindung **22**, **43**, **50**, **110**
Zweitwohnungssteuer **67**, **166**