Bericht

des Landesbeauftragten für den Datenschutz

bei dem Präsidenten des Schleswig-Holsteinischen Landtages

Zweiundzwanzigster Tätigkeitsbericht
(Berichtszeitraum: 1999, Redaktionsschluß: 28.02.2000)

In der Anlage übersende ich gemäß § 23 Abs. 3 Satz 2 des Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Informationen vom 30. Oktober 1991 den zweiundzwanzigsten Tätigkeitsbericht des Landesbeauftragten für den Datenschutz bei dem Präsidenten des Schleswig-Holsteinischen Landtages.

Dr. Helmut Bäumler

Inhaltsverzeichnis

1 Situation des Datenschutzes in Schleswig-Holstein

1.1 Gesetzgeber stellt das Informationsrecht auf eine zukunftsweisende Grundlage

Mit der Verabschiedung des neuen Landesdatenschutzgesetzes (LDSG) und des Gesetzes zum freien Zugang zu Informationen hat der Landtag das Informationsrecht auf eine neue Grundlage gestellt. Schleswig-Holstein, das bei der Entwicklung der Informationsgesellschaft gerne eine Vorreiterrolle einnehmen will, hat durch diese rechtlichen Rahmenregelungen zweifellos eine richtungsweisende Position eingenommen. Bemerkenswert ist zudem, dass das neue Landesdatenschutzgesetz von allen Fraktionen mitgetragen wurde und demgemäß ohne Gegenstimme verabschiedet werden konnte.

Die Novellierung des LDSG war zwar vorrangig notwendig geworden, weil die Europäische Datenschutzrichtlinie in Landesrecht umgesetzt werden musste. Die neuen Bestimmungen gehen aber weit über die Umsetzung der Richtlinie hinaus. Sie greifen aktuelle technische Entwicklungen auf und geben gesetzliche Spielräume für neue Ansätze im Datenschutz. Aus der Fülle der Veränderungen des Datenschutzrechts sind folgende besonders hervorzuheben:

- **Förderung datenschutzfreundlicher Techniken**

Seit sich die Sommerakademie 1996 mit dem Thema “Datenschutz durch Technik” befasste, sind viele neue Ideen für einen Einsatz der Informationstechnik für einen besseren Schutz der Privatsphäre entwickelt worden. Einige davon haben Eingang in das neue Gesetz gefunden.

Die gesetzliche Verpflichtung der Behörden zur **Datenvermeidung und Datensparsamkeit** wird dazu beitragen, dass in vielen Fällen datenschutzrechtliche Risiken von vornherein vermieden werden. Alle Daten verarbeitenden Stellen müssen künftig vorrangig Produkte einsetzen, deren datenschutzgerechte Gestaltung in einem förmlichen Audit (“Produktsiegel”) festgestellt wurde. Das Audit-Verfahren wird die Landesregierung durch Verordnung regeln.

Die Begriffe **Anonymisierung und Pseudonymisierung** werden nicht nur gesetzlich definiert, die Verwendung pseudonymisierter Daten wird darüber hinaus z. B. bei der wissenschaftlichen Forschung oder bei der Datenübermittlung privilegiert. Dadurch wird ein Anreiz geschaffen, wo immer es geht, auf einen Personenbezug zu verzichten.

Die **Verschlüsselung** von Daten, mit deren Hilfe viele Risiken für die Vertraulichkeit von Informationen abgebaut werden können, wird definiert. Ihr Einsatz wird verbindlich vorgeschrieben, wenn Daten außerhalb der Dienststellen verarbeitet werden, z. B. durch Außendienstmitarbeiter.

- **Höherer Standard bezüglich der Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung**

Der bislang schon hohe Standard der schleswig-holsteinischen Datensicherheitsbestimmungen wird weiter verbessert:

Automatisierte Verfahren dürfen künftig nur eingesetzt werden, nachdem sie von der **Dienststellenleitung** förmlich freigegeben worden sind. Damit ist klargestellt, dass der Computereinsatz in der Verwaltung Chefsache und auch von der Chefebene zu verantworten ist.

Der Zugang zu Computersystemen ist zwingend davon abhängig zu machen, dass sich die betreffende Person durch ein **Passwort** o. Ä. identifiziert.

Die Arbeit von **Systemadministratoren** und anderen Personen, die zu Änderungen des Betriebssystems befugt sind, muss künftig protokolliert werden. Dies dient nicht nur dem Datenschutz, sondern es ist darüber hinaus ein wichtiger Beitrag zur Revisionssicherheit des Verwaltungshandelns.

- **Berücksichtigung der Verwaltungsmodernisierung**

Das Gesetz berücksichtigt bereits die anstehenden Veränderungen in der öffentlichen Verwaltung. Notwendige Effizienzsteigerungen werden nicht durch datenschutzrechtliche Formvorschriften blockiert:

Wenn Verwaltungen künftig Informationen nur noch **automatisiert** und nicht zusätzlich auch in Akten speichern wollen, dann finden sie im neuen LDSG die dabei zu beachtenden Vorschriften.

Die Risiken bei der Einführung von **Telearbeit** werden bei Beachtung der Verschlüsselungsregelung für die ausgelagerten personenbezogenen Daten auf ein vertretbares Maß reduziert.

Wenn Behörden Dienstleistungen über das **Internet** anbieten, so können die eventuell notwendigen datenschutzrechtlichen Einwilligungen von Bürgerinnen und Bürgern auch über das Netz erteilt werden.

Damit das für den öffentlichen Bereich erforderliche Datenschutzniveau nicht durch **Outsourcing** umgangen wird, ist das Gesetz auch für Privatfirmen im Besitz der Verwaltung anwendbar. Außerdem gelten die Bestimmungen für die Auftragsdatenverarbeitung auch für externe Serviceunternehmen.

- **Gesetzliches Fundament für den *neuen* Datenschutz**

Die Sommerakademie 1998 hatte das Thema “Der *neue* Datenschutz” diskutiert. Viele der damals entwickelten Vorstellungen für eine moderne Datenschutzkonzeption haben nunmehr ein solides gesetzliches Fundament erhalten.

Die Kontrollinstanzen für den Datenschutz im öffentlichen Bereich und in der Privatwirtschaft werden in Schleswig-Holstein zusammengelegt. Dadurch ergeben sich **Synergieeffekte** und mehr **Bürgerfreundlichkeit**.

Die Aufgaben werden künftig von einer neu gebildeten Anstalt des öffentlichen Rechts mit der Bezeichnung "**Unabhängiges Landeszentrum für Datenschutz**" wahrgenommen. Der Name ist Programm: Das Landeszentrum ist nicht in die Hierarchie der Verwaltung eingebunden und trägt damit den Anforderungen der Europäischen Datenschutzrichtlinie an die Unabhängigkeit von Datenschutzkontrollinstanzen Rechnung.

Neben die Kontrollen treten verstärkt **Service**, **Beratung** und **Prävention** in Fragen des Datenschutzes und der Datensicherheit sowie insbesondere die Beratung der Bürgerinnen und Bürgern zum besseren Selbstdatenschutz.

Das Unabhängige Landeszentrum hat ausdrücklich die Aufgabe erhalten, Fortbildungsveranstaltungen durchzuführen und damit zur Vermittlung von **Medienkompetenz** beizutragen.

Erstmals in Deutschland wird ein **Datenschutzaudit** für Verwaltungsbehörden eingeführt. Sie können ihre Datenschutzkonzeption künftig beim Unabhängigen Landeszentrum für Datenschutz zur Prüfung und Zertifizierung vorlegen.

- **Verschlankung des Datenschutzrechts**

Das neue LDSG hat an vielen Stellen zu einer einfacheren und verständlicheren Sprache zurückgefunden. Außerdem werden die Weichen in Richtung auf eine Abkehr von der weiteren Verrechtlichung und bereichsspezifischen Zersplitterung des Datenschutzes gestellt:

Die Verarbeitung bestimmter, nicht besonders sensibler Daten kann jetzt unmittelbar auf das LDSG als **Befugnisgrundlage** gestützt werden. Eine Fülle von gleich oder ähnlich lautenden Generalklauseln in den Fachgesetzen sowie in kommunalen Satzungen ist künftig überflüssig.

Für die Einrichtung von **Online-Verbindungen** ist künftig kein Gesetz bzw. keine Rechtsverordnung mehr notwendig. Die schutzwürdigen Belange der Bürgerinnen und Bürger werden bereits durch detaillierte Verfahrens- und Sicherheitsbestimmungen im LDSG selbst gewahrt.

Ohnehin **allgemein zugängliche Daten** darf auch die Verwaltung unter erleichterten Bedingungen nutzen.

Alles in allem bietet das neue LDSG gute Chancen für eine Verbesserung des Datenschutzes der Bürgerinnen und Bürger unter veränderten technischen und gesellschaftlichen Bedingungen. Der Weg zu konsequenter Datensicherheit ist ohne Alternative. Das weltweite Zittern vor dem Jahr-2000-Problem und die horrenden Summen, die zu seiner Bewältigung ausgegeben werden mussten, dürften auch den letzten Zweiflern die Augen geöffnet haben. Rechtzeitige Datenschutz- und Datensicherheitsaufwendungen, konsequente Realisierung der

Revisionsfähigkeit der Datenverarbeitung und Kontrolle sind alle Mal billiger als die Unsummen, die nachträgliche Korrekturen verschlingen. Der Weg in die Informationsgesellschaft ist ohne einen zeitgemäßen, wirksamen Datenschutz und das Grundprinzip der Transparenz demokratisch nicht zu verantworten. Das neue LDSG ist ein wichtiger Beitrag zur Erreichung dieses Ziels.

1.2 Neues Informationsfreiheitsgesetz verabschiedet

Zusammen mit dem LDSG hat der Landtag das Informationsfreiheitsgesetz für das Land Schleswig-Holstein (IFG-SH) verabschiedet. Das zeitliche Zusammentreffen unterstreicht die enge Verwandtschaft zwischen Datenschutz und Informationszugang. Beide Prinzipien haben ihre Wurzeln im Bild der **aufgeklärten Bürgergesellschaft**.

Das IFG-SH gewährt allen Bürgerinnen und Bürgern das grundsätzliche Recht des freien Zugangs zu allen Verwaltungsinformationen. Sie brauchen hierfür weder eine Begründung abzugeben noch sich auf Informationen zu beschränken, die sie selbst betreffen. Damit wird das Verhältnis zwischen Bürgern und Verwaltung auf eine neue Grundlage gestellt. Die nunmehr entstehende **Transparenz** der staatlichen Informationssammlungen ist ein Spiegelbild der stärkeren Betonung des Dienstleistungscharakters der Verwaltung.

Natürlich kann ein solcher Informationsanspruch nicht uneingeschränkt bestehen. Das IFG-SH enthält deshalb sorgfältig formulierte **Ausnahmeklauseln**. Auch die datenschutzrechtlichen Belange Dritter sind durch entsprechende Vorbehalte gesichert. Damit die Trennung personenbezogener Daten von den allgemein zugänglichen Informationen erleichtert wird, sehen sowohl das IFG-SH als auch das neue LDSG vor, dass Unterlagen möglichst von vornherein so organisiert werden, dass sie für unterschiedliche Verwendungszwecke leichter getrennt werden können.

Das neue Gesetz wird sicherlich einige Anlaufschwierigkeiten bereiten. Es sieht vor, dass sich Bürgerinnen und Bürger bei **Streitfragen** über seine Auslegung und Anwendung an das Unabhängige Landeszentrum für den Datenschutz wenden können. Außerdem hat das Landeszentrum auch in diesem Bereich seine Beratungs- und Serviceaufgaben. Auf diesem Wege soll vermieden werden, dass Auslegungsstreitfragen ausschließlich mithilfe der Gerichte geklärt werden müssen.

1.3 Schwerpunkte der Kontrolltätigkeit im abgelaufenen Jahr

Die im Berichtsjahr durchgeführten Kontrollen und Überprüfungen auf Grund von Beschwerden haben neben durchaus positiven Beispielen erneut Fälle von Schlamperei, unverantwortlichem Umgang mit der Informationstechnik und bedenklicher Gesetzesauslegung erbracht. Bei aller Akzeptanz und gestiegener Sensibilität aufseiten der Verwaltung ist der Datenschutz noch lange kein Selbstläufer. Es stellt sich immer wieder heraus, dass die Notwendigkeit eines überzeugenden und wirksamen **Datenschutzkonzeptes** entweder gar nicht

gesehen oder die Verantwortung auf andere abgeschoben wird. So entstehen unvertretbare Risiken, die die Verwaltung von der Technik abhängig machen und das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger gefährden. Kontrollen bleiben deshalb auf absehbare Zeit ein unverzichtbarer Bestandteil einer effizienten Datenschutzkonzeption.

Besonders bedenklich ist es, wenn **medizinische Daten** in komplexen Informationssystemen erfasst und verarbeitet werden, ohne dass die rechtlichen Grenzen eingehalten werden (vgl. Tz. 6.5). Umso weniger ist es hinzunehmen, wenn festgestellte Mängel nur sehr zögerlich behoben werden (vgl. Tz. 6.4). Es ist zudem erstaunlich, wie unsensibel manchmal in Kliniken mit der Intimsphäre von Patienten umgegangen wird. Die Betroffenen sind nämlich häufig gar nicht in der Lage, sich während ihres Krankenhausaufenthaltes zu wehren. Wenden sie sich später an uns, so treten bisweilen haarsträubende Zustände zutage (vgl. Tz. 4.7.5).

In den Kommunen gibt es trotz aller Fortschritte fast bei jeder Kontrolle einiges zu beanstanden. Besonders zu erwähnen sind festgestellte Mängel bei der **Fernwartung**. Der Datenzentrale war es ohne weiteres möglich, sich auf den Datenverarbeitungssystemen ihrer kommunalen Kunden zur Nachtzeit umzusehen, ohne dass diese davon etwas geahnt hätten. Es fehlten klare Vereinbarungen ebenso wie wirksame Kontrollmechanismen. Und das, obwohl wir bereits 1994 detaillierte Kriterien für sichere Fernwartungsverfahren im Amtsblatt veröffentlicht hatten.

Digitale Telekommunikationsanlagen sind mit erheblichen Sicherheitsrisiken behaftet, da ihre Komfortmerkmale sich leicht missbrauchen lassen. Die Apparate können unter bestimmten Voraussetzungen wie Abhöranlagen sogar für Raumgespräche benutzt werden. Notwendig sind dafür nur Veränderungen in der Software. Wer nun glauben würde, dass die Aktivitäten der Systemadministratoren genau registriert und regelmäßig überprüft würden, muss durch das Ergebnis unserer Kontrollen enttäuscht werden (vgl. Tz. 6.2). Zumeist sind die Strukturen moderner Telekommunikationsanlagen so komplex, dass die Behörden offenbar kapitulieren und sich auf die Liefer- und Wartungsfirmen verlassen. Die besondere Brisanz dieser Konstellation liegt darin, dass das Land Schleswig-Holstein seine Telekommunikationsinfrastruktur insgesamt privatisieren möchte, inklusive so sensibler Bereiche wie Polizei, Gesundheitswesen oder Finanzverwaltung. Aus unserer Sicht ist dies ohne umfassende Sicherheitsvorkehrungen und insbesondere ohne Vorhaltung der für die Kontrolle der Einhaltung der Bestimmungen notwendigen personellen Kompetenz nicht zu verantworten (vgl. Tz. 6.3).

Seit die Senkung der Ausgaben für Sozialhilfe parteiübergreifend als Maßstab für erfolgreiche Politik gilt, sind die **Überprüfungen von Sozialhilfeempfängern** immer rigoroser geworden. Nicht dass der Datenschutz der Prüfung der Bedürftigkeit entgegenstünde oder gar die Aufdeckung von Betrug verhindern würde, aber auch Sozialhilfeempfänger haben einen Anspruch auf Fairness und Achtung ihrer Privatsphäre. Unsere Kontrollen fördern immer wieder Verstöße gegen die Bestimmungen des Sozialgesetzbuches zu Tage, die nicht akzeptabel sind (vgl. Tz. 4.6.3, 4.6.4 und 4.6.5).

Wenn Ausländer Deutsche heiraten, geschieht dies sicher gelegentlich auch nur zu dem Zweck, eine Aufenthaltsbewilligung zu bekommen. Daraus folgt aber nicht das Recht, alle bi-nationalen Ehepaare peinlichen Überprüfungen zu unterziehen. Gerade bei der Ermittlung von "**Scheinehen**" sind klare rechtliche Vorgaben und Taktgefühl bei der Durchführung notwendig. Eine Kontrolle förderte diesbezüglich dringenden Nachbesserungsbedarf zu Tage (vgl. Tz. 4.4.2).

1.4 Service, Beratung und Prävention

Wer unsere Tätigkeitsberichte über die Jahre vergleicht, kann feststellen, dass Service, Beratung und Prävention ein **immer größeres Gewicht** erhalten. Dabei kann nur ein Bruchteil dieses Tätigkeitsfeldes in diesem Bericht erfasst werden, weil sich die meisten Beratungen auf ganz spezielle Anwendungen beziehen und sich für eine allgemeine Berichterstattung nur bedingt eignen. Das Rückgrat der allgemeinen Beratungstätigkeit ist nach wie vor das Kursangebot der DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN, für das offenbar eine ungebrochene Nachfrage vorhanden ist (vgl. Tz. 14).

Zunehmend zahlen sich die Investitionen für das **IT-Labor** aus. Die dort durchgeführten Tests tragen nicht nur zur Verbesserung von Produkten bei. Die Testinstallationen erlauben auch eine praxisgerechte Beratung der Behörden, weil deren gebräuchlichste Datenverarbeitungssysteme "nachgebaut" und durchgecheckt werden können. Last but not least fließen die Ergebnisse aus dem IT-Labor in konkrete Tipps für die Bürgerinnen und Bürger ein, z. B. wie sie sich selbst im Internet am besten schützen können (vgl. Tz. 9).

Ebenfalls der Prävention und der vorausschauenden datenschutzgerechten Gestaltung von Produkten und Verfahren dienen die **Modellprojekte** (vgl. Tz. 8). Sie bieten die Möglichkeit, gemeinsam mit Entwicklern und Herstellern die Informationstechnik so zu designen, dass die Privatsphäre der Nutzer von vornherein berücksichtigt wird.

1.5 Die neuen Herausforderungen für die Dienststelle

Die Dienststelle hat sich in den letzten Jahren im Wege einer kontinuierlichen Fortentwicklung bemüht, den Herausforderungen der Beratung der Gesetzgebung, der Kontrolle und der Serviceerbringung für Anwender und Betroffene zugleich gerecht zu werden. Im Jahr 2000 sind jetzt mehrere nachhaltige Veränderungen auf einmal zu bewältigen. Dass sie fast zur gleichen Zeit auf der Tagesordnung stehen, macht die Sache für die Mitarbeiterinnen und Mitarbeiter nicht einfacher:

- Ab 1. Juli 2000 gilt ein in weiten Teilen neues Landesdatenschutzgesetz, das völlig neue Ansprüche der Bürger und der Verwaltung mit sich bringt.
- Zum gleichen Zeitpunkt wird die Dienststelle des Landesbeauftragten für den Datenschutz umgewandelt in eine Anstalt des öffentlichen Rechts mit der Bezeichnung “Unabhängiges Landeszentrum für Datenschutz”.
- Ebenfalls zum 1. Juli 2000 geht die Zuständigkeit für die Datenschutzaufsicht im nichtöffentlichen Bereich vom Innenministerium auf das Unabhängige Landeszentrum für Datenschutz über. Es gilt, zwei über 20 Jahre nebeneinander bestehende Organisationseinheiten ohne Reibungsverluste miteinander zu verschmelzen.
- Nach In-Kraft-Treten des neuen Informationsfreiheitsgesetzes können sich Bürgerinnen und Bürger bei Streitigkeiten über das Informationszugangsrecht an das Unabhängige Landeszentrum für Datenschutz wenden. Diese neue “Schiedsrichterfunktion” bedarf einer sorgfältigen Einarbeitung in die Materie.

Es bleibt zu hoffen, dass der Landtag seiner Verpflichtung gerecht wird, hierfür die ausreichende Sach- und Personalausstattung zur Verfügung zu stellen.

2 Der Weg in die Informationsgesellschaft

2.1 CityServer – die kommerzielle Ausbeutung personenbezogener Daten

Unter der Bezeichnung CityServer baut ein Verlag aus Niedersachsen eine bundesweite Gebäudedatenbank auf. Viele Bürger aus Schleswig-Holstein sind empört darüber, dass ihre Daten zu Geld gemacht werden sollen.

Mit Kameras ausgerüstete Kleinbusse fahren durch Deutschlands Städte und erfassen mithilfe von Digitalkameras sämtliche von der Straße aus einsehbaren Objekte. Diese Daten sollen – so der Verlag – die Arbeit von Hilfsdiensten wie der Feuerwehr, der Rettungsdienste der ärztlichen Hilfe und der Polizei unterstützen. Sie sollen aber nicht nur an diese Abnehmer verkauft werden, sondern auch an jeden sonstigen Interessierten, etwa an Immobilienmakler, Finanzdienstleiter oder Adressenhändler. Kurz nach Bekanntwerden dieses Projektes wandten sich viele **Kommunen** an uns mit der Frage, ob das Vorgehen des Verlages datenschutzrechtlich in Ordnung sei. Es bestehe die Möglichkeit, die unter Geokoordinaten gespeicherten Bilder über die Straße und die Hausnummer und letztendlich mit den personenbezogenen Daten von Hauseigentümern und Bewohnern zu verknüpfen. Wir bestätigten den Anfragenden, dass das Herstellen und Verbreiten der digitalen Gebäudebilder unseres Erachtens mit dem Bundesdatenschutzgesetz nicht in Einklang zu bringen ist. Betroffenen Bürgerinnen und Bürgern empfahlen wir gemeinsam mit dem Grundeigentümerverband, der Erfassung ihrer Wohnungen und Häuser beim Verlag zu widersprechen.

> **?** ***Geokoordinaten***
>
> *Jeder Ort auf der Erde lässt sich mit geografischen Koordinaten punktgenau angeben. Frühe Koordinatensysteme z. B. von Ptolemäus um 150 v. Chr. sollten das Erstellen von Karten ermöglichen. Das bekannteste der Geokoordinatensysteme basiert auf der Breite und der Länge und wird in Grad, Minuten und Sekunden angegeben. Über diverse Internet-Angebote oder mit Empfängern des Satellitensystems GPS kann man diese Angaben unter Umständen auf den Meter genau herausfinden.*

Einige Kommunen in Schleswig-Holstein wandten sich direkt an den Verlag und protestierten gegen die Gebäudeerfassung auf ihrem Gemeindegebiet. Der **Schleswig-Holsteinische Landtag** fasste einen einstimmigen Beschluss, in dem er die Datenerfassung ohne Zustimmung der Betroffenen missbilligt, die Betroffenen zum Widerspruch ermuntert und dafür plädiert, den Schutz der Bürgerinnen und Bürger gegen unzulässige kommerzielle Datenverarbeitung zu verbessern.

Unsere Stellungnahmen und Pressemitteilungen finden Sie unter:

www.schleswig-holstein.datenschutz.de
(Rubrik: weitere Materialien/Bekanntmachungen)

Eine völlig andere Sichtweise hat der **Verlag**. Es sei objektiv falsch, dass den Geokoordinaten Adressen und damit Personen zugeordnet werden könnten. Damit befände man sich außerhalb des Datenschutzrechtes. Wir dagegen hätten durch die Beratung von Gemeinden und Betroffenen eine unerlaubte Rechtsberatung vorgenommen. Unserer Bitte, die Unmöglichkeit, einen Personenbezug herstellen zu können, durch einen Praxistest mit "echten" CityServer-Datenbeständen in unserem IT-Labor überprüfen zu lassen, wollte der Verlag allerdings nicht entsprechen.

Inzwischen liegen erste gerichtliche Entscheidungen zum CityServer vor. Dabei hat sich noch keine einheitliche **Rechtsprechung** herausgeschält. Soweit Gerichte zu Gunsten des Verlages entschieden haben, vertraten sie die Ansicht, die digitalen Gebäudebilder hätte keinen Personenbezug, deren Sammlung sei keine Datei und beeinträchtige keine Rechte der Eigentümer. Leider setzen sich diese Urteile weder mit der aktuellen datenschutzrechtlichen Diskussion noch mit den technischen Gegebenheiten auseinander. Gebäudebilder enthalten nicht ein Merkmal, sondern sind in vieler Hinsicht aussagekräftig. Die Geokoordinaten sind die Verknüpfungsmerkmale zwischen den Einzelpersonen und diesen Aussagen. Dass derartige Verknüpfungen mit im Internet verfügbarer Standardsoftware möglich sind, sollte kein Geheimnis mehr sein.

Ärgerlich ist die teilweise von Gerichten vorgenommene Bewertung **schutzwürdiger Interessen**. Während bei Prominenten sehr schnell eine – geldwerte – Persönlichkeitsbeeinträchtigung selbst bei Auftritten in der Öffentlichkeit angenommen wird, soll die kommerzielle Nutzung von Daten von Jedermann völlig unproblematisch sein. Dabei zeigt sich schon bei der Auswertung einer vom Verlag unter der Bezeichnung "Talkshow" auf den Markt gebrachten 50 DM teuren Billigversion des CityServers auf CD-ROM, welche Rückschlüsse auf Personen möglich sind. Arbeitgeber bei Bewerbungen, Banken bei der Kreditvergabe oder die Werbewirtschaft können sehr wohl aus den Bildern der Wohngegend, der Straße und der Nachbarschaft eine Einschätzung von Personen vornehmen. Wo werden hier der Wirtschaft Grenzen bei der Ausbeutung fremder Persönlichkeitsrechte gesetzt?

Unser Ziel ist es nicht, kreativen Initiativen zur Nutzung der Informationstechnik im Weg zu stehen. Erst recht liegt es uns fern, Unternehmen wirtschaftlichen Schaden zuzufügen. Wohl aber ist es unsere Aufgabe, angesichts der vielfältigen neuen technischen Möglichkeiten die damit verbundenen Gefahren für das Persönlichkeitsrecht zu benennen und im Rahmen unserer Möglichkeiten abzuwenden. Insofern hat das Problem "CityServer" und die damit beabsichtigte **Vermarktung** von **personenbezogenen Massendaten** Modellcharakter. Es dürfte nur eine Frage der Zeit sein, wann hochauflösende Daten im Internet gegen Geld heruntergeladen werden können. Soziodemografische Angaben, Finanz- oder Konsumdaten fallen in alphanumerischer oder in Bildform oft bei unverfänglichen Anlässen in der Öffentlichkeit an. Beim Verkauf dieser Daten darf nicht aus dem Blick verloren werden, dass das Verfügungsrecht hierüber im Grundsatz nicht beim Verarbeiter, sondern bei den Betroffenen liegt; die Vermarktung kann nur nach gesetzlich definierten Kriterien zugelassen werden.
Ein Großteil der rechtlichen Verunsicherung ist darauf zurückzuführen, dass das

Bundesdatenschutzgesetz für die **Bewertung hochmoderner Technologie** nur noch bedingt taugt. Satellitenüberwachung und –kommunikation, flächendeckende Videoerfassung, automatische Mustererkennung und Data-Warehouse-Verfahren sind nicht mehr mit dem Maßstab der Generation von Datenschutzgesetzen nach dem Volkszählungsurteil zu messen.

Was ist zu tun?
Der Gesetzgeber ist aufgefordert, durch klare Einbeziehung von Bilddarstellungen und sonstigen modernen Techniken eine umfassende Anwendbarkeit und Durchsetzbarkeit des Datenschutzrechtes zu Gewähr leisten.

2.2 Wie mit der Ökonomisierung des Datenschutzes umgehen?

Der CityServer ist exemplarisch für die Ökonomisierung des Datenschutzes. Nicht nur fremde Firmen, der Betroffene selbst macht sein Wissen über sich zu klingender Münze. Dieses Phänomen ist im Internet besonders offensichtlich.

Man kann fast sagen: Personenbezogene Daten über die User sind die **heimliche Währung des globalen Netzes**. Viele Web-Anbieter fordern für ihre Dienstleistungen kein oder wenig Geld, verlangen aber das Ausfüllen detaillierter Fragebögen, um ein (Persönlichkeits-)Bild von den Kundinnen und Kunden zu erhalten. Computer können für wenig Geld gemietet werden, wenn man bereit ist, über Hobbys, Einkommmensverhältnisse und Kreditkartennutzung Auskunft zu geben. Im Wirtschaftsbereich sind die Daten für die Beurteilung der finanziellen Verhältnisse (Bonität) oder der beruflichen Fähigkeiten (Arbeitsvermittlung), vor allem aber der Konsumgewohnheiten (Direktmarketing) relevant. Eine amerikanische Firma, die Videos für das Internet anbietet, hat den Betreiber einer Internet-Suchmaschine auf insgesamt vier Milliarden US-Dollar verklagt, weil er entgegen einer Vereinbarung die im Netz anfallenden Registrierungs- und Nutzerdaten nicht weitergab. Die beklagte Firma wehrt sich damit, ihre Privacy Policy (vgl. Tz. 9.3) erlaube die Datenherausgabe nicht.

Unbestreitbar ist, dass nicht irgendwelche Firmen, sondern grundsätzlich die Betroffenen die – auch ökonomische – Verfügungsbefugnis über ihre Daten haben. Die Zweckbindung von Daten verbietet es prinzipiell, die für einen speziellen Zweck, etwa die Abwicklung eines Vertragsverhältnisses, erhobenen Daten für einen anderen Zweck zu verkaufen. Der rechtliche Rückgriff auf ein “berechtigtes Interesse” der Unternehmen trägt nicht. Es gibt ein “schutzwürdiges Interesse” der Betroffenen, die Vermarktung ihrer eigenen Daten zu verhindern und zu lenken. Wie aber steht es mit der **Selbstvermarktung**? Folgt man dem Volkszählungsurteil des Bundesverfassungsgerichtes, so gehört auch diese zur informationellen Selbstbestimmung. Nun darf es aber nicht sein, dass das Persönlichkeitsrecht und die Privatheit als solche zu Markte getragen werden. Wohl aber lässt es sich nicht aufhalten, dass einzelne personenbezogene Daten vom Betroffenen selbst versilbert werden.

Damit dies nicht in Ausbeutung, in geschmackloses Auswälzen privater Dinge und letztendlich in der Verramschung des Datenschutzes auf dem freien Markt endet, ist es erforderlich, **Rahmenbedingungen für die Vermarktung** von Daten zu schaffen. Dabei ist nicht nur der Gesetzgeber gefordert. Vielmehr kommt es in erster Linie darauf an, durch bürgerfreundliche Auslegung der Gesetze, durch die Information der Betroffenen über ihre Rechte, durch die Stärkung der unabhängigen Streitschlichtungsinstanz der Datenschutzbeauftragten und durch die Festlegung von Verhaltensrichtlinien durch die Wirtschaft selbst eine ausgewogene Balance zwischen den Interessen der Bürgerinnen und Bürger einerseits und der Wirtschaft andererseits zu schaffen. Um zu vermeiden, dass unabsichtliche Datenschatten von Datenhaien skrupellos verhökert werden, sind technische Methoden der Datenvermeidung von zentraler Bedeutung. In einem engen Bereich muss zudem das Prinzip "Geld gegen Daten" völlig untersagt bleiben. Dies gilt etwa für die Vermarktung von Daten über Kinder, über genetische Anlagen oder aus dem Kernbereich der Intim- und Privatsphäre. Aber auch hier sind mit heißer Nadel gestrickte Gesetze weniger gefragt als die Nutzung des bestehenden rechtlichen Instrumentariums, vom Jugend- und Kinderschutz bis hin zum Verbot sittenwidriger Verträge.

Was ist zu tun?
Die Entwicklung der Ökonomisierung personenbezogener Daten ist aufmerksam zu verfolgen. Vorrangiges Ziel muss zunächst sein, durch Stärkung der Selbstbestimmungsfähigkeit die Marktmacht und das Selbstbewusstsein der Betroffenen zu verbessern. Erst wenn sich diese Mittel als ungenügend erweisen, ist der Gesetzgeber gefordert.

3 Datenschutz im Landtag

3.1 Datenschutzordnung nur zögerlich umgesetzt

Nach langwierigen Diskussionen hatte sich der Landtag im letzten Jahr eine Datenschutzordnung (DSO-LT) gegeben. Mit der Umsetzung hapert es.

Im letzten Tätigkeitsbericht musste schon darauf hingewiesen werden, dass eine Unsicherheit verbleibt, wie Betroffene ihre Datenschutzrechte gegenüber den Landtagsfraktionen wahrnehmen können (21. TB, Tz. 3.1). So ist z. B. das Auskunftsrecht gegenüber Fraktionen, die Verpflichtung zu technisch-organisatorischen Maßnahmen wie auch die Datenschutzkontrolle bei Fraktionen nicht ausdrücklich geregelt. Unbestreitbar ist, dass hier kein datenschutzfreier Raum bestehen darf. Wir wiesen daher die **Fraktionen** des Landtags darauf hin, dass sie wie eine nichtöffentliche Stelle nach dem Bundesdatenschutzgesetz betrachtet werden könnten. Dies hätte zur Folge, dass das Innenministerium als Kontrollbehörde zuständig sein könnte, was mit dem verfassungsrechtlichen Status der Fraktionen schwerlich zu vereinbaren wäre. Um diese Unklarheit zu beseitigen, regten wir an, durch eine freiwillige Selbstverpflichtung die DSO-LT für entsprechend anwendbar zu erklären und einen internen Verantwortlichen für den Datenschutz zu benennen.

Die Resonanz auf diese Bitte war wenig positiv: Drei Fraktionen antworteten. Und deren Credo war eindeutig: Jede Form externer Kontrolle wurde zurückgewiesen. Zu einer gewissen internen Kontrolle wollte sich nur eine Fraktion verpflichten. Angesichts dessen ist nur zu hoffen, dass die **Regelungslücke** nicht eines Tages zu Konflikten führt.

Die Situation wird nicht dadurch verbessert, dass es – trotz ausreichender Zeit – vom Landtag bislang unterlassen wurde, das nach der DSO-LT vorgeschriebene eigene **Datenschutzgremium**, in dem jede Fraktion durch ein Mitglied vertreten sein soll, zu bestellen. Eine Datenschutzkontrolle im Landtag, die dessen verfassungsrechtliche Rolle berücksichtigt, besteht damit leider bis heute nicht.

Was ist zu tun?
Die Landtagsfraktionen sollten für sich klären, wie der Datenschutz intern sichergestellt wird. Das Datenschutzgremium muss endlich benannt werden und mit seiner Arbeit beginnen.

3.2 Wieviel darf das Parlament wissen?

Die Auskunftsansprüche des Parlaments gegenüber der Regierung haben zwar Verfassungsrang, die Rechte von Bürgerinnen und Bürgern, um deren personenbezogene Daten es dabei geht, dürfen aber nicht unter den Tisch fallen. Das gilt ganz besonders, wenn es um sensible Vorgänge wie z. B. medizinische und Personaldaten geht.

Wenden sich Ministerien, Abgeordnete und Parlamentsausschüsse an uns mit der Frage, inwieweit aus Gründen des Datenschutzes dem Landtag Auskunft oder Akteneinsicht aus Verwaltungsvorgängen verweigert werden darf, handelt es sich nicht selten um heikle politische Fragen. So war es z. B. bei der Aufklärung von Todesfällen nach der Havarie des Frachters "**Oostzee**" und bei einer umstrittenen Besetzung einer **Professorenstelle**. Hier ging es um medizinische Daten, die der ärztlichen Schweigepflicht unterliegen, und um Personalaktengeheimnisse. Wir konnten die Anfragenden auf Artikel 23 der Landesverfassung, die Geschäfts-, die Datenschutz- und die Geheimschutzordnung des Landtags, das Fraktionsgesetz und schließlich auf eine Vereinbarung zwischen Landesregierung und Landtag aus dem Jahr 1992 verweisen.

Angesichts der zentralen demokratischen Funktion des Parlaments kann eine **Auskunftsverweigerung** aus Datenschutzgründen nur die Ausnahme sein. Allerdings muss eine **Abwägung** zwischen den Ansprüchen des Parlaments und dem Persönlichkeitsschutz erfolgen. In der Regel kann der Persönlichkeitsschutz durch folgende **Sicherungsmaßnahmen** hinreichend gewahrt werden:

- Soweit es auf den Personenbezug in den Akten nicht ankommt, sind Kopien der Dokumente durch Schwärzen zu anonymisieren.
- Die Akten sind durch die Landtagsverwaltung so zu verwahren, dass Unbefugte keinen Zugriff erhalten.
- Der Einblick in sensible Unterlagen sollte auf so wenige Abgeordnete wie möglich begrenzt werden.
- Das Erstellen von Kopien wird ausgeschlossen.
- Aufzeichnungen aus den Akten sollten soweit möglich keinen Personenbezug enthalten (z. B. durch die Benutzung einfacher Pseudonyme).
- Beratungen der Ausschüsse, in denen personenbezogene Daten zur Sprache kommen, sollten nichtöffentlich erfolgen.
- Öffentliche Bewertungen durch den Landtag, die Ausschüsse oder Abgeordnete sollten in einer Form erfolgen, die keine Rückschlüsse auf bestimmte Personen zulassen.

Was ist zu tun?
Vor einer Auskunftsverweigerung gegenüber dem Parlament hat die Regierung alle Möglichkeiten auszuschöpfen, um eine unangemessene Beeinträchtigung persönlicher Betroffenenbelange zu verhindern. Der Landtag sollte seine Verfahrensweisen dem gleichen Ziel ausrichten.

4 Datenschutz in der Verwaltung

4.1 Kommunalbereich

4.1.1 Überblick

Der Trend zur Umgestaltung der öffentlichen Verwaltung in flexible, kompetente und bürgernahe Anlaufstellen nach Art von **Dienstleistungsunternehmen** hat sich auch in den ländlichen Bereichen bis hin in die kleineren Kommunalverwaltungen fortgesetzt. So wird z. B. die Einrichtung "ländlicher Dienstleistungszentren" gefördert. Gaststätten, "Tante-Emma-Läden" oder auch die örtliche Bankfiliale sollen zu Dorfzentren umgewandelt werden, die nicht nur Waren des täglichen Bedarfs anbieten. Hier soll man demnächst im Internet surfen und auf elektronischem Wege Auskunftsterminals oder Ticket-Services nutzen, Reisen buchen und Fahrkarten kaufen oder auch per Bildtelefon in der Amtsverwaltung den eigenen Personalausweis verlängern lassen und den Wohnsitz ummelden können. Die Bürgerinnen und Bürger hätten wenig Verständnis, wenn sie die schöne moderne Verwaltung mit einer Minderung ihrer Datenschutzrechte bezahlen müssten. Hier gilt es, sich rechtzeitig über die datenschutzrechtlichen Anforderungen zu informieren (Tz. 4.1.3).

Immer mehr Kommunen möchten die verschiedenen **Internet-Dienste** nutzen. Das Angebot an die Bürger, mit ihrer Gemeindeverwaltung elektronisch zu kommunizieren, erscheint attraktiv und könnte zu mehr Kundenorientierung führen. Die Kommunen müssen sich aber, bevor sie "ans Netz" gehen, grundsätzlich darüber im Klaren sein, welche Angriffe aus dem Internet heraus auf die eigenen Datenbestände möglich sind und ob bzw. wie dem wirksam vorgebeugt werden kann (Tz. 4.1.4).

Wie wir im Rahmen unserer durchgeführten Prüfungen im Bereich der **Datensicherheit** in den Verwaltungen feststellen konnten, wächst bei vielen Behördenleitern das Problembewusstsein für sicherheitstechnische Fragestellungen, sodass die Einhaltung ausreichender Sicherheisstandards immer selbstverständlicher wird. Am Beispiel der Fernwartung durch externe Dienstleister zeigt sich allerdings exemplarisch, dass zugleich auch eine Entwicklung in die entgegengesetzte Richtung stattfindet. Die Distanz zwischen denjenigen, die die Datensicherheitsfragen beherrschen, und denen, die diese aus Gedankenlosigkeit oder Ignoranz übergehen, wird offensichtlich immer größer (Tz. 4.1.5).

Auf dem Gebiet der Gesetzgebung kommt der Verabschiedung der Novelle zum **Landesmeldegesetz** herausragende Bedeutung zu. Es verbessert die Rechte der Bürgerinnen und Bürger spürbar. Damit die Umsetzung der neuen Regelungen leichter fällt, haben wir ein umfangreiches Fortbildungsprogramm durchgeführt und Informationsschriften herausgegeben (Tz. 4.1.2).

4.1.2 Neues Melderecht verabschiedet

Das im Februar 2000 in Kraft getretene neue Melderecht wird spürbare Verbesserungen für den Umgang mit den in den Melderegistern gespeicherten Daten mit sich bringen. Wir haben die Bürger und die Verwaltung umfassend über die Neuerungen aufgeklärt.

Die Änderung des Landesmeldegesetzes war durch das **Melderechtsrahmengesetz** des Bundes vorgegeben. Die Entwicklung der Melderegister hin zum "Informationssystem für die unterschiedlichsten kommunalen und staatlichen Dienststellen und Behörden über verwaltungsrelevante Daten der Bürgerinnen und Bürger", so die amtliche Begründung, führte gleichwohl zu sehr kontroversen Stellungnahmen und Diskussionen.

Auch unsere Vorstellungen von einem optimalen bürgerfreundlichen Melderecht ließen sich nicht alle verwirklichen. Folgende Aspekte können aber als **datenschutzrechtliche Verbesserungen** verbucht werden: Aus der Vielzahl der Verbesserungen sind folgende hervorzuheben.

- In Zukunft sind die Betroffenen nicht nur darüber aufzuklären, was mit ihren Daten bei der Meldebehörde geschieht, sondern sie haben auch einen verbesserten Auskunftsanspruch.
- Vor der Erteilung einer Melderegisterauskunft über Bürgerinnen und Bürger hat die Meldebehörde künftig sorgfältiger zu verfahren**,** um Verwechslungen zu vermeiden.
- Ist zum Schutz besonders gefährdeter Personen eine **Auskunftssperre** im Melderegister vermerkt, verbietet diese nicht nur die Weitergabe von Namen und Anschrift bei privaten Anfragen; sie ist auch bei der Datenübermittlung an andere öffentliche Stellen zu berücksichtigen.

Wir hätten uns weitere Verbesserungen gewünscht. Statt der an vielen Stellen vorgesehenen Widerspruchslösung wäre das **Erfordernis der Einwilligung** bürgerfreundlicher gewesen.

Die umfangreichen Gesetzesänderungen waren für uns Anlass, auch im melderechtlichen Bereich den Schwerpunkt unserer Arbeit weiter auf die **Service- und Beratungsebene** zu verlagern. In Zusammenarbeit mit der Verwaltungsakademie Bordesholm haben wir für die Mitarbeiterinnen und Mitarbeiter der Meldeämter landesweit 17 Sonderkurse der DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN abgehalten, in denen die Gesetzesänderungen erläutert wurden.

Außerdem haben wir in der Reihe **"Datenschutz leicht gemacht"** ein Heft mit umfangreichen "Erläuterungen und Praxistipps zum neuen Landesmeldegesetz" herausgegeben, das bei den Meldeämtern reißenden Absatz findet.

Der Inhalt ist auch im Internet veröffentlicht unter

www.schleswig-holstein.datenschutz.de
(Rubrik: Informationen speziell für Behörden).

Parallel dazu beraten wir auch die Hersteller und Vertreiber der in den Meldeämtern eingesetzten Software bei der erforderlichen Umstellung der Programme zur elektronischen Datenverarbeitung.

Für die Bürgerinnen und Bürger haben wir gemeinsam mit dem Innenminister ein **Faltblatt "Datenschutz im Melderecht"** herausgegeben, um über die Datenverarbeitungsvorgänge in den Meldeämtern und die den Einwohnern zustehenden Rechte zu informieren. Die Faltblätter werden in großer Zahl durch die Meldebehörden abgefordert und durch Verteilung an Haushalte, Auslegung auf Stadtfesten oder Veröffentlichung in gemeindeeigenen Mitteilungsblättern weiterverbreitet.

Der *neue* Datenschutz setzt auch beim Schutz der Meldedaten vorrangig auf Dienstleistung. Folglich hat unsere Dienststelle im Bereich des Melderechts ein umfassendes Beratungs- und Serviceangebot bereitgestellt, das auf eine selbst für uns überraschend große Nachfrage gestoßen ist.

4.1.3 Tipps zur Verwaltungsmodernisierung

Die Modernisierung in der öffentlichen Verwaltung ist in aller Munde. So weit das Feld der Modernisierungsvorhaben ist, so breit gestreut sind auch die damit verbundenen datenschutzrechtlichen Fragestellungen.

Hinter dem Schlagwort **"Modernisierung der öffentlichen Verwaltung"** verbergen sich die verschiedensten Bestrebungen und Vorhaben, deren gemeinsame Triebfeder nicht nur die angespannte Haushaltslage der Kommunen ist, sondern auch die Anforderungen der Bürgerinnen und Bürger. Sie erwarten kompetente und schnelle Dienstleistungen. Die Gesetze der Marktwirtschaft erobern klassische Felder der öffentlichen Verwaltung. Diese ist gefordert, sich umfassend zu reorganisieren und sich zu einem auf hohem Standard bürgernah und wirtschaftlich arbeitenden Dienstleistungsbetrieb weiterzuentwickeln.

Die **Ziele der Modernisierung** lauten daher:

- Wirtschaftlichere Aufgabenerfüllung,
- Qualitätsteigerung bei der Aufgabenerfüllung,
- Verbesserung des Bürgerservice.

Für die "Modernisierer" muss klar sein, dass all diese Vorhaben, Reformen und Projekte ohne Berücksichtigung der datenschutzrechtlichen Belange nicht möglich sind. Die Bürgerinnen und Bürger würden sich schön bedanken, wenn sie die Verwaltungsmodernisierung mit einer Verschlechterung des Schutzes ihrer

Daten bezahlen müssten. Je eher dies erkannt wird, umso einfacher lassen sich praxisgerechte Lösungen entwickeln. Dabei stellt sich zumeist heraus, dass sich **Modernisierung und Datenschutz** keineswegs widersprechen, zumal wir selbst den Datenschutz in organisatorischer und auch technischer Hinsicht modernisieren. Es geht also nicht darum, Modernisierungsvorhaben mit überholten Vorstellungen zu blockieren, sondern neue Perspektiven und neue Lösungsansätze zu entwickeln.

Im Mittelpunkt unserer zeit- und arbeitsaufwändigen Beratungstätigkeit standen bislang folgende Projekte:

- Personalentwicklung und –management (ressortübergreifend und dezentral),
- Kosten- und Leistungsrechnung/Berichtswesen,
- Dezentralisierung/Outsourcing/Privatisierung/Organleihe,
- Bürgerbüros und Dienstleistungszentren,
- Vernetzung und Automation in der Datenverarbeitung,
- digitale Aktenführung,
- Nutzung des Internet/Verwaltung online.

Die Ergebnisse dieser Arbeit werden in eine Publikation einfließen, die allen interessierten Stellen und Personen als Einstieg in diese Thematik dienen kann. Allerdings kann eine solche Ausarbeitung keine endgültigen und allumfassenden Antworten liefern. Jedes konkrete Projekt gestaltet sich in der Umsetzung vor Ort anders und bedarf auch in Zukunft spezifischer Ideen zur Problemlösung.

Was ist zu tun?
Modernisierungsvorhaben müssen schon in der Planungsphase datenschutzgerecht konzipiert und ebenso realisiert werden.

4.1.4 Kommunen ins Internet?

Das Internet bietet eine kostengünstige Basis für die Beschaffung und Bereitstellung von Informationen. Damit wird es zunehmend auch für die Kommunalverwaltungen zu einem interessanten Präsentations- und Kommunikationsinstrument. Mit dem Anschluss eines Verwaltungsnetzes an das Internet stellen sich allerdings anspruchsvolle datenschutzrechtliche Herausforderungen.

Das Internet hat sich mittlerweile zu einem Massenmedium entwickelt. Das Spektrum der Nutzungsmöglichkeiten, das die Internet-Dienste WWW und E-Mail bieten**,** ist nahezu unbegrenzt und findet deshalb auch in den Kommunalverwaltungen zunehmend Anklang. Gerade im Rahmen von kommunalen Modernisierungsvorhaben, die sich mit effizienzsteigernden Maßnahmen in der Verwaltung, mit der Vereinfachung und Beschleunigung von Verwaltungsverfahren und dem **Ausbau des Bürgerservice** (vgl. Tz. 4.1.3)

befassen, sollen die Möglichkeiten des Internet nutzbar gemacht werden. Folgende Ideen und Nutzungsmöglichkeiten sind uns bislang in der Praxis begegnet:

- Kommunen präsentieren sich zu Werbezwecken auf einer eigenen Homepage, veröffentlichen elektronische Stadtpläne, verweisen auf kulturelle und touristische Attraktionen und Adressen und führen ein "Gästebuch".
- Auch die einzelnen Verwaltungsbereiche werden auf der Homepage umfassend präsentiert. Beschrieben werden nicht nur die verschiedenen Ämter mit ihren Zuständigkeitsbereichen und Anschriften, sondern auch einzelne **Mitarbeiterinnen und Mitarbeiter** mit ihren Namen und individuellen Erreichbarkeitsdaten, häufig sogar mit Foto.
- Dasselbe gilt für die kommunalen Ausschüsse und andere Gremien einschließlich der Daten der ehrenamtlich tätigen **Mandatsträgerinnen und -träger**.
- Die elektronische Post – **E-Mail** – dient dem schnellen und bequemen Nachrichtenaustausch zwischen den Verwaltungen und auch der Kommunikation mit Außenstehenden.

Viele Kommunalverwaltungen sitzen noch in den Startlöchern, möchten jedoch lieber heute als morgen ein "**virtuelles Rathaus**" errichten. Dabei hat sich aber bei den Vorreitern schon gezeigt, dass der Anschluss des Verwaltungsnetzes an das Internet mit seinen Diensten nicht ohne Nebenwirkungen bleibt. In diesem Bereich hat sich deshalb ein Schwerpunkt unserer Arbeit, insbesondere der beratenden Tätigkeit, gebildet (vgl. die Beiträge unter Tz. 7.1).

Sinnvoll und überlegt eingesetzt, ist das Internet durchaus als Instrument zur **Flexibilisierung** und **Ökonomisierung** der öffentlichen Verwaltung geeignet. Sobald aber über das Internet personenbezogene Daten übermittelt werden sollen, bedarf es umfangreicher Vorkehrungen, bis hinreichend sichere Lösungen präsentiert werden können. Wir geben den nachfragenden Kommunen Folgendes zu bedenken:

- Rechner, die vom Internet aus erreicht werden können, sind diversen **Angriffsmöglichkeiten** ausgesetzt, die nicht zuletzt auch die auf ihnen gespeicherten Daten gefährden. Beschränkt sich der Internet-Zugang auf einen unvernetzten Einzelplatzrechner, der nicht zu sonstigen Zwecken genutzt wird, hat dies in der Regel keine gravierenden Auswirkungen. Sobald jedoch eine Öffnung des Verwaltungsnetzes dem Internet gegenüber geschaffen wird, entsteht z. B. die Gefahr der Vireninfizierung der internen IT-Systeme bei Dateiübertragungen, durch die das gesamte Verwaltungsnetz lahm gelegt werden kann. Schlimmstenfalls kann es zum Ausspähen oder zur Manipulation der dienstlichen Daten kommen – spektakuläre Internet-Angriffe, über die die Fachpresse regelmäßig berichtet. Wie man sich durch technische Maßnahmen gegen diese Angriffe schützen kann, wird unter Tz. 7.1.1 dargestellt.

- Elektronische Nachrichten können auf dem Weg über das Internet mitgelesen, verändert oder verfälscht werden. Eine vertrauliche Kommunikation ist also im Internet ohne eine **zuverlässige Verschlüsselung** nicht gegeben. Es liegt an der Verwaltung, entsprechende Verschlüsselungsangebote zur Verfügung zu stellen. Die Bürger nehmen das Angebot, unverschlüsselt mit "ihrer Verwaltung" per E-Mail zu kommunizieren, leider häufig an, ohne die damit verbundenen Risiken zu erkennen.
- Die Veröffentlichung dienstlicher Erreichbarkeitsdaten von **Mitarbeiterinnen** und **Mitarbeitern** ist grundsätzlich unbedenklich, solange sie sich auf konventionelle Behördenverzeichnisse oder kommunale Mitteilungsblätter beschränkt. Sie erhält aber eine völlig neue Dimension, wenn sie im Internet erfolgt, da die Daten dann plötzlich weltweit zugänglich und verfügbar sind. Die Daten sind elektronisch auswertbar und können mit anderen elektronischen Datenbeständen zusammengeführt werden. Wegen der damit verbundenen Gefahren dürfen die "Funktionsträger-Daten" nicht gegen den Willen der Betroffenen im Internet veröffentlicht werden (vgl. Tz. 7.1.3).

Was ist zu tun?
Kommunen sollten das Internet nur mit geeigneten Sicherheitsvorkehrungen nutzen. Ein Anschluss an das Internet darf die Sicherheit des gesamten Verwaltungssystems nicht gefährden.

4.1.5 Datensicherheit in der Kommunalverwaltung

Die Diskrepanz zwischen guten oder gar perfekten Sicherheitskonzepten und dem Schlendrian in anderen Verwaltungen wird immer größer. Die Datenzentrale trägt ihren Teil dazu bei. Das Thema Datensicherheit in der Kommunalverwaltung kommt auch bei Mitgliedern von Vertretungskörperschaften an. Sie merken, dass auch im häuslichen Bereich die Vertraulichkeit kommunaler Unterlagen gewahrt werden muss.
Warum immer wieder diese Ausreißer?

Der sich in den letzten Jahren abzeichnende Trend festigt sich: Die Zahl der Kommunalverwaltungen, die ihre automatisierte Datenverarbeitung "im Griff" haben, wird größer. War vor einigen Jahren unsere Meldung, dass wir erstmals bei einer Prüfung **keine Sicherheitsmängel** feststellen konnten, noch Schlagzeilen wert, so kann man heute sagen, dass derartige Ergebnisse schon fast zur **Normalität** gehören. Manchmal sind unsere Prüfer von der Selbstverständlichkeit überrascht, mit der ihnen schlüssige Sicherheitskonzepte und vollständige Verfahrensdokumentationen vorgelegt werden. In einem Fall waren diese Unterlagen so aussagefähig und die realisierten Sicherheitsmaßnahmen qualitativ so gut, dass die Prüfung dieser – übrigens durchschnittlich großen – Amtsverwaltung praktisch nach einer Stunde beendet war. Danach entwickelte sich "nur noch" eine intensive Fachdiskussion darüber, wie die gefundenen Lösungen noch optimiert werden könnten und welche sicherheitstechnischen Konsequenzen sich aus den sich abzeichnenden technischen Innovationen ergeben. Bemerkenswert ist, dass in diesen Fällen keine der handelnden Personen

über eine Mehrarbeit zur Erlangung des Sicherheitsstandards geklagt hat. Man betrachtete die Aktivitäten auch nicht als eine datenschutzrechtliche Pflichtübung. Vielmehr waren sowohl die betreffenden Behördenleiter als auch die Administratoren davon überzeugt, dass der personelle Aufwand für den laufenden Betrieb eines EDV-Systems umso geringer ist, je sorgfältiger das Organisations-, das Konfigurations- und das Sicherheitskonzept erarbeitet und in die Praxis umgesetzt worden ist.

Vor diesem Hintergrund ist es schwer verständlich, dass es noch immer so viele "Ausreißer" bezüglich der Sicherheit und Ordnungsmäßigkeit der automatisierten Datenverarbeitung im kommunalen Bereich gibt. In den letzten beiden Tätigkeitsberichten (vgl. 20. TB, Tz. 6.6.1; 21. TB, Tz. 4.1.2) haben wir ein **"Sündenregister"** von über dreißig gravierenden Missständen aufgeführt. Die meisten der dargestellten Probleme und Sicherheitslücken haben wir auch in diesem Jahr wieder vorgefunden und beanstandet (schlecht ausgebildete Administratoren, ungesicherte Systemzugänge, Mängel bei der Passwortvergabe, fehlende Abschottung der Administrationsebene der Systeme, undurchschaubare Dokumentationen und Protokollierungen, unzulängliche Zugriffsbeschränkungen auf Datenbestände usw.). Es wäre ermüdend, gleiche Sachverhalte alljährlich erneut in aller Ausführlichkeit darzustellen. Stattdessen soll deshalb anhand eines Einzelfalles deutlich gemacht werden, welche Gedankenlosigkeit auch heute noch besteht.

Spätestens seitdem wir im Jahr 1994 in einer Veröffentlichung im Amtsblatt Kriterien für die Gestaltung von **Fernwartungsverfahren** beschrieben und erläutert haben, ist unter Fachleuten unbestritten, dass auf diesem Gebiet ohne schriftliche Verträge "gar nichts" geht. Immerhin ist der Zugriff eines externen Dienstleisters auf das Betriebssystem eines Verwaltungscomputers sicherheitstechnisch eine äußerst brisante Aktion, der Externe wird nur eingeschaltet, weil er seine Leistungen billiger erbringt als es das eigene Personal könnte. Dieser wirtschaftliche Vorteil darf nicht durch Sicherheitsrisiken erkauft werden. Das Landesdatenschutzgesetz ist insofern eindeutig. Es fordert schriftliche Verträge, klare Weisungen und die Überwachung der Arbeiten des externen Dienstleisters. Außerdem verpflichtet es öffentliche Stellen, "personenbezogene Daten als Auftragnehmer nur im Rahmen der Weisungen der Auftraggebenden zu verarbeiten".

Für einige Kommunen und die **Datenzentrale** waren diese gesetzlichen Regelungen offenbar nicht existent. Bei Prüfungen entdeckten wir nicht nur, dass die Fernwartung ohne jede schriftliche Vereinbarung erfolgte. Die Datenzentrale tummelte sich sogar **zur Nachtzeit** auf den Systemen, ohne dass die betreffenden Verwaltungen etwas davon wussten. Die Mitarbeiter der Kommunen hatten bis zu unserer Prüfung noch gar nicht entdeckt, dass die Datenzentrale **Benutzerkonten** eingerichtet hatte, über die sie eine so genannte Softwareinventarisierung betrieb. Dies kam erst heraus, als ein Administrator diese Konten auf unser Anraten hin kurzerhand deaktivierte. Daraufhin beschwerte sich die Datenzentrale, dass sie die Fernwartung in Teilbereichen nicht mehr durchführen konnte.

Das Verfahren der Softwareinventarisierung mag durchaus sinnvoll sein, um

Ergänzungslieferungen mit dem bereits vorhandenen Bestand zu synchronisieren. Es ist aber nicht akzeptabel, dass ein DZ-Kunde von diesem Verfahren allenfalls dadurch erfährt, dass er seinen Einzelverbindungsnachweis in der Telefonrechnung daraufhin überprüft, wann die Datenzentrale auf sein Rechnersystem zugegriffen hat. Auf Grund dieser Vorkommnisse haben wir die Fernwartungsaktivitäten der Datenzentrale bei anderen Kunden näher durchleuchtet und **weitere Nachlässigkeiten** entdeckt. Unter Fachleuten ist unstreitig, dass Folgendes hätte gewährleistet sein müssen:

- Jeder Fernwartungsvorgang muss von der auftraggebenden Stelle einzeln freigeschaltet werden. Hierauf sollte nicht nur der Auftraggeber, sondern auch das Fernwartungsunternehmen bestehen, um die missbräuchliche Nutzung dieser Zugänge von vornherein zu verhindern.
- Alle Benutzer der gewarteten Systeme müssen **programmgesteuert** gezwungen werden, das bei der Eröffnung des Benutzerkontos systemseitig generierte Passwort bei der ersten regulären Anmeldung durch ein **individuelles Passwort** zu ersetzen. Auch hierfür sollte das Wartungsunternehmen sorgen, um seine Mitarbeiter nicht dem Verdacht auszusetzen, sie könnten unter der Kennung von legalen Nutzern Datenverarbeitungsprozesse ablaufen lassen, denn sie bräuchten nur die ihnen bekannten Systempasswörter zu verwenden.
- Vor der Auslieferung von vorkonfigurierten Systemen (Slogan: “Hardware und Software aus einer Hand”) müssen alle nicht benötigten **Benutzerkonten**, die im Zuge der Installation des Betriebssystem und der sonstigen Software eingerichtet worden sind, wieder deaktiviert werden. Salopp formuliert: Jeder ordentliche Handwerker verlässt die Baustelle besenrein.

All dies war nicht geschehen, was wir gegenüber den Kommunen und auch der Datenzentrale nachdrücklich beanstandet haben.

Der Datenzentrale waren die von uns aufgedeckten Versäumnisse offenbar peinlich. Jedenfalls hat sie umgehend reagiert und ihre Verfahrensweise geändert. Die Schwachstellen wurden beseitigt und die Kunden informiert. Wenn allerdings aus derartigen Fehlentscheidungen im Rahmen der “Qualitätssicherung” keine Konsequenzen gezogen werden, sind Wiederholungsfälle nicht ausgeschlossen. Diese Erwartung bzw. Befürchtung äußerten uns gegenüber auch die betroffenen Kunden.

Sicherheitsmaßnahmen im häuslichen Bereich der Mitglieder von Vertretungskörperschaften

Immer wieder wird in Gesprächen mit Bürgermeistern und leitenden Verwaltungsbeamten die Frage erörtert, welche Sicherheitsmaßnahmen die Mitglieder von Gemeinde- und Stadtvertretungen, von Ratsversammlungen und Kreistagen im **häuslichen Bereich** bezüglich der Beratungsunterlagen, Protokolle und des sonstigen Schriftgutes zu treffen haben, um, so wird formuliert, “den Anforderungen des Datenschutzes gerecht zu werden”. Der vor Jahren ausführlich und teilweise kontrovers diskutierte Aspekt, dass auch Mitglieder von Vertretungskörperschaften die Regeln des Landesdatenschutzgesetzes zu beachten

haben (vgl. 18. TB, Tz. 4.1.5; 20. TB, Tz. 4.1.3), ist inzwischen unstreitig. In Anbetracht der Datenmengen, die ihnen von den Verwaltungen wöchentlich ins Haus geschickt werden, und der Tatsache, dass die meisten dieser Unterlagen auch personenbezogene Daten enthalten, werden die Ehrenamtler offensichtlich zunehmend vorsichtig. Sie fragen nach einer Richtschnur, deren Einhaltung sie nicht dem Vorwurf der groben Fahrlässigkeit aussetzt, falls doch einmal etwas passiert.

Zieht man ein Fazit aus diesen Gesprächen, so kann man die **nachfolgenden Kriterien** als **allgemein gültig** bezeichnen:

- Unterlagen, deren Inhalt Gegenstand von Beratungen in öffentlichen Sitzungen ist

  Diese müssen im häuslichen Bereich nicht unbedingt unter Verschluss gelagert werden, gehören aber nach Gebrauch auch nicht in den allgemein zugänglichen Müllcontainer. Sobald sie nicht mehr benötigt werden, sollten sie der Verwaltung zur geordneten Entsorgung zurückgegeben werden.

- Unterlagen, deren Inhalt Gegenstand von Beratungen in nichtöffentlichen Sitzungen ist

  Sie gehören im häuslichen Bereich grundsätzlich unter Verschluss, also wie in der Verwaltung in einen abgeschlossenen Schrank, wenn sie nicht bearbeitet werden. Der Schlüssel sollte nicht stecken bleiben, sondern sich am Schlüsselbund befinden, den Reserveschlüssel sollte man bei einer Vertrauensperson deponieren. Der Umfang der Unterlagen sollte auf ein Mindestmaß reduziert werden. “Alte” Beschlussvorlagen und Protokolle können auch in der Verwaltung eingesehen werden. Die Entsorgung nicht mehr benötigter Unterlagen muss grundsätzlich durch die Verwaltung erfolgen.

- Dienstliche PC im häuslichen Bereich

  Wollen die Verwaltung und die (einzelnen) Mitglieder der Vertretungskörperschaft über IT-Systeme kommunizieren, empfiehlt sich die Nutzung normaler Telefonleitungen. Die Systeme bei den Ehrenamtlern sollten von der Verwaltung zur Verfügung gestellt und konfiguriert werden. Wie bei anderen Telearbeitsplätzen auch, trägt die Verwaltung dann die Verantwortung für die Wirksamkeit der Sicherheitsmaßnahmen. Die Benutzer sollten daher auf eine genaue Beschreibung der Sicherheitsregeln bestehen und sie genau beachten, damit man ihnen keinen Vorwurf machen kann, wenn doch einmal etwas schief geht. Die dienstlichen Geräte sollten nicht zu privaten Zwecken und nicht durch Dritte genutzt werden.

- Benutzung des eigenen PC für “dienstliche” Zwecke

  Bei der Benutzung von eigenen PC zur Unterstützung der Arbeit als Mitglied einer Vertretungskörperschaft liegt die Verantwortung für die Datensicherheit ausschließlich beim Systeminhaber. Die Kommune sollte daher eine direkte Vernetzung mit dem Verwaltungsrechner ablehnen. Es mag allenfalls ein Datenträgeraustausch über Disketten vereinbart werden. Sollen Informationen aus nichtöffentlichen Sitzungen gespeichert werden, scheidet in der Regel eine Mitbenutzung des PC durch Dritte (auch durch Familienmitglieder) aus.

Hinreichend wirksame Zugriffsbeschränkungen lassen sich durch die Installation einer entsprechenden Sicherheitssoftware realisieren. Vertrauliche Daten (insbesondere auch Textdokumente) sollten in jedem Fall verschlüsselt gespeichert werden. Welche Verschlüsselungsprogramme sinnvoll eingesetzt werden können, sollte man mit der Verwaltung absprechen.

- Kommunikation zwischen der Verwaltung und den Vertretern über das Internet

  Auf die Kommunikation zwischen der Verwaltung und den Mitgliedern der Vertretungskörperschaft über das Internet sollte einstweilen noch verzichtet werden. Dies bedingt nämlich den Einsatz von "Firewalls" (vgl. 21. TB, Tz. 7.1.2) und Verschlüsselungstechnik, z. B. "Virtuellen privaten Netzen" (VPN). Nach unseren Erfahrungen sind diese Hard- und Softwarekomponenten noch nicht so "kommunaltauglich", dass sie problemlos von den Administratoren in der Verwaltung und den normalen Benutzern im häuslichen Bereich beherrscht werden können (vgl. auch Tz. 4.1.4 und 7.1.1).

Was ist zu tun?
Die Kommunen sollten sich von der Datenzentrale oder anderen Softwarehäusern schriftlich bestätigen lassen, dass in den Verträgen die Funktionalitäten der gelieferten Produkte vollständig beschrieben sind. Die Mitglieder der Vertretungskörperschaften sollten sich durch die zuständigen Verwaltungsmitarbeiter, z. B. durch die behördlichen Datenschutzbeauftragten, beraten lassen, wenn es um die Datensicherheit im häuslichen Bereich geht. Technische Lösungen müssen von der Verwaltung und von den Ehrenamtlern gemeinsam entwickelt und verantwortet werden.

4.2 Polizeibereich

4.2.1 Überblick

Nennenswerte gesetzgeberische Aktivitäten zu polizeilichen Befugnissen hat es im letzten Jahr in Schleswig-Holstein und auf Bundesebene erstmals seit vielen Jahren nicht gegeben. Von der 1998 neu eingeführten Befugnis zum Großen Lauschangriff wird nach unseren Informationen in Schleswig-Holstein bislang zurückhaltend Gebrauch gemacht. Die Zahlen aus dem ersten Berichtszeitraum über stattgefundene Lauschangriffe sind von Justiz und Polizei wie von der Verfassung gefordert an den Landtag übermittelt worden. Das entsprechende **Landesgesetz zur Umsetzung** der Vorgaben des **Art. 13 Grundgesetz** wurde vom Landtag verabschiedet, ohne jedoch das Verfahren der Behandlung der Berichte im Detail zu regeln. Diese Berichte sind anonym. Wir treten daher nachdrücklich dafür ein, dass sie in dem zuständigen Ausschuss, den der Landtag zu bestimmen hat, öffentlich beraten werden und nur bei Gründen für eine Gefährdung der Aufgaben der Strafverfolgung im Einzelfall eine nichtöffentliche Verfahrensweise gewählt wird.

Das im letzten Jahr verabschiedete Gesetz für den Aufbau einer präventiven **DNA-Datei (**DNA-Identitätsfeststellungsgesetz**)** war im Berichtsjahr Grundlage vor allem für die Erfassung des Genprofils von Gefangenen in schleswig-holsteinischen Justizvollzugsanstalten. Der Aufbau der Datei schreitet voran. Dabei umgehen allerdings einige Bundesländer den Richtervorbehalt für die Untersuchung und Speicherung des Identifizierungsmusters vielfach dadurch, dass vom Betroffenen eine "Einwilligung" in diese Verarbeitung seiner Gendaten erlangt wird. Überlegungen, diese datenschutzrechtlich und strafprozessual unhaltbare Praxis auch in Schleswig-Holstein einzuführen, sind zurückzuweisen.

Neben Grundsatzfragen wie der polizeilichen **Bilddatenerhebung bei Demonstrationen** hat uns im letzten Jahr vor allem die Beratung der Polizei bei der Einführung von **neuen Informationssystemen** wie INPOL-neu, ViCLAS und EURAS und bei der Nutzung neuer technischer Möglichkeiten wie der Internet-Öffentlichkeitsfahndung beschäftigt. Deutlich wird hierbei, dass auch die polizeiliche automatisierte Datenverarbeitung einem enormen Wandel unterliegt, der gegenüber den bisherigen Systemen unvergleichliche Recherche- und Verknüpfungsmöglichkeiten bringt. Die Frage der Verhältnismäßigkeit des Eingriffs in die Persönlichkeitsrechte von Beschuldigten, Opfern, aber auch dritten Personen stellt sich dabei in ganz neuen Dimensionen.

4.2.2 INPOL-neu

Das Projekt INPOL-neu wird die gesamte polizeiliche Datenverarbeitungslandschaft verändern. Die Planungen zur Anpassung der Landessysteme befinden sich zwar noch in einem frühen Stadium. Auf Ebene des Bundesprojektes gibt es in wesentlichen Punkten datenschutzrechtlichen Nachbesserungsbedarf.

Die datenschutzrechtliche Begleitung des Großprojekts der Polizei INPOL-neu war ein Schwerpunkt der Beratung (vgl. 21. TB, Tz. 4.2.2). Obwohl das neue System mit dem Probebetrieb ab **Mitte 2000** beginnen soll und die Aufnahme des vollständigen Parallelbetriebes zu INPOL-aktuell als weitere Zwischenphase der Realisierung ab Februar 2001 geplant ist, sind noch längst nicht alle datenschutzrechtlich bedeutsamen Weichen gestellt. Insbesondere befinden sich die Überlegungen zu den entscheidenden Einzelfestlegungen noch in einem frühen Stadium: Das Sicherheitskonzept liegt erst als interner Entwurf vor, die Vorarbeiten für die Umsetzung von INPOL-neu in den Landessystemen sind noch nicht abgeschlossen.

In den bundesweiten **Kriminalaktennachweisen (KAN)** sollen gegenüber dem jetzigen Verfahren bei Vorliegen einer INPOL-relevanten Straftat auch solche Taten eines Beschuldigten gespeichert werden, die für sich genommen keine länderübergreifende oder erhebliche Bedeutung aufweisen. Diese Aufnahme der **kriminellen Historie** einer Person läuft dem eindeutigen Wortlaut des Bundeskriminalamtsgesetzes (BKAG) zuwider, wonach jede in INPOL eingestellte Straftat die so genannte Erheblichkeitsschwelle überschritten haben muss. Dennoch hat der Lenkungsausschuss INPOL-neu diese Erweiterung beschlossen.

Einige Länder – allerdings nicht Schleswig-Holstein – bemühen sich im Zusammenhang mit der Neustrukturierung der gesamten polizeilichen Datenhaltung aus Anlass von INPOL-neu um eine Auslagerung der polizeilichen **Landesdatenhaltung** an das Bundeskriminalamt (BKA) im Wege der **Auftragsdatenverarbeitung**. Welche Datenbestände genau hiervon betroffen sein sollen, ist bislang noch nicht hinreichend klar. Dass bestimmte Daten zwar aus rechtlichen Gründen nicht im polizeilichen Informationsverbund erscheinen dürfen, jedoch "ausgerechnet" beim BKA im Auftrag verarbeitet werden sollen, läuft nach Auffassung der Datenschutzbeauftragten den föderalen Vorgaben für die polizeiliche Datenverarbeitung zuwider. Auch das BKAG erlaubt nur eine Unterstützung der Datenverarbeitung der Länder durch das BKA im Einzelfall, nicht jedoch eine Verschiebung der wesentlichen Teile der Datenverarbeitung auf das BKA.

Eine **Vollprotokollierung** der Zugriffe auf die INPOL-Datenbestände soll nach den Vorstellungen des Bundesinnenministeriums nicht erfolgen. Die schleswig-holsteinische Polizei sollte an der bestehenden Vollprotokollierung aller Zugriffe über einen Zeitraum von sechs Monaten auch für das neue System festhalten, zumal mittelfristig ein direkter INPOL-Zugriff aller polizeilichen Sachbearbeiter über das Vorgangsbearbeitungssystem COMPAS bestehen wird.

Das **Berechtigungskonzept**, welches die Struktur des künftigen "integrierten Datenpools" INPOL-neu festschreibt, ist außerordentlich grob angelegt. Sämtliche **Fallinformationen**, soweit sie nicht aus polizeifachlichen Gründen besonders abgeschottet sind (Organisierte Kriminalität, Staatsschutz, Geldwäsche etc.), befinden sich nun in einem einheitlichen Berechtigungsbereich zusammen mit der sog. Grundinformation über Kriminalakten, erkennungsdienstliche Informationen, Haftdaten u. a. mehr. Falldaten, die auch Nichtbeschuldigte betreffen oder auf ungeklärten Verdachtsfällen beruhen können, dürfen den polizeilichen Sachbearbeitern nur so weit zur Verfügung gestellt werden, wie es deren fachlicher Aufgaben- und Zuständigkeitsbereich erfordert. Damit es nicht zu einer uferlosen Datenübermittlung kommt, die nicht mehr vom Erforderlichkeitsgrundsatz gedeckt ist, müssen die ausführenden Berechtigungskonzepte der Länder die technischen Differenzierungsmöglichkeiten nutzen und dürfen sich nicht einfach am technisch möglichen Maximalprofil orientieren.

Das Grundkonzept eines redundanzfreien einheitlichen Datenpools lässt sich mit dem BKAG nur vereinbaren, wenn für die vielen logischen Dateien jeweils eigene Zweckbestimmungen, Zugriffsregelungen, Prüf- und Löschfristen in **Errichtungsanordnungen** festgelegt werden. Dieser für die datenschutzrechtliche Bewertung der Neukonzeption entscheidende Schritt wurde jedoch zeitlich sehr weit nach hinten geschoben. Es liegen lediglich erste Vorüberlegungen zur Struktur und zu den Inhalten der logischen Dateien vor, die noch stark überarbeitungsbedürftig sind. Auch die sensible **DNA-Datei** und wahrscheinlich **ViCLAS** (vgl. Tz. 4.2.5) sollen Teil von INPOL-neu werden. Dies setzt eine funktionierende **Abschottung** gegen Zugriffe von Personen außerhalb des für beide Dateien sehr eng definierten Nutzerkreises voraus.

INPOL-neu soll die bisherigen polizeilichen **Meldedienste** vollständig integrieren. Die vorgegebene pauschale Gewichtung von Deliktskategorien in "Muß"-, "Regel"- und "Kann"-Fälle muss mit den Anforderungen der Erheblichkeit oder Überregionalität der einzelnen INPOL-relevanten Straftat gemäß BKAG übereinstimmen und Ausnahmen nach Einschätzung des Sachbearbeiters im Einzelfall zulassen. Insbesondere darf es **keinen automatisierten Datenabfluss** an den Verbund geben, auf den der Datenbesitzer keinen Einfluss mehr hat.

Dem Polizeilichen Führungssystem (PFI) soll eine anonymisierte, vom operativen Teil von INPOL getrennte Datenbank zugrundeliegen, um Lagebilder, Statistiken und andere strukturelle, kriminalgeografische Führungsinformationen auch zu nicht INPOL-relevanten Delikten erstellen zu können. Dieser Neuansatz für die polizeiliche Datenverarbeitung ist nur dann datenschutzrechtlich unproblematisch, wenn die Datensätze nicht mehr personenbeziehbar sind. Da den Fallinformationen jedoch eine Personenkennziffer zugeordnet wird, um Doppelzählungen von Mehrfachtätern zu verhindern, bedarf es zusätzlicher technisch-organisatorischer Maßnahmen, um dieses Zuordnungsmerkmal geheim zu halten.

Was ist zu tun?
Der Innenminister darf den künftigen Errichtungsanordnungen für INPOL-neu nur zustimmen, wenn die datenschutzrechtlichen Anforderungen eingehalten sind. Bei der Umsetzung von INPOL-neu müssen die Spielräume für Landessysteme genutzt werden.

4.2.3 Videoüberwachung von Versammlungen

Die Polizei darf Demonstrationen nicht flächendeckend per Video überwachen, sondern lediglich bei vorliegender Gefahr die Störer und die einer Straftat Verdächtigen, allenfalls noch unmittelbar daneben stehende Versammlungsteilnehmer filmen. Gemeinsam mit den Experten der Polizei haben wir im vergangenen Jahr die datenschutzrechtlichen Anforderungen an Bilderhebungen bei Versammlungen und Veranstaltungen für die polizeiliche Praxis aufgearbeitet.

Die Polizei ist inzwischen technisch so gut ausgestattet, dass sie bei immer mehr Veranstaltungen wie Fußballspielen und bei Versammlungen die Geschehnisse per Video festhalten kann. Durch die ständige **Präsenz von Polizeikameras** entsteht jedoch bei vielen Demonstranten Unsicherheit, ob die Polizei tatsächlich alles filmen und dauerhaft speichern darf. Wir informierten uns bei mehreren Polizeidienststellen und durch Teilnahme an einem konkreten Einsatz über die praktische Handhabung der in diesem Zusammenhang zu beachtenden Datenschutzbestimmungen. Eine Arbeitsgruppe der polizeiinternen Datenschutzbeauftragten erstellte einen **Handlungsleitfaden** für die Durchführung von Bilddatenerhebungen bei Versammlungen und anderen Veranstaltungen.

In der Diskussion wurde Einigkeit in folgenden Punkten erzielt: Bilddatenerhebungen von Demonstrationsteilnehmern stellen nach der Rechtsprechung des Bundesverfassungsgerichts einen Eingriff in das für ein demokratisches Gemeinwesen besonders bedeutsame Versammlungsgrundrecht aus Art. 8 Grundgesetz dar. Weil die Furcht vor einer Registrierung durch die Polizei dazu führen könnte, dass Bürger auf eine Teilnahme an Versammlungen von vorneherein verzichten, müssen die gesetzlichen Anforderungen an Bildaufnahmen von Demonstrationen der hohen Wertigkeit dieses Grundrechts gerecht werden. Vor diesem Hintergrund verlangt das Versammlungsgesetz (VersG), dass **tatsächliche Anhaltspunkte** dafür bestehen müssen, dass von einer Person **erhebliche Gefahren** für die öffentliche Sicherheit und Ordnung ausgehen. Nur dann darf sie gefilmt werden. Dies gilt nicht für unvermeidbar mit ins Bild geratene Nichtstörer. Grundsätzlich sind die Aufnahmen nach Beendigung der Versammlung unverzüglich zu vernichten, wenn sie nicht zur Strafverfolgung oder Abwehr künftiger erheblicher Gefahren bei Demonstrationen gebraucht werden.

Im Wortlaut:
§ 12 a Versammlungsgesetz (VersG)

(1) Die Polizei darf Bild- und Tonaufnahmen von Teilnehmern bei oder in Zusammenhang mit öffentlichen Versammlungen nur anfertigen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass von ihnen erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen. Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.
(2) Die Unterlagen sind nach Beendigung der öffentlichen Versammlung oder zeitlich und sachlich damit unmittelbar in Zusammenhang stehender Ereignisse unverzüglich zu vernichten, soweit sie nicht benötigt werden
1. für die Verfolgung von Straftaten von Teilnehmern oder
2. im Einzelfall zur Gefahrenabwehr, weil die betroffene Person verdächtigt ist, Straftaten bei oder im Zusammenhang mit der öffentlichen Versammlung vorbereitet oder begangen zu haben, und deshalb zu besorgen ist, dass von ihr erhebliche Gefahren für künftige öffentliche Versammlungen oder Aufzüge ausgehen.
Unterlagen, die aus den in Satz 1 Nr. 2 aufgeführten Gründen nicht vernichtet wurden, sind in jedem Fall spätestens nach Ablauf von drei Jahren seit ihrer Entstehung zu vernichten, es sei denn, sie würden inzwischen zu dem in Satz 1 Nr. 1 aufgeführten Zweck benötigt.
(3) Die Befugnisse zur Erhebung personenbezogener Informationen nach Maßgabe der Strafprozessordnung und des Gesetzes über Ordnungswidrigkeiten bleiben unberührt.

Praktisch bedeutet dies, dass eine filmische **Dokumentation des gesamten Versammlungs- und Einsatzgeschehens** durch Polizeikräfte nicht zulässig ist, wenn diese Voraussetzungen nicht vorliegen. Es dürfen also z. B. nicht der Gesamtverlauf oder friedliche Abschnitte einer Demonstration nur deshalb festgehalten werden, um etwa das Einsatzkonzept der Polizei oder die allgemeine Situation und Entwicklung des Aufzuges zu belegen. Derartige Informationsbedürfnisse, denen sich einsatzleitende Dienststellen in der Praxis häufig ausgesetzt sehen, finden keine Stütze im Versammlungs- oder im

Strafprozessrecht. **Friedlichen Demonstranten** dürfen nicht gezielt erfasst werden.

Beim Einsatz von Bildaufzeichnungsgeräten zur Gefahrenabwehr muss die polizeiliche **Gefahrenprognose**, die vor dem Einsatz zur Planung und Erstellung des Einsatzbefehls erstellt wurde, im realen Geschehen laufend daraufhin überprüft werden, ob zum Zeitpunkt der Bildaufzeichnungen tatsächliche Anhaltspunkte für erhebliche Gefahren im Sinne des Versammlungsgesetzes vorliegen.

Nach Beendigung der Versammlung müssen die gefertigten **Aufzeichnungen vernichtet** werden mit Ausnahme solcher Sequenzen, die für die Verfolgung von Straftaten benötigt werden oder wegen der Gefahr einer Wiederholung von Straftaten bei künftigen Versammlungen für maximal drei weitere Jahre aufbewahrt werden dürfen. Die Aufzeichungen auf Grundlage der Strafprozessordnung werden zum Ermittlungsvorgang gegeben und unterliegen den diesbezüglichen Aufbewahrungsbestimmungen.

Die Polizei möchte Videomaterial von Demonstrationen auch für den Unterricht in der **Aus- und Fortbildung** von Polizeibeamten verwenden, um diese mit realitätsgetreuem Material auf schwierige Einsätze im Versammlungsgeschehen vorzubereiten. Obwohl das Versammlungsgesetz insoweit keine ausdrückliche Ausnahme vom Grundsatz der unverzüglichen Vernichtung des Bildmaterials vorsieht, ist den Gesetzgebungsmaterialien immerhin zu entnehmen, dass die Aus- und Fortbildungsbedürfnisse der Polizei auch in diesem Bereich nicht gänzlich unberücksichtigt bleiben sollten. Der Schutz des Art. 8 Grundgesetz verlangt jedoch eine strenge Erforderlichkeitsprüfung für eine derartige zweckdurchbrechende Nutzung. Deshalb sind die Aufnahmen grundsätzlich durch Balken oder Flimmerflecken im Gesichtsbereich erkennbarer Demonstranten zu anonymisieren. Schwierigkeiten ergeben sich jedoch bei Gruppenaufnahmen, deren filmtechnische Bearbeitung auf diese Weise nicht geleistet werden könnte bzw. die gesamte Szene für Schulungszwecke unbrauchbar machen würde.

Insgesamt müssen die Anfertigung, der Verbleib und die Vernichtung von Videos über Versammlungen ausreichend **dokumentiert** sein. Das Innenministerium beabsichtigt, die nachgeordneten Polizeibehörden über diese Anforderungen zu unterrichten.

Was ist zu tun?
Das Innenministerium sollte sicherstellen, dass die gesetzlichen Regelungen bei der Anfertigung von Videoaufzeichnungen durch nachgeordnete Polizeibehörden beachtet werden.

4.2.4 Erinnerungsfotos im Polizeimassengewahrsam

Nimmt die Polizei im Zusammenhang mit Großveranstaltungen wie Demonstrationen oder Fußballspielen Personen zur Gefahrenabwehr in Polizeigewahrsam, so darf sie nur dann von ihnen Polaroidaufnahmen

fertigen, wenn die Abwicklung des Gewahrsams auf Grund der hohen Anzahl der Personen und der Anforderungen des Polizeieinsatzes anders nicht möglich wäre. Nach Beendigung des Gewahrsams dürfen nur die Bilder von Personen zur Strafverfolgung weitergegeben werden, gegen die ein Anfangsverdacht vorliegt.

Zwei junge Demonstrantinnen, die im Verlauf einer sog. "Großlage" mehrerer, teilweise gegeneinander gerichteter Versammlungen von der Polizei gemeinsam mit mehreren hundert anderen Personen in Polizeimassengewahrsam genommen worden waren, wandten sich an uns. Bei Einlieferung in den Gewahrsam hatte die Polizei von ihnen und sämtlichen anderen Betroffenen **Polaroidfotos** gefertigt und diese nach Beendigung des Gewahrsams an die Polizeidienststelle abgegeben, welche wegen mehrerer Straftaten in Zusammenhang mit der "Großlage" ermittelte. Dort wurden die Fotos u.a. mit Videomaterial von den Versammlungen abgeglichen. Nachdem geklärt werden konnte, dass gegen die beiden Petentinnen keine Verdachtsmomente vorlagen, wurden deren Fotos vernichtet. Darüber, ob sie zu Recht erhoben worden waren, konnte zunächst keine Einigkeit erzielt werden.

Die **Polizei** argumentiert wie folgt: Die Bilddatenerhebung zur Abwicklung des Massengewahrsams stellte ein standardisiertes Verfahren dar, um Einsatzkräfte möglichst schnell wieder verfügbar zu machen und dennoch die erforderliche Zuordnung der Betroffenen sowie eine rasche und **zweifelsfreie Identifizierung** innerhalb des Gewahrsams bis hin zur Entlassung zu Gewähr leisten. Anhand des Fotos mit Namen des Betroffenen könnten die Beamten rasch und zuverlässig bestimmen, wer für einen Transport, die Abnahme bzw. Aushändigung mitgebrachter Sachen oder Kontaktaufnahmen von Angehörigen und Rechtsanwälten und schließlich für die Entlassung aus dem Gewahrsam anzusprechen sei, und dies für ihre Dokumentation vermerken. Wenn es zu einer großen Anzahl von Fest- bzw. Ingewahrsamnahmen komme, würde es vielfach zu lange dauern, die Betroffenen jeweils anhand ihrer ggf. mitgeführten Ausweispapiere zu identifizieren. Fotos würden bei Einlieferung in den Gewahrsam teilweise auch vom Betroffenen gemeinsam mit dem einliefernden Polizeibeamten eines sog. Festnahmetrupps gefertigt, damit für eine spätere Beweisführung in Gerichtsverfahren festgehalten werde, wer als Zeuge infrage komme. Wenn der Polizeieinsatz eine sofortige Rückkehr des Beamten an den Ort weiterer Festnahmen erfordere, solle ihm auf diese Weise ein zeitlich nicht vertretbares Ausfüllen von Formularen erspart werden.

Die **Rechtslage** stellt sich aus unserer Sicht wie folgt dar: Wenn, wie im Ausgangsfall, ein strafrechtlicher Anfangsverdacht nicht gegenüber allen in Gewahrsam Genommenen besteht, kann die Aufnahme der Polaroidfotos nicht auf Befugnisse zur Identifizierung und Beweisführung aus der Strafprozessordnung gestützt werden. Nach Landespolizeirecht ist eine Lichtbilderhebung in einer solchen Situation als "verkürzte" erkennungsdienstliche Maßnahme nur zulässig, um die Identität der Betroffenen zur Gefahrenabwehr im Einzelfall festzustellen, wenn eine Identitätsfeststellung auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist. Häufig führen Versammlungsteilnehmer oder andere in Gewahrsam zu nehmende Personen jedoch identifizierende Ausweispapiere bei

sich. Dann ist eine **Lichtbildanfertigung** nur schwer begründbar, da die erstellten Bilder auch Aussagen über die Teilnahme der Betroffenen an der vorangehenden Versammlung zulassen. Sie ist als anerkanntermaßen **letzte Möglichkeit** einer sicheren Identifizierung allerdings vertretbar, wenn die Situation auf Grund der Anzahl der nach Lage der Dinge Betroffenen für die Polizei ohne Bildaufnahmen nicht zu bewältigen wäre.

Nach Beendigung des Gewahrsams bzw. Entlassung einzelner Personen aus dem Gewahrsam sollten die Bilder grundsätzlich entweder dem **Betroffenen ausgehändigt** oder gesondert zu Dokumentationszwecken befristet aufbewahrt werden, um nachweisen zu können, dass die Person im Gewahrsam war und welche Maßnahmen dort getroffen wurden. Eine zweckdurchbrechende Nutzung der Bilder insbesondere in Form eines Abgleichs mit Videomaterial über die Versammlung zum Zwecke der Strafverfolgung kommt nur bei einem bestehenden Anfangsverdacht als Voraussetzung für Maßnahmen nach der Strafprozessordnung in Betracht.

Was ist zu tun?
Der Innenminister sollte seine Erlasse an die polizeirechtlichen Vorgaben anpassen. Die polizeilichen Einsatzleiter müssen sensibel mit der Möglichkeit einer Ablichtung von Gewahrsamspersonen umgehen und in jedem Falle prüfen, ob die Verfahrensweise angemessen ist.

4.2.5 "ViCLAS" – Fahndungsmethode nach amerikanischem Vorbild

Schleswig-Holstein plant, sich an einer neuartigen polizeilichen Analysedatei zur Aufklärung schwerer Straftaten zu beteiligten. Die entsprechende Errichtungsanordnung muss aber vor allem im Hinblick auf den Schutz von Opfern datenschutzgerecht gestaltet werden.

Im Frühjahr 2000 wollen Bundeskriminalamt (BKA) sowie einige Landeskriminalämter die in Kanada entwickelte Software "**ViCLAS**" (Violent Crime Linkage Analysis System = Analysesystem zur Serienzusammenführung von Gewaltverbrechen) als Verbunddatei zum Einsatz bringen. Dieses System wird schon in den EU-Staaten Großbritannien, Belgien, den Niederlanden und Österreich eingesetzt. Durch **Fallanalysen** werden alle objektiven Spuren und Erkenntnisse zu einer bestimmten Tat zusammengestellt und mit anderen Taten abgeglichen. Anhand der dadurch gewonnenen Täterprofile verspricht sich die Polizei eine schnellere und gezielte Aufklärung von Straftaten und das Erkennen von **Serientätern**. Darüber hinaus sollen mit diesem Verfahren auch Gefährdungsanalysen, Gefährlichkeitseinstufungen von Tätern sowie weitere Analysen möglich sein.

Anhand eines umfangreichen Fragebogens werden im Rahmen von ViCLAS nicht nur täterspezifische Informationen erhoben, sondern auch Daten zur **Opferpersönlichkeit**, zum vordeliktischen **Opferverhalten** sowie andere Informationen, die sehr weit in die Persönlichkeitssphäre, ja bis in den intimsten Bereich dieser und anderer Personen hineinreichen. Die Daten sollen in ein

Analyse- und Datenbanksystem beim BKA eingespeichert werden, das mittelfristig als Verbunddatei betrieben werden soll.

Das ViCLAS-Datenbanksystem hat eine völlig neue Qualität polizeilicher Datenverarbeitung. Aus datenschutzrechtlicher Sicht ist dabei Folgendes zu berücksichtigen:

- Da über **Opfer** sehr weitgehende und unter Umständen intime Informationen eingestellt werden sollen und damit Rückschlüsse auf ihre persönlichen Verhaltens- und Lebensgewohnheiten möglich sind, muss grundsätzlich eine Speicherung **ohne die Personalien** erfolgen.
- Es dürfen nur **Straftaten** von **erheblicher** und **überregionaler Bedeutung** erfasst werden.
- Der **Umfang** der einzustellenden **Daten** sollte sich nach der Erforderlichkeit im Einzelfall richten.
- Die vorgesehenen **Fristen** zur Prüfung und **Löschung** der Daten sollten deutlich unter den bisher vorgesehenen 10 Jahren liegen.
- Der Zugriff auf diese sensiblen Informationen sollte auf wenige, speziell geschulte Mitarbeiter beschränkt werden. Eine Vollprotokollierung der Zugriffe ist notwendig.

Was ist zu tun?
Der Innenminister sollte sich in Anbetracht der hohen Sensibilität von Informationen innerhalb von ViCLAS für die Umsetzung der datenschutzrechtlichen Forderungen einsetzen.

4.2.6 Angekündigte Unangekündigte Kontrollen (AUK) im Polizeibereich

Auch in diesem Jahr haben wir einige Polizeidienststellen im Rahmen der AUK aufgesucht. In den geprüften Dienststellen der Polizeidirektionen West und Nord ist ein insgesamt positiv zu bewertendes Datenschutzbewusstsein vorhanden. Jedoch ergaben sich Mängel beim PC-Einsatz.

Festgestellte Detailmängel in der konventionellen Datenverarbeitung konnten von den betreffenden Dienststellen zumeist umgehend behoben werden. Der Umgang mit der eingesetzten EDV gibt jedoch immer wieder Anlass zu Beanstandungen, insbesondere dann, wenn die Dienststellen noch nicht an COMPAS angeschlossen sind. Zur Erleichterung des Arbeitsalltags wird in den Dienststellen vielfach ein **Einzel-PC** beschafft oder ein ausgedienter Privat-PC mitgebracht. Diese Geräte sollen lediglich als Schreibmaschinenersatz genutzt werden. In mühevoller Arbeit werden die polizeilichen Vordrucke in die elektronische Version gebracht. Der Fantasie sind offenbar keine Grenzen gesetzt, so werden beispielsweise auch das Führen von Stundennachweisen, Urlaubs-/Abwesenheitslisten, verschiedenen Dienst- und Tätigkeitsnachweisen mithilfe der PC automatisiert.

Die Regelungen des Innenministeriums zum Umgang mit

Datenverarbeitungsanlagen werden allzu oft nicht beachtet. Zu beanstanden waren folgende Mängel:

- fehlende Test- und Freigabeverfahren nach der Datenschutzverordnung,
- mangelhafte Dokumentation der eingesetzten Verfahren,
- unzureichende Authentifizierung durch ein individuelles Passwort,
- keine eindeutige Vergabe von Zugriffs- und Nutzungsberechtigungen,
- unterbliebene Aufnahme der Datenverarbeitungsanlagen in ein Geräteverzeichnis,
- unterlassene Beteiligung des behördlichen Datenschutzbeauftragten bereits bei der Planung des Einsatzes einer Datenverarbeitungsanlagen,
- fehlende Berücksichtigung der Richtlinien für die Nutzung privater Datenverarbeitungsanlagen in Diensträumen.

Was ist zu tun?
Die Polizeidirektionen als Daten verarbeitende Stellen sollten künftig unter Mitwirkung der behördlichen Datenschutzbeauftragten die Einhaltung der vom Innenministerium erlassenen Regelungen beim Umgang mit PC genauer kontrollieren.

4.2.7 Freiwillige DNA-Analysen?

Das Gesetz verlangt für die Durchführung von DNA-Analysen und deren präventive Speicherung eine richterliche Anordnung. Manche Polizei- und Justizbehörden meinen, es genüge, wenn der Betroffene eine formularmäßige Einwilligungserklärung unterschrieben hat. In Schleswig-Holstein wird bislang für die präventive Nutzung des "genetischen Fingerabdrucks" nicht mit Einwilligungen gearbeitet. Hierbei muss es aus rechtlicher Sicht auch bleiben.

Nach der Verabschiedung des DNA-Identitätsfeststellungsgesetzes im vergangenen Jahr (vgl. 21. TB, Tz. 4.2.4) ist die **DNA-Datei** beim Bundeskriminalamt (BKA) aufgebaut worden. Auch aus Schleswig-Holstein wurden Datensätze eingegeben; die ersten hiesigen Erfolge mit der Datei bei der Aufklärung erheblicher Straftaten konnten ebenfalls schon verzeichnet werden.

> **?** ***DNA***
>
> *Die DNA (Desoxyribonukleinsäure) ist ein Molekül in jeder Körperzelle, das den gesamten genetischen Bauplan des Menschen enthält. Der sog. codierende Teil der DNA enthält die Erbinformationen. Anhand des nicht-codierenden Teils kann mit äußerst hoher Wahrscheinlichkeit die Identität einer Person, z. B. durch Abgleich mit einer Tatortspur, festgestellt werden.*

Die Verfahrensweise bis zur Speicherung in der Datei ist dank eines Erlasses des Justiz- und des Innenministeriums bislang klar und gesetzeskonform:

Die Entnahme von Körperzellen (z. B. von Gefangenen einer Justizvollzugsanstalt) ist – wie bei Blutproben – auf Grundlage einer Einwilligung des Betroffenen zulässig; für die anschließende molekulargenetische Untersuchung zur Erstellung des DNA-Profils und für die Einspeisung in die Datenbank des BKA, auf die im Land nur das Landeskriminalamt unmittelbaren Zugriff hat, ist eine **vorherige richterliche Anordnung** einzuholen. Dies gilt ausdrücklich für die präventive Speicherung eines im Verlauf eines Strafverfahrens zu Beweiszwecken erstellten DNA-Analyseergebnisses, denn das Gesetz sieht zusätzliche materielle Kriterien der erheblichen Schwere der Tat und der Wiederholungsgefahr vor, die eine richterliche Prüfung durchlaufen müssen.

In der Praxis haben Richter bereits verschiedentlich Anträge der Ermittlungsbehörden auf präventive Speicherungen abgelehnt. Der Richtervorbehalt ist also keine bloße Formalie, sondern eine entscheidende Verfahrenssicherung für die Rechte des Betroffenen.

Das **Innenministerium** teilte uns jedoch zwischenzeitlich mit, dass sich die schleswig-holsteinische Polizei den z. B. in Bayern beschrittenen Weg für die Zukunft offen halten wolle, präventive DNA-Analysen und deren dauerhafte Speicherung in der Datei mit **bloßer "Einwilligung"** des Betroffenen vorzunehmen. Worauf sich dieser Wunsch nach einer Umgehung der richterlichen Prüfung gründet, wird dabei nicht deutlich. Auch im Verfahren der Zustimmung zu einer neugefassten Errichtungsanordnung für die DNA-Datei hat sich Schleswig-Holstein zusammen mit Bayern für die Aufnahme einer ausdrücklichen Bestimmung eingesetzt, nach der Speicherungen unter bestimmten Voraussetzungen auf der Grundlage einer Einwilligung vorgenommen werden dürfen.

Vereinzelte Gerichtsurteile und Stimmen in der Literatur meinen, die "freiwilligen" DNA-Analysen und –Speicherungen seien zulässig, weil dann kein Rechtseingriff vorliege. Die durch andere Gerichte vertretene gegenteilige Auffassung weist zutreffend darauf

Im Wortlaut: § 81 g StPO

(1) Zum Zweck der Identitätsfeststellung in künftigen Strafverfahren dürfen dem Beschuldigten, der einer Straftat von erheblicher Bedeutung, insbesondere eines Verbrechens, eines Vergehens gegen die sexuelle Selbstbestimmung, einer gefährlichen Körperverletzung, eines Diebstahls in besonders schwerem Fall oder einer Erpressung verdächtig ist, Körperzellen entnommen und zur Feststellung des DNA-Identifizierungsmusters molekulargenetisch untersucht werden, wenn wegen der Art oder Ausführung der Tat, der Persönlichkeit des Beschuldigten oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass gegen ihn künftig erneut Strafverfahren wegen einer der vorgenannten Straftaten zu führen sind.
(2) Die entnommenen Körperzellen dürfen nur für die in Abs. 1 genannten molekulargenetische Untersuchung verwendet werden; sie sind unverzüglich zu vernichten, sobald sie hierfür nicht mehr erforderlich sind. Bei der Untersuchung dürfen andere Feststellungen als diejenigen, die zur Ermittlung des DNA-Identifizierungsmusters erforderlich sind, nicht getroffen werden; hierauf gerichtete Untersuchungen sind unzulässig.
(3) § 81 a Abs. 2 und § 81 f. gelten entsprechend. (Richtervorbehalt)

hin, dass vielfach eine **faktische Zwangssituation** für die Betroffenen besteht, nicht durch eine Weigerung, das Einwilligungsformular zu unterschreiben, negativ aufzufallen, insbesondere im Strafvollzug. Außerdem ist es für den Betroffenen in der Regel nicht zu überblicken, welche Folgen die Speicherung in der Datei für ihn haben kann, z. B. eine Übermittlung an dritte Behörden oder einen Abgleich mit dem Bestand an DNA-Spuren unmittelbar bei Einstellung des Profils in die Datei, wodurch eine Zuordnung zu noch nicht aufgeklärten Straftaten versucht wird. Es ist realitätsfremd anzunehmen, dass eine Belehrung des Betroffenen dies alles abdecken kann. Anders als im Strafverfahren, wo er sich durch eine DNA-Analyse auch entlasten kann, bringt eine präventive Speicherung für den Betroffenen keinerlei Vorteile, die als Motiv für seine Einwilligung dienen könnten. Aber auch die richterliche Prüfung der **materiellen Voraussetzungen** einer präventiven DNA-Analyse, nämlich eine erhebliche Straftat und die Wiederholungsgefahr, kann nicht durch eine Einwilligung ersetzt werden. Weder der Betroffene selbst noch die Polizei oder die Staatsanwaltschaft sind nach dem Gesetz entscheidungsbefugt.

Schließlich ist zu bedenken, dass Zwangsmaßnahmen nach Strafprozessrecht generell nicht einfach auf eine Einwilligung gestützt werden können, nur weil Verfahrensvoraussetzungen nicht vorliegen oder ein **Anordnungsvorbehalt** als **lästig** angesehen wird. Die freiwillige Herausgabe von Gegenständen etwa ist ausdrücklich gesetzlich genannt und kann jederzeit widerrufen werden. Was wäre jedoch die Folge des Widerrufs einer Einwilligung in die Speicherung des DNA-Profils? Die Vorstöße einiger Polizeien, leider auch der schleswig-holsteinischen, in Richtung “freiwilliger” DNA-Analysen stellen daher einen sachlich wie rechtlich nicht zu begründenden Bruch mit der rechtsstaatlichen Verfahrenssicherung des Richtervorbehalts dar, gegen den sich auch die Konferenz der Datenschutzbeauftragten einhellig ausgesprochen hat.

Was ist zu tun?
Der Innen- und der Justizminister sollten bei der bisherigen gesetzeskonformen Verfahrensweise bleiben und eine richterliche Prüfung für DNA-Analysen und deren Speicherung in jedem Einzelfall beibehalten.

4.2.8 Öffentlichkeitsfahndung im Internet

Die Fahndung nach mutmaßlichen Straftätern per Internet kann – insbesondere bei Fällen mit Auslandsbezug – sinnvoll sein. Sie birgt aber gegenüber anderen Medien aus technischen Gründen besondere Risiken für die Authentizität und Rückholbarkeit des Fahndungsaufrufs. Deshalb sollte sie nur gegen Verbrecher eingesetzt werden.

Zur Frage, ob eine Öffentlichkeitsfahndung der Polizei im Internet aus rechtlichen und technischen Gründen vertretbar ist, besteht unter den Länderpolizeien und Datenschutzbeauftragten ein breites Meinungsspektrum, das sich auch in einer stark **divergierenden Fahndungspraxis** der Landeskriminalämter widerspiegelt. Während etwa Sachsen-Anhalt eine Öffentlichkeitsfahndung nach Personen im

Internet – mit Ausnahme der Verbreitung von Phantombildern – wegen fehlender gesetzgeberischer Vorgaben gänzlich ausschließt, macht die bayerische Polizei in sehr weitem Umfang, bis in Bereiche der mittleren Kriminalität hinein, vom Internet zu Fahndungszwecken Gebrauch. Wie von der Konferenz der Datenschutzbeauftragten bereits 1996 kritisiert wurde, enthält das geltende Recht bislang keine hinreichend spezifische Rechtsgrundlage für Öffentlichkeitsfahndungen.

Es handelt sich beim Internet um einen sehr großen, räumlich nicht eingeschränkten **Verbreitungsradius** für Fahndungsinformationen. Durch die dauerhafte Abrufbarkeit wird die Einwirkung auf die Persönlichkeitssphäre des Betroffenen im Vergleich zu Presse- und Fernsehpublikationen gesteigert. Außerdem kann eine Rücknahme von Fahndungsmaßnahmen bei Wegfall des Fahndungsgrundes – z. B. weil jemand irrtümlich verdächtigt wurde – auf Grund der technischen Gegebenheiten des Internet nicht vollständig umgesetzt werden. Fahndungsaufrufe und Bildinformationen können an jede beliebige andere Stelle im Internet kopiert werden, ohne dass die Polizei überhaupt in der Lage wäre, die Tatsache der Erstellung einer Kopie festzustellen und sämtliche vorhandenen Kopien im Netz aufzufinden. Nach dem bisherigen Stand der Technik ist es auch nicht möglich, die Kopierbarkeit von Informationen im Internet einzuschränken. Somit müssen dort eingestellte Informationen derzeit generell als **nicht rückholbar** angesehen werden mit der Konsequenz, dass die Einhaltung von Löschungsverpflichtungen z. B. für den Fall, dass der Tatverdacht gegen die ausgeschriebene Person entfällt, aber auch nach ihrer Ergreifung, letztlich nicht gewährleistet werden kann.

Selbst bei Anwendung der derzeit verfügbaren Verfahren zur Datensicherheit und zum Datenschutz kommt auf Grund der verbleibenden, spezifischen Risiken einer Veröffentlichung personenbezogener Daten im Internet eine Nutzung dieses Mediums zu Fahndungszwecken – mit Ausnahme der Sachfahndung ohne Personenbezug – lediglich zur Verfolgung herausragender Straftaten wie Verbrechen oder zur Vollstreckung entsprechender Freiheitsstrafen in Betracht. Zusätzlich sollte eine **Internet-Fahndung** stets **subsidiär** gegenüber anderen Fahndungsmaßnahmen sein, die den Betroffenen weniger beeinträchtigen, z. B. regional begrenzten Aufrufe, falls der vermutete Aufenthaltsort des Gesuchten näher konkretisiert werden kann. Die Dringlichkeit des Tatverdachts, die Schwere des Tatvorwurfs und die vom Gesuchten ausgehende Gefahr sind in jedem Falle mit seinem Persönlichkeitsrecht abzuwägen.

Die schleswig-hosteinische Polizei ist mittlerweile mit einer eigenen Homepage im Internet vertreten. Die wenigen dort aufgeführten Personenfahndungen betreffen herausragende Taten wie Bankraub und Mord sowie einen entflohenen, verurteilten Sexualstraftäter. Eine verbindliche Regelung, unter welchen Voraussetzungen eine **Internet-Personenfahndung** zulässig ist, fehlt zwar bislang auf Landesebene. Die Praxis des Landeskriminalamtes entspricht bislang allerdings unseren Vorschlägen.

Was ist zu tun?
Die bisherige Praxis in Schleswig-Holstein, Internet-Fahndungen nur für

besondere, schwerste Taten einzusetzen, sollte beibehalten und durch Justiz- und Innenminister verbindlich gemacht werden. Der Bundesgesetzgeber sollte eine internetspezifische Regelung über Öffentlichkeitsfahndungen in der Strafprozessordnung verankern.

4.2.9 Personenverwechslung in einem Bußgeldverfahren und ihre fatalen Folgen

Wegen unzureichender Prüfung der Personalien durch die Polizei wurde eine falsche Person mit den Folgen eines nicht bezahlten Bußgeldes bis hin zum Versuch einer Gehaltspfändung belastet.

Da staunte die Betroffene nicht schlecht, als sie von ihrem Arbeitgeber auf eine gegen sie gerichtete **Pfändungs- und Überweisungsverfügung** angesprochen wurde. Dies war der Gipfel einer Reihe von unerklärlichen Vorgängen. So wurde ihr u. a. durch einen Mobilfunkbetreiber die Anschaffung eines Mobiltelefons verweigert. Des Weiteren wurde sie von den Stadtwerken wegen angeblich nicht bezahlter Rechnungen behelligt. Ausgangspunkt für die Gehaltspfändung beim Arbeitgeber war eine Ordnungswidrigkeit im Straßenverkehr, die, wie sich später herausstellte, aber von einer anderen, namensgleichen Person begangen worden war. Anhand des Geburtsdatums hätten die beteiligten Behörden die unterschiedliche Identität beider Personen eigentlich sofort feststellen müssen.

Da die Post an die verantwortliche Person im Bußgeldverfahren als unzustellbar zurückkam und auch sonst keine Klärungsmöglichkeit bestand, ersuchte die zuständige Kreisbußgeldstelle die Polizei um Ermittlung des Aufenthaltsortes. Durch Befragung der auch der Polizei online zur Verfügung stehenden Meldedaten wurde eine **namensgleiche Person** innerhalb des gleichen Wohnortes ausfindig gemacht, wobei dem ermittelnden Beamten unverständlicherweise das unterschiedliche Geburtsdatum nicht auffiel. Diese Person wurde bei einer Überprüfung an der Wohnadresse nicht angetroffen, sodass der Beamte es bei dem Abgleich des Vor- sowie Zunamens anhand des Briefkastens bewenden ließ. Damit nahm die Irrtumskette mit erheblichen Folgen für die zu Unrecht Betroffene ihren Lauf. Der peinliche Irrtum wurde von polizeilicher Seite eingeräumt. Sie setzte sich mit der Betroffenen in Verbindung und entschuldigte sich für die entstandenen Unannehmlichkeiten.

Was ist zu tun?
Die Polizei sollte bei Personenfeststellungen äußerst sorgfältig vorgehen.

4.3 Justizverwaltung

4.3.1 Automationsvorhaben bei der Justiz

Das elektronische Grundbuch und andere ehrgeizige Projekte bei der Automatisierung der Justiz kommen nur schleppend voran. Am Datenschutz liegt es nicht.

Das Land Schleswig-Holstein (21. TB, Tz. 5.1) will zusammen mit Mecklenburg-Vorpommern und inzwischen auch Brandenburg das **elektronische Grundbuch** einführen. Erfreulich ist, dass die Frage, wie der Grundbuchbeamte elektronisch unterschreiben soll, mittlerweile auch von den beteiligten Justizverwaltungen im Sinne der von uns von Anfang an vorgeschlagenen sicheren Lösung beantwortet wurde. Wir hatten gefordert, dass die im elektronischen Grundbuch vorgesehene **"elektronische Unterschrift"** im Wege einer digitalen Signatur erfolgen muss. Dabei ist den einzelnen eintragungsberechtigten Grundbuchbeamten jeweils ein eigenes Schlüsselpaar zur Eintragung zuzuordnen, welches auf einer nicht auslesbaren Chipkarte gespeichert wird. Mittlerweile sind alle Beteiligten auf diese Verfahrensweise eingeschwenkt.

Die Automatisierung der Datenverarbeitung der Staatsanwaltschaften und der Gerichte hat deutlich zugenommen. Namentlich in den Gerichten, in denen die Staatsanwaltschaft im selben Gebäude sitzt und die Automatisierung mit MEGA bzw. MESTA bereits vollzogen ist, tauchte der Wunsch auf, die **Verfahrensdaten automatisiert** von der Staatsanwaltschaft an die Gerichte zu **übergeben**. Grundsätzlich können Daten, die in Papierform in herkömmlichen Akten von der Staatsanwaltschaft an das Gericht weitergegeben werden dürfen, auch auf elektronischem Wege übermittelt werden. Es ist bei automatisierten Verfahren allerdings darauf zu achten, dass die Anforderungen der Datenschutzverordnung (Dokumentation, Test, Freigabe der Verfahren) eingehalten werden. Bei der Abklärung der Details zwischen den beteiligten Justizbehörden, dem Justizministerium und uns stellte sich heraus, dass keine datenschutzrechtlichen, sondern **technische Probleme** bestehen. Zwar kann das bei Staatsanwaltschaften eingesetzte Verfahren MESTA die entsprechenden Daten in einer Exportfunktion zur Verfügung stellen. Jedoch ist das bei den Gerichten eingesetzte, schon vor längerer Zeit konzipierte Verfahren MEGA nicht in der Lage, derartige Daten aufzunehmen.

Bis zur Behebung dieser Defizite wurde angedacht, wenigstens die Schriftstücke, die bisher von der Staatsanwaltschaft vorbereitet und den Gerichten in Papierform vorgelegt werden, in elektronischer Form zu übermitteln. Dies sind z. B. Strafbefehle, die von den Gerichten nur abgezeichnet werden, oder bestimmte strafprozessuale Anträge (z. B. Antrag auf Haftbefehl oder auf Überwachung der Telekommunikation), die vom Gericht in der Regel inhaltlich nicht verändert, sondern lediglich bestätigt werden. Auch dagegen ist datenschutzrechtlich nichts einzuwenden. Die technisch mögliche Übermittlung derartiger Schriftstücke in elektronischer Form per **E-Mail** stößt momentan allerdings auf sicherheitstechnische Hürden. Es muss gewährleistet werden, dass Unbefugte nicht Kenntnis von den Daten nehmen können und dass sie nicht an unzuständige

Mitarbeiter gelangen. Zudem verbietet zurzeit eine Dienstvereinbarung über den Einsatz der IT-Systeme bei der Justiz die Übermittlung von E-Mails mit personenbezogenen Daten. An diesem Verbot muss nicht festgehalten werden, wenn sichergestellt wird, dass die genannten organisatorischen Maßgaben beachtet und die E-Mails zumindest in offenen Netzen verschlüsselt übersandt werden.

Was ist zu tun?
Sollen Daten zwischen den Justizbehörden auf elektronischem Wege ausgetauscht werden, so ist vor allem auf ein geordnetes Verfahren und die sichere Verschlüsselung in offenen Netzen zu achten.

4.3.2 Kurzer Draht zwischen Bewährungshelfern und Polizei?

Bewährungshelfer unterliegen gegenüber Dritten – also auch gegenüber der Polizei – einer beruflichen Schweigepflicht. Nur bei akuter Gefahr für wesentliche Rechtsgüter dürfen sie Informationen über ihre Probanden unmittelbar an die Polizei weitergeben. Gleichzeitig muss das Gericht informiert und die Datenübermittlung dokumentiert werden.

Ein Bewährungshelfer, der vor allem mit verurteilten Sexualtätern arbeitet, ersuchte uns um Beratung, ob es datenschutzrechtlich zulässig sei, dass er die Personalien, Adresse und weitere Daten von Probanden, die er nach seiner Erfahrung weiterhin für gefährlich halte, **ohne Einschaltung des Richters** unmittelbar an dessen örtliche Polizeidienststelle weitergibt. Er halte diese von ihm bereits praktizierte Vorgehensweise insbesondere dann für unerlässlich, wenn

- ein Proband aus einem anderen Bundesland zugezogen ist und die Polizei die neue Adresse möglicherweise nicht kennt,
- nach Einschätzung des Bewährungshelfers eine generelle Gefahr erneuter Straftaten des Probanden auch ohne konkrete Anhaltspunkte vorliegt,
- der Proband im Gespräch mit seinem Bewährungshelfer eine neue Tat mehr oder weniger deutlich angekündigt hat, oder
- ein Zeitungsbericht über eine begangene Tat die “Handschrift” oder Täterbeschreibung eines Probanden aufweist.

Der Bewährungshelfer ist gesetzlich eng an das **Gericht** gebunden, das ihn bestellt hat, um die Lebensführung des Probanden zu überwachen und ihm Hilfestellung für ein Leben ohne weitere Straftaten zu geben: Er muss dem Gericht regelmäßig sowie bei Verstößen gegen gerichtliche Auflagen oder Weisungen berichten, damit dieses über die weitere Ausgestaltung der Bewährung, ggf. auch deren Widerruf, entscheidet. Er kann auch den Erlass nachträglicher Auflagen und Weisungen durch das Gericht anregen, beispielsweise Meldepflichten des Probanden bei der Polizei oder ein Verbot des Umgangs mit bestimmten, gefährdeten Personenkreisen, und die **Einhaltung** solcher **Auflagen überwachen**. In diesem Rahmen kann er sich z. B. unter

Mitteilung der Personalien des Probanden bei der Polizei erkundigen, ob der Meldepflicht nachgekommen wurde. Wegen dieser im Strafgesetzbuch vorgesehenen Bindung an das allein entscheidungsbefugte Vollstreckungsgericht darf ein Bewährungshelfer weder selbst Auflagen erteilen noch auf eigene Initiative ohne Kenntnis und Zustimmung des Gerichts quasi als Ermittlungshelfer der Polizei oder Staatsanwaltschaft auftreten.

Die Unterstützung von Straffälligen durch Bewährungshelfer ist ein Beitrag zur Kriminalprävention. Wesentlich hierfür ist ein gesetzlich geschütztes **Vertrauensverhältnis**, ohne das der Proband seinem Bewährungshelfer Probleme, die vielleicht zu neuen Taten führen, nicht mitteilen würde. Deshalb hat der Gesetzgeber entschieden, dass Bewährungshelfer (zumeist Diplom-Sozialpädagogen oder -Sozialarbeiter) einer beruflichen **Schweigepflicht** unterliegen und sich bei unbefugter Offenbarung von Informationen aus dem Betreuungsverhältnis strafbar machen.

Hiervon muss es zum Schutz Dritter allerdings Ausnahmen geben, wenn bedeutende Rechtsgüter – z. B. die körperliche Unversehrtheit oder die sexuelle Selbstbestimmung – unmittelbar bedroht sind und der Bewährungshelfer sich sofort an die Polizei wenden muss, um Schlimmeres zu verhüten, ohne eine Entscheidung des Gerichts abzuwarten. Er darf seine Schweigepflicht dann auf Grund eines **rechtfertigenden Notstands** brechen. Dies muss er nachvollziehbar in seinen Unterlagen **dokumentieren** und zeitgleich **das Gericht informieren**, damit dieses seiner Entscheidungsverantwortung über die Aussetzung der Strafe zur Bewährung nachkommen kann.

Konkret folgt hieraus:

- Eine regelmäßige Übermittlung der Personalien und Wohnanschrift von Probanden an örtliche oder andere Polizeidienststellen ohne gerichtliche Weisung ist unzulässig. Da in Schleswig-Holstein ein **regelmäßiger Meldedatenabgleich** durch die Polizei durchgeführt und die Haftentlassung automatisch an die Polizei gemeldet wird, besteht keine zusätzliche allgemeine Meldepflicht für Straftäter bei der Polizei. Der Bewährungshelfer muss erforderlichenfalls im Einzelfall eine Meldeauflage durch das Gericht anregen und deren Einhaltung – ggf. durch Kontaktaufnahme mit der Polizei – überwachen.
- Ohne Vorliegen einer unmittelbaren Gefahr ist auch die "**vorsorgliche**" **Übermittlung weiterer Daten** – z. B. "Vorlieben" bei der Tatbegehung, Personenbeschreibung, Kfz-Kennzeichen – an die Polizei nicht zulässig. Die Polizei verfügt ohnehin im Rahmen der elektronisch erschlossenen Kriminalaktenführung über diese Daten aus den früheren Ermittlungen
- Wenn ein Proband selbst weitere erhebliche Straftaten angekündigt hat oder sonstige Anhaltspunkte auf eine gegenwärtige Gefahr schließen lassen, muss der Bewährungshelfer abwägen, ob eine **Durchbrechung der Schweigepflicht** im Hinblick auf die bedrohten Rechtsgüter geboten ist. Solche schwierigen Entscheidungssituationen gehören zum Berufsalltag etwa von Kinderärzten bei Verdacht auf Missbrauch, von Psychologen, Psychiatern und weiteren Berufsgeheimnisträgern, bei denen Vertrauensschutz und Verantwortung zur

Verhinderung von Straftaten miteinander in Widerstreit geraten können.
Das Ergebnis unserer Beratung wurde mittlerweile unter Beteiligung des Justizministeriums in landesweiten Gremien der Straffälligenhilfe erörtert und als praxisgerecht anerkannt. Aufgeregte Meldungen, "der Datenschutz" stehe der Verhinderung von Rückfallstraftaten entgegen, entpuppten sich bei näherem Zusehen als oberflächliche Stimmungsmache.

Was ist zu tun?
Die vorgesehenen Informationswege zwischen Justiz und Polizei sollten genutzt werden. Für Alleingänge am Richter vorbei besteht außer in Gefahrenfällen keine Berechtigung.

4.4 Ausländerverwaltung

4.4.1 Überblick

Der Regierungswechsel auf Bundesebene hat zunächst keine grundlegende Änderung der Erfassungsinstrumente im Ausländerbereich gebracht. Trotz schwerwiegender datenschutzrechtlicher Einwände wird das Projekt einer **AsylCard** (vgl. 21. TB, Tz. 4.5.2) vom Bundesinnenministerium zäh weiterverfolgt. Auf dessen Anfrage hin meinte die Innenministerkonferenz wie auch das Innenministerium des Landes, die Einsatzmöglichkeiten einer Chipkarte im Asylverfahren sollten weiterverfolgt werden. Es wurde uns aber zugesichert, dass unsere im letzten Jahr dargestellten Bedenken berücksichtigt würden. Vorgeschlagen wurde ein Pilotversuch auf freiwilliger Basis. Schleswig-Holstein will sich hieran nicht beteiligen.

Sachdienlich war in diesem Zusammenhang ein Beschluss des Schleswig-Holsteinischen Oberverwaltungsgerichtes (OVG), in dem festgestellt wird, dass es sich bei einem **Texteintrag** "Abschiebungshindernis selbst zu vertreten" **in einer Duldungsbescheinigung** um eine unzulässige Datenübermittlung handelt. Diese Praxis basierte auf einem Erlass des Innenministeriums. Das OVG begründet seinen Beschluss damit, dass ein Ausländer verpflichtet ist, diese Duldungsbescheinigung bei unterschiedlichen Anlässen vorzulegen. Ohne Notwendigkeit gelange so eine für den Betroffenen negative behördliche Bewertung zur Kenntnis Dritter. Das Innenministerium reagierte prompt: Es nahm seinen Erlass zurück. Stattdessen stellt die Ausländerbehörde eine Bescheinigung zur Vorlage beim Sozialamt und beim Arbeitsamt aus, wenn das Abschiebungshindernis nicht zu vertreten ist. Mit dieser OVG-Entscheidung ist klargestellt, dass sich Ausländerbehörden die Kenntnisnahme von Informationen, die sie in – bei verschiedenen Anlässen zwangsläufig vorzulegenden – Ausweisen aufnehmen, als Übermittlungen zurechnen lassen müssen. Die Ausländerbehörden sind in Umsetzung des Prinzips der Datensparsamkeit verpflichtet, nur die Daten in einen Ausweis, eine Bescheinigung oder eine Chipkarte aufzunehmen, die rechtmäßig übermittelt werden dürfen.

Hinsichtlich des aus Datenschutzsicht heftig kritisierten **Ausländerzentralregisters** (21. TB, Tz. 4.5.1; 17. TB, Tz. 4.1.3.3) haben sich bisher keine Verbesserungen ergeben. Gegen das Registergesetz im Jahr 1995 eingelegte Verfassungsbeschwerden sind bis heute nicht entschieden. Statt das Gesetz auf die verfassungsrechtlich akzeptablen Kernaufgaben – die Koordination auf den Austausch von aufenthaltsrechtlich relevanten Informationen – zurückzuführen, ist weiterhin eine Erweiterung durch eine sog. Warndatei und die Einbeziehung der Sozialleistungsverwaltung in der Diskussion.

4.4.2 Scheinehen-Überprüfung nicht korrekt

Bei der Überprüfung, ob eine eheliche Lebensgemeinschaft besteht, ist im Interesse des Schutzes der Intim- und Privatsphäre äußerste Zurückhaltung geboten. Kontrollen ergaben, dass dies bei der Überprüfung von Ausländern durch die Stadt Kiel bislang nicht hinreichend beachtet wurde.

"**Scheinehen** im Visier – schwere Vorwürfe an Ausländerbehörde". Mit dieser Zeitungsüberschrift wurde die Ausländerbehörde wegen ihrer Ermittlungen zur Überprüfung ehelicher Lebensgemeinschaften angegriffen. Worum ging es?

Im Ausländerrecht hängt die Erteilung einer Aufenthaltsgenehmigung oft davon ab, dass eine **eheliche Lebensgemeinschaft** besteht. Es genügt nicht, formal mit einer oder einem deutschen Staatsangehörigen verheiratet zu sein, um ein Aufenthaltsrecht zu erhalten; die Partner müssen auch zusammenleben. Offensichtlich heiraten immer wieder Menschen nur, um an die begehrte Aufenthaltsgenehmigung zu kommen. Um dies festzustellen, beauftragt das Ausländeramt den Ermittlungsdienst der Stadt Kiel mit Außenprüfungen in der Wohnung der Betroffenen. Im Jahr 1999 gab es über zweihundert solcher Ermittlungsersuchen. In ca. 10 % der Fälle verdichtete sich dabei der Verdacht einer "Scheinehe". Bei vielen der Überprüften verursachte aber die Prüfung ihrer Ehe **Angst und Unbehagen**, wird doch dadurch die Ehrlichkeit von Gefühlen infrage gestellt und tief in die Privatsphäre eingedrungen. Sie konnten den Eindruck gewinnen, ihre binationale Ehe sei gesellschaftlich unerwünscht, ja trage gar den Hauch des Kriminellen in sich.

Unsere Querschnittskontrolle bei der Ausländerbehörde ergab denn auch, dass bei den amtlichen Ermittlungen einiges im Argen lag: Schon **nichtige Anlässe** führten zu einer Überprüfung. Dem eingeschalteten Ermittlungsdienst wurde, ohne dass hierfür eine Notwendigkeit bestand, die gesamte Ausländerakte mitgegeben. Die **Dokumentation** der Gründe für die Ermittlung sowie der Ermittlungsergebnisse waren **unzureichend**. Ohne Not wurden Dritte – Nachbarn, Postbote, Hausmeister – befragt und dadurch zumindest indirekt über den "Scheinehenverdacht" in Kenntnis gesetzt. Die Betroffenen selbst erfuhren oft von der Überprüfung und der Befragung Dritter nichts, sodass sie unbegründete Verdächtigungen nicht ausräumen konnten.

In unserem Prüfbericht machten wir der Ausländerbehörde zahlreiche Vorschläge zur **Verbesserung des Verfahrens**. Die Stadt Kiel erklärte sich sofort bereit,

diesen Vorschlägen zu entsprechen. Danach soll künftig eine genauere Prüfung erfolgen, ob der Ermittlungsdienst überhaupt eingeschaltet werden soll. Die Kriterien für die Annahme eines "Scheinehenverdachtes" wurden bereinigt. So ist z. B. die Inhaftierung des deutschen Ehegatten, die unzulässige Einreise des Ausländers oder gar eine anonyme Denunziation nicht mehr ausreichendes Indiz für eine "Scheinehe" und damit Auslöser von Ermittlungen. Der Ermittlungsdienst erhält ein präzise begründetes Ermittlungsersuchen und nicht mehr die gesamte Ausländerakte. Er muss zunächst versuchen, bei den Betroffenen selbst die Frage des Bestehens einer Lebensgemeinschaft zu klären, bevor Dritte befragt werden dürfen. Der Vorgang wird künftig in der Ausländerakte nachvollziehbar dokumentiert; die Betroffenen werden benachrichtigt. Die nunmehr geltenden Anweisungen sind geeignet, künftig die Beeinträchtigung der Intim- und Privatsphäre auf ein erforderliches Minimum zu reduzieren.

Was ist zu tun?
Die neuen Anweisungen der Ausländerbehörde sind umzusetzen. Zugleich werden wir versuchen, auch auf Landesebene ein einheitliches datenschutzfreundliches Verfahren bei der "Scheinehenermittlung" zu erreichen.

4.4.3 Datenübermittlung Sozialamt – Ausländerbehörde

Sozialbehörden dürfen den Ausländerbehörden nicht routinemäßig alle Fälle von Sozialhilfebezug übermitteln. Neu entwickelte Kriterien sollen den Informationsfluss steuern.

Die Ausländerbehörde der Landeshauptstadt Kiel vertrat die Ansicht, das 1990 erlassene Ausländergesetz verpflichte Sozialbehörden in jedem Fall zur Mitteilung des Bezugs von Sozialhilfe – das Sozialamt war ganz anderer Ansicht. Zu Recht: In jedem Einzelfall muss eine Prüfung durchgeführt werden, ob durch **Sozialhilfebezug** ein **Ausweisungsgrund** entstanden ist. Unsere Aufforderung an die Ausländerbehörde, aus ausländerrechtlicher Sicht Fallgruppen zu benennen, blieb lange Zeit unbeantwortet.

Wir sahen uns daher selbst veranlasst, darauf hinzuweisen, wann eine Übermittlung zulässig ist und wann nicht:

- Bei einem gesicherten Aufenhaltsstatus ist eine Datenübermittlung nicht zulässig.
- Eine durch die Übermittlung ausgelöste ausländerrechtliche Maßnahme darf eine vorrangige sozialrechtliche Zielsetzung nicht vereiteln, so wie dies bei Hilfen in besonderen Lebenslagen oft der Fall wäre.
- Den Umstand der Darlehensgewährung oder medizinische Angaben halten wir nicht für übermittlungsfähig.

- Bei Übermittlungsersuchen muss die Anfrage präzise begründet werden, insbesondere, weshalb auf eine Datenerhebung beim Betroffenen verzichtet werden soll.
- Eine Übermittlung durch das Sozialamt von sich aus erfolgt beim Vorliegen von Ausweisungsgründen im konkreten Einzelfall. Solche Gründe können längerfristige Obdachlosigkeit und Sozialhilfebezug sein. Dabei darf es sich aber nicht um kurzfristigen Hilfebezug handeln.
- Nicht die Antragstellung, sondern erst nach positiver Entscheidung über den Sozialhilfeantrag darf übermittelt werden.
- Mitgeteilt werden dürfen dann die Personalien sowie die erforderlichen Daten über Art und Umfang der Leistung.

4.5 Wirtschaft, Technik, Verkehr

4.5.1 Theorie und Praxis bei gaststättenrechtlichen Erlaubnisverfahren

Eine Prüfung gaststättenrechtlicher Erlaubnisverfahren zeigte erhebliche Mängel bei der Umsetzung der neuen Gaststättenverordnung. Die geprüfte Stadtverwaltung will künftig auf überflüssige Datenerhebungen verzichten.

Bereits in den vergangenen Jahren haben wir uns eingehend mit gaststättenrechtlichen Erlaubnisverfahren befasst (17. TB, Tz. 4.3.5; 18. TB, Tz. 4.1.3). Auf der Grundlage unserer Prüfungsergebnisse wurde vom Wirtschaftsministerium in der Folge eine **neue Gaststättenverordnung** (GastVO) erlassen, die das Verwaltungsverfahren abschließend regelt. Es lag daher nahe, hier eine "**Erfolgskontrolle**" durchzuführen. Das Ergebnis hat eine erhebliche Diskrepanz zwischen Theorie und Praxis aufgezeigt. Verschiedene Neuregelungen waren von der geprüften Stelle schlicht ignoriert worden. Folgende Beispiele sind zu nennen:

- Obwohl die von den Betroffenen im Antragsverfahren vorzulegenden Unterlagen in der Verordnung abschließend aufgezählt sind, wurden von den Antragstellern darüber hinaus z. B. die Vorlage vollständiger Mietverträge, **Unbedenklichkeitsbescheinigungen** eines Elektromeisters sowie des Bezirksschornsteinfegermeisters gefordert. Die Beschaffung der nicht notwendigen Unbedenklichkeitsbescheinigungen war für die Betroffenen mit erheblichem Aufwand und Kosten verbunden.
- Entgegen den Festlegungen in der GastVO wurden die Industrie- und Handelskammer, die Allgemeine Ortskrankenkasse, das Amtsgericht, das Finanzamt, die örtliche Polizeistation sowie der Kreis als Brandschutzbehörde nach ihrer Meinung befragt. Eine solche **überflüssige Anhörungspraxis** führt zu unnötigen Datenübermittlungen.
- Nach Erteilung einer Gaststättenerlaubnis erhielten sowohl die örtliche **Polizeistation** wie auch das **Finanzamt** jeweils eine Durchschrift des Erlaubnisbescheides zur Kenntnis. Diese Unterrichtung ist weder erforderlich noch zulässig.

- **Eignungsbedenken** gegen den Betroffenen wurden durchweg über die **Verjährungsfrist** von drei Jahren hinaus dauerhaft gespeichert.

Die undifferenzierte Aufnahme von Schriftstücken in Erlaubnisakten ohne ausreichende Klärung, Prüfung und Bewertung der zugrunde liegenden Sachverhalte sowie die versäumte Löschung abgeschlossener Erlaubnisvorgänge musste außerdem beanstandet werden. In ihrer Stellungnahme hat die Stadt zugesagt, die Maßgaben der neuen GastVO "ab sofort" zu beachten. Die Bereinigung der vorhandenen Erlaubnisakten wurde unverzüglich in Angriff genommen.

Was ist zu tun?
Alle schleswig-holsteinischen Konzessionsbehörden sollten die Beanstandungen zum Anlass nehmen, ihre Verfahrensweise auf die Übereinstimmung mit der Gaststättenverordnung hin zu überprüfen und gegebenenfalls entsprechend zu ändern.

4.5.2 "Wer weiß, wofür man das noch mal gebrauchen kann"

Eine Kontrolle bei der Datenverarbeitung der Handwerkskammer Flensburg ergab mehrere Gründe zu Beanstandungen. Eine umfangreiche "Schwarzarbeiterdatei" muss bereinigt werden.

Handwerkskammern sind Körperschaften des öffentlichen Rechts, ihre gesetzlichen Aufgaben sind es u.a., aktiv das Handwerk zu fördern und die damit befassten Behörden zu unterstützen sowie die Handwerksrolle und die Lehrlingsrolle zu führen. Daneben haben sie Prüfungsausschüsse einzurichten, die Geschäfte des Meisterprüfungsausschusses wahrzunehmen und die ordnungsgemäße Durchführung der Gesellenprüfungen zu überwachen. Ein wichtiger Aufgabenbereich besteht schließlich im Zusammenhang mit der ordnungsgemäßen Handwerksausübung. Die Handwerkskammern gehen Hinweisen auf illegale Handwerksausübung und **Schwarzarbeit** nach und haben das Recht, selbst in diese Richtung zu ermitteln. Bei hinreichenden Verdachtsmomenten wird eine Ordnungswidrigkeiten-Anzeige erstattet oder eine Untersagungsverfügung beantragt. Die Durchführung dieser Verfahren obliegt den Kreisordnungsbehörden.

Für den Bereich der Handwerks- und Lehrlingsrollenführung ergab unsere Prüfung bei der Handwerkskammer Flensburg keine wesentlichen datenschutzrechtlichen Verstöße. Im Zusammenhang mit der **Überwachung der ordnungsgemäßen Handwerksausübung** und der Bekämpfung der Schwarzarbeit stießen wir hingegen auf sehr umfangreiche Datensammlungen, von deren Rechtmäßigkeit uns die Kammer nicht zu überzeugen vermochte. Die bis zu 15 Jahre alten Vorgänge reichten von "verdächtigen Gewerbeanmeldungen" über "Anzeigen" von Bürgern, dass der Nachbar in seiner Garage nebenbei Autos repariere oder Polstermöbel auffrische, bis hin zu ausgeschnittenen und gesammelten Zeitungsannoncen und Grundlagenmaterial für konkrete Ordnungswidrigkeitenverfahren. Der größte Teil war in keiner Weise

verwendet worden und seine Erforderlichkeit konnte auch auf Nachfrage nicht dargelegt werden. Oftmals ließ sich nämlich aus den einzelnen Papieren noch nicht einmal ein zusammenhängender Sachverhalt rekonstruieren, sodass die gespeicherten Informationen auch für die Handwerkskammer wertlos waren. Nach der Devise "wer weiß, wofür man das noch mal gebrauchen kann" wurde aber dennoch jede Information vorsichtshalber erst einmal archiviert.

Die Kammer begründete ihre Sammelpraxis mit der "Erfahrung", dass es im Bereich der illegalen Handwerksausübung und der Schwarzarbeit auf lange Sicht immer wieder zu **Wiederholungstaten** komme. Nach unseren Feststellungen waren allerdings nur in drei Prozent aller Sachverhalte Rückfälle zu verzeichnen. Zudem kann die Handwerkskammer für sich keine längeren Speicherfristen in Anspruch nehmen als die für die Verfolgung von Ordnungswidrigkeiten zuständigen Stellen. Wir haben den Umfang und die Dauer der Datenspeicherung deshalb beanstandet und die Kammer aufgefordert, den gesamten Datenbestand hinsichtlich seiner Speicherungserforderlichkeit zu überprüfen sowie alle nicht mehr benötigten Daten unverzüglich zu löschen. Die Kammer will die Speicherung in einem ersten Schritt auf die Dauer von fünf Jahren beschränken. Der Gesamtbestand wird unverzüglich durchgesehen und alle nicht benötigten Vorgänge werden vernichtet. Der dann verbleibende und aus Sicht der Kammer unbedingt erforderliche Datenbestand wird anschließend nochmals mit dem Ziel geprüft, ob die Speicherfrist weiter gesenkt werden kann.

Parallel zu diesen Vorgängen führte die Kammer seit einem Jahr eine so genannte **"Schwarzarbeiterdatei"** in elektronischer Form. Entgegen ihrer Bezeichnung enthielt diese Datei letztlich alle personenbezogenen Daten, für die papierene Vorgänge der oben genannten Art existierten. Abgesehen davon, dass für die Führung einer solchen Datei keine Rechtsgrundlage besteht, vermochte die Kammer uns auch hier nicht die Erforderlichkeit zu belegen. Die Handwerkskammer wird diese Datei jetzt auf ein Suchregister für zulässigerweise noch vorhandene papierene Informationen reduzieren und nur noch solche Daten speichern, die im Zusammenhang mit Ordnungswidrigkeitenverfahren stehen. Nach Abschluss der Verfahren werden die Informationen unverzüglich gelöscht.

Was ist zu tun?
Die Handwerkskammer Flensburg muss die Speicherung personenbezogener Daten auf das erforderliche Maß begrenzen und ihre Datenbestände bereinigen.

4.5.3 Unannehmlichkeiten durch Falschauskunft der IHK

Wer sein Gewerbe aufgibt und dieses ordnungsgemäß beim zuständigen Ordnungsamt abmeldet, sollte sich darauf verlassen können, dass auch die zuständige Industrie- und Handelskammer (IHK) dies zeitnah berücksichtigt. Dies ist leider nicht immer der Fall.

Ein Petent berichtete uns, dass er mit einer gerichtlich geltend gemachten Forderung in Höhe von nahezu 17 000 DM konfrontiert wurde, ohne dass ihm der in der Klage geschilderte Sachverhalt überhaupt bekannt war. Seine Recherchen

ergaben, dass ein Rechtsanwalt für seinen Mandanten telefonisch bei der **IHK** nach einem Gewerbebetrieb gefragt hatte, von dem ihm nur die Geschäftsadresse, nicht aber der Name bekannt war. Die IHK nannte daraufhin den Petenten als Geschäftsführer.

Diese **Auskunft** war in doppelter Hinsicht **falsch**. Zum einen war sein Betrieb schon seit Monaten beim Gewerbeamt abgemeldet, ohne dass dies in den Datenbeständen der IHK vermerkt gewesen wäre. Zum anderen befanden sich auf dem bezeichneten Gewerbegrundstück zum fraglichen Zeitpunkt mehrere Betriebe, die infrage hätten kommen können. Der Petent war jedenfalls unbeteiligt. Wie diese Falschauskunft zustandekam, konnte nicht mehr aufklärt werden. Jedenfalls ist Folgendes nicht beachtet wurden:

- Die regelmäßige Übermittlung von Daten aus den Gewerbeanzeigen an die Industrie- und Handelskammern ist in der Gewerbeordnung gesetzlich vorgesehen. Ergänzend dazu müssen die Gewerbeämter die **Abmeldungen** "**nachberichten**". Ob dies im konkreten Fall geschehen ist, konnte das zuständige Gewerbeamt nicht mehr nachvollziehen.
- Wegen der Vielzahl der An-, Ab- und Ummeldungen kommt es bei der Bearbeitung in der IHK regelmäßig zu zeitlichen **Verzögerungen** von sechs bis acht Wochen. Der Auskunftssuchende wurde auf diese zeitliche Diskrepanz nicht hingewiesen.
- Die Auskunftserteilung war **nicht dokumentiert**.

Wir wiesen die IHK auf Folgendes hin: Auch wenn für die Übermittlung von Daten der Kammerzugehörigen durch die IHK die **Schriftform** nicht ausdrücklich vorgeschrieben ist, sollte eine mündliche Auskunft nur ausnahmsweise und nur dann erfolgen, wenn der Sachverhalt eindeutig auf der Hand liegt, der Betroffene klar identifiziert ist und die Auskunftserteilung auch in rechtlicher Hinsicht unproblematisch erfolgen kann. Diese Vorgehensweise hilft sicherzustellen, dass die relevanten tatsächlichen und rechtlichen Aspekte beachtet werden. Fernmündlich erteilte Auskünfte bergen in ihrer Spontanität immer das Risiko, dass sie sich bei näherer Prüfung als unzulässig oder falsch bzw. unvollständig erweisen.

Was ist zu tun?
Auskunftsgebende Stellen müssen dafür Sorge tragen, dass ihre Datenbestände stets einen aktuellen Stand haben. Bei Erteilung einer Auskunft muss deren Richtigkeit und Vollständigkeit geprüft werden.

4.6 Sozialbereich

4.6.1 Überblick

Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden (Sozialgeheimnis). So hat es der Gesetzgeber festgelegt; doch wie sieht es in der Praxis aus? Die Zusammenarbeit sozialer Einrichtungen soll verbessert und die unberechtigte Inanspruchnahme von Sozialleistungen verhindert werden. Man will Verwaltungskosten einsparen, zugleich soll der Service für die Bürgerinnen und Bürger, den "Kunden der Verwaltung", besser werden. Wie können diese Ziele erreicht werden, ohne dass das **Sozialgeheimnis** auf der Strecke bleibt? Unsere Erfahrungen mit Eingaben und Anfragen zeigen, dass diese Fragen lösbar, aber oft nicht befriedigend gelöst sind. Wir stehen innovativen Ideen auch im Sozialverwaltungsbereich positiv gegenüber. Ziel muss es jedoch sein, den Sozialdatenschutz bei der Verwirklichung solcher Ideen zu integrieren, wenn möglich weiter zu verbessern.

Das Ministerium für Arbeit, Gesundheit und Soziales des Landes Schleswig-Holstein nahm ein Projekt "Digitale Kundenakte" in Angriff, bei dem zunächst eine **gemeinsame elektronische Aktenführung von Sozial- und Arbeitsamt** vorgesehen war. Zweck der Maßnahme sollte eine verbesserte Beratung und eine schnellere Bearbeitung sein. So sehr wir diese Zielsetzung unterstützten, so wenig sahen wir die ersten Planungen als geeignet an. Durch eine gemeinsame Aktenführung würden die Verantwortlichkeiten der kommunalen Sozialverwaltung und der auf Bundesebene angesiedelten Arbeitsverwaltung verwischt. Die Zweckbindung der vorhandenen Daten würde aufgehoben. Zudem erweist sich die Schnittmenge der wahrgenommenen Aufgaben bei näherem Zusehen nicht als so groß, dass der technische Aufwand einer vollständigen Digitalisierung der Akten gerechtfertigt wäre. Wir haben daher weniger ambitionierte, dafür aber datenschutzrechtlich realisierbare Alternativen vorgeschlagen: die teilweise organisatorische Zusammenlegung der Datenerhebung und die Verbesserung der Kommunikation auf elektronischer Basis unter Einbeziehung der Betroffenen.

www.schleswig-holstein.datenschutz.de
(Rubrik: weitere Materialien/Vorträge)

Ein Schwerpunkt unserer diesjährigen Tätigkeit lag im **Sozialhilfebereich**. Im Dialog mit den Sozialleistungsträgern wurden datenschutzgerechte Lösungsansätze erarbeitet. So wurden Hinweise zur Zulässigkeit eines Datenaustausches zwischen den Sozialleistungsträgern (Tz. 4.6.3) oder zur Gewährung von einmaligen Beihilfen (Tz. 4.6.5) herausgegeben. Außerdem wurde ein Konzept für die Prüfung der Datenverarbeitung in den Sozialämtern entwickelt, das die Verfahrensabläufe von der Antragstellung bis zur Archivierung im Sozialamt erfasst. Ergänzend bieten wir im neuen Jahresprogramm der DATENSCHUTZAKADEMIE erstmals gezielt Fortbildungsveranstaltungen für Mitarbeiter von Sozial- und Wohngeldämtern an, die auf die Bedürfnisse der täglichen Praxis abgestellt sind.

4.6.2 Keine Extrawurst für Geheimdienste

Auch Geheimdienste wie der Verfassungsschutz, der Militärische Abschirmdienst (MAD) und der Bundesnachrichtendienst müssen bei Übermittlungsersuchen den Zweck und die Rechtsgrundlage darlegen. Die Verantwortung für die Zulässigkeit der Übermittlung von Sozialdaten liegt bei dem Sozialleistungsträger.

Eine Sozialamtsmitarbeiterin berichtete uns vom Anruf eines MAD-Mitarbeiters, der einen Auskunftsbesuch ankündigte. Man wolle sich Akten anschauen. Welche Akten und zu welchem Zweck er einsehen wollte, mochte er nicht angeben. Einige Tage später erschienen die Mitarbeiter des **MAD** im Sozialamt und begehrten Einsicht in sämtliche Vorgänge über die in der Zeit vor der Wiedervereinigung gewährten Hilfsmaßnahmen zu Gunsten von Besuchern aus der DDR und Berlin (Ost), die so genannten Besuchergelder.

Dazu war das Sozialamt nicht bereit, denn die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle, die das Ersuchen zu prüfen hat. Dies ist jedoch nur möglich, wenn die ersuchende Stelle **Zweck und Aufgabe,** für deren Erfüllung die Daten benötigt werden, benennt. Ohne diese Angaben ist das Ersuchen nicht zu prüfen und darf die Übermittlung nicht erfolgen. Nur bestimmte gesetzlich definierte Sozialdaten, wie Name, Vorname, Geburtsdatum, Geburtsort, derzeitige und frühere Anschriften des Betroffenen sowie Namen und Anschriften seiner derzeitigen und früheren Arbeitgeber dürfen außerdem übermittelt werden, keinesfalls vollständige Akten.

Im konkreten Fall kam erschwerend hinzu, dass die Vorgänge über die gewährten Besuchergelder **längst** hätten **vernichtet** werden müssen, da sie für die Aufgabenerfüllung nicht mehr erforderlich waren. Eine “zeitlich unbegrenzte” Speicherung ist unzulässig. Unzulässig gespeicherte Daten dürfen erst recht nicht übermittelt werden. Der MAD-Mitarbeiter musste daher das Sozialamt unverrichteter Dinge verlassen.

Was ist zu tun?
Fehlen Angaben in einem Übermittlungsersuchen und kann daher eine Prüfung nicht vorgenommen werden, so darf dem Ersuchen nicht stattgegeben werden. Dies gilt auch gegenüber Geheimdiensten.

4.6.3 Datenaustausch zwischen Sozialhilfeträgern

Wenn ein Sozialhilfeempfänger umzieht, dürfen nur die Sozialdaten an das Sozialamt des neuen Wohnsitzes übermittelt werden, die dort für die weitere Sozialhilfegewährung erforderlich sind. Auch ein Kreissozialamt kann nur solche Sozialdaten von einer Gemeinde anfordern, die es für seine Aufgabenerfüllung benötigt. Die Übersendung vollständiger Sozialhilfeakten ist nur in wenigen Fällen zulässig.

Sozialhilfeempfänger, die von einer Gemeinde in eine andere Gemeinde umziehen, werden häufig von dem neuen Sozialamt "aufgefordert", schriftlich ihr Einverständnis in eine vollständige **Aktenübersendung** zu geben. Das Einverständnis des Betroffenen kann jedoch die gesetzliche Verpflichtung der Sozialämter nicht ersetzen, nur die Daten zu übermitteln, die zur weiteren Sozialhilfegewährung **erforderlich** sind (vgl. 20. TB, Tz. 4.7.3). Mit unseren im Amtsblatt Schleswig-Holstein von November 1998 veröffentlichten Hinweisen haben wir den Kommunen die Rechtslage detailliert dargestellt.

www.schleswig-holstein.datenschutz.de
(Rubrik: speziell für Behörden)

In einem anderen Fall stellte sich die Frage, ob ein **Kreissozialamt** ohne weiteres in die Sozialhilfeakten der kreisangehörigen Städte, Amtsverwaltungen bzw. amtsfreien Gemeinden Einblick nehmen darf. Grundsätzlich sind die Kreise und kreisfreien Städte für die Sozialhilfegewährung zuständig. Um bürgerfreundlich und bürgernah zu sein, haben sie die Gemeinden mit der Aufgabenerfüllung betraut und durch Satzung festgelegt, welche Sozialhilfeleistungen von den örtlichen Sozialämtern gewährt werden. Damit geht auch die Verantwortung auf die Datenverarbeitung an diese Stellen über. Sie treffen die **Entscheidungen in eigenem Namen**. Dem Kreis verbleibt in dem Umfang der Aufgabenübertragung kein Selbsteintrittsrecht, er kann Einzelfälle nicht einfach an sich ziehen und entscheiden.

Dies bedeutet, dass ein genereller, vom Einzelfall unabhängiger Datenzugriff des Kreises auf Sozialdaten einer oder aller zugehörigen Gemeinden unzulässig ist. Zulässig ist eine Datenübermittlung nur, wenn sie zur Erfüllung der Aufgaben, die der Kreis nicht an die Gemeinden übertragen hat, erforderlich ist. Dies ist z. B. in einem Widerspruchsverfahren oder dann der Fall, wenn ein Hilfeempfänger den Kreis auffordert, eine bestimmte sozialhilferechtliche Entscheidung der Gemeinde zu überprüfen. Ein pauschales Prüfrecht steht dem Kreis jedoch nicht zu.

Was ist zu tun?
Ein Austausch von Sozialdaten zwischen den Sozialämtern der Gemeinden kann ebenso wie ein Datenaustausch zwischen dem Sozialamt einer Gemeinde und einem Kreissozialamt nur erfolgen, wenn die Daten für die weitere Sozialhilfegewährung erforderlich sind.

4.6.4 Datenübermittlung an private Arbeitsvermittler

Ein Hilfesuchender muss zwar seine Arbeitskraft zur Beschaffung des Lebensunterhaltes für sich und seine unterhaltsberechtigten Angehörigen einsetzen. Seine Sozialdaten dürfen im für die Vermittlung erforderlichen Umfang an private Arbeitsvermittler jedoch nur dann übermittelt werden, wenn er zuvor eingewilligt hat.

Sozialämter gehen neue Wege, um die Hilfesuchenden aus der Sozialhilfeabhängigkeit herauszubringen. Längst vorbei sind die Zeiten, in welchen nur der **Nachweis der Arbeitssuche** durch das Arbeitsamt verlangt wurde. Eigeninitiative ist gefragt. Der Hilfesuchende wird aufgefordert, Durchschriften von Bewerbungen vorzulegen. Sozialämter ermuntern Hilfeempfänger, sich gezielt auf aus der Tagespresse entnommene aktuelle Stellenangebote zu bewerben. Mit speziellen Beratungskonzepten versuchen besonders geschulte Mitarbeiter auf die Möglichkeiten einzelner Hilfeempfänger einzugehen. Angaben über schulische und berufliche Vorbildung, bisherige Tätigkeiten, aber auch über persönliche Neigungen, die familiäre Situation oder gesundheitliche Einschränkungen werden erfragt, um zu ergründen, welche Arbeitsstelle infrage kommt.

Sozialämter suchen zudem verstärkt die Zusammenarbeit mit **privaten Arbeitsvermittlern**. Eine private Arbeitsvermittlung ist nur eine von mehreren Möglichkeiten der Arbeitssuche. Ein Hilfeempfänger kann die ihm obliegende Mitwirkungspflicht bei der Arbeitssuche ggf. auch anderweitig erfüllen. Daher kann eine private Arbeitsvermittlung nur beauftragt werden, wenn der Hilfeempfänger zuvor schriftlich seine **Einwilligung** erteilt hat. Er muss über den Umfang der beabsichtigten Datenübermittlung, den Empfänger und den Verwendungszweck der Daten informiert werden. Seine Einwilligungserklärung kann er jederzeit widerrufen. Nur in den Grenzen der Einwilligung dürfen die für die Vermittlung erforderlichen Sozialdaten an die private Arbeitsvermittlung übermittelt werden, in keinem Fall die komplette Sozialhilfeakte mit einer Vielzahl von zum Teil hochsensiblen Daten.

Was ist zu tun?
Bevor eine private Arbeitsvermittlung mit der Arbeitssuche beauftragt werden kann, ist der betroffene Hilfeempfänger über Umfang, Zweck und Empfänger der Datenübermittlung zu informieren. Wenn er seine Einwilligung erklärt, kann ein Datenaustausch im erforderlichen Umfang erfolgen.

4.6.5 Diskriminierende Bestellscheine

Bei der Entscheidung, ob eine einmalige Beihilfe zur Beschaffung von Gebrauchsgütern von längerer Lebensdauer wie z. B. Elektro-Großgeräte oder Möbeln per Bestellschein oder als Barbeihilfe gewährt wird, haben die Sozialämter nicht ohne weiteres freie Hand.

Neben der monatlichen Sozialhilfeleistung, der so genannten laufenden Hilfe zum Lebensunterhalt, können Hilfeempfänger einmalige Beihilfen, z. B. für

Bekleidung, Hausrat oder Gebrauchsgüter von längerer Lebensdauer und höherem Anschaffungswert, beantragen. Durch Eingaben wurden wir darauf aufmerksam gemacht, dass viele Sozialämter pauschal und unabhängig vom Einzelfall diese Leistungen in Form von **Bestell- oder Warengutscheinen** gewähren. Hilfeempfänger schilderten uns wiederholt ihre Erlebnisse, wie sie mit den Bestellscheinen von Geschäft zu Geschäft wanderten, sich als Sozialhilfeempfänger zu erkennen geben mussten, Preise erfragten und von Verkäufern oder "zuhörenden" Käufern mitleidig bestaunt wurden.

Sozialleistungsträger sind bei der Wahl der Form einer einmaligen Beihilfe nicht frei. Über Form und Maß der Sozialhilfe ist vielmehr nach pflichtgemäßem Ermessen und unter Berücksichtigung des Einzelfalles zu entscheiden. Wünschen des Hilfeempfängers ist zu entsprechen, wenn diese angemessen sind und keine unverhältnismäßigen Mehrkosten verursachen. Aufgabe der Sozialhilfe ist es, den Hilfeempfängern die Führung eines **menschenwürdigen Lebens** zu ermöglichen. Hierzu gehört, erwachsenen und mündigen Menschen die Möglichkeit zu belassen, im Rahmen der gesetzlich zustehenden Mittel ihre Bedarfsdeckung frei zu gestalten. Dem wird der Sozialleistungsträger dadurch gerecht, dass er die Sozialhilfe in der ganz überwiegenden Zahl der Fälle in Geld gewährt. Die grundsätzliche Gewährung der Beihilfen in der Form von Bestellscheinen berücksichtigt nicht die Besonderheiten des Einzelfalles und läuft der Zielsetzung der Sozialhilfe zuwider. Eine solche Entscheidung ist ermessensfehlerhaft.

Die Gewährung von einmaligen Beihilfen in der Form von Bestellscheinen zwingt den Hilfeempfänger zur Offenbarung von **besonders geschützten Sozialdaten**, und zwar von Namen, Anschrift und sozialem Status gegenüber dem Geschäft. Es ist nicht entscheidend, dass der Hilfeempfänger den Bestellschein selbst übergibt, da ihm keine andere Wahl bleibt. Der Sache nach liegt eine Übermittlung von Sozialdaten durch das Sozialamt vor, die nur im Rahmen des Erforderlichen zulässig ist. Bestellscheine sind dann erforderlich, wenn z. B. die begründete Sorge besteht, dass die gewährte Hilfe nicht zweckentsprechend verwendet wird, oder dem Sozialamt hierdurch ermöglicht wird, Sozialhilfemittel, z. B. durch Rabattvereinbarungen mit dem Einzelhandel, einzusparen.

www.schleswig-holstein.datenschutz.de (Rubrik: speziell für Behörden)

Was ist zu tun?
Gutscheine sollten bei der Gewährung von einmaligen Beihilfen nur in begründeten Einzelfällen benutzt werden.

4.7 Schutz des Patientengeheimnisses

4.7.1 Überblick

Ein großes Risiko für das Patientengeheimnis resultiert offenbar aus der **Geldknappheit im Gesundheitswesen**. Mithilfe von Forschungsprojekten, Qualitätssicherungsmaßnahmen oder Wirtschaftlichkeitsprüfungen will man einen möglichst effektiven Mitteleinsatz erreichen. Grundlage hierfür sind die medizinischen Behandlungsdaten. Eine Lösung dieses Konfliktes kann in der Pseudonymisierung der medizinischen Daten liegen, bevor sie für

behandlungsfremde Zwecke genutzt werden (Tz. 4.7.2). Dieses Mittel scheidet aber aus, wenn ganz konkrete medizinische Leistungsabrechnungen kontrolliert werden sollen. Von den Leistungserbringern wird hier gerne der Datenschutz zur Abwehr von Kontrollen bemüht. Natürlich geht es nicht an, dass mit dieser Begründung die Rechnungskontrolle unmöglich gemacht wird. Daher sind wir sowohl im Rahmen der Gesetzgebung als auch bei der praktischen Umsetzung bemüht, das Patientengeheimnis zu sichern und gleichwohl die notwendigen Abrechnungskontrollen zu ermöglichen (Tz. 4.7.3).

Mit dem Ministerium für Arbeit, Gesundheit und Soziales fand ein Meinungsaustausch darüber statt, wie in Schleswig-Holstein das Patientengeheimnis gesetzlich besser geschützt werden kann. Auch nach Verabschiedung des Gesetzes für Psychisch Kranke bestehen im Lande weiterhin gewaltige Defizite: Weder im Krankenhausbereich noch im öffentlichen Gesundheitswesen gibt es bereichsspezifische Regeln, mit der Folge, dass die Beteiligten die Beachtung der ärztlichen Schweigepflicht mehr oder weniger freihändig realisieren müssen. Vom Ministerium wurde die Absicht geäußert, ein umfassendes **Gesundheitsdatenschutzgesetzes** zu formulieren, in dem nicht nur das öffentliche, sondern auch das privatwirtschaftliche Gesundheitswesen (ambulante Versorgung, private Krankenhäuser) normiert würde. Dabei könnten die neuesten technischen Entwicklungen der Digitalisierung und Vernetzung berücksichtigt werden. Leider blieb es bei Vorüberlegungen.

Im Rahmen der Enquetekommission des Landtages "**Chancen und Risiken der Gentechnologie**" wurden wir um eine datenschutzrechtliche Stellungnahme gebeten. Diese hat Eingang in die vom Landtag beschlossenen Empfehlungen gefunden. Darin wird die Landesregierung einstimmig aufgefordert, sich dafür einzusetzen, dass die Erhebung und Verarbeitung von Daten über die erbliche Veranlagung durch Versicherungen und Arbeitgeber ausgeschlossen wird. Nicht nur das Recht auf Kenntnis, sondern auch auf Nichtwissen der eigenen genetischen Veranlagungen muss – so die Landtagsempfehlung – gesichert werden. Wegen der Sensibilität der Daten sei eine enge Zweckbestimmung und Zweckbindung sowie ein weitgehendes Verbot der Datenweitergabe zwingend. In medizinischen Registern soll eine Speicherung von genetischen Daten grundsätzlich ausgeschlossen sein.

4.7.2 Gesundheitsreform: Es wär' so schön gewesen!

Der Bundestag hat sich die Aufgabe gestellt, im Interesse der Begrenzung der Ausgaben im Gesundheitswesen eine groß angelegte Reform der gesetzlichen Krankenversicherung vorzunehmen. Bestehende Datenschutzdefizite hätten dabei in vorbildlicher Form abgebaut werden können.

Das, was uns im Rahmen der Länderbeteiligung als Gesetzentwurf zur Gesundheitsreform zunächst vorgelegt worden ist, ließ einem aus Datenschutzsicht die Haare zu Berge stehen. Wir haben folgende **Kritikpunkte** geäußert:

- Das Instrumentarium der Kontrollen und Prüfungen von Patientenunterlagen sollte beträchtlich erweitert werden, ohne dass die einzelnen Maßnahmen aufeinander abgestimmt gewesen wären. Neben kostenträchtiger Doppelarbeit und Überschneidungen hätte dies zu unvertretbaren Risiken für das Patientengeheimnis geführt.
- Der Gesetzentwurf verschob die Klärung wichtiger Einzelheiten auf noch zu schließende "Verträge und Vereinbarungen", sodass die Patientinnen und Patienten oft nicht hätten erkennen können, mit welcher Datenverarbeitung sie rechnen mussten.
- Wiederholt wurde die Einwilligung der Patienten vorausgesetzt, etwa bei der Einführung des Hausarztmodells und der sog. integrierten Versorgung, ohne dass sichergestellt gewesen wäre, dass sie freiwillig gegeben wird.
- Abrechnungsdaten sollten ohne überzeugende Begründung beim Medizinischen Dienst der Krankenkassen zehn Jahre personenbezogen aufbewahrt werden. Dies war umso weniger akzeptabel, als zugleich die Zweckbindung dieser Daten bei den Kassen weitgehend aufgehoben werden sollte.
- Für die geplanten Überprüfungen der Behandlung und der Abrechnung ist der Name des Patienten zunächst nicht erforderlich. Der Gesetzentwurf enthielt aber keine überzeugenden Anonymisierungs- oder Pseudonymisierungsverfahren.

Wir haben unsere Kritik mit **Vorschlägen** verbunden, durch die die Datenschutzrechte der Patienten trotz verbesserter Abrechnungskontrolle gewahrt werden. Unsere Forderung, bei der Kostenabrechnung ein Pseudonymisierungsverfahren zu verwenden, konnten wir auch im Gesundheitsausschuss des Bundestages präzisieren.

Die Reaktion des Bundesministeriums für Gesundheit auf unsere Kritik war positiv. In enger Abstimmung mit anderen Datenschutzbeauftragten sollte insbesondere unser zentrales Anliegen der **pseudonymisierten Kostenabrechnung** bei den Krankenkassen gesetzgeberisch umgesetzt werden. Dadurch, dass künftig nicht nur die ambulanten Abrechnungen, sondern auch die der Krankenhäuser, der Apotheken usw. pseudonymisiert werden sollten, wäre nun im Sinne der Datensparsamkeit sogar ein Mehr an Datenschutz erreicht worden. Es war vorgesehen, dass das Bundesamt für die Sicherheit in der Informationstechnik ein Einwegverschlüsselungsverfahren zur Verfügung stellt, mit dessen Hilfe in den Datenannahmestellen der Krankenkassen sämtliche Abrechnungsdaten pseudonymisiert werden sollten. Eine Rückführung des Pseudonyms in den Klarnamen sollte nur unter streng definierten Voraussetzungen und unter Einschaltung eines unabhängigen Trust Centers erlaubt werden. Dieses Verfahren hätte auf der einen Seite sowohl eine umfassende Abrechnungskontrolle wie auch die statistische Auswertung der Abrechnungsdaten kassenübergreifend und zeitunabhängig erlaubt und auf der anderen Seite verhindert, dass bei den Krankenkassen Gesundheitsprofile entstehen, die die Mitglieder zu "gläsernen Patienten" machen würden.

Auch ansonsten wurden vom Bundestag unsere **Argumente** aufgenommen: Die Zweckbindung der Datenverarbeitung innerhalb der Kassen wurde präzisiert. Den Mitgliedern wurde die Möglichkeit eingeräumt, den kassenweiten Zugriff auf die sensiblen medizinischen Daten auszuschließen – wie seit langem von den Datenschutzbeauftragten gefordert. Die Zweckbindung der einzelnen Datenbestände wurde ausdrücklich festgeschrieben. In besonderem Maße sollte dies für die Dateien gelten, die im Rahmen der sensiblen Beratungstätigkeiten angelegt werden.

Von all diesen datenschutzrechtlichen Verbesserungen ist am Ende leider nicht allzu viel übrig geblieben, nachdem der **Bundesrat** – aus Gründen, die nichts mit den Datenschutzregelungen zu tun hatten – das **Gesetz gestoppt** hat. Da aber hinsichtlich der vorgeschlagenen Pseudonymisierungsverfahren zwischen allen politischen Parteien Konsens zu bestehen scheint, haben wir das Gesundheitsministerium aufgefordert, es in einem eigenständigen Gesetzentwurf erneut einzubringen.

www.schleswig-holstein.datenschutz.de
(Rubrik: weitere Materialien/Pressemitteilungen)

Was ist zu tun?
Das Land sollte über den Bundesrat darauf hinwirken, dass die Pseudonymisierung in die Gesetzgebung zur Gesundheitsreform eingefügt wird.

4.7.3 Keine Krankenhausentlassungsberichte an die Kassen

Inakzeptabel sind Verfahrensweisen, bei denen aus Bequemlichkeit und Rechtsanmaßung bewusst eindeutige Gesetze ignoriert werden. Ein Beispiel hierfür ist die Praxis vieler Krankenkassen, bei den Krankenhäusern und anderen behandelnden Einrichtungen hochsensible und detaillierte Entlassungsberichte anzufordern. Im letzten Jahr verging kaum ein Monat, in dem wir insofern nicht tätig werden mussten.

Die Abrechnungskontrolle der Krankenkassen gegenüber den Krankenhäusern ist im Sozialgesetzbuch eindeutig geregelt. Anhand von klar festgelegten Parametern erfolgt diese zunächst bei den Kassen selbst.
Bedarf es auf Grund der Art, Schwere, Dauer oder Häufigkeit der Erkrankung oder auf Grund des Krankheitsverlaufes einer näheren Prüfung, so ist diese vom Medizinischen Dienst der Krankenversicherung (MDK) vorzunehmen. Die Anforderung der **Entlassungsberichte** kann zwar von den Kassen erfolgen. Sie müssen aber **direkt an den MDK** gesandt werden; eine Kenntnisnahme der detaillierten und sensiblen medizinischen Angaben durch die Kassen ist gesetzlich nicht vorgesehen. Die Mitarbeiter der Kassen verfügen für eine Bewertung auch nicht über den erforderlichen medizinischen Sachverstand.

Dies hindert manche Kassen aber nicht, sich die ärztlichen Berichte zuschicken zu lassen. Nachdem dies von uns immer wieder beanstandet wurde, gingen einige Kassen dazu über, sich für die Einsichtnahme in die medizinischen Unterlagen von den Patienten Einwilligungen einzuholen. Diese **Einwilligungserklärungen**

waren aber praktisch durchgängig **unwirksam**, da sie zu unbestimmt waren, eine ungenügende oder gar falsche Aufklärung über Zweck, Rechtsgrundlage und Datenumfang enthielten und zudem eine Umgehung der gesetzlichen Abrechnungskontrollregelungen darstellten. Die Krankenkassen haben nun einmal kein "medizinisches Vorprüfungsrecht" vor Einschaltung des MDK.

Die Mitarbeiter der Krankenhäuser befinden sich in einer Zwickmühle: Kommen sie dem Ansinnen der Kassen nach, so machen sie sich womöglich wegen Verletzung ihrer beruflichen Schweigepflicht **strafbar**. Geben sie ihre ärztlichen Berichte aber nicht weiter, so handeln sie sich viel Ärger und Schwierigkeiten bei der Kostenerstattung ein. Nicht nur das. Bei den Einrichtungen grassiert die Angst, dass, wer sich nicht kooperativ mit den Kassen zeigt, unter Umständen bei der Beschickung mit Patienten nicht mehr berücksichtigt wird. Um Klarheit herzustellen, haben wir die Rechtslage in Veröffentlichungen der Ärztekammer und in unserem Internet-Angebot ausführlich dargelegt – bislang leider ohne den erhofften durchgreifenden Erfolg. Die Zahl der Anfragen und Beschwerden ging noch nicht nennenswert zurück.

Medizinischer Dienst der Krankenversicherung

Der Medizinische Dienst der Krankenversicherung (MDK) ist eine Körperschaft des öffentlichen Rechts, die an die Stelle des früheren vertrauensärztlichen Dienstes getreten ist. Er ist eine Arbeitsgemeinschaft der Krankenkassen, die Gutachter-, Beratungs- und Prüfungstätigkeiten ausübt. So hat der MDK u. a. die Aufgabe, bei der Feststellung der Pflegebedürftigkeit mitzuwirken, Vorschläge zur Sicherung des Heilerfolgs und zur Einleitung von Rehabilitationsmaßnahmen zu machen und Gutachten bei Zweifeln an der Arbeitsunfähigkeit zu erstatten.

www.schleswig-holstein.datenschutz.de
(Rubrik: weitere Materialien/Bekanntmachungen)

Was ist zu tun?
Krankenhausentlassungsberichte haben bei Krankenkassen grundsätzlich nichts verloren. Das Sozialministerium sollte darauf hinwirken, dass die gesetzlichen Krankenkassen Entlassungsberichte nicht mehr bei den Kliniken anfordern.

4.7.4 Wenn Handelsvertreter AOK-Mitglieder werben

Unter dem Titel AOK 2000 hat die AOK ein neues Verfahren zur Anwerbung von neuen Beitragszahlern und zur besseren Betreuung der Mitglieder eingeführt. Erst nach einer Vielzahl von Modifikationen war das Konzept datenschutzrechtlich nicht zu beanstanden.

Die AOK will bei der **Mitgliederwerbung und –betreuung** selbstständige Versicherungsvertreter einschalten. Hierauf sind wir sowohl bei eigenen Kontrollen als auch durch Beschwerden der Konkurrenz, die befürchtete, dass die AOK mit einem neuen Vertriebskonzept unzulässige Wettbewerbsvorteile erlangt, aufmerksam geworden. Legitimiert sei dieses Verfahren als **Datenverarbeitung**

im Auftrag, meinte die AOK. Diese rechtliche "Konstruktion" trägt jedoch nicht. Die Betreuung von Mitgliedern stellt keine Hilfstätigkeit im Bereich der Datenverarbeitung nach Weisung dar, sondern eine selbstständige und freie Arbeit mit einem völlig anderen Schwerpunkt.

Nach einer Vielzahl von Gesprächen, bei denen auch das zuständige Ministerium einbezogen war und in deren Verlauf von der AOK immer wieder neue Konzepte vorgelegt worden sind, wurde schließlich erreicht, dass den Versicherungsvertretern nur ein **reduzierter Datensatz** ohne sensible Angaben zur Verfügung gestellt und einer strengen Zweckbindung unterworfen wird. Sie sollen einer weitgehenden Aufsicht unterstellt und die AOK-Mitglieder in das Verfahren einbezogen werden. Ihnen bleibt die Wahlmöglichkeit einer direkten Betreuung durch die AOK offen. Durch die zugesicherten Vorkehrungen sahen wir keine akute Gefahr einer materiellen Beeinträchtigung des Sozialdatenschutzes.

Was ist zu tun?
Das neue Betreuungs- und Vermittlungskonzept der AOK steht und fällt mit der exakten Einhaltung der verabredeten Verfahrensregeln

4.7.5 Liderlicher Umgang mit dem Patientengeheimnis

Die Missachtung der ärztlichen Schweigepflicht in einigen öffentlichen Krankenhäusern ist eklatant. Manche Ärzte handeln unverantwortlich, und die Klinikleitungen drücken offenbar beide Augen zu.

- **Die Behandlungsverweigerung wegen fehlender Einwilligung in Forschung**

Als eine Frau in der Klinik für Kiefer- und Gesichtschirurgie an der Medizinischen Universität zu Lübeck behandelt werden wollte, forderte man sie auf, zuvor eine **Einwilligungserklärung** zur Nutzung ihrer Daten für "Zwecke der Lehre und Forschung" zu unterzeichnen. Als sie dies auch nach ärztlichem "Bedrängen" ablehnte, **verweigerte** man ihr die **Behandlung**. In ihrer Stellungnahme uns gegenüber meinte die Klinik, von Bedrängen könne keine Rede sein, sondern von einer ausführlichen "Aufklärung". Da ein Notfall nicht vorgelegen habe und kein Vertrauensverhältnis zu Stande gekommen sei, habe man der Patientin nahe gelegt, "von ihrer freien Arztwahl" Gebrauch zu machen. Es sei nun mal Aufgabe einer Universitätsklinik zu forschen und zu lehren; durch einen "falsch verstandenen Datenschutz" dürfe ihr nicht die Arbeitsgrundlage entzogen werden. Der Gipfel der Rechtsunkenntnis bestand darin, von der Petentin eine Entbindung der Schweigepflicht zu fordern, bevor man uns gegenüber überhaupt inhaltlich Stellung beziehen wollte.

Wir haben die Klinikleitung zusammen mit dem Rektor der Klinik darüber aufgeklärt, dass wir nicht nur berechtigt, sondern gesetzlich verpflichtet sind, im Rahmen der Datenschutzkontrolle Einblick in dem Patientengeheimnis unterliegende Unterlagen zu nehmen. Zweck einer Einwilligung ist, dass dem Patienten eine eigene Entscheidungsmöglichkeit eingeräumt wird. Es ist nicht

zulässig, eine medizinische Behandlung davon abhängig zu machen, dass der Patient sich für noch nicht bekannte Forschungsprojekte als **"Versuchskaninchen"** zur Verfügung stellt. Der Vorstand des Klinikums schloss sich unserer Ansicht an und informierte hierüber in einer internen Mitteilung alle behandelnden Ärzte.

- **Wo bleibt die gebotene Diskretion im Krankenhaus?**

Acht Tage lang konnte ein Petent in einem anderen Krankenhaus Erfahrungen mit der Beachtung des Patientengeheimnisses sammeln. Bereits in der **"Zentralen Aufnahme"** waren andere Patienten sowohl bei der Erfragung seiner Krankenvorgeschichte als auch bei den ersten Untersuchungen – u. a. im analen Bereich – in Hör- und Sichtweite. Bei der stationären Unterbringung in einem Zwei-Bettzimmer erfolgten viele weitere Untersuchungen, bei denen stets der Bettnachbar anwesend war, dem so ganz selbstverständlich die Untersuchungsergebnisse bekannt wurden. Umgekehrt konnte der Petent natürlich auch die Gespräche zwischen den Ärzten und seinem Bettnachbarn verfolgen. So erzählte ihm ein anderer Patient, der dies auf diesem Wege erfahren hatte, dass ein guter Bekannter an Krebs erkrankt sei und im gleichen Krankenhaus behandelt werde. Darauf angesprochen, zeigte sich dieser Bekannte wenig begeistert, dass seine Krankengeschichte "die Runde macht".

Ein Krankenhaus kann vielleicht nicht ein so verschwiegener Ort wie eine kleine Arztpraxis sein. Bei einer stationären Behandlung ist eine "völlige Abschottung" der Patienten- und ihrer Krankheitsdaten praktisch nicht möglich. Die Diskretion muss in jedem Fall aber für **sensible medizinische Informationen** ("Krebsdiagnose", "Untersuchung im analen Bereich") gelten, oder wenn der Patient zu erkennen gibt, eine Untersuchung und Gespräche unter "vier Augen" zu wünschen. Hierauf haben auch Patientinnen und Patienten Anspruch, die sich kein Einbettzimmer leisten können. Das Krankenhauspersonal darf nicht auf einen ausdrücklichen "Widerspruch" des Patienten warten.

Das betroffene Krankenhaus reagierte prompt. Patienten werden über ihre Rechte zukünftig schriftlich informiert. Zudem wurden Dienst- und Arztbesprechungen durchgeführt und eine Arbeitsgruppe eingerichtet, um weitere Verbesserungen bei der Wahrung des Patientengeheimnisses zu erreichen.

- **Privat-öffentliche Forschung einer Doktorandin**

Ein früherer Patient der Universitäts-Augenklinik, wollte zunächst seinen Ohren und dann seinen Augen nicht trauen. Er erhielt von der Klinik einen Telefonanruf, in dem ihm mitgeteilt wurde, es sei eine Untersuchung seiner Augen erforderlich. Wenig später erhielt er außerdem ein Schreiben mit privatem Briefkopf, in dem eine **Doktorandin** erneut bei ihm wegen eines Untersuchungstermins für ihre Promotion nachfragte. Er hatte gerade wenige Tage zuvor bei seinem Augenarzt diese – äußerst schmerzhafte – Untersuchung durchführen lassen. Auf die Rückfrage beim Klinikum, wie die Doktorandin an seine Daten gekommen sei, wurde erst nach vielen Monaten und mehrfacher Mahnung unbefriedigend reagiert.

Wir erhielten von der Klinik die kurze Mitteilung, dass die Doktorandin Studentin sei und ein offizielles Forschungsprojekt der Universitätsklinik durchführe. Sie gehöre, so die Klinik, zum Behandlungsteam des Klinikoberarztes als Funktionsnachfolger des ursprünglich behandelnden Arztes. Erst auf weitere Nachfrage – eineinhalb Jahre nach dem Vorfall – erhielten wir endlich eine präzise Darstellung des Vorgangs. In unserer **Beanstandung** haben wir der Klinik Folgendes ins Stammbuch geschrieben: Doktoranden gehören grundsätzlich nicht zum Behandlungsteam und dürfen daher keinen allgemeinen Zugang zu Daten ihrer "Doktorväter" für Forschungszwecke haben. Die Ansprache hätte nicht durch die Doktorandin, sondern durch die Klinik erfolgen müssen. Eine Datenweitergabe wäre erst zulässig gewesen, wenn von dem jeweiligen Patienten eine Einwilligung vorgelegen hätte.

- **Die verführerische Kraft von Klinik-Briefköpfen**

In einem anderen Fall wurden wir darauf hingewiesen, dass sich eine private Firma als Datenschutzbeauftragter von Universitätskliniken in Schleswig-Holstein betätige. Es könne nicht sein, "dass der Klinikdatenschutz von Unternehmen wahrgenommen werde, welche diese verantwortungsvolle Aufgabe an billige Hilfskräfte delegierten". Unsere Nachforschungen ergaben, dass zwar für Zweifel an der fachlichen Kompetenz der Datenschutzberatung keine Anhaltspunkte bestehen. Wohl war aber zu befürchten, dass Patienten und Klinikmitarbeiter sich vertrauensvoll an den **"Klinik-Datenschutzbeauftragten"** wenden würden in der Annahme, hierbei handele es sich um einen Mitarbeiter der Uni, dem Patientengeheimnisse unbesorgt anvertraut werden könnten. Diese Einschätzung wurde dadurch genährt, dass das Unternehmen mit dem Briefkopf des Klinikums und dem Zusatz "Der Datenschutzbeauftragte" firmierte.

Wir forderten das Klinikum auf, dafür zu sorgen, dass im öffentlichen Auftreten **eindeutig erkennbar** ist, dass die Datenschutzberatung durch ein privates externes Unternehmen erfolgt. Es wurde klargemacht, dass eine Offenbarung von Patientendaten gegenüber externen Dienstleistern nur nach vorheriger Einwilligung der Betroffenen zulässig ist. Schwerpunkt der Tätigkeit des externen Datenschutzbeauftragten solle daher die allgemeine Klinikberatung sein.

Was ist zu tun?
Bezüglich des Patientendatenschutzes steht nicht alles zum Besten. Dieser Bereich wird auch in Zukunft ein Schwerpunkt unserer Arbeit sein.

4.8 Schul- und Hochschulbereich

4.8.1 Wenn die Einschulungsuntersuchung zweckentfremdet wird

Die nach dem Schulgesetz vorgeschriebenen Einschulungsuntersuchungen dürfen nicht dazu genutzt werden, zusätzliche Informationen über die Kinder für wissenschaftliche Zwecke zu erheben.

Schülerinnern und Schüler werden vor der Einschulung durch das Gesundheitsamt auf ihre **Schulreife** hin untersucht. Die entsprechende Vorschrift im Schulgesetz

enthält klare Regelungen über den Zweck und den Umfang der Datenverarbeitung.

An einer Grundschule sollten mit dem so genannten "**Mannheimer Elternfragebogen**" zusätzliche personenbezogene Angaben über den Gesundheitszustand und das psychosomatische Verhalten von einzuschulenden Kindern erhoben werden. Der Fragebogen wurde den Eltern gemeinsam mit einem schulärztlichen Fragebogen vom zuständigen Gesundheitsamt übersandt, verbunden mit dem Hinweis, dass die Angaben in beiden Fragebögen freiwillig seien und der ärztlichen Schweigepflicht unterlägen. Was aus dem Begleitschreiben allerdings nicht hervorging, war die Tatsache, dass diese Datenerhebung im Rahmen des "Mannheimer Elternfragebogens" mit der Einschulungsuntersuchung gar nichts zu tun hatte und diese Angaben für **private Studienzwecke** vorgesehen waren. Zudem erfolgte entgegen den Regelungen des Landesdatenschutzgesetzes keinerlei Aufklärung über die weitere Verwendung der Daten. Nachdem wir auf die unzulässige Datenerhebung hingewiesen hatten, wurde das Vorhaben gestoppt und die bereits eingesammelten Fragebögen unverzüglich vernichtet.

Die Verknüpfung von wissenschaftlichen Untersuchungen mit den Einschulungsuntersuchungen sind nur dann datenschutzrechtlich zulässig, wenn eine **umfassende Aufklärung** der Eltern über die Identität der forschenden Einrichtung stattfindet, eine frühestmögliche Anonymisierung bzw. statistische Aufbereitung der erhobenen Daten erfolgt und das Bildungsministerium als oberste Schulaufsichtsbehörde die hierfür erforderliche Genehmigung erteilt hat.

Was ist zu tun?
Gesonderte Erhebungen im Zusammenhang mit gesetzlich vorgeschriebenen schulärztlichen Untersuchungen müssen eindeutig als solche gekennzeichnet werden.

4.8.2 Familiäre Lebensumstände im internationalen Vergleich

Internationale Studien an Schulen zum Bildungsstand der Schüler werfen datenschutzrechtliche Fragen auf. Sie müssen auf der Grundlage des Landesrechts geklärt werden.

Internationale Organisationen führen nach einem standardisierten mehrstufigen Verfahren weltweit in über 20 Staaten Studien zum Wissensstand der Schülerinnen und Schüler durch. Dabei geht es im Wesentlichen um Fragen der politischen Bildung, des Leseverständnisses sowie um die Bereiche der Mathematik und Naturwissenschaften. Die Studien sollen einen **internationalen Vergleich** hinsichtlich des **Bildungsstandes** ungefähr gleichaltriger Schülerinnen und Schüler ermöglichen. In der Bundesrepublik Deutschland werden diese Studien im Auftrag der Kultusministerkonferenz von einem Berliner Institut durchgeführt und zentral organisiert.

Auch in Schleswig-Holstein sollten einige ausgewählte Schulen beteiligt werden. Als sich das Bildungsministerium als zuständige Genehmigungsbehörde an uns

wandte, war es bereits **“fünf vor zwölf”**. Wegen des weltweit zeitgleichen Ablaufs hätte innerhalb von wenigen Tagen das umfangreiche Material gesichtet und eine datenschutzrechtliche Stellungnahme erarbeitet werden müssen. Schon bei einer ersten Durchsicht der Unterlagen stellte sich heraus, dass zum Teil recht sensible Informationen aus dem privaten Bereich der Schülerinnen und Schüler sowie deren Eltern erfragt werden sollten. Von Interesse sollte nicht nur sein, ob die Schüler ein eigenes Zimmer und einen eigenen Fernseher hatten, wie viele Bücher im Haus vorhanden waren oder wie der Haushalt sonst ausgestattet war, sondern auch, welche berufliche Stellung die Eltern hatten und wie die Erziehungsmethoden waren. Ganz ähnliche Daten wurden mit einem speziellen Fragebogen auch von den Eltern erhoben.

Das beauftragte Institut hatte vorher den beteiligten Länderministerien versichert, dass sämtliche datenschutzrechtlichen Vorgaben erfüllt seien. Die Landesdatenschutzbeauftragten verständigten sich kurzfristig auf eine gemeinsame Stellungnahme. Die **Elternanschreiben** waren in erheblicher Weise umzugestalten. Weiterhin war zu rügen, dass in den Fragebögen nicht in ausreichender Weise auf die Freiwilligkeit der Teilnahme hingewiesen wurde und dass sie den Anforderungen an die erforderliche Aufklärung nicht genügten.

Was ist zu tun?
Vor der Genehmigung von Forschungsvorhaben, die eine Erhebung sensibler Daten aus dem Familienleben beinhalten, sollte sich das Ministerium frühzeitig über alle relevanten datenschutzrechtlichen Aspekte informieren.

4.8.3 Der NDR misstraut Studenten

Bedienen sich Rundfunkanstalten bei der Entscheidung, ob Rundfunkteilnehmer von der Gebührenpflicht befreit werden können, der Hilfe von Sozialämtern, so unterliegt die Datenverarbeitung bei den Sozialämtern den Regelungen des Landesdatenschutzgesetzes. Es dürfen nur Daten erhoben werden, die zur Feststellung der Befreiungsvoraussetzungen erforderlich sind.

Personen mit geringem Einkommen können auf Antrag von der Rundfunkgebührenpflicht befreit werden. Die Möglichkeit zur Befreiung besteht regelmäßig, wenn das Einkommen den eineinhalbfachen Sozialhilferegelsatz plus Kaltmiete nicht überschreitet. Insbesondere Rentner, **Studierende** und Arbeitslosenhilfeempfänger nutzen diese Möglichkeit. Antragsunterlagen sind auch in den **Sozialämtern** zu erhalten. Die Anträge werden auch dort geprüft und unter Umständen positiv beschieden.

Der NDR verlangt nun von Studierenden zusätzlich Daten auf einem **besonderen Fragebogen**. Darin werden detailliert Fragen zum Einkommen und zu den Ausgaben gestellt. Verlangt werden u. a. Angaben über Heiz- und Stromkosten, Versicherungsbeiträge verschiedenster Art, Sparprämien, Telefon- und Handygebühren, Kabel- und Internetgebühren, Fahrtkosten, Studiengebühren und –material sowie Kosten für die Unterhaltung eines Pkw. Diese Ausgaben sollen

durch die Vorlage von Belegen (“letzte Telefonrechnung?”) nachgewiesen werden. Nicht-Studierende müssen den Fragebogen nicht ausfüllen. Sinn der vielen Fragen ist es, die Glaubwürdigkeit der Angaben zu “prüfen”. Verlässt man sich bei anderen Antragstellern darauf, dass diese mit dem angegebenen Einkommen “leben können”, so wird dies bei Studenten pauschal bezweifelt. Der NDR vermutet wohl, dass Studierende, die im Internet nach Informationen surfen, eine hohe Telefonrechnung oder gar ein Auto haben, Einkommen verschweigen. Diese müssen damit rechnen, dass ihr Antrag wegen “Unglaubwürdigkeit der Angaben” abgelehnt wird.

Problematisch ist der Umstand, dass neben dem NDR und der GEZ auch das Sozialamt einen tiefen Einblick in die Haushaltskasse der Studenten erhält. Die Zweckmäßigkeitserwägungen des NDR ersetzen nicht die **Notwendigkeit** einer **rechtlichen** Befugnis zur Datenerhebung in diesem Umfang. Die Befreiungsverordnung definiert abschließend, welche Rundfunkteilnehmer unter welchen Voraussetzungen von der Rundfunkgebührenpflicht befreit werden können. Sie fordert von den Antragstellern den Nachweis der Unterkunftskosten (ohne Strom- und Heizkosten) und gundsätzlich nicht mehr. Eine Sonderbehandlung für Studierende sieht sie nicht vor. Von diesen kann nicht verlangt werden, dass sie ihre Ausgaben “auf Heller und Pfennig” beim NDR nachweisen.

www.schleswig-holstein.datenschutz.de
(Rubrik: weitere Materialien/Arbeitspapiere)

Inzwischen hat der NDR signalisiert, dass der Fragebogen überarbeitet werden soll.

Was ist zu tun?
Der Fragebogen für Studierende ist auf jene Fragen zu beschränken, die nach der Befreiungsverordnung erforderlich sind, um über den Befreiungsantrag entscheiden zu können.

4.9 Steuerverwaltung

4.9.1 Dickhäuter in den Finanzämtern

Strikte Anweisungen der vorgesetzten Behörden werden ignoriert. Türen von unbesetzten Büros sind nicht verschlossen. EDV-Systeme werden nicht abgeschaltet, bevor die Benutzer den Raum verlassen. Reinigungspersonal von Fremdfirmen wird nicht beaufsichtigt. Sollte dies alles mit dem Steuergeheimnis vereinbar sein?

Wie ein roter Faden zieht sich das Problem des fahrlässigen Umgangs mit dem Gebot der **Vertraulichkeit von Akten** und sonstigen Unterlagen der Verwaltung durch die nunmehr über 20-jährige Datenschutzgeschichte unseres Landes. Es gibt wohl keinen Tätigkeitsbericht, in dem wir nicht über exemplarische Fälle berichtet haben. Auch die Medien greifen in schöner Regelmäßigkeit die Skandale

und Skandälchen auf. Mal findet man medizinische Unterlagen in verlassenen Kellern oder anderen frei zugänglichen Räumen, ein anderes Mal vergisst eine Bank zum Verkauf stehende Schreibtische leer zu machen; Papierschrott mit höchst sensiblem Inhalt in Mülltonnen ist ein "Dauerbrenner". Wenn derartige Dinge ruchbar werden, stehen die Verantwortlichen meist mit "roten Ohren" da, suchen nach Endschuldigungen und geloben Besserung.

So geschehen auch im Jahr 1992, als wir in mehreren Finanzämtern erhebliche Sicherheitsmängel feststellten, die dem Gebot, das Steuergeheimnis zu wahren, diametral entgegenstanden (vgl. 17. TB, Tz. 4.5.1). Drei Jahre dauerte es, bis der **Finanzminister** die Verwaltung anwies,

- Steuerakten nur in verschlossenen Räumen bzw. in abgeschlossenen Schränken zu lagern,
- Reinigungspersonal, Handwerker, Techniker usw. von Fremdfirmen nicht unbeaufsichtigt im Kontakt mit steuerlichen Unterlagen kommen zu lassen,
- über den Verbleib von Steuerakten, die an andere Stellen weitergegeben werden, Buch zu führen und
- Außendienstmitarbeiter in die Lage zu versetzen, Steuerakten im häuslichen Bereich und unterwegs in verschlossenen Behältnissen zu verwahren.

Dies sind alles sinnvolle Regelungen, die wegen ihrer Eindeutigkeit keine größeren Auslegungsspielräume zulassen. Deshalb waren wir erstaunt, dass wir im letzten Jahr in einem Finanzamt gleichwohl eine für **jedermann zugängliche "Aktenzentrale"** vorfanden, weil angeblich kein Geld für Schlüssel vorhanden war. Den Zustand haben wir bereits in unserem 21. Tätigkeitsbericht mit deutlichen Worten beanstandet (Tz. 4.10.4).

Wer nun glaubt, es habe daraufhin von der Oberfinanzdirektion bzw. dem Finanzministerium ein "Donnerwetter" gegeben und in allen Finanzämtern seien die Sicherheitsdefizite schleunigst abgestellt worden, der irrt. Erneute Kontrollen im abgelaufenen Berichtszeitraum haben Ergebnisse erbracht, die man sarkastisch kommentieren kann mit den Worten: "Die haben Nerven, die Finanzamtsvorsteher!" Dass während der Öffnungszeiten für den Publikumsverkehr unbesetzte Räume nicht verschlossen waren (selbst ein stellvertretender Vorsteher vergaß abzuschließen), dass Akten auf den Böcken und Schreibtischen nach Dienstschluss offen herumlagen, dass die PC nicht abgeschaltet waren, obwohl sich kein Sachbearbeiter im Raum befand usw., wurde von der Leitungsebene stets mit "**menschlichem Versagen**" entschuldigt und eine strenge Ermahnung der Betroffenen angekündigt.

Einige der ach so entrüsteten Vorsteher sitzen aber selbst im Glashaus. Sie lassen es nämlich entgegen den Weisungen des Finanzministeriums und der Oberfinanzdirektion nach wie vor zu, dass das **Reinigungspersonal** von Fremdfirmen völlig **unbeaufsichtigt** seiner Arbeit nachgeht und somit in den Aktenzentralen hunderttausende von Steuerakten einsehen kann. Lediglich als "Steuergeheimnis-Feigenblatt" dient die Zusicherung der Reinigungsunternehmen, ihre Bediensteten seien vergattert worden, nichts

anzufassen oder zur Kenntnis zu nehmen. Es klingt schon fast wie Hohn, einerseits vom Steuergeheimnis als einem qualifizierten Amtsgeheimnis zu sprechen (so die gängigen Kommentare zur Abgabenordnung) und andererseits namentlich völlig unbekannten und nahezu täglich wechselnden Personen den Schlüssel für eine Außenstelle eines Finanzamtes zu geben mit der Maßgabe, wieder abzuschließen, wenn man das Gebäude verlässt. Auch das Argument, dass bisher noch nichts passiert sei, geht ins Leere. Oder haben die Verantwortlichen schon vergessen, dass vor einigen Jahren unter Ausnutzung von Sicherheitsmängeln Steuerakten gestohlen worden sind (vgl. 18. TB, Tz. 4.10.2)?

Was ist zu tun?
Nachdem sich herausgestellt hat, dass schriftliche Weisungen allein nicht fruchten, muss sich die Finanzverwaltung endlich etwas einfallen lassen, damit das Steuergeheimnis wirksam geschützt wird.

4.9.2 FISCUS wird datenschutzrechtlich durchleuchtet

Bisher haben die 16 Bundesländer bezüglich der Gestaltung der automatisierten Verfahren zur Festsetzung und Erhebung von Steuern jeweils ihre "eigene Suppe gekocht". Unter der Bezeichnung FISCUS wird nunmehr ein bundesweiter Verbund angestrebt. Auch die datenschutzrechtliche Begutachtung bedarf der Koordinierung.

> **?** ***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.*

Die Steuerverwaltung ist seit über 30 Jahren einer der Vorreiter der automatisierten Datenverarbeitung in der öffentlichen Verwaltung. Nicht nur die große Zahl der zu bearbeitenden Fälle, sondern auch die Komplexität des Steuerrechts haben den IT-Einsatz zu einem unverzichtbaren Bestandteil des Verwaltungshandelns gemacht. Obwohl diese Ausgangslage in allen Bundesländern in gleicher Weise gegeben ist, ließ jedes Finanzministerium seine Software von eigenen Programmierern entwickeln und betreibt **unterschiedlich konzipierte Computersysteme**. In Schleswig-Holstein stehen deshalb ca. 150 hoch qualifizierte Fachleute auf der Gehaltsliste des Bereiches "Automation" der Oberfinanzdirektion. Es könnte sehr viel Geld und Personal eingespart werden, wenn man sich bereits von Anfang an, wie z. B. in der Statistikverwaltung und bei den gesetzlichen Krankenkassen, auf eine Verbundprogrammierung und eine einheitliche "IT-Welt" geeinigt hätte.

Diese Auswirkungen des Föderalismus sind natürlich auch den Finanzministern bekannt. Man hat deshalb im Jahr 1994 ein "**Verwaltungsabkommen** zur Zusammenarbeit des Bundes und der Länder auf dem Gebiet der Automationsunterstützung im Besteuerungsverfahren" abgeschlossen. Darin sind

eine Vielzahl von datenschutzrechtlich und sicherheitstechnisch bedeutenden Festlegungen getroffen worden:

- Ausdehnung der DV-Verfahren auf neue, bisher noch nicht automatisierte Bereiche (Vollstreckung, Betriebsprüfung, Steuerfahndung),
- Erweiterung des DV-Mengengerüstes (Vergrößerung der Speichermenge und Speicherdauer je Fall),
- Dezentralisierung der Datenverarbeitung,
- "ganzheitliche" Fallbearbeitung,
- Gestaltungsfreiheit der Arbeitsabläufe,
- papierarme Bearbeitung,
- Wiederverwendung gespeicherter Daten,
- landesweite Vernetzung sowie
- länderübergreifender Datenaustausch.

Vereinbart wurde, dass ab 1995 bundesweit zusätzlich 120 Entwickler in den Ländern und 30 Personen in der Koordinierungsstelle beim Bund mit der Planung und Realisierung befasst sein sollen. Das Gesamtprojekt sollte **bis zum Jahr 2006** realisiert sein. Zwischenzeitlich ist man mit dem Zeitplan jedoch offenbar etwa zwei Jahre in Verzug geraten.

Der Arbeitskreis "Steuer" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die Entwicklung von Anfang an sorgfältig beobachtet. Da sich die FISCUS-Projektgruppen bis vor ca. einem Jahr im Wesentlichen mit Koordinierungs- und Konzeptionsfragen befasst haben, bestand noch keine Möglichkeit für eine unmittelbare datenschutzrechtliche und sicherheitstechnische Begutachtung. Nunmehr steht der "Echteinsatz" der ersten FISCUS-Module aber direkt bevor. Deshalb ist durch den Arbeitskreis "Technik" eine **spezielle Arbeitsgruppe** eingerichtet worden. Die Federführung wurde uns angetragen. Welcher Umfang an Arbeit auf diese Gruppe zukommt, wird daran deutlich, dass allein der Entwurf der allgemeinen "Security Policy" des Projektes FISCUS 70 Seiten umfasst; hinzu kommen die Unterlagen zu den Teilprojekten. Über die Oberfinanzdirektion Kiel sind zwischenzeitlich Kontakte zur Projektleitung beim Bundesfinanzministerium aufgenommen wurden. Auch dort wird eine kritisch-konstruktive Zusammenarbeit für sinnvoll erachtet.

4.9.3 Brechen jetzt die Dämme?

Bisher bekommen auf Grund des Steuergeheimnisses mit Ausnahme der Steuerpflichtigen nur wenige Mitarbeiter der Finanzämter bzw. der Oberfinanzdirektion den Inhalt eines Steuerbescheides zu Gesicht. Aus Gründen der Kostenreduzierung soll dieser Kreis auf Mitarbeiter der Datenzentrale ausgedehnt werden. Dies könnte der Anfang eines umfangreichen Outsourcing sein.

Es kommt nicht eben häufig vor, dass wir in einem Tätigkeitsbericht berichten können, eine Angelegenheit sei nach schwierigen Verhandlungen nunmehr in "trockenen Datenschutztüchern". Eine solche Erfolgsmeldung enthält der Tätigkeitsbericht aus dem Jahr 1997 (vgl. 20. TB, Tz. 4.10.1). Nachdem 20 Jahre lang die Rechenzentren der Datenzentrale und der Oberfinanzdirektion aus Gründen der Wahrung des Steuergeheimnisses getrennt betrieben worden waren, erfolgte 1997 aus Kostengründen eine Zusammenlegung. Zu entscheiden war damals die Frage, ob es mit dem Steuergeheimnis zu vereinbaren gewesen wäre, wenn nach der Bildung des Gemeinschaftsrechenzentrums Mitarbeiter der Datenzentrale Einblick in die Inhalte von Steuerbescheiden hätten nehmen können. Man entschied sich im Finanzministerium, offenbar nicht zuletzt wegen eines eindeutigen Votums des Finanzausschusses (vgl. Protokoll der 34. Sitzung von Mai 1997), für eine organisatorische Trennung dergestalt, dass im Hause der Datenzentrale Mitarbeiter der Oberfinanzdirektion den Druck, die Kuvertierung und die Versendung der steuerlichen Unterlagen vorzunehmen haben. Wir haben diese Entscheidung begrüßt, da unseres Erachtens rein ökonomische Gründe ein Aufweichen des Steuergeheimnisses nicht rechtfertigen.

Zwischenzeitlich ist eine weitere Rechenzentrums-Konzentration vollzogen worden. Um einen Kostenvorteil von erhofften insgesamt ca. 7 Mio. DM zu realisieren, haben die Länder Hamburg und Schleswig-Holstein sich darauf verständigt, die hamburgischen Rechnersysteme gemeinsam zu nutzen und in Altenholz ein überregionales Druck- und Nachbereitungszentrum einzurichten. Ein geringer, bislang nicht bezifferter Anteil des vorgenannten Einsparpotenzials soll dadurch erwirtschaftet werden, dass die bisherige **organisatorische Trennung** zwischen dem Bereich "Steuerdaten" und den anderen Bereichen nun doch **aufgehoben** wird. Man glaubt, dadurch Personal und Maschinen effektiver einsetzen zu können.

> ***§ 30 Abs. 4 Nr. 1 Abgabenordnung*** *(sinngemäß)*
>
> *Die Offenbarung von Verhältnissen eines Steuerpflichtigen ist zulässig, soweit sie der Durchführung eines Verwaltungsverfahrens in Steuersachen dient.*

Da sich das geltende Recht nicht geändert hat, bedarf es zur Rechtfertigung dieser neuen Verfahrensweise einer **neuen Interpretation** der gesetzlichen Tatbestände zum Steuergeheimnis. Mit anderen Worten: Man muss die bisherige juristische Auslegung des geltenden Rechts als falsch deklarieren. Dies bereitet dem Finanzministerium offensichtlich Schwierigkeiten, denn, obwohl die Verwaltungsabkommen zwischen Hamburg und Schleswig-Holstein bereits im Juli 1999 unterzeichnet worden sind, lag bis zum Redaktionsschluss dieses Tätigkeitsberichtes noch keine endgültige Entscheidung vor. Vieles deutet aber darauf hin, dass man sich auf den (neuen) Standpunkt stellen will, dass die "Offenbarung" der steuerlichen Verhältnisse für die Durchführung des Besteuerungsverfahrens nützlich ist; damit seien die Voraussetzungen für die Ausnahmeregelung im § 30 Abs. 4 Nr. 1 erfüllt.

Dieses wäre im Vergleich zu der in der Vergangenheit restriktiven Auslegung der Steuergeheimnisvorschriften ein völlig neuer Standpunkt. Man bedenke: Das

Finanzerwaltungsgesetz fordert für die Schaffung von Rechenzentren der Steuerverwaltungs-internen Rechenzentren und deren Einbindung in das Besteuerungsverfahren eine Rechtsgrundlage in Form einer Rechtsverordnung der Landesregierung. Die Beauftragung eines nicht der Steuerverwaltung zuzurechnenden externen **Dienstleisters als "Unterauftragnehmer"** soll dagegen nun ohne weiteres möglich sein, weil der dadurch erwartete Kostenvorteil dem Besteuerungsverfahren "dient".

Vielleicht bleiben diese Überlegungen hypothetisch. Wir sehen uns aber veranlasst, deutlich auf die Konsequenzen hinzuweisen, die eine solche Neuinterpretation des Steuergeheimnisses nach sich ziehen würde: Seine Funktion als Schutzvorschrift zur Wahrung der Interessen der steuerzahlungspflichtigen Bürgerinnen und Bürger dürfte immer dann eingeschränkt werden, wenn es darum geht, den finanziellen Aufwand bei der Festsetzung und Erhebung von Steuern zu reduzieren. Ein so "**verschlanktes**" **Steuergeheimnis** ließe es auch zu, in vielen anderen Bereichen des Besteuerungsverfahrens die wirtschaftlichen Vorteile des "Outsourcing" zu nutzen (vielleicht sogar Call-Center, Fernadministrationen, externes Factoring, freiberufliche Mitarbeit von Wirtschaftsprüfern?). Eine Verschwiegenheitsverpflichtung nach dem Verpflichtungsgesetz ist schnell unterschrieben.

Was ist zu tun?
Nach den jahrelangen Diskussionen über die vielfältigen finanziellen "Sachzwänge" sollte die Grundsatzfrage, ob das Steuergeheimnis Geld kosten darf oder nicht, entschieden werden. Es wäre sicher hilfreich, wenn der Finanzausschuss des neuen Landtages sich das Votum aus der 14. Legislaturperiode zu Eigen machen würde.

4.10 Personalwesen

4.10.1 Abschottung der Beihilfedaten unverzichtbar

Die notwendige organisatorische und personelle Abschottung von Beihilfedaten erfordert einen gewissen Aufwand. Als Alternative bietet sich eine Übertragung der Aufgaben auf die Versorgungsausgleichskasse an.

Bei der **Beihilfebearbeitung** ist bezüglich der Vertraulichkeit der Daten ein besonderer Maßstab anzulegen. Da die Gefahr der bewussten oder unbewussten Beeinflussung von Personalentscheidungen durch die Kenntnis von sensiblen Krankheitsdaten ungleich höher ist als bei anderen Verwaltungsverfahren, ist im Beamtenrecht neben dem ausdrücklichen Zweckbindungsgebot auch eine räumliche, organisatorische

Im Wortlaut:
§ 106 b Satz 1 – 3 Landesbeamtengesetz

Unterlagen über Beihilfen sind stets als Teilakte zu führen. Diese ist von der übrigen Personalakte getrennt aufzubewahren. Sie soll in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden; Zugang sollen nur Beschäftigte dieser Organisationseinheit haben.

und personelle Trennung dieser Aufgaben von der übrigen Personalverwaltung vorgeschrieben. Damit eine ausreichende Abschottung dieser Aufgaben auch im kommunalen Bereich gewährleistet werden kann, hat der Gesetzgeber die Möglichkeit eröffnet, Beihilfeangelegenheiten zur selbstständigen Erledigung auf die Versorgungsausgleichskasse zu übertragen.

Für uns stellte sich im Rahmen einer Prüfung nun die Frage, ob z. B. eine **kreisangehörige Stadt** in der Lage ist, die Beihilfeaufgaben selbst wahrzunehmen bzw. unter Beteiligung einer Kreisbesoldungsstelle im Wege der Auftragsdatenverarbeitung so zu gestalten, dass dabei ausreichende datenschutzrechtliche Standards gewährleistet sind. Das Ergebnis unserer Prüfung spricht für sich: die Stadt ist inzwischen der Versorgungsausgleichskasse beigetreten. Die Gründe: Die Stadt hatte zwar die Beihilfebearbeitung auf den Standesbeamten übertragen und damit diese Aufgabe aus der allgemeinen Personalverwaltung herausgelöst. Dabei hatte sie es jedoch versäumt, auch für eine **Vertretungsregelung** zu sorgen, was dazu führte, dass weiterhin ca. 20 bis 25 Prozent aller Fälle von Mitarbeitern der Personalverwaltung zu bearbeiten waren. Sonstige Organisationsregelungen zur Abschottung der Beihilfe fehlten.

Auch die Einschaltung der **Kreisbesoldungsstelle** konnte nicht zur Lösung der anstehenden Probleme beitragen. Bei der Auftragsdatenverarbeitung bleibt die Stadt als Auftraggeberin immer für die Rechtmäßigkeit der Aufgabenerfüllung sowie für die Einhaltung der Vorschriften über den Datenschutz verantwortlich. Die auftragnehmende Stelle ist im Gegenzug strikt weisungsgebunden, was z. B. dazu führt, dass dort keine selbstständige Führung von Personalakten möglich ist. Eine weitergehende Aufgabenübertragung wie bei der Versorgungsausgleichskasse ist hier wegen fehlender gesetzlicher Grundlagen nicht möglich.

Im Wortlaut:
§ 2 Abs. 3 Nr. 3 des Gesetzes über die Versorgungsausgleichskasse der Kommunalverbände

Die Versorgungsausgleichskasse kann ferner Beihilfen in Krankheits-, Geburts- und Todesfällen und freie Heilfürsorge nach den beamtenrechtlichen Vorschriften oder den ihnen entsprechenden Regelungen an Mitarbeiterinnen und Mitarbeiter und an Versorgungsempfängerinnen und Versorgungsempfänger gewähren, sofern das Mitglied oder die Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts, für die die Versorgungsausgleichskasse auftragsweise tätig wird, dies beantragt.

Da nur bei der Bearbeitung, nicht aber bei der Verantwortlichkeit für die Aufgabenerfüllung eine Hilfestellung durch die Kreisbesoldungsstelle möglich war, hätte eine Organisationsregelung für die notwendige Abschottung bei der Stadt folgende Fragen beantworten müssen:

- Wer soll für die Erteilung der Beihilfebescheide verantwortlich sein?
- Wer soll die kassentechnische Umsetzung vornehmen?
- Auf welche Weise soll eine ausreichende Vertretung für die Aufgabenwahrnehmung gewährleistet werden?

- In wessen Zuständigkeit soll die Bearbeitung von Beschwerden und Widerspruchsangelegenheiten fallen?

Zu einer befriedigenden Regelung sah sich die Stadt nicht in der Lage. Wir begrüßten daher die Aufgabenübertragung auf die **Versorgungsausgleichskasse** als die beste Lösung des Problems. Eine Kenntnisnahme von Beihilfedaten durch Mitarbeiter der Stadt kann dadurch gänzlich ausgeschlossen werden.

Was ist zu tun?
Kommunen, die hinsichtlich der Beihilfebearbeitung noch nicht der Versorgungsausgleichskasse angeschlossen sind, sollten prüfen, ob sie tatsächlich in der Lage sind, die notwendigen datenschutzrechtlichen Standards selbst zu erfüllen.

4.10.2 Potenzialanalysen für Führungskräfte nur auf freiwilliger Basis

Methoden des Personalmanagements sollen als neue Steuerungsinstrumente in der Landesverwaltung eingeführt werden. Eines davon ist das Personalentwicklungskonzept. Bei seiner Realisierung kommt es aus Datenschutzsicht entscheidend auf die Einwilligung der Betroffenen an.

Ein wesentliches Element des Personalentwicklungskonzeptes ist die "Personalentwicklung für Führungskräfte", in deren Rahmen eine **"Potenzialanalyse"** (vgl. 21. TB, Tz. 4.11.1) durchgeführt wird. Diese dient der Förderung der Fähigkeiten von Führungskräften und der Erkundung und Bewertung von Führungspotenzialen bei Nachwuchskräften. Zentrales Instument hierfür ist die ressortübergreifende Durchführung von Personalentwicklungsseminaren, an deren Ende für den Teilnehmer ein individueller Förderplan erstellt wird, der ihm die Wahrnehmung bestimmter Personalentwicklungsmaßnahmen empfiehlt. Nach Anlaufen dieser Teilkomponenten soll ein **Controlling** installiert werden, um zu klären, ob die inhaltlichen und verfahrensbezogenen Ziele der Potenzialanalyse erreicht werden und auf welche Akzeptanz diese Maßnahmen stoßen. Daneben sollen Struktur und Qualität der individuell empfohlenen Fördermaßnahmen und nicht zuletzt auch die Wirtschaftlichkeit der gesamten Maßnahme überprüft werden.

Im Rahmen der Durchführung der Potenzialanalyse kommt es zwangsläufig zur Verarbeitung von personenbezogenen Daten der Mitarbeiterinnen und Mitarbeiter. Die Auswahl der Teilnehmer der **Personalentwicklungsseminare** soll nach dem Prinzip der Bestenauslese unter Heranziehung verschiedener Befähigungsmerkmale in den dienstlichen Beurteilungen und dem Ergebnis der Leistungsbeurteilung erfolgen. Als Erkenntnisquellen sollen u.a. Beurteilungen, Ergebnisse aus den Personalentwicklungsseminaren, Bewertungen der Projektarbeit, die Meldung über absolvierte Fortbildungen sowie eine Selbsteinschätzung der Betroffenen herangezogen werden.

Wir haben darauf hingewiesen, dass sowohl der Zugang zu Personalakten innerhalb des Ressorts als auch die Auskunftserteilung an ressortfremde

Mitarbeiter oder private Dritte an präzise gesetzliche Voraussetzungen geknüpft ist. Die vorgesehene Verarbeitung der Personalaktendaten durch **externe Berater und ressortfremde Mitarbeiter** war damit nicht vereinbart. Da die Potenzialanalyse nun als reines Förderinstrument und nicht als Auswahlinstrument angesehen und als "Gewinner/Gewinner-Modell" ausgestaltet wird, setzt dies eine **Teilnahme auf rein freiwilliger Basis** voraus, ohne dass bei einer Nichtteilnahme mit negativen Folgen in der weiteren beruflichen Entwicklung gerechnet werden muss. Ein Zusammenhang mit Auswahlentscheidungen besteht nur insofern, als die Bewerber sich auf Grund der gewonnenen Erkenntnisse aus der Potenzialanalyse gezielt weiterqualifizieren können und sich dies vermutlich positiv in späteren Regel- oder Anlassbeurteilungen niederschlagen wird.

Bereits vor Einreichung der Bewerbung zur Potenzialanalyse müssen die Betroffenen über die beabsichtigte Datenverarbeitung, insbesondere über die Weitergabe ihrer Daten an externe Berater, aufgeklärt werden, damit von vorneherein und unmissverständlich deutlich wird, welche Aspekte die Einwilligung abdecken soll. Diese **Vorschläge** sind von der Staatskanzlei sowohl in das Umsetzungskonzept als auch in das gesondert erstellte Controlling-Konzept **übernommen** worden.

Was ist zu tun?
Vor Einreichung einer Bewerbung zur Durchführung einer Potenzialanalyse müssen die Betroffenen über das Verfahren und die Konsequenzen aufgeklärt werden.

4.11 Sonstiges

Neue Aktenordnung der Landesverwaltung mit Mängeln

Das Innenminsterium sah sich auf Grund der Kritik des Landesrechnungshofes veranlasst, die Aktenordnung für die gesamte Landesverwaltung zu überarbeiten, um die Schriftgutverwaltung auf diesem Wege wirtschaftlicher zu gestalten. Leider ist es dabei zu einigen missverständlichen Formulierungen und Widersprüchen zu gesetzlichen Vorschriften gekommen.

Der Entwurf für die neue Aktenordnung wurde uns bereits im **September 1997** mit der Bitte um Stellungnahme übersandt. Wir kamen dieser Bitte nach und äußerten uns damals ausführlich zu Fragen der Schriftgutverwaltung, der Aufbewahrung von Altschriftgut sowie dessen Aussonderung, der Andienung an das Landesarchiv und der Vernichtung. Wir haben **konkrete Änderungsvorschläge** formuliert. Da die Modalitäten der Aktenvernichtung durch beauftragte Firmen sehr komplexe datenschutzrechtliche Fragen aufwarfen, wurde hierzu eine gesonderte Kontaktaufnahme und Bearbeitung vorgeschlagen. Etwa eineinhalb Jahre später wurde im Amtsblatt (1999, S. 260) die neue "Aktenordnung für die schleswig-holsteinische Landesverwaltung (AktenO)" als Erlass veröffentlicht. Darin finden sich zwar eine ganze Reihe unserer Vorschläge

wieder, bedauerlicherweise wurden dafür aber andere wichtige Anmerkungen nicht berücksichtigt. Eine nähere Regelung der Aktenvernichtung erfolgte nicht.

Bezüglich der weiteren Behandlung der vom **Landesarchiv** übernommenen Unterlagen hatten wir vergeblich auf die einschlägigen gesetzlichen Vorschriften hingewiesen. So sollen die abgebenden Dienststellen laut Aktenordnung jederzeit berechtigt sein, ihr dem Landesarchiv übergebenes Schriftgut einzusehen oder zu entleihen, obwohl das Landesarchivgesetz deren Nutzung nur noch eingeschränkt erlaubt. Das Landesarchiv soll außerdem die Zustimmung der abliefernden Dienststelle einholen müssen, bevor es übernommenes Schriftgut vernichtet. Diese Regelung widerspricht ebenfalls dem Gesetz, wonach Unterlagen, bei denen die Voraussetzungen für die Archivwürdigkeit nicht oder nicht mehr vorliegen, zu vernichten sind, soweit nicht die abgebende Stelle erklärt, dass die Voraussetzungen für eine Sperrung an Stelle der Löschung vorliegen. Die Verantwortung für die Vernichtung liegt allein beim Landesarchiv.

Die Aktenordnung stimmt außerdem mit einigen Passagen des neuen **LDSG** (vgl. Tz. 1.1) nicht überein. Dieses sieht z. B. eine Ordnung der Vorgänge auch nach Personenbezügen vor und trägt damit neben den datenschutzrechtlichen Belangen auch denen des neuen Informationsfreiheitsgesetzes Rechnung. Darauf hatten wir den Innenminister vergeblich hingewiesen. Jetzt wird es notwendig sein, die neue Aktenordnung schon bald wieder zu ändern.

Was ist zu tun?
Bei der Anwendung der Aktenordnung ist zu beachten, dass gesetzliche Vorschriften vorrangig bleiben, auch wenn die Aktenordnung abweichende Regelungen vorsieht.

4.12 Angekündigte Unangekündigte Kontrollen (AUK)

Auch in diesem Jahr zeigen die Ergebnisse der Angekündigten Unangekündigten Kontrollen, dass in den Verwaltungen des Landes weiterhin Mängel im Umgang mit personenbezogenen Daten bestehen. Dabei verlagert sich der Schwerpunkt von der konventionellen auf die elektronische Datenverarbeitung.

Wie in den Vorjahren hatten wir wieder 50 Behörden am Jahresbeginn schriftlich "vorgewarnt" und davon im Laufe des Berichtsjahrs acht tatsächlich unangemeldet überprüft (zum Konzept vgl. 19. TB, Tz. 1.1). Im Verlaufe dieser Prüfungen konnten wir feststellen, dass sich die Sensibilität der Mitarbeiterinnen und Mitarbeiter in den öffentlichen Verwaltungen hinsichtlich der "äußeren" Datensicherheit zumindest im **konventionellen Bereich** deutlich erhöht hat. So erfahren unsere Prüfer durch Gespräche oder auf Grund eigener Feststellungen vor Ort, dass es immer selbstverständlicher wird, bei kurzfristigem Verlassen der Büros die Türen abzusperren oder nach Dienstschluss alle Vorgänge in den Schränken wegzuschließen. Im Vergleich zu den vorangegangenen Jahren fanden sich bei unseren unangemeldeten Rundgängen durch die Verwaltungsgebäude nur relativ selten offen stehende und unbesetzte Büros. Auch das alte Mobiliar in den

Büroräumen, welches eine verschlossene Aufbewahrung personenbezogener Daten gar nicht ermöglichte, verschwindet mehr und mehr und wird gegen abschließbare Schränke o. Ä. ausgetauscht.

Im **EDV-Bereich** scheinen viele Verwaltungsleitungen aber darauf zu vertrauen, dass ihre Mitarbeiterinnen und Mitarbeiter intuitiv wissen, wie eine ausreichend sichere Datenverarbeitung zu gestalten ist. In den wenigsten Fällen gab es Dienstanweisungen, die den Beschäftigten eindeutige Vorgaben hierfür machten. So verwundert es nicht, dass wir an den einzelnen Arbeitsplätzen nur selten auf aktivierte Bildschirmschoner in Verbindung mit einem Passwortschutz stießen. Auch ungesicherte Disketten- und CD-ROM-Laufwerke in den PC ließen sich fast überall feststellen. Die Passwortvergabe genügte nicht den Anforderungen. Unter diesen Umständen wäre es den Mitarbeiterinnen und Mitarbeitern oder sogar dritten Personen ohne viel Aufwand möglich gewesen, unbefugt das EDV-System zu manipulieren. Betroffen hätten davon häufig auch sensible Daten aus dem Sozial- und Steuerbereich oder auch die Personaldaten der eigenen Mitarbeiterinnen und Mitarbeiter sein können. Dies mussten wir deshalb jeweils beanstanden.

Zwei "**Highlights**" aus den Kontrollen dieses Jahres:

- In einer Behörde "gingen" der Bürgermeister und der Leitende Verwaltungsbeamte mit ihren dienstlichen Notebooks ins Internet. Hiergegen wäre auch nichts einzuwenden, wenn diese Geräte nicht gleichzeitig mit dem EDV-System der Verwaltung verbunden gewesen wären. Mit den von uns aufgezeigten Sicherheitslücken hatte der Bürgermeister "keine Probleme" und verwies darauf, dass mit den Notebooks nur eingegangene E-Mails heruntergeladen würden und er schon aufpassen könne, dass dabei keine schädigenden Dateien (z. B. Viren) in das System gelangten. Schutzmaßnahmen gegen ein unbefugtes Eindringen von außen (etwa eine Firewall, vgl. dazu Tz. 7.1.1) hielt er nicht für erforderlich. Davon abgesehen war kein Virenscanner für das EDV-Netz installiert; auch hier glänzten alle Arbeitsstationen durch offene Disketten- und CD-ROM-Laufwerke.
- In einer anderen Verwaltung fanden wir das Vorzimmer des Leitenden Verwaltungsbeamten unverschlossen und unbesetzt vor und konnten dort ungestört in verschiedenen Bewerbungsunterlagen stöbern, die offen auf dem Schreibtisch lagen.

5 Datenschutz bei Gerichten

5.1 Wenn Bequemlichkeit zum Arbeitsplatzrisiko wird

Durch eine bequeme Verfahrensweise bei der Begründung eines Pfändungs- und Überweisungsbeschlusses gerieten höchst sensible Informationen über einen Mitarbeiter an dessen Arbeitgeber, die ihm letztlich vielleicht den Job kostete.

Eine Rechtspflegerin eines Amtsgerichts erließ einen Pfändungs- und Überweisungsbeschluss wegen erheblicher Unterhaltsrückstände gegen den Geschäftsführer eines Unternehmens und fügte als Anlage zur Begründung des Beschlusses nicht nur Forderungsaufstellungen der zuständigen Jugendämter bei, sondern auch einen **Schlussbericht des Jugendamtes**, in dem stand, dass der Schuldner für längere Zeit inhaftiert war. Die gesamten Unterlagen wurden dem Arbeitgeber des Betroffenen als Drittschuldner zum Zwecke der Gehaltspfändung zugesandt. Dieser hatte vom Vorleben seines Mitarbeiters wohl bislang keine Kenntnis gehabt und kündigte dem Mann – möglicherweise als Folge der Informationsübermittlung. Die Erfüllung seiner Unterhaltspflicht wurde hierdurch sicherlich nicht erleichtert.

Gerade eine Datenübermittlung an den Arbeitgeber kann für Betroffene erhebliche berufliche und persönliche Nachteile zur Folge haben. Nach den Vorschriften der Zivilprozessordnung muss dem Drittschuldner zwar der vollständige **Pfändungs- und Überweisungsbeschluss** einschließlich der Begründung zugestellt werden. Darin dürfen jedoch nur solche Informationen enthalten sein, die zur Begründung erforderlich sind. Dies traf auf die Tatsache der Inhaftierung sicherlich nicht zu. Wenn einem Beschluss zur Begründung ungekürzte Schriftstücke anderer Behörden bzw. von Gläubigern beigefügt werden, ist die Gefahr groß, dass nicht erforderliche Daten persönlichen Schaden anrichten.

Das betreffende Amtsgericht bedauerte den Vorgang. Es sei allgemeine Praxis, Pfändungs- und Überweisungsbeschlüsse durch Bezugnahme auf hinzugefügte Forderungsaufstellungen des Gläubigers zu begründen und diese Informationen auch dem Drittschuldner zuzustellen. Allerdings sei der Rechtspflegerin in diesem Fall die **Sensibilität der Information** über die Haftverbüßung nicht aufgefallen. Die Mitarbeiter des Amtsgerichts würden angehalten, eine Übermittlung nicht erforderlicher Informationen an Drittschuldner in Zukunft zu unterlassen.

5.2 Ein Durchsuchungsbeschluß für alle

Durch die Abfassung eines Durchsuchungsbeschlusses mit sämtlichen Personalien wurde einer größeren Anzahl von Beschuldigten bereits in einem frühen Stadium der Ermittlungen die Tatsache des strafrechtlichen Verdachts gegen die anderen Betroffenen bekannt. Aufseiten der Gerichte will man sich jetzt generell darum bemühen, dieses durch Erlass getrennter Durchsuchungsanordnungen zu vermeiden.

In einem Ermittlungsverfahren mit mehreren Beschuldigten aus verschiedenen Wirtschaftsunternehmen erging ein **Durchsuchungsbeschluss** gegen eine Beschuldigte, in welchem auch die Personenangaben der übrigen Beschuldigten vollständig aufgeführt waren. Sie befürchtete nun, dass die Tatsache ihrer vermuteten strafrechtlichen Verwicklung auf diesem Wege den übrigen Betroffenen zur Kenntnis kam. Sie bangte um ihren guten Ruf in der Branche und ggf. um ihre Chancen für eine Neubeschäftigung.

Der Erlass eines Durchsuchungsbeschlusses unterliegt der richterlichen Unabhängigkeit, die eine Kontrollkompetenz des Landesdatenschutzbeauftragten ausschließt. Dennoch teilte uns das betreffende Gericht, als wir ihm den Sachverhalt zur Kenntnis gaben, mit, dass, soweit verfahrensrechtlich möglich, **getrennte Beschlüsse** gegen die jeweiligen Beschuldigten erlassen würden. Dies geschehe unabhängig davon, wie die Staatsanwaltschaft ihren Antrag an das Gericht auf Erlass einer Durchsuchungsanordnung abgefasst habe. Möglich sei jedoch im Einzelfall, dass ein Verfahren und damit der Tatvorwurf nur unter Hinzunahme der Personalien der übrigen Beschuldigten hinreichend bezeichnet werden könne, was einen einheitlichen Beschlusstext erforderlich mache.

6 Sicherheit und Ordnungsmäßigkeit der automatisierten Datenverarbeitung

6.1 Die Crux mit den Netzen

Wie zu Zeiten des Post- und Fernmeldemonopols gilt für die meisten Datennetze das Prinzip "Sicherheit durch Undurchschaubarkeit". Die Kunden sind angeblich froh, von den Sicherheitsrisiken nichts wissen zu müssen; die Betreiber sehen sich nicht veranlasst, schlafende Hunde zu wecken.

Wer die Deutsche Post oder die Telekom einschaltet, um einen Brief zu transportieren bzw. ein Telefonat zu führen, weiß nicht, wie der Brief- und Paketverkehr vor unbefugten Zugriffen geschützt wird, geschweige denn, wie das Fernmeldenetz abgesichert ist und welche Spuren in welchen Rechnersystemen z. B. die ISDN-Datenpakete hinterlassen. Das ist gewiss kein befriedigender Zustand. Man **vertraut blind** darauf, dass diese Institutionen die Sicherheitsrisiken im Griff haben. Dieses Denken ist offenbar ein Relikt aus der Zeit des Post- und Fernmeldemonopols: Warum soll man derartige Dinge kritisch hinterfragen, wenn man einerseits sowieso keine Handlungsalternative hat und andererseits die Erfahrung zeigt, dass "fast nie etwas passiert"? Es gibt ja das durch die Verfassung garantierte Post- und Fernmeldegeheimnis.

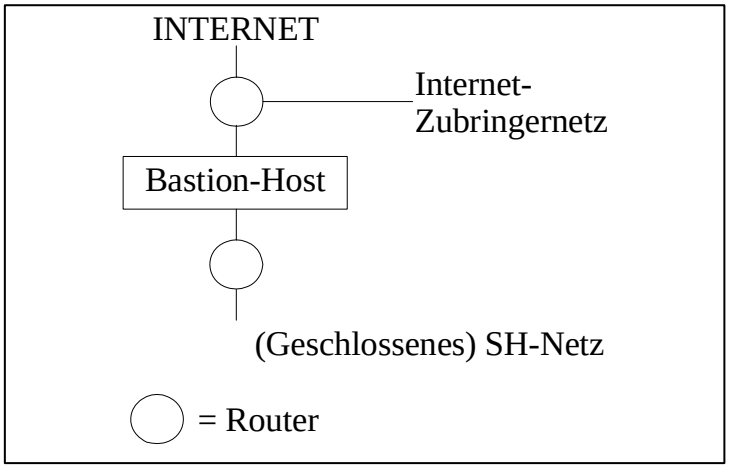
Zwischenzeitlich wurde der Telekommunikationsmarkt liberalisiert. Es gibt eine Vielzahl von Unternehmen, die Datentransport- und Datenvermittlungsdienstleistungen anbieten. Besteht weiterhin kein Grund, sich um die Sicherheit beim Datentransport zu kümmern? Das Verhalten der von uns zu kontrollierenden Daten verarbeitenden Stellen im Lande lässt darauf schließen, dass die **Denkstrukturen aus der "Kaiserzeit"** immer noch vorherrschen. So wie in der Vergangenheit technische Innovationen (z. B. Time-Sharing-Systeme, Datenbank-Management-Systeme, individuelle Datenverarbeitung oder Client-Server-Architekturen) zunächst in recht ungeordneten Bahnen verliefen und erst nach und nach um die Komponenten "Sicherheit" und "Revisionsfähigkeit" angereichert wurden, so rechtfertigt zurzeit anscheinend das Zauberwort "Netz" jedwedes Abweichen von dem Pfad einer grundsätzlich transparenten und für Dritte nachvollziehbaren Datenverarbeitung.

Seit Jahren bemühen wir uns, dem Innenministerium und der Datenzentrale als den Anbietern und Betreibern des Schleswig-Holstein-Netzes und des Campus-Netzes sowie ihren Kunden (Ministerien, Kommunalbehörden, Landesbehörden) deutlich zu machen, dass sie diese Netze nicht als **Black Box** anbieten bzw. benutzen dürfen, sondern dass gerade in diesem Bereich ein Höchstmaß an Transparenz bei den Schnittstellendefinitionen erforderlich ist – bisher nur mit mäßigem Erfolg (vgl. 19. TB, Tz. 7.8 und 7.9; 20. TB, Tz. 6.7.6 und 6.7.7; 21. TB, Tz. 6.4 und 6.5).

Wer z. B. einen Vertrag mit der Datenzentrale zur Nutzung des Schleswig-Holstein-Netzes abschließt, wird bezüglich des "Nutzungsobjektes" zunächst auf

eine Leistungsbeschreibung verwiesen. Dort werden dann alternativ zwei Leistungsarten angeboten, der “Standardanschluss für DZ-Online-Verfahren und Abfragedienste” und der “Komfortanschluss für LAN to LAN-Kopplung”. Welche Anschlussart man vertraglich vereinbart hat, bleibt nicht nur im Vertrag selbst, sondern auch in einer zusätzlichen Anlage “Beschreibung der Transportdienstleistung” ungeklärt. In der **Leistungsbeschreibung** findet die vorhandene Firewall als eine Netzkomponente keine Erwähnung.

Das als weiterer Vertragsbestandteil deklarierte Sicherheitskonzept beginnt dagegen mit den “erhellenden” Worten: “Das nachstehende Sicherheitskonzept bezieht sich auf die Bereitstellung von Datenvermittlungsdienstleistungen und entsprechende Anschlusstechnik für Kunden zur Herstellung einer digitalen Kommunikation mit definierten oder freien Zielteilnehmern. Dabei wird ein **mittleres Schutzniveau** im Sinne der Klassifizierung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für das geschlossene Netz beschrieben und angestrebt. Die DZ SH betreibt zwei Netze, deren Übergang durch eine Firewall kontrolliert wird. Das SH-Netz ist im Sprachgebrauch gleichbedeutend mit dem geschlossenen SH-Netz. Das Internet-Zubringernetz besteht aus der Bereitstellung von freien Anschluss- und Kommunikationsdienstleistungen. Dieses Netz ist nicht Bestandteil des SH-Netzes”. Erläutert wird dies durch die nachfolgende Grafik:



Sicher werden sich professionelle **Netzspezialisten** aus dem Vertrag, der Leistungsbeschreibung, zwei Anlagen und dem Sicherheitskonzept ein Gesamtbild machen können, aber eben nur Spezialisten. Welchem **Bürgermeister** oder **leitenden Verwaltungsbeamten** wird jedoch im Sicherheitskonzept unter der Tz. 5.4.3.1 vierter Absatz, sechster Spiegelstrich, die Fomulierung auffallen: “Der Firewall enthält zurzeit keine Filtermechanismen für Anwendungsobjekte (z. B. gegen Viren, Makroviren). Der Schutz wird hier am Arbeitsplatz durch Online-Virenscanner und Verhaltensanweisungen geleistet. Diese Verantwortung liegt in der Organisationseinheit Kunde oder DZ SH, in der der Arbeitsplatz liegt.” Mit diesen wenigen Worten wird nämlich klargestellt, dass trotz einer Firewall bei einer Verknüpfung des lokalen Netzes mit dem Internet wesentliche Sicherheitsrisiken entstehen, die von der einzelnen Behörde zu bewältigen sind.

Auch bezüglich des Campus-Netzes zwischen den obersten Landesbehörden besteht nach wie vor ein völlig unbefriedigender Status quo. Die einzelnen Ressorts nutzen die "externen" Dienstleistungen des Innenministeriums und der Datenzentrale, ohne dass hierüber verbindliche **Vereinbarungen** getroffen worden sind. Aus der Tatsache, dass die Nutzungsvereinbarungen im Laufe mehrerer Jahre nur bis zum **Entwurfsstadium** gediehen sind, ist abzuleiten, dass über die tatsächlichen Konsequenzen dieser Aufgaben- und Verantwortungsdelegation noch kein Einvernehmen besteht. Diese Situation kann auch nicht dadurch "geheilt" werden, dass die Beteiligten sich ihres gegenseitigen Vertrauens versichert haben und das "Ausbleiben" von sicherheitsrelevanten Problemen in der Vergangenheit als positives Qualitätsmerkmal bewerten. Zudem besteht die schlichte Fiktion eines einheitlichen Sicherheitsbedürfnisses in allen Behörden. Die unterschiedliche Schutzbedürftigkeit der in den einzelnen Häusern verarbeiteten Daten ist bisher noch nicht systematisch untersucht worden.

Es ist deshalb davon auszugehen, dass das **Campus-Netz** derzeit noch nicht als mit den Grundsätzen einer "ordnungsgemäßen automatisierten Datenverarbeitung" im Sinne der **Datenschutzverordnung** im Einklang steht. Diese Feststellung sollte Anlass sein, entweder das Campus-Netz kurzfristig auf eine datenschutzrechtlich einwandfreie Grundlage zu stellen oder aber so schnell wie möglich durch das geplante Landesnetz (vgl. Tz. 6.3) zu ersetzen. Das Sicherheitskonzept für das Landesnetz sollte unseres Erachtens "unbelastet" von der historischen Entwicklung des Schleswig-Holstein-Netzes und des Campus-Netzes völlig neu erarbeitet werden. Zuvor wäre allerdings im Hinblick auf das **Landessystemkonzept** die Rolle des Innenministeriums als Netzbetreiber detailliert zu beschreiben. Ohne eine formale Zuständigkeits- und Verantwortungsübertragung wird von ihm nämlich auch das neue Netz nicht gemanagt werden können.

Was ist zu tun?
Zügiges Handeln ist von Nöten: Das neue Landesnetz sollte sorgfältig geplant und für jedermann nachvollziehbar beschrieben werden. Wenn über das Konzept Konsens erzielt worden ist, sollte es mit Nachdruck realisiert werden, damit die bestehenden Netze so bald wie möglich ersetzt werden können.

6.2 Gravierende Sicherheitsrisiken bei Telekommunikationsrechnern

Den Aspekten der Sicherheit und Kontrollierbarkeit von Telekommunikationsrechnern ist in der Vergangenheit viel zu wenig Aufmerksamkeit geschenkt worden. Bei genauem Hinsehen stellt man fest, dass die Speicherung von Gesprächsinhalten und das Abhören von Räumen möglich und nur schwer nachweisbar ist.

Wer sich als "normal" ausgebildeter EDV-Kontrolleur mit der Funktionsweise und den Sicherheitsaspekten von **Telekommunikationsrechnern** befassen will, muss im wahrsten Sinne des Wortes viel "Lehrgeld" bezahlen. Die Betriebssysteme und die Programmiersprachen, mit denen derartige IT-Systeme gesteuert werden, unterscheiden sich wesentlich von denen marktgängiger

Verwaltungsrechner. Deshalb hieß es für unsere Mitarbeiter zunächst einmal, viele Informationsgespräche mit Spezialisten zu führen und sich in die (nur sehr schwer erhältliche) Fachliteratur einzuarbeiten, bevor Prüfungsmaßnahmen in der Außenstelle Itzehoe des Amtes für Ländliche Räume Lübeck und bei der Hansestadt Lübeck begonnen werden konnten. Die beiden Stellen hatten wir als repräsentativ ausgewählt, weil im Amt für Ländliche Räume ein älteres Standardsystem und bei der Hansestadt Lübeck eine neue, hochmoderne Anlage installiert war.

Ziel unserer Nachschau war es, eventuelle Schwachstellen im Bereich des Schutzes der Telekommunikationsdaten zu untersuchen und dabei Transparenz in einen Bereich der personenbezogenen Datenverarbeitung zu bringen, über dem bisher ein dichter Grauschleier lag. Den damit verbundenen personellen und zeitlichen Aufwand haben wir massiv unterschätzt. Denn neben vielen anderen Problemen haben die Prüfungen eines aufgezeigt: Die derzeit installierten Telekommunikationsrechner sind (fast) **nicht revisionsfähig**. Das gilt nicht nur für Kontrollen durch “Externe” wie den Landesbeauftragten für den Datenschutz, sondern auch für die Betreiber selbst.

Zunächst muss man die **Größenordnung** der installierten Hardware betrachten. Das vergleichsweise kleine System in Itzehoe bestand zum Zeitpunkt der Prüfung aus einem Haupt- und zwei Unterrechnern, einer Richtfunkanlage, einem Administrations- und zwei Gebühren-PC sowie zwei Modems für die Fernwartung. Über diese zentralen Komponenten wurden zirka 1 000 Anschlussgeräte in zehn verschiedenen Behörden (z. B. Amtsgericht, Landgericht, Sozialgericht, Staatsanwaltschaft, Finanzamt, Landesbezirkskasse) betrieben. Die Installation in Lübeck übertrifft diese Dimension bei weitem. Sie besteht aus 83 Telekommunikationsanlagen, einem Server für das Telekommunikations-Management, sechs PC bzw. Laptops für die Administration, einem Voice-Mail-Server mit mehreren angeschlossenen PC für dessen Administration, einem PC für das “Call-Traffic-Management”, sechs PC im Bereich der Vermittlungsstellen, einem PC für die Gebührenabrechnung, einem PC für die Verwaltung des elektronischen Telefonbuches sowie weiteren IT-Komponenten für die Fernwartung und für die Verbindung zu einem Intranet. Die mehr als 3 500 angeschlossenen Nebenstellen sind über 237 Standorte im ganzen Stadtgebiet verteilt.

Eine auch nur ansatzweise Beschreibung der Betriebssystem- und sonstigen **Softwarekomponenten** würde den Rahmen dieses Berichtes sprengen. Deshalb nur so viel: Die Telekommunikationsrechner in Lübeck werden von den Administratoren durch mehr als 200 unterschiedliche Betriebssystembefehle gesteuert. Dies entspricht dem Befehlsvorrat von Großrechnersystemen.

Auch der Umfang und die **Vielzahl der Datenbestände** war für uns überraschend. Wir fanden nicht nur Leistungsmerkmals- und Gebührendateien, sondern in Lübeck auch Dateien mit gesprochenen oder geschriebenen Texten im Voice-Mail-Server (Inhalte von Fax-Schreiben und E-Mails sowie von Nachrichten, die im Anrufbeantworter hinterlassen worden waren). Diese Datenbestände sind auf den Festplatten der Rechner abgelegt und bleiben solange

gespeichert, bis die Administratoren den Löschbefehl geben. Weder die Anrufer noch die Angerufenen dürften sich dieser Tatsache bewusst sein.

Von ganz besonderer Bedeutung sind auch die "**Gestaltungsmöglichkeiten**", die die so genannten **Leistungsmerkmale** bieten. Nachfolgend einige mit besonderer datenschutzrechtlicher Relevanz:

- Nicht angenommene Anrufe können mit Rufnummer, Datum, Uhrzeit und Anzahl der Versuche aufgezeichnet werden (Anruferliste).
- Teilnehmer können sich direkt in bestehende Verbindungen einschalten (Aufschalten).
- Eingehende Telefongespräche können mittels des Voice-Mail-Servers aufgezeichnet werden (Voice-Mail).
- Über das integrierte Mikrofon kann trotz aufgelegten Hörers in einen Raum hineingehört werden (Raumhören bzw. direktes Ansprechen).

Derartige Aktivitäten lassen sich zwar mit Anzeigen auf dem Display und mit Aufmerksamkeitstönen koppeln. Dieselben Administratoren, die die Leistungsmerkmale aktivieren, können aber z. B. auch die Lautstärke des Aufmerksamkeitstons praktisch wegregulieren. Obwohl wir sicher noch nicht einmal alle Finessen der vielfältigen Betriebssystembefehle kennen, haben unsere Tests ergeben, dass de facto ein **unbemerktes "Abhören"** eines Sitzungszimmers möglich ist. Wie das im Einzelnen bewerkstelligt werden kann, gehört sicher nicht in einen der Öffentlichkeit zugänglichen Bericht. Es ist nämlich nicht möglich, die besonders problematischen Leistungsmerkmale beim Lieferanten gar nicht erst mitzubestellen, um sicherzugehen, dass sie nicht "aus Versehen" eingeschaltet werden.

Diese Feststellungen sind der Hintergrund für unsere Forderungen nach genauen **Vorgaben** für die Vergabe von **Leistungsmerkmalen**, für die Speicherungsdauer von Inhaltsdaten und für die Behandlung von Gebührendaten sowie nach einem Höchstmaß an Revisionsfähigkeit der Aktivitäten der Systemadministratoren durch eine auswertbare Protokollierung. Beide geprüften Stellen konnten den datenschutzrechtlichen Ansprüchen nicht genügen, was zu einer Vielzahl von Beanstandungen führte.

Ein besonderes Gewicht kommt in diesem Zusammenhang den Mängeln bei der **Fernadministration** durch die Systemlieferanten zu. Wir mussten feststellen, dass die zuständigen Mitarbeiter der von uns geprüften Behörden erhebliche Probleme hatten, die komplexen Strukturen der Telekommunikationssysteme zu durchdringen. Deshalb beauftragte man die gleichen Unternehmen, die die Systeme geliefert hatten, auch mit der Administration. Soweit über deren Arbeiten überhaupt Protokolle erstellt worden waren, wurden sie nicht systematisch ausgewertet. Das führte im Ergebnis dazu, dass ungewollt bzw. unbefugt geschaltete "problematische" Datenspeicherungen oder Leistungsmerkmale nur durch Zufall oder Ausprobieren hätten aufgedeckt werden können.

Das Amt für Ländliche Räume hat in einer ersten Stellungnahme mitgeteilt, dass im Rahmen des landesweiten Sprachnetzes (vgl. Tz. 6.3) durch das Ministerium für Finanzen und Energie zwischenzeitlich ein neuer Telekommunikationsrechner installiert worden ist. Über dessen Funktionsweise will man uns unterrichten, wenn die Einzelheiten von der Lieferfirma bzw. dem Finanzministerium als dem neuen Systembetreiber bekannt gegeben worden sind.

Die Hansestadt Lübeck hat unverzüglich eine Neuordnung der internen Zuständigkeiten für die Telekommunikationsdienste beschlossen. Damit soll sichergestellt werden, dass künftig klare Verantwortungszuweisungen bestehen. Wegen der Vielschichtigkeit der von uns gegebenen Hinweise war es ihr gleichwohl nicht möglich, in dem üblichen Zeitrahmen eine Stellungnahme abzugeben. Sie hat zunächst die mit der Planung und Realisierung ihrer Telekommunikationsanlagen beauftragten Firmen mit den festgestellten sicherheitstechnischen Problemen konfrontiert.

Was ist zu tun?
Man wird zweigleisig fahren müssen: Die Betreiber der Telekommunikationsrechner werden lernen müssen, sie zu beherrschen, um sich aus der Abhängigkeit von den externen Administratoren zu befreien. Die Anbieter und Beschaffer wird man kritisch fragen müssen, warum sie Geräte mit Funktionen anbieten bzw. einsetzen, die nicht wirklich gebraucht werden, deren sicherheitsrelevanter Missbrauch aber kaum zu verhindern ist.

6.3 Privatisierung der Telekommunikationsanlagen birgt Risiken

Das Land zieht sich bezüglich des Telefonbereiches aus dem "Telekommunikationsgeschäft" zurück. Wer kontrolliert künftig die Administrationsaktivitäten der privaten Dienstleister? Wenn das privatisierte Sprachnetz und das Datennetz des Landes integriert werden, wer löst die Sicherheitsprobleme?

Mit der Ankündigung des Staatssekretärs im Ministerium für Finanzen und Energie vom 30. Juni 1999 "Landesverwaltung erhält ein **integriertes Sprach- und Datennetz**" ist aus datenschutzrechtlicher und sicherheitstechnischer Sicht ein neues Zeitalter in der zwischenbehördlichen Telekommunikation in Schleswig-Holstein angebrochen. Die Auswirkungen werden aus unserer Sicht so vielfältig sein und eine so große Tragweite haben, dass wir in unserer Dienststelle eine spezielle Arbeitsgruppe aus Juristen, Informatikern und anderen Datensicherheitsexperten gebildet haben, um eine umfassende kritisch-konstruktive Begleitung dieses Projektes zu Gewähr leisten. Bereits die wenigen uns bisher bekannten Fakten werfen zahlreiche datenschutzrechtliche und **sicherheitstechnische Fragen** auf bzw. weisen auf alsbald zu lösende Probleme hin:

Die vom Land Schleswig-Holstein mit der Telekom bzw. der Firma Siemens (als Subunternehmer) geschlossenen Verträge bezeichnen das **Finanzministerium** als **Auftraggeber** der Dienstleistungen und als Nutzer der bereitgestellten Hard- und

Software. Ob allerdings das Ministerium oder das "Gebäudemanagement Schleswig-Holstein" als Betreiber des Sprachnetzes fungieren wird, scheint noch nicht endgültig entschieden zu sein. Davon abhängig ist jedoch, wer im datenschutzrechtlichen Sinn "Daten verarbeitende" und damit verantwortliche Stelle ist. Im Moment halten wir uns an das Ministerium.

Die bisherigen **vertraglichen Vereinbarungen** decken drei an sich voneinander unabhängige Bereiche ab:

- die Anmietung von mehr als 400 Telekommunikationsrechnern und einigen 10 000 Telefongeräten sowie die Gewährung von Nutzungsrechten für die Vermittlungs- und Konfigurationssoftware,
- die Inanspruchnahme von Übertragungsleitungen der Telekom mit den jeweils erforderlichen Übertragungskapazitäten (Bandbreiten) und
- die Administration der gesamten Hard- und Software durch Mitarbeiter der Firmen Telekom und Siemens.

Im Hinblick auf die vielfältigen sicherheitsrelevanten **Konfigurationsmöglichkeiten** für die Rechnersysteme und die Leistungsmerkmale der Nebenstellen dürfte es nicht zu verantworten sein, sie aus der Sicht des Betreibers und der Nutzer als eine Black Box zu behandeln (vgl. Tz. 6.2). Da für die tatsächliche Nutzung der Systeme weiterhin die einzelnen **Behörden verantwortlich** bleiben, werden diese ihre Anforderungen dem Betreiber mitzuteilen haben, der wiederum dafür zu sorgen hat, dass der "Vermieter" nur die angeforderten Funktionalitäten auf der Geräte- bzw. Softwareebene zur Verfügung stellt. Die veranlassende Behörde wird sich durch Tests davon überzeugen müssen, dass ihre Anweisungen auch tatsächlich richtig vollzogen worden sind.

Der eigentliche **Datentransport** über die Leitungen vom bzw. bis zum Hausanschluss der jeweiligen Liegenschaften bleibt für den Betreiber und die einzelnen Behörden wie in der Vergangenheit eine **undurchschaubare Angelegenheit**. Die Telekom unterliegt nicht der Aufsicht durch den schleswig-holsteinischen Datenschutzbeauftragten und lässt sich auch nicht freiwillig von unabhängigen Sicherheitsspezialisten "in die Karten schauen". Wenn also schon ein landeseinheitliches Netz propagiert wird, so wird man im Hinblick auf die unbestreitbaren Abhörpraktiken "interessierter" Institutionen die Forderung nach einer Verschlüsselung des Datenverkehrs nicht vorschnell vom Tisch wischen können. Ein landeseinheitlicher Verschlüsselungsalgorithmus und für alle Behörden gleiche, aber häufig wechselnde Schlüssel dürften z. B. technisch realisierbar sein.

Wenn die gesamte **Administration** der Telekommunikationsrechner in die Hände eines externen Dienstleisters gegeben wird, stellt sich die Frage, wer dessen Arbeit überwachen kann. Dem Betreiber muss ein Team von **hoch qualifizierten Spezialisten** zur Verfügung stehen, die nicht nur in der Lage sind festzustellen, ob der Dienstleister alle Aufträge ordnungsgemäß erledigt hat, sondern auch, ob sicherheitsrelevante Funktionen ohne Auftrag aktiviert oder deaktiviert worden sind. Die revisionsfeste Protokollierung aller Aktivitäten der Administration und

die systematische Auswertung der Protokolle muss ein unverzichtbarer Teil eines umfassenden Sicherheitskonzeptes sein.
Die vorgenannten Probleme und eine Vielzahl weiterer Fragestellungen sind in ersten Gesprächen mit den Vertretern des Finanzministeriums, der Telekom und der Firma Siemens erörtert worden. Derzeit befindet man sich dort in der Umsetzungsphase und hat angekündigt, bereits in den nächsten Gesprächen erste Vorschläge zur Problemlösung vorzustellen. Wenn wie angekündigt über das angemietete Leitungsnetz nicht nur Telefonate geführt werden, sondern auch die gesamte **Datenkommunikation** zwischen den schleswig-holsteinischen Behörden abgewickelt wird, treten mit dem Innenministerium und der Datenzentrale zwei zusätzliche Akteure auf den Plan. Der Innenminister wird nämlich nach dem jüngst beschlossenen "**Landessystemkonzept**" der Betreiber des Datennetzes sein und die Datenzentrale wird dessen Administration als externer Dienstleister übernehmen. Das Datennetz soll dann das Campus-Netz und möglicherweise auch das Schleswig-Holstein-Netz der Datenzentrale ersetzen (vgl. Tz. 6.1).

Der Finanzminister und der Innenminister werden also die Leitungswege aus Kostengründen gemeinsam benutzen, in jeder Behörde wird aber ein wie auch immer geartetes technisches Gerät stehen, das die ankommenden digitalen Signale nach Sprach- und Dateninformationen sortiert und vielleicht auch Übergänge (z. B. beim Faxverkehr) zulässt. Sodann werden sie entweder in den Telekommunikationsrechnern oder in den "normalen" Datenverarbeitungsanlagen weiterverarbeitet. Da das Datennetz mit den vielen lokalen Netzen der einzelnen Behörden und entweder direkt oder über die Behördennetze mit dem zwar weltweiten, aber ungesicherten Internet verbunden sein wird, ergibt sich die Notwendigkeit zur Installation hochwirksamer Sicherheitsmechanismen (z. B. Firewalls). Je mehr das **Sprach- und das Datennetz** miteinander verwoben werden, umso mehr müssen die Sicherheitskonzepte der beiden Betreiber aufeinander abgestimmt sein. Zurzeit sind hier mehr offene als gelöste Probleme zu sehen, zumal die "kommunale Familie" (Gemeinden, Ämter, Städte, Kreise) bereits signalisiert, dass auch sie sich an den vom Finanzminister prognostizierten Kosteneinsparungen von mehreren Millionen Mark jährlich "beteiligen" möchte. Im Augenblick bleibt die schlichte Erkenntnis: Der Erfolg des Projektes steht und fällt mit der Qualität der Sicherheitskonzepte.

Was ist zu tun?
Nachdem die Rahmenverträge "stehen", muss der Innenminister möglichst bald das Konzept seines Datennetzes vorlegen, damit gemeinsam mit dem Finanzminister die Sicherheitskonzepte entwickelt werden können. Hinsichtlich der Sicherheit und Transparenz des integrierten Datennetzes sind die Bestimmungen der Datenschutzverordnung strikt zu beachten.

6.4 Unterschiedliche Prioritäten bei der Behebung von Sicherheitsmängeln

Stellen wir bei Prüfungen Sicherheitsmängel fest, so fällt den Behörden das Akzeptieren von Beanstandungen offenbar leichter, als die Mängel zügig zu beheben.

Im letzten Jahr (vgl. 21. TB, Tz. 6.7) haben wir ausführlich über drei größere Prüfungsmaßnahmen aus dem Jahr 1998 berichtet, die eines gemein hatten: Wir haben **signifikante sicherheitstechnische Defizite** festgestellt, haben die Daten verarbeitenden Stellen zu einer grundlegenden Neuorientierung ihrer "Security Policy" aufgefordert und haben die Mitteilung erhalten, dass alsbald für eine Behebung der Mängel gesorgt würde. Die sich so in Zugzwang befindenden Stellen sind die Oberfinanzdirektion, das Städtische Krankenhaus in Kiel und die AOK Schleswig-Holstein. Etwa ein Jahr später zeigt sich ein recht unterschiedliches Bild bezüglich der Einhaltung der Zusagen und der Prioritätensetzung.

Die **Oberfinanzdirektion** hat quasi die weiße Flagge gehisst und uns mitgeteilt, dass "die Komplexität der auf Grund des Prüfberichtes zu untersuchenden Teilaufgaben einen hohen Arbeitsaufwand im Automationsbereich" erfordere. Im Jahr 1999 hätten jedoch andere zwingend und dringend notwendige Aufgaben wie z. B. die Umstellung auf das Jahr 2000 und die laufenden Updates auf Grund der Steuerrechtsänderungen Vorrang gehabt. "Daher konnte an den aufgeworfenen Problemen bisher leider noch nicht vertieft konzeptionell gearbeitet werden." Der erhöhte Aufwand für die softwaretechnische Bewältigung des Jahr-2000-Problems mag als Rechtfertigung für das Fortbestehen bekannter sicherheitstechnischer Schwachstellen gelten. Mit Beginn des neuen Jahres muss dieses Problem jedoch abgehakt sein, sodass auch die Lösung anderer dringender Probleme in Angriff genommen werden kann. Ein weiterer Verzug wäre jedenfalls aus unserer Sicht nicht zu rechtfertigen.

Auch das **Städtische Krankenhaus in Kiel** hat den sicherheitstechnischen Durchbruch noch nicht erreicht. Uns sind zwar im Rahmen von Beratungsgesprächen erste Unterlagen über ein so genanntes "Care-Center", das Anfang 2000 installiert sein soll, vorgelegt worden. Es handelt sich jedoch um Papiere des Softwareanbieters und nicht um Konzepte oder Vorgaben der Krankenhausleitung. Der geringe Konkretisierungsgrad wird z. B. daran deutlich, dass das zentrale Problem der Revisionsfähigkeit des geplanten Verfahrens mit einem Zweizeiler folgenden Inhalts abgehandelt wird: "Die Lösung ist revisionsfähig, da jederzeit überprüft werden kann, wie personenbezogene Daten in das System hineingekommen sind und welche Person auf dem Server tätig war." Dies als einen Teil eines "Datenschutz- und Datensicherheitskonzeptes" zu deklarieren, ist solange nicht gerechtfertigt, solange man nicht auch verrät, wie man das "in das System Hineinkommen" und "auf dem System Tätigsein" revisionsfest protokolliert. Die Verantwortlichen im Städtischen Krankenhaus haben noch viel Arbeit vor sich, wenn nicht auch hier die unter Tz. 6.5 dieses Berichtes beschriebenen Probleme auftreten sollen. Das gilt insbesondere, weil die technischen und organisatorischen Schnittstellenprobleme zwischen dem Städtischen Krankenhaus "im engeren Sinn" und der II. Medizinischen Klinik des

Universitätsklinikums, die das Städtische Krankenhaus "mitbenutzt", nach wie vor völlig ungeklärt sind.

Nur eine der drei betroffenen Stellen kann eine insgesamt positive Bilanz vorweisen, wenngleich die uns gemachten Zusagen auch nicht vollständig eingehalten wurden. Die **AOK Schleswig-Holstein** hatte sich selbst als Zieltermin für die Behebung der von uns festgestellten Mängel den 30.09.1999 gesetzt. Dieser Termin konnte nicht gehalten werden, **signifikante Fortschritte** sind jedoch unverkennbar. So enthält ein Statusbericht zum Jahresende ein knappes Dutzend von "Erledigt-Vermerken". Uns wurde z. B. mitgeteilt, dass

- die Zugriffsberechtigungen auf die Datenbanken mit Sozialdaten neu festgelegt worden sind,
- die papierenen Unterlagen nunmehr grundsätzlich in verschlossenen Behältnissen gelagert werden,
- alle Übermittlungen von Sozialdaten sorgfältig dokumentiert sind,
- die Entsorgung von Altakten neu organisiert wurde,
- nicht benutzte Bildschirme auf den Arbeitsplätzen automatisch gesperrt werden,
- die Serverräume besser gesichert sind,
- die Auftragsdatenverarbeitung im Rechenzentrum in Mecklenburg-Vorpommern auf eine neue Grundlage gestellt wurde und
- die Aufgaben der örtlichen Datenschutzbeauftragten neu festgelegt und ihnen ausreichend Zeitkontingente zur Verfügung gestellt wurden.

Die Problematik der mangelnden Diskretion bei der Versichertenberatung in den Geschäftsstellen und Filialen ist augenscheinlich erst punktuell gelöst. Hier zeigt sich, wie kostenintensiv das nachträgliche Korrigieren von Fehlentwicklungen ist. Wir haben uns beratend an **Pilotprojekten** zur **Neugestaltung** der so genannten **Kundencenter** beteiligt und selbst feststellen müssen, dass zwar vieles mit Kreativität verbessert werden kann, dass einige Räumlichkeiten und Möblierungen aber so "unpassend" sind, dass die Wahrung des Sozialgeheimnisses nur durch eine völlige Neugestaltung gewährleistet werden kann. Wenn die AOK prognostiziert, "am Ende werden wir Maßnahmen im Wert von mehreren Millionen Mark umgesetzt haben", ist dies einerseits positiv zu bewerten, andererseits ist eine solche Aussage auch ein Indiz für das Ausmaß der in der Vergangenheit entstandenen Sicherheitsdefizite. Deshalb werden wir die weiteren Aktivitäten der AOK aufmerksam beobachten und auf einen weiterhin zügigen Abbau der Defizite drängen.

Was ist zu tun?
Die Vollzugsdefizite sind zügig abzubauen, weil es nicht akzeptabel ist, Sicherheitsmängel nur zur Kenntnis zu nehmen und ihre Behebung auf die lange Bank zu schieben. Wir werden die betroffenen Stellen zu verbindlichen Terminzusagen drängen und uns vom Fortgang der Mängelbeseitigung überzeugen.

6.5 Krankenhausinformationssysteme – wer ist verantwortlich?

Der Nutzen digitaler Krankenakten und "workflow-basierter" Informationssysteme in Krankenhäusern lässt sich leicht in rosigen Farben schildern. Die damit verbundenen sicherheitstechnischen und Verantwortungsprobleme in den Griff zu bekommen, setzt dagegen eine sorgfältige Planung und Auseinandersetzung mit den rechtlichen Gegebenheiten voraus.

Spätestens seitdem auch die Krankenhäuser in öffentlicher Trägerschaft gehalten sind, nach kaufmännischen Gesichtspunkten zu wirtschaften und für Leistungs- und Kostentransparenz zu sorgen, erlebt die automatisierte Datenverarbeitung in diesem Bereich geradezu einen Boom. Da ist die Rede von der "elektronischen Krankenakte", von "workflow-basierten RIS-PACS-Systemen", von "Pflegeinformatik" und "Pflegeinformationssystemen" (natürlich auch "workflow-basiert"), von "Sprachdokumentation", und mancher stellt lapidar fest: "Das Papier hat ausgedient!". Allerdings scheint es, dass nicht nur die Datenschützer, sondern auch die Protagonisten dieser **Hightech-Krankenhäuser** selbst bemerkt haben, dass die Entwicklung von Informationstechnik eine Sache ist, die sichere Beherrschung derselben aber eine ganz andere. Vor dem Hintergrund unserer bisherigen Erfahrungen mit der Datenverarbeitung in Krankenhäusern im Allgemeinen und mit so genannten integrierten Krankenhausinformationssystemen im Besonderen kann man ein verstärktes Streben nach Transparenz und Qualität nur begrüßen (vgl. zuletzt 21. TB, Tz. 6.7.3 mit weiteren Verweisen).

Worin liegen die Ursachen für die von uns festgestellten **sicherheitstechnischen Defizite** in diesem so hochsensiblen Bereich? Die vielen Beratungsgespräche, die wir auch in diesem Jahr wieder geführt haben, lassen eine Hauptursache immer deutlicher werden: Weil man "informationstechnische Redundanzen" vermeiden will, werden die Grenzen zwischen der medizinischen Dokumentation der Ärzte und den Buchführungsunterlagen der Krankenhausverwaltung verwischt. Am Ende ist häufig völlig unklar, wer z. B. für die Vergabe von Zugriffsberechtigungen auf die ach so hochintegrierten Datenbanken die Verantwortung trägt, die kaufmännischen Leiter, die EDV-Chefs oder die behandelnden Ärzte. Auf der Strecke bleiben nicht selten die Rechte der Patienten, die von alledem nichts merken, weil sie verständlicherweise mehr um ihre Gesundheit besorgt sind als um die Sicherheit ihrer Daten.

Der IT-Einsatz ist natürlich auch unter Datenschutz- und Datensicherheitsaspekten in beiden Bereichen möglich. Es geht also nicht um das "Ob", sondern um das "Wie". Die Sicherheitsspielregeln für die computergestützte Dokumentation medizinischer Behandlungen durch Ärzte und ihre berufsmäßig tätigen Gehilfen (Pflegedienst) hat die Bundesärztekammer bereits im Jahre 1996 festgelegt (Deutsches Ärzteblatt 1996, Nr. 43). Danach ist die Führung digitaler Krankenakten nur dann zulässig, wenn **besondere Sicherungs- und Schutzmaßnahmen** getroffen werden, um deren Veränderung, Vernichtung oder unrechtmäßige Verwendung zu verhindern. Welchen Stellenwert das ärztliche

Standesrecht dem Problem der Datenintegrität und der Vertraulichkeit der Informationen beimisst, wird z. B. an folgenden Einzelforderungen deutlich: Es muss möglich sein, während der gesamten Aufbewahrungszeit auch nach einem Wechsel des IT-Systems die dokumentierten Informationen innerhalb angemessener Zeit lesbar zu machen. Die Wartung der Systeme und jegliche Fehlerbeseitigung darf grundsätzlich nur mit Testdaten erfolgen. Der Einblick Dritter in Originaldaten muss auf besondere Ausnahmefälle beschränkt bleiben. Das Wartungspersonal ist zu beaufsichtigen und dessen Arbeiten sind zu protokollieren. Das gilt auch bei einer Fernwartung. Die Fernübertragung patientenbezogener Daten muss verschlüsselt erfolgen, auszumusternde Datenträger sind zuvor unter ärztlicher Aufsicht unbrauchbar zu machen. Aus alledem ergibt sich, dass die digitalen Krankenakten (ebenso wie ihre papierenen Vorgänger) keine normalen Verwaltungsvorgänge sind, sondern als medizinische Dokumentation dem ärztlichen Sicherheitsmanagement auf der Grundlage des besonderen Vertrauensverhältnisses zwischen Arzt und Patienten unterliegen.

Für die **kaufmännische Abwicklung** der Krankenhaus-Behandlungsverträge ist stets nur eine geringe Teilmenge der Informationen erforderlich, die ein Arzt in der medizinischen Dokumentation erfasst hat. Soweit der Patient eine Abrechnung mit seiner gesetzlichen Krankenkasse wünscht, ergibt sich das Datenprofil aus dem Sozialgesetzbuch; verlangt er als “Selbstzahler” oder “Privatversicherter” eine detaillierte Rechnung, bestimmt er damit selbst, welche zusätzlichen Diagnose- und Therapiedaten vom behandelnden Arzt an die Krankenhausverwaltung herausgegeben werden müssen. Auch diese Abrechnungsbestände sind als besonders schutzbedürftig zu klassifizieren. Sie unterliegen aber anderen Verarbeitungsregeln. Die **medizinische Dokumentation** muss z. B. mindestens 10 Jahre (in der Regel 30 Jahre) gespeichert bleiben, ist aber nach Entlassung des Patienten so zu archivieren, dass nachträgliche Änderungen faktisch unmöglich sind und ein Zugriff nur den behandelnden bzw. den nachbehandelnden Ärzten gestattet wird. Die Abrechnungsdaten unterliegen dagegen nur den kaufmännischen Nachweis- und Aufbewahrungsbestimmungen, das heißt, sie können nach Eingang des Behandlungsentgeltes aggregiert werden, zumindest können jedoch die Diagnose- und Therapiemerkmale gelöscht werden.

Diese und viele weitere unterschiedliche Anforderungen an die Dokumentations- und die Abrechnungskomponenten der Krankenhausinformationssysteme müssen ihren Niederschlag in den **Sicherheitskonzepten** finden. Bei den meisten der von uns begutachteten Lösungen bzw. Planstudien fehlte es an einer klaren fachlichen Verantwortungsabgrenzung zwischen diesen Bereichen. Da man die Hard- und Software bei den Anbietern zumeist “von der Stange” kaufte, entschied im Ergebnis nicht selten der EDV-Leiter über Zugriffsrechte, Datenprofile und Sicherheitskonzepte. Die eigentlichen Verantwortungsträger, nämlich die Ärzte, waren zufrieden, wenn die EDV-Systeme denn nur liefen. Deshalb gilt diesem Bereich auch in Zukunft unser besonderes Augenmerk.

Was ist zu tun?
Bei der Planung von Krankenhausinformationssystemen ist von Anfang an zwischen den Bereichen “medizinische Dokumentation” und “Abrechnung” zu differenzieren. Die Funktionalitäts- und Sicherheitsanforderungen sind von den

jeweiligen Verantwortungsträgern zunächst getrennt festzulegen. Erst danach wird erkennbar, wo und in welchem Umfang "Integrationen" möglich sind.

6.6 Landrat macht Datenschutz zur Chefsache

Der Nutzen der datenschutzrechtlich vorgeschriebenen Sicherheitskonzepte wird häufig verkannt. Ein Landrat hat den Spieß umgedreht. Er betrachtet die Datensicherheitsvorschriften als nützliches Instrument zur Verwaltungsmodernisierung.

Schon seit einigen Jahren beschreitet der Kreis Schleswig-Flensburg einen Sonderweg bezüglich seiner "**Datenschutzpolitik**". Er bestellte eine hauptamtliche behördliche Datenschutzbeauftragte und ließ sie nicht nur an der DATENSCHUTZAKADEMIE, sondern auch durch ein "Training on the job" in unserer Dienststelle qualifiziert ausbilden. Der Nutzen dieser Investition zeigte sich darin, dass sehr frühzeitig die Bedeutung eines IT-Konzeptes erkannt wurde. Auf der Grundlage dieses "Gesamtplans" und einer "Bestandsaufnahme zur Ermittlung der Datensicherheitssituation" ist nunmehr auch ein **allgemeines Sicherheitskonzept** erstellt worden. Es enthält die Mindestanforderungen, die alle Fachbereiche der Kreisverwaltung einzuhalten haben. Die von den Dezernaten gemeinsam erarbeiteten Regelungen beziehen sich nicht nur auf die datenschutzrechtlich besonders bedeutsamen Aspekte der Vertraulichkeit von Daten, sondern auch auf die Anforderungen an die Verfügbarkeit der Systeme (z. B. Schutz vor Ausfall, Diebstahl und Zerstörung) und an die Integrität der automatisierten Verfahren (z. B. Schutz vor fahrlässiger oder vorsätzlicher Verfälschung von Programmen oder Manipulation von Dateien des Rechnungswesens). Man brauchte erstaunlicherweise gerade einmal ein Dutzend Seiten, um in prägnanten Sätzen und in einer übersichtlich gegliederten Form die grundlegenden "Sicherheitsspielregeln" zu formulieren, die bei der Beschaffung von Hard- und Software, der Nutzung der Arbeitsplatzrechner, der Verwaltung von Datenträgern und Dateien, dem Internet-Zugang, der Nutzung der Standardsoftware, der Administration der Server usw. zu beachten sind.

Bemerkenswert ist aus unserer Sicht, dass der **Landrat** selbst sich zum Protagonisten einer innovativen Datensicherheitspolitik gemacht hat. Anlässlich der Präsentation des Sicherheitskonzeptes vor der Presse hob er hervor, dass die heutigen Ziele einer Kreisverwaltung wie **Wirtschaftlichkeit**, **Bürgerorientierung** und **Verwaltungsmodernisierung** und der Schutz der Bürgerinnen und Bürger vor einer allumfassenden und ungeregelten Einbeziehung ihrer Daten in automatisierte Verarbeitungsprozesse durchaus miteinander in Einklang gebracht werden können. Die Erfahrungen hätten gezeigt, dass präzise und umsetzbare "Empfehlungen" auf Dauer mehr Akzeptanz für den **Datenschutz** schaffen als ausschließlich der Druck von Kontrollen.

Was ist zu tun?
Dem Kreis Schleswig-Flensburg ist zu raten, den eingeschlagenen Weg konsequent fortzusetzen. Die anderen Landräte sollten in ihren Häusern

vergleichbare Vorgehensweisen anstoßen.

7 Recht und Technik der Neuen Medien

7.1 Rund ums Internet

7.1.1 Mit Sicherheit ins Internet

Immer mehr Verwaltungen drängen ins Internet. Dies ist nicht ohne Risiko, denn ständig gehen Meldungen von erfolgreichen Angriffen ein: Neu ist z. B. eine Virusart, die, per Mail verschickt, einen Rechner infizieren kann, ohne dass der Nutzer die E-Mail öffnet.

Bubbleboy hieß der Computerwurm – so die Bezeichnung für ein Programm, das Kopien von sich durch das Netz schickt. Für die Aktivierung reichte der bisher für unschädlich gehaltene **Vorschau-Modus** des E-Mail-Programms Outlook der Firma Microsoft. Dies ist nur eine der vielen möglichen Gefahren, die über das Internet auch Verwaltungsrechner betreffen können. In den Vorjahren haben wir mehrfach zu der Problematik Stellung genommen, ob und wie sich ein sicherer Anschluss an das Internet realisieren lässt (vgl. 21. TB, Tz. 7.1.2; 20. TB, Tz. 7.5.1). Die Grundaussagen haben weiterhin Bestand:

Ein Anschluss von Rechnern, die physikalisch vom Verwaltungsnetz getrennt sind und keine sensiblen Datenbestände enthalten, ist recht einfach und unproblematisch möglich. Will man einen Internet-Zugang vom Verwaltungssystem aus realisieren, benötigt man ein **Firewall-System**, das das interne Netz vor möglichen Angriffen aus dem Internet abschottet. Die Filterregeln, die in der Firewall implementiert werden sollen, müssen vorher durch eine Kommunikationsanalyse ermittelt werden: Welche Dienste im Internet müssen eigentlich von welchen Rechnern oder Teilnehmern nutzbar sein?

> **?** ***Firewall***
>
> *Eine Firewall (deutsch: "Brandschutzmauer") ist ein System aus Hard- und Software, das nach bestimmten Regeln unerwünschte Kommunikation ausfiltert. Firewalls eignen sich dazu, Netze unterschiedlichen Schutzbedarfs kontrolliert zu verbinden, z. B. für den Anschluss eines lokalen Netzes ans Internet. Man unterscheidet Paketfilter, die auf Transportebene nach Rechneradresse und Dienst (IP-Adresse und Port) filtern, und Application Level Gateways, die auf Anwendungsebene dienstspezifisch agieren. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt für einen mittleren Schutzbedarf den Einsatz von kombinierten Systemen.*

Auch mit einer korrekt aufgebauten Firewall ist man noch nicht sicher: Zum einen muss man sich vor Trojanischen Pferden schützen, die über aktive Inhalte im WWW, Programme oder E-Mails ins heimische Netz eindringen können (Maßnahmen: **aktive Inhalte** deaktivieren, stets auf aktuellen Virenschutz achten; vgl. Tz. 9.2). Zum anderen muss man ständig wachsam sein und sich gegen neu entdeckte Sicherheitsrisiken wappnen. Dies erfordert Personal mit entsprechendem Know-how und zeitlichen Ressourcen.

Im Projekt “Virtuelles Datenschutzbüro” (vgl. Tz. 8.4) arbeiten wir an der Umsetzung einer datenschutzkonformen Internet-Anbindung mit einem hohen Grad an Sicherheit. Dafür beschäftigen wir uns auch mit innovativen Konzepten, die hier kurz vorgestellt werden:

- **Virtual Network Computing (VNC)**

  Beim Virtual Network Computing sind die Arbeitsplatzrechner nicht direkt mit dem Internet verbunden, sondern können lediglich die grafische Ausgabe eines speziellen VNC-Servers auf dem Monitor anzeigen (vgl. Tz. 9.4). Alle Aktionen mit Tastatur und Maus werden an diesen VNC-Server weitergeleitet, der sie entsprechend umsetzt und ans Internet weitergibt. Die eigentlichen Programme laufen also nicht auf dem Arbeitsplatzrechner mit sensiblen Daten, sondern auf dem VNC-Server ab und können daher im eigentlichen System kaum mehr Schaden anrichten. Selbstverständlich ist der VNC-Server trotzdem durch eine Firewall gesichert.

- **Protokollentkopplung**

  Wo allein die grafische Ausgabe der Daten und das Arbeiten auf dem VNC-Server nicht ausreicht, sondern die Daten auf dem Arbeitsplatzrechner zur Verfügung stehen müssen, können diese mithilfe von speziellen Kommunikationsstandards wie UUCP vom Server übertragen werden. Damit besteht keine direkte TCP/IP-Verbindung, die für Angriffe auf den Arbeitsplatzrechner genutzt werden könnte.

- **Snipped Wire**

  Die Logdateien einer Firewall, in denen möglicherweise Angriffe protokolliert werden, sind auch für Angreifer sehr interessant: Zum einen können sie sensible Informationen beinhalten, zum anderen ist der Angreifer bestrebt, seine Spuren aus den Logdateien zu tilgen. Dieser Zugriff lässt sich durch eine “Einbahnstraßenprotokollierung” verhindern, indem die Logdaten über eine zusätzliche Netzwerkkarte, deren Rückkanal physikalisch unterbrochen wurde (Snipped Wire), auf einen gesonderten Logserver geschrieben werden.

Was ist zu tun?
Bevor man sich ans Internet anschließt, muss geklärt werden, wie man den erforderlichen Grad der Sicherheit dauerhaft gewährleistet.

7.1.2 IP-Nummern als personenbezogene Daten?

Wer eine Homepage einrichtet, möchte gerne wissen, wie häufig diese besucht wird und wofür sich die Nutzer am meisten interessieren. Dies darf aber nicht dazu führen, dass über einzelne Nutzer Informationsprofile entstehen.

Vielen Surfern im World Wide Web (WWW) stellt sich die Frage: Bekommt der Betreiber des Servers eigentlich mit, welche Inhalte ich gerade abrufe? Selbst dann nämlich, wenn der Nutzer keine weiteren Daten über seine Identität offenbart (wenn er also z. B. keine Formulare ausfüllt und die E-Mail-Adresse nicht angibt), fällt am Server in jedem Fall eine Information an: Dies ist die **IP-Nummer**, unter der die Informationen abgerufen werden.

> **?** ***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 sog. Domain-Namen zugeordnet. So hat der Webserver, der sich über www.datenschutz.de adressieren lässt, die IP-Nummer 130.149.19.57. Die Zuordnung wird im sog. Domain Name System (DNS) über bestimmte DNS-Server aufgelöst.*

Für die Rechner im Internet sind IP-Nummern das, was Telefonnummern im Bereich der herkömmlichen Telefonnetze darstellen: Ohne eine Nummer lässt sich kein anderer Rechner adressieren; jeder Rechner benötigt für die Kommunikation im Internet eine IP-Nummer. Während die Internet-Server feste IP-Nummern haben, gilt dies für die allermeisten Nutzer nicht. Wer sich mit einem Online-Dienst oder über einen sonstigen so genannten Access-Provider an das Internet anschließt, muss keine eigene IP-Nummer “von zu Hause” mitbringen. Vielmehr bekommt er diese von seinem Access-Provider für die jeweilige **Internet-Session** zur Verfügung gestellt. Der Access-Provider verfügt über eine Vielzahl solcher Nummern. Diese teilt er jeweils der Reihe nach den Nutzern zu, die sich neu einwählen. Technisch bedingt kommt es teilweise auch zu einer neuen Vergabe von IP-Adressen während eines Zugriffs. Die Nutzer können hier also relativ sicher sein, dass sie mindestens bei jeder neuen Session mit einer anderen IP-Adresse im Internet aktiv werden. Wer nur die IP-Adresse des Nutzers erfährt, kann allenfalls zuordnen, zu welchem Access-Provider beziehungsweise Online-Dienst diese gehört.

> **?** ***Webserver***
>
> *Der populärste Dienst im Internet ist das World Wide Web (WWW). Es basiert auf einer Vielzahl von Computern, die über das Internet erreichbar sind. Auf diesen sog. Webservern werden unzählige digital gespeicherte Inhalte bereitgehalten. Nutzer in der ganzen Welt können diese abrufen und sie sich auf ihrem Rechner als Schrift, Bilder, Töne usw. darstellen lassen.*

Der Nutzer lässt sich also vom Betreiber des Webservers – im Gegensatz zum Access-Provider, dem die Zuordnung bekannt ist – ohne weitere Hilfsmittel nicht identifizieren. Dies ist wichtig, weil an den Webservern regelmäßig **Protokolldateien** (Logfiles) gespeichert werden, die nicht nur abstrakt die Zahl der Zugriffe zählen, sondern für jeden Zugriff die IP-Nummer mitspeichern, von der aus zugegriffen wurde. Wählt sich ein Nutzer über seinen Access-Provider ins Internet ein, so wird also am Webserver lediglich die vom Access-Provider jeweils vergebene IP-Nummer gespeichert. Dem Betreiber des Servers ist es nicht erlaubt, beim Access-Provider nachzufragen, welcher Nutzer sich hinter einer IP-Nummer verbirgt. Hat der Betreiber des Webservers keine Möglichkeit, eine Nummer dem dahinterstehenden Nutzer zuzuordnen, so stellt allein die IP-Nummer für ihn kein personenbezogenes Datum dar.

Im Wortlaut:
§ 6 Abs. 1 und 2 TDDSG

(1) Der Diensteanbieter darf personenbezogene Daten über die Inanspruchnahme von Telediensten nur erheben, verarbeiten und nutzen, soweit dies erforderlich ist ...
3. um dem Nutzer die Inanspruchnahme von Telediensten zu ermöglichen (Nutzungsdaten) oder
4. um die Nutzung von Telediensten abzurechnen (Abrechnungsdaten).
(2) Zu löschen hat der Diensteanbieter
1. Nutzungsdaten frühestmöglich, spätestens unmittelbar nach Ende der jeweiligen Nutzung, soweit es sich nicht um Abrechnungsdaten handelt.
2. Abrechnungsdaten, sobald sie für Zwecke der Abrechnung nicht mehr erforderlich sind; nutzerbezogene Abrechnungsdaten, die für die Erstellung von Einzelnachweisen über die Inanspruchnahme bestimmter Angebote auf Verlangen des Nutzers gemäß Absatz 4 gespeichert werden, sind spätestens 80 Tage nach Versendung des Einzelnachweises zu löschen, es sei denn, die Entgeltforderung wird innerhalb dieser Frist bestritten oder trotz Zahlungsaufforderung nicht beglichen.

Leider ist die Lage im Internet jedoch keineswegs immer so eindeutig. Es gibt nämlich auch eine Vielzahl von Rechnern, die über **fest vergebene IP-Adressen** verfügen. Zum einen sind dies häufig die Rechner in Universitäten und Firmen. Hier haben die Organisationen oft einen großen Bereich von Nummern erworben, die sie den einzelnen zu ihnen gehörigen Rechnern fest zuweisen. Aber auch private Nutzer, die sehr früh im Internet präsent waren, hatten seinerzeit noch gute Chancen, eine feste IP-Adresse zu bekommen. In diesen Fällen lässt sich die IP-Adresse häufig auch ohne weitere Hilfsmittel einem bestimmten Nutzer zuordnen.

Bei fest vergebenen IP-Nummern muss also davon ausgegangen werden, dass der **Personenbezug** vorliegt und die datenschutzrechtlichen Vorschriften der Multimediagesetze (TDDSG) gelten. Die Verarbeitung der Daten ist danach nur dann erlaubt, wenn diese technisch erforderlich ist, um den Dienst zu erbringen, oder wenn die Daten zu Abrechnungszwecken gebraucht werden. Beides trifft für die in den Logfiles festgehaltenen IP-Nummern nicht zu. Zwar werden diese während des Zugriffs aus technischen Gründen benötigt. Darüber hinaus sind sie jedoch nicht von Bedeutung. Auch wird im Regelfall nicht danach abgerechnet, welche IP-Adresse auf den Server zugegriffen hat. Die Speicherung der festen IP-

Adressen in den Server-Logfiles ist demnach unzulässig.

Fraglich ist nun, wie ein rechtmäßiges **Server-Logfile** erstellt werden kann. Zum einen kann vollständig auf die Speicherung von IP-Adressen verzichtet werden. In diesen Fällen ergeben sich selbstverständlich keine Probleme. Zum anderen besteht jedenfalls theoretisch die Möglichkeit, die "Adressräume" zu kennzeichnen, die bestimmten Online-Diensten oder Access-Providern zugeordnet sind und bei denen die IP-Nummernvergabe dynamisch erfolgt. Wird mit einer solchen IP-Nummer aus einem dieser Adressräume auf den Server zugegriffen, so kann dieser sicher sein, dass es sich um nichtpersonenbezogene Daten handelt und sie speichern. Andere IP-Nummern dürften nicht gespeichert werden. Eine weitere Variante, die in der Praxis möglicherweise am einfachsten umzusetzen ist, besteht darin, die letzte der vier Komponenten einer IP-Nummer (eine Zahl zwischen 0 und 255) zu löschen. Zum Beispiel würde aus der IP-Nummer 195.217.35.229 dann 195.217.35.XXX.

Leider ist diese Rechtslage bisher bei den Anbietern noch **häufig unberücksichtigt** geblieben. Dies mag auch daran liegen, dass entsprechende Standardsoftware die genannten Möglichkeiten noch nicht einräumt. Es ist daher eine wichtige Aufgabe für die Entwickler von Software, datenschutzgerechte Optionen einzubauen.

Die Problematik betrifft übrigens nicht nur die Betreiber der Webserver. Zu den Diensteanbietern, die die Pflichten der Gesetze treffen, gehören auch diejenigen, die lediglich ihre **Homepages** selbst bereitstellen (sog. Content-Provider) und sich der Betreiber von Webservern bedienen, um ihre Inhalte in das WWW einzustellen. Die Content-Provider schließen mit den Server-Betreibern Verträge über das **Web-Hosting** ab. In der Praxis gehört es regelmäßig zum Leistungsumfang, dass die Content-Provider eine mehr oder weniger ausführliche Information über die Zugriffe auf ihre Web-Seiten erhalten. Um ihren datenschutzrechtlichen Pflichten nachzukommen, haben die Content-Provider darauf zu achten, dass Inhalt der Verträge auch die datenschutzrechtlich zulässige Ausgestaltung der Logfiles ist.

? ***Web-Hosting***

Jeder, der seine Inhalte im Internet zur Verfügung stellen will, muss dafür sorgen, dass diese auf einem Webserver für alle Internet-Nutzer bereitgehalten werden. Allerdings ist es nicht erforderlich, dass er selbst den Webserver aufstellt. Wer nur die Inhalte zur Verfügung stellen möchte, kann sich dazu auch eines Webservers bedienen, der von einem anderen betrieben wird. Da in diesem Fall aus der Sicht des Server-Betreibers der eigene Rechner fremde Inhalte beherbergt (engl. to host), spricht man von Web-Hosting.

Was ist zu tun:
Öffentliche und private Stellen sollten bei der Gestaltung ihrer Server-Logfiles darauf achten, dass diese den datenschutzrechtlichen Vorschriften entsprechen. Softwareentwickler sollten daran arbeiten, Verfahren zu implementieren, die die Umsetzung der Gesetze erleichtern.

7.1.3 Mitarbeiterdaten auf der Homepage

Wenn sich öffentliche Stellen modern und bürgerfreundlich darstellen wollen, gehört dazu häufig auch die eigene Homepage im Internet. Sollen auf dieser allerdings die Namen der Mitarbeiter veröffentlicht werden, so geht dies nur mit deren Einwilligung.

Viele öffentliche Stellen verfügen bereits über eine eigene Homepage oder planen, eine solche einzurichten. Zu den regelmäßig dort veröffentlichten Informationen gehört auch der **Geschäftsverteilungsplan**. Allerdings ist es nicht ohne weiteres zulässig, dabei auch den Namen der jeweils zuständigen Mitarbeiter anzugeben. Im Zusammenhang mit der Aufgabenerfüllung wird in Behörden häufig der Name der Beschäftigten genannt, sei es, dass er auf einem dienstlichen Schreiben auftaucht, an der Bürotür oder am stummen Portier im Behördeneingang festgehalten ist. Der grundrechtlich geschützte Bereich der Betroffenen wird hier faktisch nicht beeinträchtigt; die Beschäftigten werden dabei als Organe der öffentlichen Stelle, für die sie handeln, benannt. Die Namen der Beschäftigten sind als so genannte **Funktionsträger-Daten** zu betrachten. Darüber hinausgehende Daten wie die Privatadresse, das Geburtsdatum, die private Telefonnummer oder gar ein Foto unterfallen dem informationellen Selbstbestimmungsrecht.

Im Internet erhalten die Mitarbeiterdaten eine vollständig **neue Qualität**. Zum einen geht es um ein weltweit zugängliches Medium. Noch bedeutungsvoller ist allerdings, dass sämtliche im Internet anzutreffenden Daten mit allen anderen Daten über die betroffene Person problemlos verknüpft werden können. So können Informationen über die dienstliche Stellung ohne weiteres mit Daten aus privatem Kontext zu einem Persönlichkeitsprofil zusammengeführt werden. Potenzielle Arbeitgeber, Vermieter oder andere Interessierte könnten sich so eine Vielzahl von Informationen über die Betroffenen beschaffen.

Für die Veröffentlichung in diesem Verwendungszusammenhang ist demnach grundsätzlich die **Einwilligung der Mitarbeiter** erforderlich. Bei der Einholung der Einwilligung im Rahmen eines Arbeitsverhältnisses muss darauf geachtet werden, dass kein Druck auf die Beschäftigten ausgeübt und die Erklärung wirklich freiwillig abgegeben wird. Liegt die Einwilligung der Betroffenen nicht vor, so kommt noch die Veröffentlichung auf Grund einer Rechtsvorschrift in Betracht. Eine solche dürfte jedoch in den seltensten Fällen zur Verfügung stehen. Lässt sich die Einwilligung der Mitarbeiter nicht einholen, so können die dienstlichen Kommunikationsdaten in der Weise veröffentlicht werden, dass statt des Namens der Mitarbeiter nur die jeweilige Funktion angegeben wird; also zum Beispiel: *Bearbeitung von BAFöG-Angelegenheiten: Telefonnummer 1234.*

Was ist zu tun?
Bei der Internet-Präsentation öffentlicher Stellen dürfen die Namen der Mitarbeiter nicht ohne deren Einwilligung auf den Homepages veröffentlicht werden. Lässt sich die Einwilligung nicht einholen, so dürfen lediglich die Funktionen bezeichnet werden.

7.1.4 Wie weit darf der Vorgesetzte die Internet-Nutzung kontrollieren?

Auch in der öffentlichen Verwaltung setzt sich der dienstliche Internet-Zugang für viele Mitarbeiter langsam durch. Eine klare Regelung über die Kontrollbefugnisse des Arbeitgebers bzw. Dienstherren kann spätere Streitigkeiten verhindern.

Beim Anschluss an das Internet stehen vor allem die Kommunikation via E-Mail und die Informationsrecherche im WWW für die Mitarbeiter im Vordergrund. Im 21. Tätigkeitsbericht haben wir im Zusammenhang mit dem Einsatz von Firewalls auf die Kontrollmöglichkeiten und deren rechtlichen Grenzen hingewiesen (vgl. Tz. 7.1.2). Auch unabhängig von Firewalls lässt sich z. B. schon mit den häufig zur Abrechnung vorliegenden Daten über die Dauer der Internet-Zugriffe eine gewisse Kontrolle der Mitarbeiter bewerkstelligen. Wie weit darf die **Kontrolle der dienstlichen Zugriffe** im WWW gehen? Eine pauschale Antwort, die sämtlichen Sachverhalten gerecht wird, lässt sich kaum finden. Generell geht es um den sachgerechten Ausgleich zwischen den Persönlichkeitsrechten der Beschäftigten und den berechtigten Kontrollinteressen des Arbeitgebers bzw. Dienstherrn.

Grundsätzlich hat der Arbeitgeber das Recht, nachzuprüfen, ob die dienstlichen WWW-Zugriffe noch einen angemessenen Umfang haben und ob tatsächlich dienstlich relevante Seiten angesurft wurden. Dabei lassen sich Erkenntnisse über besondere Informationsinteressen und über das Vorgehen bei der Recherche gewinnen. Es können aber auch Anhaltspunkte für Verhaltens- und Leistungskontrolle entstehen. Deshalb muss bei diesen Kontrollen der **Verhältnismäßigkeitsgrundsatz** gewahrt werden. In einer ersten Stufe kann eine nicht auf die einzelnen Beschäftigten bezogene Auswertung der häufig angesurften Internet-Angebote erfolgen.

Probleme verursacht erfahrungsgemäß vor allem das übermäßige Interesse für die zahlreichen **erotischen Angebote** im Internet. Hier lassen sich die bekannt gewordenen einschlägigen Adressen in eine Sperrliste eintragen, wodurch ein direkter Zugriff nicht mehr möglich ist. Die Auswertung der Logfiles der dienstlichen Zugriffe kann sodann – ohne Bezug zu den einzelnen Mitarbeitern – daraufhin vorgenommen werden, welche nichtdienstlichen Seiten besonders häufig besucht werden. Ergeben sich dabei unzulässige Zugriffe in signifikantem Umfang, so sollten die Beschäftigten zunächst pauschal auf die Unzulässigkeit dieses Verhaltens hingewiesen werden. Gleichzeitig sollte in Aussicht gestellt werden, dass bei Fortdauer der Verstöße eine personalisierte Kontrolle stattfindet. Fördert eine spätere Stichprobe tatsächlich weitere Zuwiderhandlungen gegen die dienstlichen Vorgaben zutage, so kann festgestellt werden, von welchem Rechner aus und unter welchem Account derartige Zugriffe stattgefunden haben. Arbeitsrechtliche Maßnahmen gegen die betroffenden Mitarbeiter sind dann nicht mehr ausgeschlossen.

Selbstverständlich sind derartige Kontrollmechanismen durch die

Personalvertretungsgremien **mitbestimmungspflichtig**. Es empfiehlt sich daher, eine Betriebsvereinbarung bzw. Dienstvereinbarung abzuschließen, die das soeben skizzierte Verfahren im Einzelnen festschreibt. Dabei sollte geregelt werden, dass auch die Arbeitnehmervertreter an den Kontrollen teilnehmen. Alternativ oder zusätzlich kann auch der betriebliche oder behördliche Datenschutzbeauftragte einbezogen werden.

Was ist zu tun?
Bei der Kontrolle der dienstlichen Nutzung des Internet ist das Verhältnismäßigkeitsprinzip zu beachten.

7.1.5 Wieviel Zusammenarbeit schulden Provider der Polizei?

Jeder Nutzer hinterlässt im Internet Datenspuren, von denen sich etliche bei Ermittlungen unter Mithilfe des Providers herausfinden lassen. Eine grundsätzliche Verpflichtung der Provider, für eventuelle spätere Ermittlungen alle Daten zu speichern, besteht nicht.

Im Jahr 1999 fanden mehrere Zusammenkünfte zwischen Strafverfolgungsbehörden, Internet-Providern und Datenschützern statt. Das Bundeskriminalamt (BKA) hatte hierzu eingeladen, um die Zusammenarbeit zwischen den **Providern** und der **Polizei** zu verbessern. Die Treffen ergaben, dass es bei einer Reihe von Fragen durchaus unterschiedliche Auffassungen gibt, unter anderem, wozu die Internet-Provider verpflichtet sind. Als problematisch stellte sich vor allem die Abgrenzung zwischen dem Tele- und Mediendienste- und dem Telekommunikationsrecht heraus. Die meisten Eingriffsbefugnisse der Strafverfolgungsbehörden richten sich an die Betreiber von **Telekommunikationsdiensten**. Große Access-Provider und Online-Dienste wie T-Online gehen allerdings davon aus, dass die strafprozessualen Eingriffsbefugnisse auch sie treffen.

Probleme in der Praxis ergeben sich z. B. dann, wenn Strafverfolgungsbehörden bestimmte IP-Adressen im Netz aufgefunden haben und nun von den Access-Providern erfahren wollen, welchen Nutzern diese Nummern zugeordnet waren. Bei den **Access-Providern** dürfen diese Daten von Rechts wegen gar nicht gespeichert werden (siehe oben Tz. 7.1.2). In der Praxis kommt es allerdings häufig zu relativ kurzfristigen Speicherungen von wenigen Tagen. In diesem Zusammenhang wird im Kreis der G8-Staaten diskutiert, im Wege einer so genannten Preservation-Order einen "**Fast Freeze – Quick Thaw**" der Verbindungsdaten herbeizuführen. Dieser soll dazu dienen, die Daten solange zu

? ***Fast Freeze – Quick Thaw***

Unter dem Stichwort "Fast Freeze – Quick Thaw" (etwa: schnelles Einfrieren, rasches Auftauen) diskutieren die G8-Staaten die Option, wonach Provider sozusagen auf Zuruf der Strafverfolungsbehörden Verbindungsdaten von der an sich vorgesehenen Löschung ausnehmen (einfrieren) und bei Vorliegen eines richterlichen Beschlusses an die Strafverfolger herausgeben (auftauen).

konservieren, bis eine richterliche Genehmigung zum Zugriff auf die Daten vorliegt.
Aus datenschutzrechtlicher Sicht ist dieses Verfahren in jedem Fall Überlegungen zur Einführung einer generellen Mindestspeicherungsdauer für sämtliche Verbindungsdaten vorzuziehen. Auch die auf Ebene der EU eingerichtete Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten hat sich dagegen ausgesprochen, Daten aus der Telekommunikation nur im Hinblick auf einen späteren eventuellen Zugriff der Strafverfolgungsbehörden zu speichern (Empfehlung 3/99 vom 07.09.1999, 5085/99). Vielmehr sollte die Speicherdauer an der **Erforderlichkeit für die Abrechnung** orientiert sein, wie es dem deutschen Recht entspricht.

7.2 Recht auf unbeobachtete Telekommunikation

7.2.1 Eckpunkte zur Kryptopolitik

Die Bundesregierung hat 1999 erstmals erklärt, dass der Einsatz von Kryptoverfahren nicht eingeschränkt werden, sondern stattdessen gefördert werden soll. Die ersten Taten folgen bereits mit der Unterstützung der Entwicklung von Open-Source-Kryptoprodukten.

Die Vertraulichkeit von elektronischer Kommunikation ist essenziell, unabhängig davon, ob es sich um private Nachrichten oder um die Teilnahme am **E-Commerce** handelt. Die Lösung heißt **Verschlüsselung**. Seit Jahren gibt es eine rege Diskussion über die Frage möglicher gesetzlicher Regulierungen der Stärke und Art der einsetzbaren Verfahren. Da die weit verbreiteten Produkte aus den USA bislang mit Exportbeschränkungen versehen sind und lediglich in einer relativ leicht entschlüsselbaren Form angeboten werden, bleibt ein unbefriedigendes Sicherheitsrisiko bestehen – so der Tenor der öffentlichen Auseinandersetzungen der letzten Jahre in fast allen demokratischen Industrieländern. Um so entscheidender tritt die Frage einer möglichen deutschen Kryptoregelung in den Vordergrund. In den vergangenen Jahren gab es mehrfach Initiativen zur gesetzlichen Begrenzung der verwendbaren Schlüssellängen bzw. zum zwingenden Einbau zur Beobachtung geeigneter "**Hintertüren**". Hiergegen haben wir uns entschieden gewandt (vgl. 21. TB, Tz. 7.4).

Mit dem **Eckpunktepapier der Bundesregierung** zur deutschen Kryptopolitik vom Juli dieses Jahres werden wesentliche positive Rahmenbedingungen für den verstärkten Einsatz kryptographischer Verfahren und Produkte abgesteckt. Die entscheidende Aussage besteht in der Zusage der Beibehaltung der "**uneingeschränkten Freiheit** der Nutzer bei der Auswahl und dem Einsatz von Verschlüsselungssystemen". Ferner wird auch von einer **Förderung** des Einsatzes von **Kryptographie** bei der Datenübermittlung gesprochen. Eine solche Förderung ist schon deshalb sinnvoll, weil Verschlüsselungsprodukte in Deutschland immer noch nicht im erforderlichen Maß eingesetzt werden. Die E-Mail-Kommunikation weist z. B. nach aktuellen Studien lediglich einen Verschlüsselungsanteil von etwa 4 % auf.

Aus unserer Sicht sind deshalb folgende Forderungen angebracht, die auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erhoben hat:

- Aktive Förderung des Einsatzes von Verschlüsselungstechniken durch Privatpersonen und Wirtschaftsunternehmen,
- Erbringung von Serviceleistungen, die den Gebrauch von effektiven Verschlüsselungsprogrammen für jedermann erleichtern,
- Maßnahmen zum besonderen Schutz der Telekommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen, wie Ärzten, Anwälten, Psychologen usw.,
- Förderung der Gründung einer "Stiftung Datenschutztest", die u. a. die Aufgabe hat, Verschlüsselungsprodukte zu testen und den Verbrauchern Empfehlungen für ihren Gebrauch zu geben,
- Unterstützung von Wirtschaftsunternehmen beim Schutz ihrer Betriebsgeheimnisse gegen Abhörversuche ausländischer Geheimdienste,
- Förderung der Entwicklung europäischer Verschlüsselungsprodukte mit offen gelegten Algorithmen.

Unsere Dienststelle propagiert seit Jahren den Einsatz von Verschlüsselungstechniken. In Kursen der DATENSCHUTZAKADEMIE kann das entsprechende Know-how erworben werden. Aufkleber und Informationsblätter sowie eine zugehörige Serviceseite im Internet werben für die Kryptographie als ein wichtiges Instrument zur Sicherung der Privatsphäre.

datenschutz.inside.tm/pgp/

Was ist zu tun?
Die Bundesregierung sollte den eingeschlagenen Weg fortsetzen, Kryptographie nicht zu reglementieren, sondern ihren Einsatz zu fördern. Die öffentlichen Stellen des Landes sind aufgefordert, den Datenschutz durch den verstärkten Einsatz der Kryptographie zu verbessern.

7.2.2 Überwachungsschnittstellen obligatorisch?

Die Bundesregierung hat in einem Eckpunktepapier zur Telekommunikations-Überwachungsverordnung (TKÜV) dargelegt, wie sie sich die Mitwirkungspflichten der Telekommunikationsunternehmen an Überwachungsmaßnahmen vorstellt.

Nach dem Telekommunikationsgesetz (TKG) sind Betreiber von Telekommunikationsanlagen verpflichtet, auf eigene Kosten technische Einrichtungen vorzuhalten, die die Überwachung und Aufzeichnung von Telekommunikation ermöglichen. Diese Pflicht trifft einen

Im Wortlaut: § 88 Abs. 1 TKG

(1) Die technischen Einrichtungen zur Umsetzung von gesetzlich vorgesehenen Maßnahmen zur Überwachung der Telekommunikation sind von dem Betreiber der Telekommunikationsanlage auf eigene Kosten zu gestalten und vorzuhalten.

sehr weiten Adressatenkreis (u.a. auch Krankenhaus- und Hotelbetreiber sowie zum Teil Arbeitgeber); um sie umzusetzen, sind Investitionen in erheblicher Höhe erforderlich. Als diese Pflicht in einer **Telekommunikations-Überwachungsverordnung (TKÜV)** konkretisiert werden sollte und absehbar war, dass es kaum Ausnahmen geben würde, kam es zu vehementer Kritik aus der Wirtschaft (vgl. 21. TB, Tz. 7.7). Daraufhin ist ein erster **Entwurf der TKÜV** zunächst zurückgestellt worden.

www.digital-law.net/papers/TKUEV.htm

Auf die nähere Ausgestaltung der Vorschriften des TKG in einer Verordnung kann jedoch auf die Dauer nicht verzichtet werden. Die Bundesregierung hat deshalb im April 1999 ein sog. **Eckpunktepapier** veröffentlicht (siehe unter *http://www.dud.de/dud/files/eckp0499.zip*). Vorgesehen ist danach eine Unterscheidung von drei Betreibergruppen:

- Betreiber von Telekommunikationsanlagen, mit denen Dienstleistungen **für die Öffentlichkeit** erbracht werden, soll die Verpflichtung zur Einrichtung und Unterhaltung der Schnittstelle in vollem Umfang treffen.
- Betreiber von nichtöffentlichen Netzen (Corporate Networks, Intranets etc.) brauchen keine permanenten technischen Vorkehrungen zu treffen. Es reicht aus, wenn im Einzelfall für Sicherheitsbehörden die Möglichkeit eingerichtet wird, die Telekommunikation vor Ort zu überwachen und aufzuzeichnen.
- Dasselbe soll für die Betreiber von Telekommunikationsanlagen gelten, mit denen Telekommunikationsdienste ohne Gewinnerzielungsabsicht angeboten werden (z. B. Nebenstellenanlagen in Krankenhäusern, Wohnheimen etc.).

Im Wortlaut:
Auszug aus § 88 Abs. 2 TKG

(2) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf,
1. die Anforderungen an Gestaltung der technischen Einrichtungen sowie an die organisatorische Umsetzung von Überwachungsmaßnahmen mittels dieser Einrichtungen und
2. das Genehmigungsverfahren und das Verfahren der Abnahme zu regeln sowie
3. zu bestimmen, bei welchen Telekommunikationsanlagen aus grundlegenden technischen Erwägungen oder aus Gründen der Verhältnismäßigkeit abweichend von Absatz 1 technische Einrichtungen nicht zu gestalten oder vorzuhalten sind.

Die Rechtsverordnung kann vorsehen, dass in technisch begründeten Ausnahmefällen auf Antrag von der Erfüllung einzelner technischer Anforderungen an die Gestaltung der Einrichtungen abgesehen und mit welchen Nebenbestimmungen die Genehmigung in diesen Fällen versehen werden kann.

Zwar ist die geplante Abstufung ein Schritt in die richtige Richtung. Problematisch bleibt aber weiterhin die Einbeziehung der Anbieter von solchen **Internet-Diensten**, die sich als **Individualkommunikation** (z. B. E-Mail) einordnen lassen. Das

Eckpunktepapier stellt ausdrücklich fest, dass derartige Dienste in die erste Gruppe einzuordnen sind. Viele kleine und mittelständische Internet-Provider könnten die kostspieligen technischen Schnittstellen sowie die organisatorischen Maßnahmen zur ständigen Verfügbarkeit finanziell nicht verkraften. Das staatliche Bedürfnis nach lückenloser Überwachbarkeit der Telekommunikation würde das Ende vieler kleinerer Hightech-Unternehmen und der von ihnen geschaffenen Arbeitsplätze bedeuten. Dies ist ein Ergebnis, das in merkwürdigem Kontrast zu den sonstigen Bemühungen des Staates um die Telekommunikations- und Internet-Branche als Motor künftiger Wirtschaftsentwicklung steht.

Durch die Verpflichtung von Internet-Providern würde eine bedenkliche **Überwachungsinfrastruktur** geschaffen. In der Regel ist die Überwachung privater Nutzer des Internet auch auf den "**letzten Metern**" möglich, die nach wie vor über herkömmliche Telekommunikationsleitungen abgewickelt werden. Die Einrichtung einer kostspieligen zusätzlichen Infrastruktur ist nicht erforderlich. Die Kosten für die Errichtung und Unterhaltung der Überwachungstechnik stehen im Übrigen in keinem angemessenen Verhältnis zu dem angestrebten Zweck. Außerdem dürften die Überwachungsschnittstellen im Internet auch die Neugierde von **Hackern** oder **Wirtschaftsspionen** wecken. Für diese wäre eine standardisierte Schnittstelle ein ideales Einfallstor. In Anbetracht der Tatsache, dass mehr und mehr sensible Daten z. B. von Ärzten und Beratungsstellen über das Internet verschickt werden, erscheint die flächendeckende Einrichtung von Abhörschnittstellen bei Internet-Providern wegen der Gefahren für den Datenschutz der Bürgerinnen und Bürger höchst bedenklich.

? *"Die letzten Meter"*

Im Bereich der Telekommunikation wird mit dem letzten Meter (auch: letzte Meile, local loop) die Verbindung vom Endgerät des Kunden (Telefon, Fax, Computer) zur nächsten Ortsvermittlungsstelle bezeichnet. Diese Verbindung wird herkömmlich über ein Kupfer- oder Glasfaserkabel realisiert. Auch nach der Privatisierung der Telekommunikation gibt es hier kaum Konkurrenz, da die Telekom noch aus der Zeit ihres staatlichen Monopols im Besitz fast sämtlicher Leitungen ist. Wenn ein Nutzer in das Internet gelangen will, muss er (jedenfalls wenn es sich um eine durchschnittliche Privatperson handelt) die letzten Meter über das Telefonnetz zurücklegen, um sich bei seinem Provider einzuwählen.

Als **Alternative** zur Bereitstellung ständig verfügbarer technischer Überwachungseinrichtungen böte es sich an, Internet-Provider den gleichen Anforderungen zu unterwerfen, wie sie für Betreiber nichtöffentlicher Netze geplant sind. Die Provider müssten dann die Überwachung und Aufzeichung von Telekommunikation nur **im Einzelfall** ermöglichen, ohne dass umfangreiche Investitionen in Abhörequipment erforderlich wären. Presseberichten zufolge hat das Bundeskriminalamt signalisiert, dass es eine solche Lösung als praktikabel erachtet.

Was ist zu tun?

Das Land sollte darauf hinwirken, dass die Verpflichtungen zum Vorhalten von Überwachungseinrichtungen auch für Internet-Provider auf ein vernünftiges Maß reduziert werden.

7.2.3 Enfopol

Auch auf europäischer Ebene wird an der Perfektionierung der Überwachbarkeit der Telekommunikation durch Strafverfolgungsbehörden gearbeitet.

Bereits im 21. Tätigkeitsbericht (Tz. 7.8) berichteten wir über die sog. Enfopol-Papiere der Europäischen Union. Ziel ist der **europaweite Zugriff auf Kommunikationsdaten** innerhalb weniger Sekunden. Dazu müssen zum einen standardisierte Überwachungsschnittstellen in allen Mitgliedsstaaten vorhanden sein, zum anderen wird ein europäisches Rechtshilfeabkommen benötigt, das den schnellen Zugriff auf Daten regelt, die in anderen Mitgliedsstaaten anfallen. Die Arbeiten an dem zweiten Element, dem Übereinkommen über gegenseitige Rechtshilfe, kommen seit über zwei Jahren nur schleppend voran, obwohl sich der Rat der EU immer wieder damit befasst hat. Immerhin sind diese Aktivitäten weitgehend nachvollziehbar.

> **?** ***Enfopol***
>
> *Eine Arbeitsgruppe des Rats der EU befasst sich mit den Problemen der polizeilichen Zusammenarbeit in Europa. Ihre Papiere zur Angleichung der staatlichen Überwachbarkeit der Telekommunikation sind unter dem Stichwort "Enfopol" bekannt geworden. Das Kürzel Enfopol steht für Enforcement Police.*

Die Papiere der seit Jahren tätigen Arbeitsgruppe zur europaweiten Angleichung von Vorschriften zur staatlichen Überwachung von Telekommunikation sind erst Ende 1998 unter dem Namen "Enfopol" bekannt geworden. Im Jahr 1999 bestätigte auch die Bundesregierung, dass sich eine "**Ratsarbeitsgruppe polizeiliche Zusammenarbeit**" mit der Frage befasse, welche Anforderungen Netzbetreiber bzw. Diensteanbieter erfüllen müssen, um die technische Durchführbarkeit von Abhörmaßnahmen zu Gewähr leisten.

Der Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation (Telefonie und Datenübertragung, z. B. im Internet) wurde vom Europäischen Parlament angenommen. Der **Rat der EU** hat dem Papier aber noch nicht zugestimmt. Nachdem erhebliche Kritik von Bürgerrechtsbewegungen aus Österreich, England und Deutschland und von Lobbyisten der europäischen Internet-Provider geäußert wurde, wollte der Rat die Enfopol-Pläne offenbar nochmals gründlich überarbeiten. Von der eigentlichen Enfopol-Ratsvorlage war dann lange nichts mehr zu hören. Anfang Dezember 1999 wurde bei einem Treffen der Innen- und Justizminister der EU lediglich über den zweiten Baustein, das Übereinkommen über gegenseitige Rechtshilfe in Strafsachen, weiter verhandelt. Das Übereinkommen soll bis März 2000 verabschiedet werden, allerdings sind noch Fragen des Datenschutzes zu klären.

Auf politischer Ebene gab es kaum Stellungnahmen zu den Plänen einer

umfassenden und flächendeckenden Überwachbarkeit der Telekommunikation auf EU-Ebene. Das **Bundesinnenministerium** hat lediglich versichert, dass die Pläne in Deutschland nur innerhalb der Vorgaben nationalen Rechts umgesetzt würden. Überhaupt war an den Enfopol-Papieren neben ihrem Inhalt (der hinsichtlich der Überwachbarkeit der Telekommunikation allerdings nicht wesentlich über die deutsche Rechtslage hinausgeht, vgl. 21. TB, Tz. 7.8) vor allem bemerkenswert, wie dieses wichtige Vorhaben abseits jeder **Öffentlichkeit** in geheimen Gremien durchgebracht werden sollte. So erfuhren selbst Bundestagsabgeordnete erst aus Presseberichten von der Existenz der Enfopol-Arbeitsgruppe. Dieser Stil dürfte kaum dazu beitragen, dass die Bürger sich mit der Intensivierung der polizeilichen Zusammenarbeit in der EU anfreunden. Im Übrigen gelten für die europaweite Einrichtung von technischen Überwachungsschnittstellen bei der Kommunikation via Internet die grundsätzlichen Bedenken, die schon hinsichtlich der TKÜV ausgeführt wurden (vgl. Tz. 7.2.2).

Was ist zu tun?
Das Land sollte auf ein transparentes Verfahren bei den Verhandlungen über die Enfopol-Pläne hinwirken. Berechtigte Zweifel an der Wirksamkeit der Überwachungsschnittstellen bei der Internet-Kommunikation und etwaige Sicherheitsrisiken für Netzinfrastrukturen müssen ausführlich diskutiert werden.

7.2.4 Echelon

Lange wurde seine Existenz bestritten; nun lässt es sich nicht länger verheimlichen: Es gibt "Echelon". Echelon ist der Codename für ein automatisiertes globales Überwachungssystem mehrerer internationaler Geheimdienste.

Überwacht wird angeblich die gesamte über Satelliten geleitete **Telefon-**, **Fax-** und **Internet-Kommunikation**. Die anfallenden Daten sollen automatisiert nach bestimmten Suchbegriffen in Echtzeit ausgewertet werden. Abgehört werden die Nachrichten offenbar über verschiedene Bodenstationen in den USA, Italien, England, der Türkei, Kanada, Australien und auch Deutschland (Bad Aibling). Zudem werden Abhörknoten an Unterseekabeln vermutet, die dem Transport von Telekommunikationsdaten zwischen den Kontinenten dienen.

Nachdem Vermutungen über ein solches globales automatisiertes Überwachungssystem von offiziellen Stellen der mutmaßlich beteiligten Staaten (USA, Großbritannien, Kanada, Australien und Neuseeland) zunächst als Hirngespinste einiger paranoider Einzelpersonen abgetan wurden, kommen nun langsam die Tatsachen ans Licht. Zwar wurde Echelon bereits 1997 in einem Bericht über Überwachungstechnologien (**STOA-Report**) an das Europäische Parlament erwähnt. Seine Existenz wurde aber seitens der beteiligten Staaten stets verschwiegen oder verneint, teilweise bis heute. Nach der kritischen internationalen Berichterstattung hat im Mai 1999 erstmals der Direktor des australischen **Defence Signals Directorate** (DSD) die Existenz von Echelon offiziell bestätigt. DSD ist u.a. Betreiber des staatlichen Satellitenkontrollzentrums Pine Gap. Allein die von DSD verantwortete

australische Sektion von Echelon fängt nach eigenen Aussagen stündlich Millionen von Botschaften ab, die in ein Computersystem eingespeist werden. Nach bestimmten Kriterien ausgewertet, werden die Ergebnisse in ein von den Echelon-Teilnehmerländern unterhaltenes Netz weitergeleitet und damit den beteiligten Geheimdiensten zur Verfügung gestellt.

Nicht zuletzt unter dem Druck besorgter Bürgerrechtsgruppen hat es zunächst in Australien Diskussionen um die Abhöraktivitäten von Echelon gegeben. Das australische DSD hat dabei behauptet, dass die Abhöraktivitäten, soweit sie die Privatsphäre australischer Bürger betreffen, streng beschränkt seien. Zwischenzeitlich ist Echelon auch in **Deutschland** zu einem innenpolitischen Thema geworden ist. Dies dürfte den Geheimdienstkoordinator im Bundeskanzleramt dazu bewegt haben, die von der amerikanischen **National Security Agency (NSA)** auf deutschem Boden betriebene Abhörstation in Bad Aibling zu besuchen. Dort versicherte ihm der Leiter der Abhöranlage, dass die Abhöraktivitäten sich nicht gegen deutsche Interessen richten oder gegen deutsche Gesetze verstoßen würden. Belege dafür wurden nach den veröffentlichten Berichten allerdings nicht vorgelegt.

Eine Offenlegung der Aktivitäten des Abhörsystems, insbesondere Aufklärung darüber, in welchem Maß Privatbürger von der Ausspähung betroffen sind, scheint mehr denn je geboten. Dank der internationalen kritischen Berichterstattung bewegt sich mittlerweile einiges: So hat der **amerikanische Kongress** die Geheimdienste und das Verteidigungsministerium im Rahmen der Budgetberatungen unter Berufung auf den o. g. STOA-Report aufgefordert, einen Bericht über die gesetzlichen Grundlagen der Abhöraktivitäten, die amerikanische Bürger betreffen, vorzulegen.

Man kann davon ausgehen, dass es weltweit mehrere, von verschiedenen Staaten betriebene, flächendeckende Abhörsysteme gibt, die nach dem Echelon-Prinzip funktionieren. So ist auch in der **Schweiz** durch Zufall ans Licht gekommen, dass es ein Abhörsystem namens “SATOS” (Satellit Observation) zum Abhören ausländischer Kommunikationssatelliten geben soll. Einige Parlamentarier verlangen nun Aufklärung über die Aktivitäten von SATOS.

Kürzlich erst hat der dänische Verteidigungsminister Hans Haekkerup bestätigt, dass **Dänemark** an einem globalen Überwachungssystem beteiligt ist. Das Rechercheergebnis dänischer Journalisten: Dänemark sei wie auch nahezu alle anderen NATO-Mitglieder Partner der Echelon-Überwachungsabkommen. Die NSA habe allerdings die führende Rolle und entscheide darüber, welche Informationen die anderen Länder – auch über die in ihrem Land abgehörten Bürger, Politiker oder Unternehmer – erhalten.

Was ist zu tun?
Das Land Schleswig-Holstein sollte im Rahmen seiner Möglichkeiten darauf hinwirken, dass die in der Bundesrepublik Deutschland zuständigen Stellen eine Offenlegung der internationalen Abhöraktivitäten “befreundeter” Staaten verlangen. Insbesondere muss geklärt werden, inwieweit deutsche Staatsbürger

von den Maßnahmen betroffen sind.

7.3 Evaluierung des Multimediarechts

Beim Erlass des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) im Juli 1997 hat das Parlament die Bundesregierung verpflichtet, die Wirksamkeit der Vorschriften nach zwei Jahren zu prüfen. Das Ergebnis ist in einem Bericht des Bundeswirtschaftsministeriums zusammengefasst worden.

Die datenschutzrechtlichen Regelungen im Teledienstedatenschutzgesetz und im Multimedia-Staatsvertrag können als vorbildlich angesehen werden (vgl. 20. TB, Tz. 7.1). Die Bewertung dieser Vorschriften im Zuge der **Evaluierung** ist **überwiegend positiv** ausgefallen. Abgesehen von einzelnen Zweifelsfragen bei der Auslegung der Gesetze werden die Vorschriften als gute und notwendige Grundlage für die weiter fortschreitende Verbreitung des Internet und den wirtschaftlichen Erfolg von E-Commerce gesehen.

Konkrete Probleme sind allenfalls im Zusammenhang mit der **elektronischen Einwilligung** aufgetreten. Nach allgemeinem Datenschutzrecht hat die Einwilligung im Regelfall in Schriftform zu erfolgen. Aus nahe liegenden Gründen ist dies für die Kommunikation im Internet nicht angemessen. Daher hat der Gesetzgeber in den Multimedia-Regelungen vorgesehen, dass die Einwilligung zur Datenverarbeitung auch abgegeben werden kann, wenn dabei Verfahren der digitalen Signatur benutzt werden, die jedoch nicht unbedingt den hohen Anforderungen des Signaturgesetzes (vgl. dazu Tz. 7.4) entsprechen müssen. Zurzeit gibt es jedoch kaum geeignete Software auf dem Markt.

Umso mehr Bedeutung haben Projekte wie dasjenige, das von der DG-Bank Frankfurt in Zusammenarbeit mit der GMD Darmstadt und der Universität Kassel unter dem Titel “Datenschutz in Telediensten” (DASIT) durchgeführt wird. Hier geht es darum, in einer echten E-Commerce-Umgebung eine beispielhafte **Umsetzung der Gesetze** zu realisieren und dabei gleichzeitig geeignete Software prototypisch zu erstellen. Wir stehen deshalb mit den Projektbeteiligten im Projekt “DASIT” in einem intensiven Gedankenaustausch.

Als generelles Problem wird im Evaluierungsbericht allerdings die Tatsache angesehen, dass die Vorschriften des Multimedia-Datenschutzes noch **unzureichend umgesetzt** werden, ja häufig noch nicht einmal bekannt sind. Die Bereitschaft, die datenschutzrechtlichen Vorgaben des Teledienstedatenschutzgesetzes und des Mediendienste-Staatsvertrages einzuhalten, dürfte allerdings in den letzten Monaten gewachsen sein. Nach und nach spricht es sich nämlich bei den Anbietern herum, dass der angestrebte Boom im E-Commerce nur dann zu erreichen ist, wenn die Nutzer darauf vertrauen können, dass ihre Daten nicht missbraucht werden.

Was ist zu tun?
Schleswig-Holstein sollte darauf hinwirken, dass die sinnvollen

datenschutzrechtlichen Regelungen des Multimedia-Datenschutzrechts beibehalten und nicht verwässert werden. Stattdessen sollte ihre Umsetzung gefördert werden.

7.4 Digitale Signatur

Der Bund und die europäische Union haben grünes Licht für die allgemeine Einführung digitaler Signaturen gegeben. Für einen breiten Einsatz müssten die Verfahren jedoch billiger werden.

Bisher haben sich die hochgespannten Erwartungen hinsichtlich der Verbreitung der digitalen Signatur (vgl. 21. TB, Tz. 7.5) nicht erfüllt. Nicht zuletzt wegen der **hohen Kosten** sind erst wenige private Anwender bereit, sich Signaturschlüssel-Zertifikate ausstellen zu lassen, die den strengen Vorschriften des Signaturgesetzes genügen. Größere Bedeutung haben Verfahren der digitalen Signatur zurzeit im Geschäftsverkehr zwischen Unternehmen (so genanntes Business-to-Business), wobei die Einhaltung des gesetzlichen Standards häufig nicht als erforderlich angesehen wird.

Auch bei der Kommunikation zwischen **Bürger** und **Verwaltung** rückt der Einsatz digitaler Signaturen näher. Das Land Bremen hat zusammen mit anderen Kommunen den vom Bundeswirtschaftsministerium ausgeschriebenen Wettbewerb **MEDIA@Komm** gewonnen, bei dem es um ein Konzept zur Realisierung der Kommunikation zwischen Kommunen, Unternehmen und Bürgern in Rechnernetzen ging. Die digitale Signatur ist in diesem Zusammenhang für die Authentizität des Absenders und zur Nachweisbarkeit etwaiger Verfälschungen der Dokumente auf dem elektronischen Übertragungsweg von großer Bedeutung. Neben tatsächlichen Maßnahmen zur Förderung des Einsatzes der digitalen Signatur wurde im Land Bremen 1999 ein Landesgesetz zur Erprobung der digitalen Signatur verabschiedet. Es sieht vor, dass in näher bezeichneten Verwaltungsbereichen der jeweils zuständige Senator durch Verordnung bestimmen kann, dass abweichend von der an sich landesrechtlich vorgeschriebenen Schriftform auch die Übermittlung in elektronischer Form bei Anwendung der digitalen Signatur zulässig ist.

Ein weiteres Beispiel ist ein in Hamburg gestarteter Pilotversuch: Das **Finanzgericht Hamburg** nimmt von bestimmten, vorher zu dem Verfahren zugelassenen Rechtsanwälten und Steuerberatern Schriftsätze auf elektronischem Wege entgegen. Auch in diesem Verfahren wird eine digitale Signatur verwendet, die jedoch nicht in jeder Hinsicht den Anforderungen des Signaturgesetzes entspricht.

Es gibt im Zusammenhang mit der digitalen Signatur auch **handfeste Sicherheitsprobleme**. Fraglich ist insbesondere in Verfahren, die nicht signaturgesetzkonform sind, wann der für die Signatur erforderliche private Schlüssel als ausreichend geschützt angesehen wird, wo doch zurzeit keine wirklich vertrauenswürdige Hardware oder Betriebssysteme vorhanden sind. Reicht es aus, den Schlüssel auf einer Chipkarte nur mit einer PIN zu schützen?

Weiterhin ist die korrekte Arbeitsweise der **Visualisierungskomponente** von großer Bedeutung. Wie wird verhindert, dass ein Dokument versehentlich signiert wird oder dass die Anzeige des Dokumentes mit dem eigentlichen Inhalt nicht übereinstimmt ("What you see is what you sign")? Im Hamburger Versuch mit den Finanzgerichten werden die zu signierenden Dokumente mit dem verbreiteten Textverarbeitungsprogramm Word von Microsoft erzeugt, das auf verschiedenen Plattformen zur Verfügung steht. Die Anzeige einiger Zeichen unterscheidet sich je nachdem, unter welchem Betriebssystem Word abläuft. So wird das Zeichen für ein Viertel (¼), eingegeben unter Word für Windows, in einem Macintosh-Word als Unterstrich dargestellt. Das digitale Dokument, das signiert werden soll, wäre jedoch in beiden Fällen gleich. Hier hilft kein noch so sicheres elektronisches Signaturverfahren. In einer unsicheren technischen Umgebung, z. B. auf der Grundlage eines unsicheren Betriebssystems, kann keine überzeugende Sicherheit gewährleistet werden.

Was ist zu tun?
Das Land Schleswig-Holstein sollte vor allem den in Bremen durchgeführten Versuch aufmerksam beobachten, um rechtzeitig eine eigene landesgesetzliche Gleichstellung der digitalen Signatur zur Schriftform vornehmen zu können. In Pilotprojekten dürfen keine problematischen Standards geschaffen werden.

7.5 Open Source und Datenschutz

Transparenz ist eine wichtige Voraussetzung beim Schutz des Rechts auf informationelle Selbstbestimmung. In der Technik wird es beispielsweise durch das Prinzip Open Source umgesetzt.

Im Gegensatz zum Closed-Source-Modell, bei dem die Nutzer das Programm als intransparente "Black Box" verwenden müssen, ist bei Open Source sowohl der Quelltext als auch die zugehörige Dokumentation offen zugänglich. Der Einsatz von Open-Source-Software ist bereits ziemlich verbreitet: Neben einer Vielzahl von Internet-Programmen unterliegt z. B. das Betriebssystem **Linux** der Open-Source-Philosophie. An Linux wird weltweit von hunderten oder gar tausenden von Programmierern gearbeitet. Neue Fassungen werden schnell über das Internet publiziert, um Fehler zu finden und die Programme weiterzuentwickeln.
Versionsverwaltungs-Tools ermöglichen das gleichzeitige Arbeiten an denselben Modulen und verhindern, dass viele Programmierer den Code verderben. In bestimmten Abständen werden konsolidierte Versionen zum allgemeinen Einsatz freigegeben, die über das Internet abrufbar oder über Distributoren zu beziehen sind, wo auch Support oder andere Dienstleistungen angeboten werden.

? *Open Source*

Open Source (deutsch: "Offene Quelle") steht für Software, deren Quelltext offen gelegt und für jeden frei verfügbar ist. So kann der Quelltext nicht nur gelesen, sondern auch geändert und an die eigenen Bedürfnisse angepasst werden.
Der Quelltext eines Programms ist deswegen etwas Besonderes, weil die Software bei ihrer Ausführung in einem speziellen Maschinencode vorliegen muss, der jedoch kaum mehr für einen Menschen verständlich ist. Fehler oder Hintertüren in der Software können selbst Experten bei Durchsicht des Maschinencodes meist nicht ermitteln, wohl aber beim Prüfen eines gut dokumentierten Quelltextes.

Im Bereich der **Kryptographie** (vgl. 20. TB, Tz. 7.3.1) gehört die Offenlegung des Quelltextes der Verfahren zu den elementaren Sicherheitsforderungen. Auf keinen Fall darf die Sicherheit auf der Geheimhaltung der Funktionsweise (Security by Obscurity, "Sicherheit durch Verschleierung") basieren. Immer wieder zeigen Beispiele, dass in diesen Fällen sicherheitsrelevante Fehler durch Bekanntwerden von internen Details, Zufall oder gezielte Angriffe ausfindig gemacht und ausgenutzt werden. Bei Open Source dagegen besteht die Möglichkeit, dass sich Fachleute den Quelltext ansehen und sich über die Qualität der Programme austauschen. Sofern Fehler gefunden werden, können sie bei Kenntnis des Quelltextes oft auch gleich korrigiert werden: Die Meldung des "**Bugs**" zieht häufig gleich die Bereitstellung des "**Patches**" nach sich. Auch bei der IT-Sicherheitszertifzierung kann mit einem Blick in den Quelltext der Code auf Trojanische Pferde oder andere Schadensfunktionen untersucht werden.

? *Bugs und Patches*

*Als **Bugs** bezeichnet man Fehler in Computersystemen. Um solche Fehler in Programmen zu beseitigen, wird spezielle Software zur Verfügung gestellt, die ins System eingespielt werden muss. Solche Fehlerbehebungsprogramme nennt man **Patches** (Flicken).*

Open Source erhöht damit die **Revisionsfähigkeit** der Programme, denn die Funktionen sind – zumindest für Fachleute – nachvollziehbar. Außerdem können

die Produkte bei Bedarf individuell angepasst werden, sodass wirklich nur die erforderliche Funktionalität zur Verfügung gestellt wird.

Open Source allein führt natürlich noch nicht zu mehr Datenschutz und Datensicherheit. Der offen gelegte Code muss auch tatsächlich von unabhängigen Experten begutachtet, und auf gefundene Mängel muss unverzüglich reagiert werden. Systematische Tests sind unverzichtbar. Selbst wenn Open-Source-Produkte mittlerweile vielfach eine hohe Stabilität erlangt haben, verlangt – wie auch bei Closed-Source-Programmen – die Bedienung und Administration ein gewisses Know-how. Gewährleistung und Service, d. h. Support oder Hotlines, werden mittlerweile auch im Open-Source-Bereich von Dienstleistern angeboten.

Das **Bundesamt für Sicherheit in der Informationstechnik** empfiehlt inzwischen Open Source aus Datensicherheitsgründen; das **Bundesministerium für Wirtschaft und Technologie** fördert Open-Source-Projekte (z. B. im Kryptobereich). In anderen Nationen wird sogar diskutiert, in der Verwaltung nichts anderes als Open Source zuzulassen.

Was ist zu tun?
Die Bundesregierung sollte die Förderung von Open Source fortsetzen und damit zum Einsatz von Software beitragen, die keine Hintertüren von ausländischen Geheimdiensten beinhaltet. Die Landesregierung sollte Open Source in ihrem Bereich fördern.

7.6 Für jeden Surfer eine Nummer – Globally Unique Identifiers (GUID)

Dass man im Internet Datenspuren hinterlässt, ist inzwischen nicht mehr neu. Der Trend in der Informationstechnik geht aber dahin, dass es immer mehr statt weniger werden: durch eindeutige Kennungen, die in Hardware, Software oder Diensten implantiert und bei der Nutzung übertragen werden. Jeder Surfer soll so eindeutig bestimmbar sein.

Im März 1999 fand der Chef einer großen Softwarefirma heraus, dass seine Microsoft-Office-Dokumente mit der Hardwareadresse seiner Netzwerkkarte als Teil einer eindeutigen Nummer, einer so genannten **Globally Unique Identifier** (GUID), versehen waren. Kaum war der Aufschrei durch die internationale Presse darüber verhallt, wurde klar, dass dieselbe Software-GUID auch bei der Registrierung von **Windows 98** an den Softwarehersteller übermittelt wird. Inzwischen weiß man, dass solche GUID außerdem bei den Media-Playern der Firmen Microsoft und RealNetworks und bei einem Programm zur nutzerspezifischen Umgestaltung von Cursorn der Firma Comet Systems zur Anwendung kommen. Es ist zu befürchten, dass noch mehr GUID existieren und die Nutzer auch in Zukunft verunsichern.

? ***GUID***

Globally Unique Identifier (GUID) heißen die weltweit eindeutigen Kennungen, die dazu dienen, die Teilnehmer bzw. ihre Rechner im Internet zu identifizieren. Eine solche Nummer wird in einem Hardware-Teil, in der Software oder bei Internet-Diensten eingetragen und dann bei bestimmten Nutzungen übertragen. Auch wenn in vielen Fällen keine Register geführt werden, wem welche GUID zugeordnet ist, kann man über die eindeutigen Nummern doch verschiedene Nutzungen eines Teilnehmers verketten und daraus aussagekräfte Profile bilden. Häufig ist darüber sogar eine Identifizierung des Nutzers möglich.

Der generelle Trend zum Einbau und zur Übermittlung von solchen eindeutigen Informationen durch immer mehr Anbieter im Internet muss beunruhigen, da somit nicht nur Dateien und Dokumente eindeutig Computern und damit den an ihnen arbeitenden Nutzern zugewiesen werden können, sondern sich auch klare Nutzerprofile erstellen und zuordnen lassen. Dies steht im direkten Widerspruch zu den Bestimmungen des Teledienstedatenschutzgesetzes und des Mediendienste-Staatsvertrages (vgl. 20. TB, Tz. 7.1). Um sich dagegen zu wehren, kann derzeit lediglich die **Nichtverwendung** der betreffenden **Programme** oder die Installation eines korrigierenden Updates empfohlen werden. Darüber hinaus kann man im Internet auf einer Vielzahl von Webseiten Anleitungen zur Entfernung der GUID bzw. deren Übermittlung finden. **Cookies** können ebenfalls zu den GUID gerechnet werden (vgl. Tz. 9.3; 20. TB, Tz. 7.5.2). Generell sollten dauerhafte Cookies in den Webbrowsern deshalb abgeschaltet und die Übermittlung von Registrierungsinformationen an Softwareanbieter weitestgehend vermieden werden.

Bezüglich neuer Hardwareprodukte sorgte vor allem die Firma Intel für Aufsehen mit der Ankündigung, ihren neuen **Pentium III-Prozessor** mit einer über das Internet abfragbaren eindeutigen Seriennummer, einer Hardware-GUID, auszustatten. Mit der Begründung des Schutzes und damit der Förderung von E-Commerce-Anwendungen standen die Firmenvertreter gegen eine Mauer von Anwendern und Datenschützern, die eine Löschung dieser Kennungen forderten. Nach dieser Kritik wurden die Chips dann tatsächlich zwar mit einer solchen Nummer ausgeliefert. Sie ist aber nur durch ein explizites Freigeben des Anwenders auslesbar. Ein Chip-Experte der Computerzeitschrift c’t demonstrierte allerdings kurze Zeit später ein Verfahren, mit dem das Auslesen der Nummer

allein durch Software möglich ist. Dies wurde auch durch Intel offiziell bestätigt, verbunden mit der Korrektur des Verfahrens zum Schutz der Chip-Kennung. Dieses Beispiel zeigt, wie notwendig es ist, sich **gegen** weitere **Datenspuren zur Wehr zu setzen.**

8 Vertrauen durch Technikgestaltung

8.1 Überblick

Die Forderung "Datenschutz durch Technik!" erweist sich immer mehr als zukunftsweisend: Wo Datenschutz- und Datensicherheitsanforderungen bereits in der Technik eingebaut werden, sind die Risiken für das Recht auf informationelle Selbstbestimmung geringer. Unsere Modellprojekte weisen den Weg in aussichtsreiche Zukunftstechnologien.

Technik wird nur dann akzeptiert und eingesetzt, wenn die Nutzer Vertrauen zu ihr fassen können. Für eine Gesellschaft, die immer mehr von einem schnellen und verlässlichen Informationsaustausch, z. B. über weltweite Rechnernetze, abhängig wird, ist das **Vertrauen der Nutzer** ein wichtiges Gut. Vertrauen kann auf vielerlei Weisen entstehen. Auf jeden Fall trägt dazu bei, wenn unabhängige Fachleute die Möglichkeit haben, die technischen Produkte und die Verfahren, in denen sie eingesetzt werden, zu analysieren und die Ergebnisse offen darzustellen (vgl. Tz. 7.5).

Institutionen wie die **Datenschutzbeauftragten**, denen wegen ihrer Unabhängigkeit von vielen Bürgerinnen und Bürgern Vertrauen entgegengebracht wird, können auf die Gestaltung von Technik Einfluss nehmen. Dies geschieht durch die Prüf- und Beratungstätigkeit, in der den Daten verarbeitenden Stellen Hinweise auch für den Einsatz technischer Produkte gegeben werden. In unserem **IT-Labor** werden Produkte in Referenzinstallationen auf ihre Datenschutztauglichkeit getestet (vgl. Tz. 9). Darüber hinaus ist es uns möglich, direkt mit Technikgestaltern zusammenzuarbeiten, z. B. Herstellern oder Wissenschaftlern. Auf diese Weise kann sich der Rat der Datenschützer unmittelbar in technischen Design-Entscheidungen niederschlagen. Damit wird auch der Stand der Technik fortgeschrieben, an dem sich die technischen und organisatorischen Maßnahmen zur Datensicherheit zu orientieren haben.

Im Folgenden werden drei **Projekte** im Bereich der Technikgestaltung vorgestellt, die seit 1999 von uns zusammen mit verschiedenen Partnern durchgeführt werden. Es handelt sich um typische Beispiele für die Anwendung des *neuen* Datenschutzes in der Praxis.

8.2 WAU – Webzugriff anonym und unbeobachtbar

In Computernetzen wie dem Internet werden von allen Nutzern – oft unbewusst – Datenspuren hinterlassen, die nach Informationen über Interessen und Nutzungsprofile der Teilnehmer ausgewertet werden können. Aus Datenschutzgründen wäre eine Zugangsmöglichkeit zu Internet-Diensten, die mit möglichst wenigen oder sogar überhaupt keinen personenbezogenen Daten auskommt, zu bevorzugen.

Im letzten Tätigkeitsbericht wurde das Projekt zur anonymen Internet-Nutzung vorgestellt (vgl. 21. TB, Tz. 7.1.1). Dieses Projekt, mittlerweile auch bekannt unter dem Namen "WAU" (Webzugriff anonym und unbeobachtbar), wird inzwischen durch die **Landesinitiative Informationsgesellschaft Schleswig-Holstein** gefördert. Die technische Realisierung, die in enger Zusammenarbeit mit der TU Dresden erfolgt, basiert auf dem Einsatz von MIXen, d. h. speziellen Rechnern im Internet, über die die Kommunikation läuft. Das Projekt hat die Entwicklung einer Software zum Ziel, die leicht handhabbar ist und grundsätzlich für jeden Nutzer finanzierbar Anonymität im Internet realisiert.

> **?** ***MIX***
>
> *Ein MIX sammelt die eingehenden Nachrichten, sortiert sie um und sendet sie nach einer gewissen Zeit weiter. Damit kann der Zusammenhang zwischen den eingehenden und den ausgehenden Nachrichten verschleiert werden. Die gesamte Kommunikation läuft verschlüsselt ab. Für die Anonymität wird eine Reihe von möglichst unabhängig betriebenen MIXen eingesetzt. Wenn auch nur ein einziger MIX in dieser Kette von MIXen vertrauenswürdig arbeitet, ist das ganze System vertrauenswürdig, d. h. die Nutzer bleiben anonym.*

Mit weiteren Kooperationspartnern, u. a. dem Multimedia-Entwicklungszentrum Schleswig-Holstein (MESH) der Medizinischen Universität zu Lübeck (MUL) und anderen Anwendern wird der Einsatz der Anonymitätstechniken für die Kommunikation hochsensibler Daten vorbereitet. Das inzwischen unter der Webadresse *http://www.xtc.mesh.de/* gestartete Projekt "**Ecstasy-Online**", eine Drogenberatung im Internet, realisiert derzeit bereits Elemente der Vertraulichkeit durch Verschlüsselung in der Kommunikation, die nach der Fertigstellung entsprechender Tools auch anonym erfolgen wird. Weitere Anwendungen wie die Telefonseelsorge und andere Beratungsangebote im Internet sind geplant.

Um die Anonymisierung der Kommunikation diensteunabhängig und damit sicherer zu entwickeln, wurde in Zusammenarbeit mit der **TU Dresden** ein einheitliches Datenformat entworfen. Neben den technischen Fragen muss geklärt werden, unter welchen Voraussetzungen eine mögliche Deanonymisierung für "Bedarfsträger" (z. B. Sicherheitsbehörden) zulässig ist. Außerdem muss die Bedienbarkeit für die Nutzer gegeben sein.

www.xtc.mesh.de/ und
www.schleswig-holstein.datenschutz.de (Rubrik: Projekte)

8.3 Datenschutzgerechte Biometrie – wie geht das?

Zutritt per Fingerabdruck, Irisscan, Stimmprobe oder Gesichtserkennung – bei diesen Stichworten dachte man früher an Agentenfilme. Inzwischen wird in den einschlägigen Computerzeitschriften fast wöchentlich ein neues Produkt vorgestellt, das die Passworteingabe am PC oder die Magnetkarte an der Tür durch biometrische Merkmale ersetzt. Für die datenschutzgerechte Entwicklung soll unsere Teilnahme an einem Projekt von TeleTrusT sorgen.

Biometrische Verfahren ermöglichen die Legitimation einer Person nicht wie bisher durch Besitz (z. B. eine Scheck- oder Chipkarte) oder Wissen (z. B. eine PIN oder ein Passwort), sondern durch die körperlichen Charakteristika (vgl. 21. TB, Tz. 7.2). Dabei werden diese Merkmale durch Sensoren erfasst, in einer bestimmten Form umgerechnet und das Ergebnis mit bereits früher erfassten und gespeicherten **Referenzdaten** verglichen. Stimmen diese Daten im Rahmen einer gewissen Schwankungsbreite überein, so wird eine Aktion ausgelöst: der Zutritt gewährt, Geld ausgezahlt, die Alarmanlage entschärft, ein Verschlüsselungscode für eine digitale Signatur aktiviert oder aber die Polizei gerufen.

Die Schwankung der Sensordaten auf Grund von Messungenauigkeiten hat Einfluss auf die Sicherheit der Verfahren: Sollen unberechtigte Personen mit hoher Sicherheit ausgeschlossen werden, sind beim Vergleich mit den vorliegenden Referenzdaten nur enge **Toleranzgrenzen** erlaubt, die aber auch berechtigte Benutzer ausschließen können (und dann wiederholte Messungen erfordern). Sind umgekehrt die Toleranzgrenzen zu weit gesteckt, so werden unter Umständen auch unberechtigte Benutzer durch das System zugelassen.

> **?** ***Biometrie***
>
> *Durch biometrische Geräte können ganz unterschiedliche Merkmale von Menschen wie Fingerabdruck, Sprachprofil, Gesichtsform, Muster von Handlinien und Venen auf dem Handrücken, Unterschriftsdynamik, Tastaturanschlag, Iris- oder Retinamuster erfasst werden. Zur Erhöhung der (Ausfall-)Sicherheit können auch verschiedene Merkmale kombiniert werden. Sie dienen, ähnlich wie ein Passwort oder eine PIN, der Authentisierung von Personen.*

Was hat nun der Datenschutz mit biometrischen Verfahren zu tun? Bei biometrischen Merkmalen handelt es sich um **dauerhaft personengebundene Merkmale**. Diese Bindung ist der Vorteil gegenüber Passwörtern, die leicht vergessen, weitergegeben oder ausgespäht werden können. Biometrische Daten sind besonders schützenswert: Es ist beispielsweise noch nicht abschließend geklärt, welche Informationen über Krankheiten, Stimmungslagen oder Drogenkonsum sich aus den Daten ermitteln lassen. Da die gespeicherten Daten meist zu einem ganz speziellen Zweck (z. B. zur Zutrittskontrolle) erhoben wurden, müssen sie vor einer unbefugten anderweitigen Auswertung geschützt werden. Wichtig für die Betroffenen ist es daher, dass auch ihre Referenzdaten allein in ihrem Besitz verbleiben (z. B. auf einer Chipkarte) oder zumindest verschlüsselt in Systemen gespeichert werden und nur nach einer Aktivierung

durch den Benutzer entschlüsselt werden können. Denkbar ist auch, die biometrischen Daten selbst als kryptographischen Schlüssel zu verwenden, über den nur der Nutzer verfügt. Dabei ist darauf zu achten, dass die Verschlüsselungsverfahren stets dem Stand der Technik angepasst und Daten ggf. durch neuere Verfahren "nachverschlüsselt" werden: Biometrische Daten müssen lange geschützt werden – womöglich ein Leben lang.

Wichtig ist zudem, dass biometrische Daten nur durch die **bewusste** und **aktive Teilnahme der Person** erfasst werden. So lassen sich einerseits Missbräuche durch unerkannt erhobene Daten einschränken, und andererseits würde es für den Nutzer deutlich machen, dass er eine Willenserklärung abgibt. Dies ist insbesondere im Zusammenhang mit der so genannten **digitalen Signatur** (vgl. Tz. 7.4) interessant, bei der elektronische Dokumente quasi per Knopfdruck durch einen kryptographischen Schlüssel signiert werden können. Einsatzbereiche sind hier vor allem Homebanking und Internet-Handel (E-Commerce). Für den Nutzer ist es wichtig, dass er Signaturen nicht unbeabsichtigt vornimmt. Bei den bisher verwendeten Verfahren wird der Signaturschlüssel auf einer Chipkarte gespeichert, die mit einer PIN gesichert ist und daher der PIN-Problematik (Vergessen, Weitergeben, Ausspähen) unterliegt. Durch biometrische Verfahren kann die PIN-Eingabe beispielsweise durch die Messung der **Unterschriftsdynamik** ersetzt oder ergänzt werden. Dies würde gleichzeitig dem Nutzer stärker bewusst machen, dass er ggf. eine rechtlich bindende Handlung vornimmt.

Seit April 1999 werden im Pilotprojekt **BioTrusT** die Einsatzmöglichkeiten von biometrischen Verfahren, die die üblichen Magnetkarten mit PIN-Eingaben ablösen sollen, bei Banken untersucht. Es werden zunächst Geräte getestet, die den Zutritt der Mitarbeiterinnen und Mitarbeiter zu ihrem Dienstgebäude bzw. ihren Arbeitsräumen regeln. Später werden auch Login-Bildschirme am PC, Geldausgabeautomaten und Homebanking-Anwendungen untersucht. Neben dem Datenschutz und dem Verbraucherschutz sind dabei etliche Hersteller und verschiedene Bankinstitutionen beteiligt. Unser Ziel ist dabei, schon in einer frühen Phase der technischen Gestaltung der Geräte datenschutzrechtliche und sicherheitstechnische Probleme zu erkennen und ihnen entgegenzuwirken. Da viele Produkte und auch die Anbindung an die Rechnersysteme der Banken noch in der Entwicklungsphase sind, sehen wir gute Chancen, diese Prozesse im Sinne des Datenschutzes beeinflussen zu können. Dies wird auch wichtig für die Akzeptanz der Verfahren sein.

In Zusammenarbeit mit der Arbeitsgemeinschaft "Biometrie" von **TeleTrusT e. V.**, einem Verband von Herstellern im IT-Sicherheitsbereich, wird derzeit ein Kriterienkatalog erarbeitet, der den Vergleich von biometrischen Verfahren erleichtert. Bestandteile diese Kataloges sind neben Kriterien zur (Daten-)Sicherheit und zu Verbraucherschutzaspekten auch solche zur **Datenschutzfreundlichkeit der Verfahren**. Der Kriterienkatalog soll Standards vorgeben, an denen sich neue Produkte zu messen haben. Das Projekt ist auf mehrere Jahre angelegt und wird vom Bundesministerium für Wirtschaft gefördert.

www.schleswig-holstein.datenschutz.de

(Rubrik: Projekte)

8.4 Das virtuelle Datenschutzbüro

"You have zero privacy anyway – get over it!" (sinngemäß: "Ihr habt ohnehin keinen Datenschutz – findet euch damit ab!"), diagnostizierte 1999 Scott McNealy, Chef des Computerriesen Sun Microsystems. Auch wenn dies übertrieben sein mag, ist es doch ein Hinweis darauf, dass der Datenschutz sich bei neuen Entwicklungen nicht abhängen lassen darf. Einen Ansatz soll das virtuelle Datenschutzbüro bieten.

Analysiert man die bisherigen Bemühungen und Konzepte der Datenschutzszene, dann merkt man schnell, dass sie den neuen Anforderungen, die das Internet und ähnliche Technologien an den Datenschutz stellen, nicht mehr gerecht werden. In ihrer derzeitigen Form können die Datenschutzbeauftragten auf die **Herausforderungen des Internet** und der Informationsgesellschaft nicht angemessen reagieren. Die Pflege einer Website genügt nicht. Stattdessen müssen die Möglichkeiten des Internet für die Sache des Datenschutzes aktiv genutzt werden.

Es besteht akuter Handlungsbedarf, damit nicht der Verlust der Privatsphäre zur Realität der Informationsgesellschaft wird. Deshalb muss der Datenschutz dort präsent sein, wo in der vorhersehbaren Zukunft große Risiken für das Recht auf informationelle Selbstbestimmung entstehen, nämlich im Internet. Dies soll durch das Projekt "**Virtuelles Datenschutzbüro**" realisiert werden, das vom schleswig-holsteinischen Datenschutzbeauftragten initiiert wurde und von der **Landesinitiative Informationsgesellschaft Schleswig-Holstein** gefördert wird.

Ein Ziel des virtuellen Datenschutzbüros besteht darin, den Datenschutz mit neuen Mitteln zu reetablieren, indem es die sich derzeit entwickelnden Kommunikationstechniken und –kulturen aufnimmt und für den "***neuen* Datenschutz**" nutzbar macht. Die neue Qualität des Datenschutzes soll sich daraus ergeben, dass die Kompetenz der Datenschützer durch eine verstärkte Praxisausrichtung ausgebaut wird. Wer im Internet mitreden will, muss seine Funktionsweise kennen, am besten aus eigener Praxis. Außerdem gibt es in der Internet-Community eine reichhaltige Datenschutzkompetenz, die einbezogen werden soll. Die Arbeitsteilung zwischen den Kooperationspartnern des virtuellen Datenschutzbüros soll eine Überbelastung der einzelnen Dienststellen vermeiden und eine höhere Spezialisierung erlauben.

Im Rahmen des virtuellen Datenschutzbüros soll es zu einem **verbesserten Workflow** innerhalb und zwischen den Datenschutzdienststellen kommen, damit sich die Fachleute für die jeweiligen Themen schnell und problemlos austauschen können. Arbeitsergebnisse sind für alle Interessierten transparent und dienen als Grundlage für Diskussionen, mit dem Ziel, die gewonnenen Resultate stets zu hinterfragen und weiterzuentwickeln. Das virtuelle Datenschutzbüro dient als **Plattform** für vielfältige Aktivitäten.

Dies bedeutet:

- eine ständige und offen zugängliche Auseinandersetzung mit unterschiedlichen Interessenslagen, insbesondere mit Personen und Stellen außerhalb der engeren Datenschutzszene zu führen,
- Denkanstöße zu geben für die Systemgestaltung, insbesondere durch das Fördern und Propagieren von Privacy-Enhancing Technologies, und
- Bürgerinnen und Bürgern Hilfen zum Selbstdatenschutz zu geben.

Zu diesem Zweck sollen sich die Datenschutzbeauftragten der diversen Kommunikationstechniken des Internet bedienen. Wir haben es übernommen, die konzeptionellen und technischen Dienstleistungen zu erbringen und in einem so genannten **Privacy-Backbone** zur Verfügung zu stellen.

Ein virtuelles Datenschutzbüro in einem globalen Netz macht nur Sinn, wenn sich möglichst **viele Datenschutzinstitutionen beteiligen**. Bis zum Redaktionsschluss dieses Berichtes haben der Bundesbeauftragte für den Datenschutz, die meisten Landesbeauftragten für den Datenschutz (Bayern, Berlin, Brandenburg, Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz und Saarland), der Datenschutzbeauftragte der Niederlande und einige Schweizer Datenschutzbeauftragte unter Führung des Kantons Zürich ihre Absicht zur Kooperation im virtuellen Datenschutzbüro erklärt.

Nach einer Phase der organisatorischen und technischen Konzeption sollen im Laufe des Jahres 2000 die **ersten Module** des virtuellen Datenschutzbüros realisiert werden, wobei ein hohes Maß an Datenschutz und Datensicherheit technisch eingebaut sein soll. Den Anfang wird der Aufbau eines E-Mail-basierten Kommunikationsforums der beteiligten Datenschutzinstitutionen machen. Anschließend soll der Schritt in die Öffentlichkeit folgen, sodass neben den Datenschutzmitarbeitern auch externe Fachleute und Bürgerinnen und Bürger miteinander über Datenschutzfragen diskutieren können, insbesondere mithilfe von thematischen Mailverteilern. Daneben sollen Antworten auf häufig gestellte Fragen (Frequently Asked Questions) oder etwa ein Datenschutz-Online-Magazin über ein gemeinsames Webangebot zugänglich gemacht werden. Der offizielle Startschuss für das virtuelle Datenschutzbüro ist anlässlich der Sommerakademie im August 2000 geplant.

www.schleswig-holstein.datenschutz.de
(Rubrik: Projekte)

9 Aus unserem IT-Labor

9.1 Überblick

Wer die Technik nicht von vornherein als Feind begreift, sondern das Motto "**Datenschutz durch Technik**" als Chance ansieht, mit cleveren Technologien mehr Datenschutz und Datensicherheit zu bewirken, dem wird ein IT-Labor beim Datenschutzbeauftragten nicht ungewöhnlich vorkommen. Dort kommt Informationstechnik (IT) auf den Prüfstand, um zu analysieren, welche Bedrohungen für das Recht auf informationelle Selbstbestimmung bestehen könnten und mit welchen Maßnahmen man sich selbst schützen kann.

Im Vordergrund steht immer das Ziel, die Technik besser einschätzen zu können und Empfehlungen für ihren Einsatz zu geben. Dazu werden typische **Szenarien** aufgebaut. Einige Firmen stellen ihre Produkte zu Testzwecken eine Zeit lang kostenlos zur Verfügung. Wichtige Ergebnisse werden an die Hersteller zurückgemeldet, um z. B. Fehler zu beseitigen oder zu einer Weiterentwicklung im Sinne des Datenschutzes beizutragen. Damit ist das IT-Labor ein wichtiger Baustein für den *neuen* Datenschutz.

Angefangen hat das IT-Labor als kleiner Raum voller verschiedener Rechner mit unterschiedlichen Betriebssystemen, teilweise vernetzt, teilweise auch speziell ausgestattet, z. B. mit Chipkartenlesegerät oder Online-Zugriff. Da es mit mehreren Personen in diesem Raum zu eng wurde, gerade wenn viel geschraubt und umkonfiguriert werden musste, entwickelte sich ein "**virtuelles IT-Labor**". Dies bedeutet, dass in den Dienstzimmern der Techniker gesonderte Computer für IT-Untersuchungen zur Verfügung stehen, die wiederum teilweise mit anderen IT-Labor-Rechnern vernetzt sind. In den folgenden Abschnitten stellen wir einige Ergebnisse aus dem IT-Labor vor.

9.2 Safer surfen!

Internet-Surfer sind zum Lustobjekt der Datenschnüffler geworden. Um sich selbst vor derlei Begierden zu schützen, reichen oft schon kleine Änderungen in den Standard-Einstellungen der benutzten Software. In der Reihe "Safer surfen!" werden hierfür Tipps gegeben.

Browser nennt man die Programme, mit denen sich Inhalte des Internet auf dem heimischen Rechner darstellen lassen. Schaut man sich einmal an, welche Programm-Einstellungen eine **Standard-Installation** der bekannteren Browser **Netscape Communicator** oder Microsoft **Internet Explorer** hervorbringt, so stellt man fest, dass schon mit wenigen Handgriffen einiges mehr zum Schutz der eigenen Daten getan werden kann.

Nach dem Erfolg des Faltblattes "Verschlüsseln – ich?" (vgl. 21. TB, Tz. 7.1.3), das den Nutzern des Netzes die Verschlüsselung ihrer Kommunikation mit PGP erleichtern sollte, haben wir in Kooperation mit dem **Europäischen**

Verbraucherzentrum erneut ein Faltblatt in der Reihe “Safer surfen!” und eine dazugehörige Präsentation im Internet veröffentlicht. Darin werden nicht nur die Schritt-für-Schritt-Anleitungen bereitgehalten, sondern auch Software für weitergehende Schutzmaßnahmen vorgestellt.

datenschutz.inside.tm/safer/

Für die Anleitungen wurden in unserem IT-Labor die **Konfigurationsmöglichkeiten** der **Browser** von Netscape und Microsoft detailliert begutachtet. Es zeigte sich schnell, dass die Standard-Einstellungen bei beiden Produkten in punkto Schutz der Privatsphäre alles andere als vorbildlich sind, unabhängig davon, ob es um Cookies, um aktive Inhalte oder um spezielle Browser-Funktionen ging. Der IT-Labor-Test hat auch gezeigt: Ohne Zusatz-Software ist eine vollständige Kontrolle der Daten, die der Browser über den Nutzer preisgibt, nicht möglich.

Die positive Resonanz auf das Angebot “Safer surfen!” ist groß. Die Faltblätter werden ständig angefordert, und die Serviceseite ist gut besucht. Auch die zu dem Thema eingehenden E-Mails (auch PGP-verschlüsselt möglich) zeigen, dass die Nachfrage nach Serviceinformationen im Rahmen des *neuen* Datenschutzes groß ist.

9.3 Privacy-Tools

Datenschutz im Internet? Spezielle Programme sollen helfen. Bei einigen steht aber mehr Datenschutz drauf, als drin ist.

Immer häufiger wird das Internet nicht nur zum Vergleichen von Preisen und Angeboten, sondern auch zum elektronischen Einkauf verwendet. Beim Kaufen sind persönliche Daten wie Adresse und Zahlungsmodalitäten (z. B. Kreditkartennummer) oft unabdingbar. Viele Firmen möchten ihre **Webangebote individuell** auf den Kunden zuschneiden und sammeln hierfür Daten: Ein Reiseveranstalter möchte beispielsweise die vom Kunden bevorzugten Fluggesellschaften anbieten, ein Buchhändler ihm den neuesten Titel seiner Lieblingsautorin präsentieren, eine Internet-Suchmaschine ihm eine persönlich zugeschnittene Oberfläche anbieten. Dazu muss der Kunde bei einem erneuten Besuch der Website vom System wiedererkannt werden.

Für diese “**personalisierten Angebote**” sind die persönlichen Daten des Benutzers in der Regel nicht erforderlich – es ist lediglich die Wiedererkennung wichtig. Hierfür werden häufig so genannte **Cookies** verwendet – dies sind kleine Dateien auf dem Computer des Kunden, die beim Aufruf einer Webadresse dem Server übermittelt werden und anhand derer ein Besucher identifiziert werden kann. An Stelle dieser “Kekse” werden auch Benutzerkonten verwendet, die die Eingabe eines Benutzernamens und eines Passwortes verlangen. Mit diesem Konto identifiziert der Server die einzelnen Benutzer und richtet sein Angebot auf deren Vorlieben ein. Häufig verlangt der Webanbieter die Eingabe von Namen und E-Mail-Adressen, obwohl sie für die Wiedererkennung eines Benutzers gar

nicht benötigt werden. Auch Marketing-Umfragen werden gerne mit der Einrichtung eines Kontos verbunden. Wenn man seinen wirklichen Namen nicht nennen möchte, kann man durch die Eingabe von Fantasienamen selbst eine **Pseudonymisierung** durchführen. Sie bietet aber keinen umfassenden Schutz, da man mit technischen Mitteln meist den Urheber herausfinden kann.

Anders sieht die Situation beim Kauf von Produkten im Internet aus – hier will man schließlich, dass die Ware im eigenen Briefkasten landet, und muss daher bei der Kontoeröffnung die richtigen Daten angeben. Die Abrechnung erfolgt meistens über Kreditkarten, deren Nummer ebenfalls in ein Formular eingetragen werden muss. Aus Sicherheitsgründen sollte man darauf achten, dass die Übertragung nur **verschlüsselt** erfolgt – oder die Kartennummer lieber telefonisch, per Fax oder Brief übermitteln.

> **?** ***Privacy Policy***
>
> *In einer **Privacy Policy** erklären Unternehmen, wie und ob sie personenbezogene Daten an Dritte übermitteln, im Sinne einer rechtlich nicht bindenden Selbstverpflichtung.*

Während in Deutschland die Nutzung von Konsumentendaten gesetzlich stark beschränkt ist, unterscheidet sich die Situation in anderen Staaten ganz erheblich. Auf **US-amerikanischen Websites** kann man häufig seine Daten gegen die angebotenen Dienstleistungen "verkaufen" – nach dem Motto: "Gibst du mir deine Daten, bekommst du mein Webangebot oder mein Programm" (vgl. Tz. 2). Andererseits verpflichten sich die Webanbieter in einer **Privacy Policy** häufig selbst zu einem verantwortungsvollen Umgang mit den Daten, der aber ganz verschieden ausgestaltet sein kann – vom totalen Verzicht auf die Nutzung für Werbezwecke bis zu weit reichender Übermittlung an "befreundete" Webanbieter. An dieser Stelle setzen so genannte **Privacy-Tools** an. Dies sind kleine Programme mit zwei Zielrichtungen: Zum einen speichern sie persönliche Daten des Benutzers wie Name, Adresse, Telefon- und Kontonummern, um automatisch Webformulare für den Benutzer auszufüllen und ihm so den Kauf per Internet so bequem wie möglich zu machen. Ob die Daten zentral auf einem Server oder lokal auf der Festplatte des jeweiligen Benutzers gespeichert werden, hängt vom verwendeten Programm ab, ebenso, ob die Datenübertragung verschlüsselt erfolgt oder nicht.

Zum Zweiten unterstützen sie den Benutzer beim Schutz seine Privatsphäre. Diese Schutzfunktion reicht von der Suche derjenigen Website eines Anbieters, auf der dieser seine Privacy Policy darstellt, bis hin zu einer Filterfunktion: Zunächst gibt der Benutzer in einem Profil seine Vorstellung von Privatsphäre ein – von der Stufe "Datenschutz ist mir egal" bis zu "Ich will keinerlei Übermittlung". Das Privacy-Tool vergleicht dieses Wunschprofil mit der Privacy Policy des Webanbieters und warnt gegebenenfalls, wenn diese nicht übereinstimmen. Anderenfalls werden die Webformulare automatisch ausgefüllt.

Das Hauptanliegen dieser Programme liegt eindeutig in einer korrekten und vollständigen Datenübermittlung bei einer Internet-Bestellung, an der die Anbieter besonders interessiert sind. Der **Schutz der Privatsphäre** ist **zweitrangig**. Insofern sind diese Programme eher "Bequemlichkeitstools" als

"Datenschutz-Tools". Dass eine Funktion mit der Bezeichnung "Schutz der Privatsphäre" angeboten wird, zeigt allerdings das wachsende Interesse der Konsumenten an der vertraulichen Behandlung seiner Daten.

Ein Beispiel ist das Internet-Protokoll **P3P** (Platform for Privacy Preferences), das mittlerweile in der Standardisierung weit fortgeschritten ist und vermutlich demnächst auch in gängigen Browsern zum Einsatz kommen wird (vgl. 21. TB, Tz. 7.1.4). Auch hier sind jedoch noch nicht alle Probleme gelöst, doch eines ist sicher: Der Einsatz von P3P entbindet die Anbieter nicht von ihren Rechtspflichten nach dem Multimedia-Gesetzen. Wir arbeiten mit bei der Standardisierung durch das World Wide Web Consortium.

Einige der Privacy-Programme haben wir in unserem IT-Labor näher daraufhin unter die Lupe genommen, ob **offensichtliche Sicherheitslücken** bestehen. Einmal konnte beispielsweise das konfigurierte Nutzerprofil auf einfache Weise von anderen Rechnern aus manipuliert oder ausgelesen werden. Ein Mitschneiden der vom Nutzerrechner übertragenen Daten ergab, dass in bestimmten Fällen zusätzlich zu den dokumentierten Informationen weitere Daten, z. B. personenbezogene Computer- oder Teilnehmerinformationen, transportiert wurden. Dies haben wir der amerikanischen Herstellerfirma zurückgemeldet, die den Fehler sofort in der nächsten Version behoben hat.

Neben Anforderungen der Datensicherheit testen wir im IT-Labor auch die **Bedienfreundlichkeit**, da der Nutzer bei mangelhaften Benutzungsoberflächen oft Fehler mit Auswirkungen auf seinen Datenschutz machen kann. Dies beinhaltet die Prüfung, ob eine datenschutzfreundliche Konfiguration bei der Installation voreingestellt ist und ob die Informationen aus der Online-Hilfe oder Dokumentation verständlich sind. Unsere Tests zeigen, dass gerade bei der Transparenz der Systeme – eine zentrale Datenschutzforderung – noch viel nachgebessert werden muss.

9.4 Praxistests für neue Betriebssysteme

Sicherheitslücken in Betriebssystemen können nur selten durch technische oder organisatorische Maßnahmen "geheilt" werden. Praxistests sind unverzichtbar. Kritik an bestehenden Systemen befruchtet die Entwicklung besserer Produkte.

Als vor einigen Jahren die ersten Client-Server-Systeme ihren Einzug in die Behörden hielten, stellte man sehr schnell fest, dass ihre Flexibilität mit einem schwer zu bewältigenden Administrationsaufwand verbunden war. Kleine Organisationseinheiten mit 20 bis 30 Mitarbeitern mussten aus ihren Reihen jemanden rekrutieren, der sich mit bis zu fünf verschiedenen Betriebssystemen (bzw. betriebssystemnahen Programmen) auskannte. Die Steuerung der zentralen Rechner (Server) und die der Arbeitsplatzrechner (Clients) erfolgte nämlich durch unterschiedliche Betriebssysteme. Als das erste universell einsetzbare Betriebssystem für kleinere Client-Server-Systeme angeboten wurde, haben wir dies in unserem IT-Labor einem Praxistest unterzogen und waren mit die Ersten,

die zum Einsatz von **Windows NT** in den Fällen geraten haben, in denen aus anwendungsspezifischen Gründen nicht das Betriebssystem Unix zur Anwendung kommen musste. Einer großen Anzahl von Systemadministratoren hatten wir zwischenzeitlich in der DATENSCHUTZAKADEMIE oder in Beratungsgesprächen Tipps zur sinnvollen Gestaltung der in diesem Betriebssystem enthaltenen Sicherheitskomponenten gegeben (vgl. Tz. 9.6). Leider enthält auch Windows NT **konzeptionelle Schwachstellen**. Diese liegen insbesondere im Bereich der Software- und Datenverwaltung auf der Ebene der Arbeitsplatzrechner.

Deshalb befassen wir uns zurzeit intensiv mit einem neuen Angebot auf dem "Betriebssystemmarkt" mit der Bezeichnung "**Windows NT-Terminal-Server**". Dessen Konzept besteht darin, nicht nur die gesamte Software- und Datenverwaltung, sondern auch die Verarbeitungsprozesse vom Client auf den Server zu verlagern. Die Arbeitsplatzrechner werden als schlichte Eingabe-, Darstellungs- und Ausgabegeräte billiger. Die Server müssen allerdings größer ausgelegt werden als bisher. Wenn das neue System tatsächlich das hält, was die Anbieter versprechen, könnte hierin ein wesentlicher Fortschritt für Client-Server-Systeme in kleineren Behörden liegen. Wir werden unsere Testergebnisse unmittelbar nach Abschluss der Untersuchungen veröffentlichen und entsprechende Schulungen in der DATENSCHUTZAKADEMIE anbieten.

9.5 Das Beste aus den Gegebenheiten machen

Die derzeit in den Behörden standardmäßig eingesetzten Hard- und Softwarekomponenten sind unter Sicherheitsaspekten nicht als optimal zu bezeichnen. Die Datensicherheit kann aber verbessert werden, wenn man deren Potenzial voll ausnutzt. Wie das geschehen kann, demonstrieren wir an einem Referenzsystem.

Die Macht des Faktischen ist größer, als man vielfach annimmt. Bei der Auswahl von Betriebssystemen und **Standardsoftwarepaketen** lassen sich die Behördenleitungen beileibe nicht immer von der "reinen Datenschutz- und Datensicherheitslehre" leiten. Das hat zur Folge, dass besonders kostengünstige, als "modern" geltende oder von den Lieferanten favorisierte Produkte dominant sind. Ein klassisches Beispiel ist die Windows-Software der Firma Microsoft.

Nun hilft es nicht, über andere, bessere Kaufentscheidungen zu philosophieren, die installierte Hard- und Software befindet sich im täglichen Einsatz. Die ihr innewohnenden Sicherheitsrisiken gilt es so weit wie möglich zu verringern. Deshalb haben wir ein **Referenzsystem konfiguriert**, das weitgehend den Installationen entspricht, die wir bei unseren Prüfungen vor Ort vorfinden. Dieses System haben wir so sicher gemacht, wie es auch jeder Behörde (mit Bordmitteln) möglich ist. Ziel ist nicht die aus der Sicht von Profis bestmögliche, sondern die "machbare" **Sicherheit für den Hausgebrauch**.
Ein gutes Dutzend Problemlösungen haben wir realisiert. Dabei geht es z. B. um die Vermeidung von Dateileichen in den Ablageverzeichnissen, die Verhinderung der Installation nicht freigegebener Software durch die Benutzer, die Vermeidung

von Vireninfektionen. Wir werden dieses System künftig im Rahmen unserer Öffentlichkeitsarbeit präsentieren, die **Sicherheitseffekte vorführen** und insbesondere interessierten Behördenleitern eine Dokumentation an die Hand geben, die sie ihren EDV-Verantwortlichen mit der Frage vorlegen können: "Der Datenschutzbeauftragte hat gesagt, diese Sicherheitsmaßnahmen seien in jedem Fall realisierbar, haben wir das auch gemacht?"

9.6 Datensicherheit läßt sich nicht am grünen Tisch trainieren

Ohne speziell konfigurierte Schulungsrechner würden sich unsere Sicherheitsberatungen darin erschöpfen, Passagen der einschlägigen Handbücher zu verlesen. Datensicherheit lässt sich aber nicht am grünen Tisch trainieren.

Der Inhalt gesetzlicher Regelungen und ihre praktischen Auswirkungen lassen sich in der Regel leidlich mittels bedrucktem Papier, Schaubildern und schriftlichen Ausarbeitungen darstellen. Die Funktionsweise von Hardwarekomponenten, Betriebssystemen und sonstiger Software analysieren zu wollen, ohne ein funktionsfähiges Rechnersystem benutzen zu können, erweist sich dagegen sehr schnell als ein hoffnungsloses Unterfangen. Will man zudem ganz bestimmte Effekte ausprobieren, muss das **Testsystem** entsprechend vorkonfiguriert sein und bei einem Misslingen des Versuches schnell wieder in den Urzustand zurückversetzt werden können.

Bei der Darstellung von Datensicherheit in der DATENSCHUTZAKADEMIE oder im Rahmen von Beratungen vor Ort sind wir deshalb darauf angewiesen, die **speziellen Schulungssysteme** selbst mitzubringen. Dies ist leichter gesagt als getan. Nicht alle Fallgestaltungen sind auf ein- und demselben System darstellbar, weil die unterschiedlichen Konfigurationen oft nicht miteinander kompatibel sind. Außerdem erfordern die in immer kürzeren Abständen auf den Markt kommenden Softwareprodukte nahezu selbstverständlich auch größere Hardwarekapazitäten. In vielen Fällen genügt es auch nicht, die betreffenden Verfahrensweisen durch unsere Mitarbeiter zu demonstrieren und die Ergebnisse an die Wand zu projizieren. Der anzustrebende Workshop-Charakter unserer Fortbildungsveranstaltungen lässt sich am besten dadurch erreichen, dass die Teilnehmer selbst aktiv werden und alternative Lösungsmöglichkeiten ausprobieren können. Deshalb erweitern wir derzeit unsere Schulungsrechner vom Einplatz- auf Mehrplatzsysteme. Der damit verbundene hohe finanzielle und personelle Aufwand ist unvermeidlich, wenn wir im Rahmen unserer Beratungen den Bedürfnissen der Praxis gerecht werden wollen.

10 Europa

10.1 Unmittelbare Anwendung der EG-Datenschutzrichtlinie

Der Pflicht, die EG-Datenschutzrichtlinie in nationales Recht umzusetzen, waren nach Fristablauf im Oktober 1998 weder der Bund noch bis Januar 2000 das Land Schleswig-Holstein nachgekommen. Unter bestimmten Voraussetzungen kann die EG-Richtlinie unmittelbare Wirkung entfalten. Betroffene können beispielsweise bei Vorliegen überwiegender schutzwürdiger Gründe dagegen Widerspruch einlegen, dass sie betreffende Daten verarbeitet werden.

Eine Mutter schilderte, dass sie und ihr Kind vom Kindesvater bedroht wurden. So bestand die berechtigte Vermutung, dass das Kind vom Kindesvater entführt werden sollte. Die wegen dieser **Bedrohung** eingeschaltete Kriminalpolizei riet, den Vor- und Familiennamen des Kindes zu ändern. Eine solche **Namensänderung** ist aus "wichtigem Grund" möglich. Mutter und Kind bekamen neue Namen. Groß war jedoch das Erstaunen bei der Mutter, als ihr von dem zuständigen Jugendamt bzw. Standesamt mitgeteilt wurde, dass der Kindesvater ein Recht darauf habe, diese neuen Namen zu erfahren. Wozu den Namen ändern, wenn der Kindesvater, wegen dessen Drohungen die Prozedur vorgenommen wurde, hierüber informiert wird? In ihrer Verzweiflung bat sie uns um Hilfe.

Tatsächlich sieht das Personenstandsgesetz ein umfassendes, vermeintlich nicht einschränkbares Informationsrecht für den Kindesvater vor. **Sperrvermerke** in Personenstandsbüchern sind nicht vorgesehen. Die Standesämter sind dem Kindesvater zur Auskunftserteilung verpflichtet. Dagegen ist im Normalfall nichts einzuwenden. Liegen die Dinge aber so wie bei der Petentin, kann das Ergebnis haarsträubend sein.

Eine Lösungsmöglichkeit genau für Sonderfälle dieser Art eröffnet nun die EG-Datenschutzrichtlinie. Sie verpflichtet die Mitgliedsstaaten, für die Betroffenen das Recht vorzusehen, "jederzeit aus überwiegenden schutzwürdigen, sich aus ihrer besonderen Situation ergebenden Gründen dagegen **Widerspruch** einlegen zu können, dass sie betreffende Daten verarbeitet werden". Zweck der Regelung ist es, eine Korrekturmöglichkeit bei an sich zulässiger Datenverarbeitung zu eröffnen, die wegen besonderer Umstände des Einzelfalles geboten ist. Bei begründetem Widerspruch hat die Datenverarbeitung zu unterbleiben. Auf unseren Hinweis gegenüber den zuständigen Standesämtern und Ordnungsbehörden hin sagten diese zu, dem Kindesvater keine Auskunft mehr zu erteilen. Damit ist in Schleswig-Holstein die EG-Datenschutzrichtlinie erstmals unmittelbar angewandt worden. Inzwischen hat der Gesetzgeber im neuen LDSG unter der Bezeichnung "Einwand" das entsprechende Rechtsinstitut vorgesehen (vgl. Tz. 1.1).

10.2 Safe-Harbour-Prinzip

Die EG-Datenschutzrichtlinie macht die Zulässigkeit des Exports personenbezogener Daten in Länder außerhalb der EU davon abhängig, dass dort ein angemessener Schutzstandard herrscht. USA und EU sind sich weiterhin uneinig darüber, wie ein solcher Standard für die in die Vereinigten Staaten exportierten Daten sichergestellt werden kann.

Zu den wichtigsten Vorschriften der EG-Datenschutzrichtlinie vom Oktober 1995 gehört die Regelung über den Export personenbezogener Daten in Länder außerhalb des Gebiets der Europäischen Union. Vereinfacht gesagt ist dieser nur zulässig, wenn in dem Drittstaat ein **angemessenes Schutzniveau** für die personenbezogenen Daten herrscht. Ist dies nicht der Fall, so kann der Datenexport zulässig sein, wenn durch vertragliche Verpflichtung ein entsprechendes Schutzniveau für die exportierten Daten hergestellt wird. Die **Artikel-29-Gruppe**, die für die Koordination des Datenschutzes in den Mitgliedsstaaten zuständig ist, hat Kriterien entwickelt, mit deren Hilfe die Angemessenheit des Schutzniveaus in Drittstaaten festgestellt werden kann.

> **?** ***Artikel-29-Gruppe***
>
> *Die Datenschutzrichtlinie sieht zwei Gremien vor, die den Datenschutz auf europäischer Ebene koordinieren. Das eine ist die Datenschutzgruppe nach Art. 29 der Richtlinie. Diese setzt sich aus den Vertretern der nationalen Kontrollstellen zusammen (für die Bundesrepublik gibt es neben einem Vertreter des Bundesbeauftragten für den Datenschutz auch ein von den Landesbeauftragten bestimmtes Mitglied). Außerdem gibt es einen Vertreter der Kommission in der Art.-29-Gruppe. Daneben existiert der Ausschuss nach Art. 31 der Richtlinie. Dieser unterstützt die Kommission bei der Durchführung der Datenschutzrichtlinie. Ein Vertreter der Kommission führt in ihm den Vorsitz, hat jedoch kein Stimmrecht. Im Übrigen gehören ihm Vertreter der Mitgliedsstaaten an. Der Ausschuss gibt zu jeder von der Kommission geplanten Maßnahme eine Stellungnahme ab. Beide Gremien befassen sich mit dem Problem der transatlantischen Datenflüsse.*

Für viele Länder wie z. B. die Schweiz, Norwegen oder Kanada ist die Erfüllung dieser Anforderungen kein Problem. Dort existieren gesetzliche Regelungen zum Datenschutz, die für ein vergleichbares oder wenigstens angemessenes Schutzniveau sorgen. Etwas anderes gilt jedoch für die **USA**. Dort gibt es lediglich sektorale Regelungen, die zum Teil von Bundesstaat zu Bundesstaat variieren. Es fehlt jedoch an einem generellen Datenschutzgesetz für den privaten Sektor. Eine von der Universität Edinburgh auf der Grundlage der Kriterien der Artikel-29-Gruppe durchgeführte Untersuchung ergab, dass das Datenschutzniveau in den USA nicht als angemessen betrachtet werden kann. Damit wäre der Datenexport eigentlich unzulässig.

In Kreisen der EU hoffte man zunächst darauf, dass diese Feststellung die amerikanischen Verantwortlichen dazu bewegen würde, ihrerseits eine allgemeine Datenschutzregelung für den privaten Sektor auf den Weg zu bringen; doch diese Erwartung wurde enttäuscht. Vor allem von wirtschaftsnahen Zirkeln wird in den

USA die Auffassung vertreten, solche Regelungen seien dem amerikanischen Rechtssystem fremd. Datenschutz (bzw. Privacy) werde in den USA traditionell dadurch sichergestellt, dass sich die beteiligten Wirtschaftskreise eigene **Codes of Conduct** geben würden. Von einer gesetzlichen Regelung müsse auch deswegen abgesehen werden, weil sie die in den USA berüchtigten Sammelklagen nach sich ziehen könnte, mit denen bei Verletzung der Vorschriften horrende Beträge als Schadensersatz gefordert werden.

Von amerikanischer Seite zielte man eher darauf ab, in den Genuss einer Ausnahme von dem Erfordernis des angemessenen Datenschutzniveaus zu kommen. Dies ist nach Art. 26 Abs. 2 der Richtlinie dann möglich, wenn der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Person sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet. Die USA entwickelten zu diesem Zweck das so genannte **Safe-Harbour-Prinzip**. Es sieht im Grundsatz vor, dass US-amerikanische Firmenzusammenschlüsse sich gemeinschaftlich verpflichten, für die von Europa zu ihnen exportierten Daten ein Datenschutzniveau einzuhalten, das europäischen Maßstäben entspricht. Es soll also ein sicherer Hafen für die personenbezogenen Daten der EU-Bürger geschaffen werden.

Dazu gehören folgende **sieben Prinzipien**:

- "notice" – Informationspflichten über die Art der Datenerhebung und -verarbeitung sowie über ihren Zweck, die Empfänger und die Wahlmöglichkeiten hinsichtlich der Begrenzung und der Nutzung und Übermittlung,
- "choice" – ein Wahlrecht hinsichtlich der Nutzung der Daten,
- "onward transfer" – bei der Weiterübermittlung der Daten an Dritte wird sichergestellt, dass dort das Datenschutzniveau nicht abfällt,
- "security" – technische und organisatorische Maßnahmen zur Sicherheit der Datenverarbeitung,
- "data integrity" – Sicherstellung der Integrität der Daten, also von Richtigkeit, Vollständigkeit, Aktualität und Erforderlichkeit im Einzelfall,
- "access" – das Recht der Betroffenen auf Auskunft über die zu ihrer Person gespeicherten Daten,
- "enforcement" – die effektive Durchsetzung der Prinzipien.

Weitere Informationen zu den sieben Prinzipien sind zu finden unter:

www.ita.doc.gov/td/ecom/menu.html

Die Gremien der Europäischen Union akzeptieren inzwischen zwar grundsätzlich die amerikanische Herangehensweise. Es gibt jedoch im Hinblick auf einige Fragen noch **Präzisierungsbedarf**. So ist nach wie vor nicht geklärt, wie weit das Auskunftsrecht reichen soll. Darüber hinaus ist hinsichtlich des Prinzips der

Durchsetzbarkeit unklar, wie sichergestellt werden kann, dass im Zweifelsfall eine offizielle Institution die Kontrolle der Datenverarbeitung durchführt.

Dies hat die **Artikel-29-Gruppe** zu der Feststellung veranlasst, dass die vorliegende Fassung der Safe-Harbour-Abmachungen immer noch unbefriedigend ist. Außerdem müssten die Teilnehmer an den Safe-Harbour-Abmachungen klar als solche erkennbar sein. Wichtig sei weiterhin die Durchsetzbarkeit der Prinzipien, mithin die Kontrolle der Einhaltung durch eine öffentliche Stelle. Insgesamt müssten die Ausnahmen und Einschränkungen zurückgenommen und klarer definiert werden. Außerdem müsse das Wahlrecht hinsichtlich der Datenverarbeitung verbessert werden.

Die Konflikte zwischen der USA und der europäischen Seite sind also noch keineswegs ausgeräumt. Wenn es hart auf hart geht, wird die Missachtung eines angemessenen Datenschutzstandards bzw. die Weigerung, die Safe-Harbour-Prinzipien zu verbessern, dazu führen, dass die Datenschutzkontrollinstanzen in den Mitgliedstaaten der EU den **Export** personenbezogener Daten in die USA **untersagen**. Es dürfte im Interesse beider Seiten sein, einen Kompromiss zu finden, bevor dieser Fall eintritt.

Was ist zu tun?
Die Gremien der Europäischen Union sollten weiterhin auf die Einhaltung der sinnvollen und erfüllbaren Vorschriften für den Datenexport in Drittstaaten drängen.

10.3 E-Commerce-Richtlinie der EU

Verschiedene Regelungsvorhaben der Europäischen Union beschäftigen sich mit Fragen des Verbraucherschutzes im Internet. Genauso wichtig ist eine Harmonisierung des für das im Internet geltenden Datenschutzrechts, wofür der gute Standard der deutschen Regelungen als Vorlage dienen sollte.

Die Gremien der Europäischen Union legten bereits Ende 1998 den Vorschlag für eine Richtlinie über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt vor (sog. **E-Commerce-Richtlinie**). Im September 1999 wurde die endgültige Fassung präsentiert. Neben Fragen der Verantwortlichkeit im Internet (für das deutsche Recht finden sich dazu Aussagen im Multimediarecht) regelt die Richtlinie vor allem die **verbraucherschutzrechtlichen Aspekte** bei grenzüberschreitendem elektronischen Geschäftsverkehr innerhalb der EU.

Von datenschutzrechtlichem Interesse ist in diesem Zusammenhang die Vorschrift über die unerbetene kommerzielle Kommunikation sowie die für kommerzielle Kommunikationen vorgesehenen Informationspflichten. Als **Mindeststandard** wird festgelegt, dass **Werbe-E-Mails** eindeutig gekennzeichnet und ihre Absender angegeben werden. In mehreren Gerichtsentscheidungen wurde festgestellt, dass das unerbetene Zusenden von Werbe-E-Mails in Deutschland sowohl an private als auch an geschäftliche Adressen ein unzulässiger

Wettbewerbsverstoß ist. Damit sind deutsche Verbraucher zumindest rechtlich gut gegen unerwünschte Mails geschützt. Nach europäischen Standards wird künftig zusätzlich darauf hingewiesen werden müssen, dass es sich um Werbung handelt. Auf diese Weise können die Mails sofort bei oder nach Empfang aussortiert werden.

Die europäischen Gremien sollten sich auch mit der Harmonisierung des europäischen **Datenschutzrechts im Internet** beschäftigen. Verschiedene Studien haben festgestellt, dass ein Hemmnis für die weitere Entfaltung des E-Commerce gerade in Europa darin besteht, dass viele potenzielle Nutzer kein Vertrauen darin haben, dass die Anbieter mit ihren Daten datenschutzgerecht umgehen. Für die europäischen Unternehmen in diesem Sektor wird es bei steigendem Datenschutzbewusstsein einen Wettbewerbsvorteil darstellen, wenn sie künftig strenge europäische Regelungen einzuhalten hätten. Eine ähnliche Tendenz zeigt sich bereits bei der Frage des Datenexports in die USA (vgl. Tz. 10.2).

Was ist zu tun?
Schleswig-Holstein sollte auf den Erlass europäischer Datenschutzvorschriften für das Internet hinwirken.

10.4 Ausschreibungen im Schengener Informationssystem (SIS)

Im Schengener Informationssystem wurden zu Unrecht abgelehnte Asylbewerber gespeichert. Die Praxis musste geändert werden.

Über den Bundesdatenschutzbeauftragten als nationale Kontrollinstanz gemäß Schengener Durchführungsübereinkommen (SDÜ) waren wir an der Bearbeitung der Eingabe eines Petenten beteiligt, der im SIS zu Unrecht gespeichert war. Er hatte bei der Ausländerbehörde eines Kreises in Schleswig-Holstein einen **Asylantrag** gestellt, der vom Bundesamt für die Anerkennung ausländischer Flüchtlinge als offensichtlich unbegründet **abgelehnt** wurde. Daraufhin ordnete die Kreisverwaltung die Ausreise des Petenten auf. Ob der Petent seiner Ausreisepflicht nachgekommen oder im Inland untergetaucht war, blieb unklar.

? SIS

Das Schengener Informationssystem (SIS) ist ein staatenübergreifendes computergestütztes polizeiliches Fahndungssystem. Es besteht aus einem Zentralrechner in Straßburg (Central Schengen Information System – C.SIS) und den derzeit 10 nationalen Schengener Informationssystemen, den N.SIS.

Die Ausländerbehörde des Kreises veranlasste daraufhin die **Ausschreibung** des Petenten gem. Art. 96 Abs. 3 SDÜ **im SIS**. Danach können Drittausländer, denen nach einer Ausweisung oder Abschiebung die Wiedereinreise untersagt ist, im SIS gespeichert werden. Mit der Maßnahme der Ausländerbehörde muss ein Verbot der Einreise oder des Aufenthalts verbunden sein.

Im Wortlaut: Art. 96 Abs. 3 SDÜ

(1) Die Daten bezüglich Drittausländern, die zur Einreiseverweigerung ausgeschrieben sind, werden auf Grund einer nationalen Ausschreibung gespeichert, die auf Entscheidungen der zuständigen Verwaltungsbehörden und Gerichte beruht, wobei die Verfahrensregeln des nationalen Rechts zu beachten sind.

(3) Die Entscheidungen können ... darauf beruhen, dass der Drittausländer ausgewiesen, zurückgewiesen oder abgeschoben worden ist, wobei die Maßnahme nicht aufgeschoben oder aufgehoben worden sein darf, ein Verbot der Einreise oder des Aufenthalts enthalten oder davon begleitet sein muss und auf der Nichtbeachtung des nationalen Rechts über die Einreise oder den Aufenthalt von Ausländern beruhen muss.

In diesem Fall war aber weder eine Ausweisungsverfügung erlassen noch die Abschiebung tatsächlich vollzogen worden. Damit waren die Voraussetzungen für eine Ausschreibung nicht gegeben. Zur Aufenthaltsermittlung hätte er nur im polizeilichen Informationssystem INPOL oder im Ausländerzentralregister (AZR) ausgeschrieben werden dürfen.. So sehen es auch die vom Innenministerium herausgegebenen Allgemeinen Anwendungshinweise zum Schengener Durchführungsübereinkommen vor. Die zu diesem Zweck erfolgte **Ausschreibung** im SIS war **unzulässig**.

Wir haben die **Löschung** der Daten veranlasst. In diesem Zusammenhang hat sich herausgestellt, dass in vielen Ausländerbehörden des Landes entsprechend verfahren wird und Ausschreibungen im SIS ohne Vorliegen der rechtlichen Voraussetzungen veranlasst werden. Das Innenministerium hat nun kurzfristig einen Erlass an alle Ausländerbehörden herausgegeben, um die Beachtung der Rechtslage sicherzustellen.

Was ist zu tun?
Künftig haben die Ausländerbehörden darauf zu achten, dass Speicherungen im SIS ausschließlich auf Grund der Voraussetzungen des Art. 96 SDÜ veranlasst werden.

11 Was es sonst noch zu berichten gibt

11.1 Erfolgreiche Kooperation der behördlichen Datenschutzbeauftragten

Bislang sah das Landesdatenschutzgesetz die Bestellung behördlicher Datenschutzbeauftragter gar nicht vor, da zeigte sich bereits, welch konstruktiven Beitrag sie im Rahmen überbehördlicher Zusammenarbeit zur Verbesserung der datenschutzrechtlichen und sicherheitstechnischen Situation leisten können. Die Arbeitskreise der bereits tätigen Datenschutzbeauftragten im Bereich der Polizei- und Kreisverwaltungen haben in kurzer Zeit gute Resultate hervorgebracht. Ähnlich wie in der IT-Kommission des Landes und dem Kommunalen Forum für Informationstechnik (KomFIT) sind wir auch in diesen Gremien beratend vertreten. Die sich daraus ergebenden vielfältigen Kontakte und "Querverbindungen" führen ganz von selbst zu einem immer größer werdenden "Datenschutz-Netzwerk", das viele zunächst scheinbar unlösbare Probleme in einer erstaunlich effektiven und pragmatischen Weise zu bewältigen in der Lage ist. Die Synergieeffekte derartiger Kooperationen sprechen sich offenbar herum; schon gründen sich die ersten Arbeitsgruppen zu speziellen Fachfragen (z. B. zur Internetnutzung) und bitten ebenfalls um unsere beratende Teilnahme.

11.2 Praxisgerechte Handlungsvorschläge ersetzen Musterlösungen

Vor Jahren haben wir auf Grund nachdrücklicher Anregungen aus der Praxis eine Reihe von Musterlösungen veröffentlicht. Es handelte sich z. B. um ein "Muster-IT-Konzept", ein "Muster-Sicherheitskonzept" und um "Muster-Dienstanweisungen". Inzwischen haben wir damit begonnen, unter dem Titel "backUP – Magazin für IT-Sicherheit" eine Schriftenreihe aufzulegen, die praktische Handlungsvorschläge für die Lösung thematisch eingegrenzter Problemstellungen und Sicherheitsmaßnahmen gibt. Nicht ein (mögliches) fertiges Ergebnis wird dargestellt, sondern der (methodisch) richtige Weg zu dem behördenspezifischen Ergebnis.

www.schleswig-holstein.datenschutz.de
(Rubrik: Datenschutz und Technik)

Die backUP-Magazine sollen in unregelmäßigen Abständen erscheinen und unentgeltlich zur Verfügung gestellt werden. Sie sind Teil unserer Konzeption des *neuen* Datenschutzes, der neben der Kontrolltätigkeit vor allem auf Beratung und Service setzt. Das erste backUP-Magazin befasst sich mit der Planung, Erstellung und Umsetzung von IT-Sicherheitskonzepten und hat (obwohl eine Art Prototyp) eine positive Resonanz gefunden. Als Nächstes werden wir uns mit dem Thema "Betriebssystem MS-Windows-NT 4.0 – Schwachstellen und Sicherheitsmaßnahmen" auseinander setzen.

11.3 Kooperation der Datenschutzbeauftragten von Hamburg und Schleswig-Holstein

Nach Abschluss des Verwaltungsabkommens zwischen der Hansestadt Hamburg und dem Land Schleswig-Holstein betreffend die Zusammenarbeit des Landesamtes für Informationstechnik (LIT) und der Datenzentrale (DZ; vgl. Tz. 4.9.3) haben auch der Hamburgische Datenschutzbeauftragte und wir eine spezielle Kooperationsvereinbarung getroffen. Ziel ist es, durch eine unbürokratische und effektive Verfahrensweise dafür zu sorgen, dass die länderübergreifende Kooperation des LIT und der DZ nicht zu einem ökonomischen Mehraufwand bzw. zu Abstimmungsproblemen bei der Kontroll- und Beratungstätigkeit auf der Ebene der Datenschutzbeauftragten führt.

Deshalb haben wir uns darauf verständigt, dass Bewertungen, Rechtsauffassungen, Beanstandungen oder Beratungen, die im Zusammenhang mit der Kooperation stehen, stets als gemeinsame Meinung der Datenschutzbeauftragten von Hamburg und Schleswig-Holstein gelten sollen. Prüfungen vor Ort werden wir gemeinsam durchführen, soweit grundsätzliche Fragestellungen berührt sind. In der Regel erfolgen sie durch den jeweiligen "ortsnahen" Datenschutzbeauftragten. Unsere Mitarbeiter bilden eine Arbeitsgruppe, die für die erforderliche interne Abstimmung der gemeinsamen Positionen sorgt und die Strategien und Zeitplanungen für evtl. Aktivitäten (z. B. Prüfungen) festlegt. Sie wird die sicherheitstechnischen und organisatorischen Anforderungen an die beiden Produktionsstätten in einem gemeinsamen Papier zusammenfassen. Beschwerden und sonstige Anliegen von Betroffenen sowie Anfragen und Beratungsersuchen anderer Stellen werden, soweit sie die Kooperation zwischen LIT und DZ betreffen, grundsätzlich von dem Datenschutzbeauftragten beantwortet, an den sich der Anfragende gewandt hat. Handelt es sich jedoch um die Auslegung landesspezifischer Rechtsvorschriften, erfolgt eine Abgabe an den gesetzlich zuständigen Datenschutzbeauftragten.

11.4 Software für Feuerwehren

An die Freiwilligen Feuerwehren im Land wurde vom Innenministerium kostenlos Software verteilt, mit deren Hilfe die personenbezogenen Daten der Mitglieder der Feuerwehren verarbeitet werden können. Die Kommunen selbst wurden über die Einführung dieses Programmes nicht informiert. Bei dieser Vorgehensweise waren die Vorschriften des Landesdatenschutzgesetzes und der Datenschutzverordnung nicht beachtet worden. So war weder das Programm hinreichend dokumentiert, noch war die Frage geklärt, wer das Verfahren zu testen und freizugeben hat. Der vom Programm vorgesehene Umfang der personenbezogenen Daten stimmte nicht mit dem zulässigen Datenprofil des Brandschutzgesetzes überein mit der Folge, dass einige der vorgesehenen Daten nur mit der Einwilligung der Betroffenen in den Datenbestand hätten einfließen dürfen. Das Innenministerium gab nach unserer Intervention die erforderliche Dokumentation sowie Erläuterungen und Checklisten für die einzelnen Feuerwehren heraus. Darüber hinaus wurde zugesichert, einen standardisierten

Erfassungsbogen als Muster für die Feuerwehren zu entwickeln, der nur die vom Brandschutzgesetz vorgegebenen Daten umfasst. Weitere personenbezogene Daten, an deren Kenntnis die Feuerwehren interessiert sein könnten, müssen gegenüber den betroffenen Mitgliedern als freiwillige Angaben ausreichend kenntlich gemacht werden.

11.5 Brisante Aktenbündel als Irrläufer

In der Zentralen Aktenaustauschstelle der Freien Hansestadt Hamburg ging ein Bündel von Akten und Schriftstücken des Kreises Steinburg ein. Bemerkenswert daran war, dass diese Akten und Schriftstücke unverschlossen, allein durch ein Gummiband zusammengehalten und ohne Anschreiben auf die Reise geschickt worden waren. Es handelte sich u. a. um Melderegisteranfragen, Fahrzeugabmeldungen mit Fahrzeugbriefen, Vollstreckungs- und Fahrerermittlungsersuchen, Akten der Ausländerbehörde u. a. mit Urteilen aus Asylverfahren. Von der Zentralen Aktenaustauschstelle gelangten die Unterlagen als "Irrläufer" zum Wirtschaftssenator und von dort zum Hamburger Datenschutzbeauftragten, der sie uns zuständigkeitshalber übersandte. Wir haben die Akten und Schriftstücke dem Kreis unverzüglich zusammen mit einer Beanstandung zurückgesandt. Zu kritisieren war nicht nur das Ignorieren des datenschutzrechtlichen Einmaleins, sondern auch der dadurch verursachte unnötige Verwaltungsaufwand. Es bleibt zu hoffen, dass durch die Rundreise der Unterlagen keine unwiederbringlichen Nachteile durch Fristablauf o. Ä. entstanden sind.

11.6 Brauche ich Schüleradressen, veranstalte ich ein Quiz

Erneut wandten sich verärgerte Eltern an uns, deren Sohn von einer gesetzlichen Krankenkasse ein persönliches Schreiben erhielt, in welchem ihm u. a. ein kostenloser Service zur Unterstützung bei Bewerbungen angeboten wurde. Unsere Prüfung ergab, dass die Krankenkasse zwei Jahre zuvor im Rahmen einer Veranstaltung zur Suchtprävention, an der der damals 14-jährige Sohn teilnahm, ein Quiz veranstaltete und dabei Preise auslobte. Alle Teilnehmer mussten "natürlich" ihren Namen und ihre Anschriften angeben. Auf der Quizkarte befand sich der Hinweis, dass die Angabe der persönlichen Daten freiwillig erfolge. Darunter stand: "Ich bin damit einverstanden, dass sie zur weiteren Informationsvermittlung verwendet werden." Die so erhobenen Daten hatte die Krankenkasse gespeichert, um damit beim späteren Schulabgang der Quizteilnehmer "Direktmarketing" zu betreiben. Die Quizkarte entsprach nicht den Voraussetzungen des Landesdatenschutzgesetzes hinsichtlich einer wirksamen Einwilligungserklärung. Bei Jugendlichen zwischen 12 und 14 Jahren kann nicht davon ausgegangen werden, dass sie bei einem derart lapidaren Satz hinreichend klar erkennen, welche Datenverarbeitung sie durch ihre Einwilligung zulassen. Hierauf hatte schon Monate vorher die Datenschutzbeauftragte der Krankenkasse in einem internen Vermerk hingewiesen. Allerdings war die Krankenversicherung erst nach unserem Einschreiten bereit, Abhilfe zu schaffen.

11.7 Zentralisierung der Fahrerlaubnisdaten

Die örtlichen Fahrerlaubnisregister der Straßenverkehrsbehörden werden bis zum Jahr 2005 sukzessive aufgelöst und die Daten der Fahrerlaubnisinhaber zentral beim Kraftfahrt-Bundesamt (KBA) gespeichert. Die erforderlichen Datenübermittlungen von den örtlichen Fahrerlaubnisbehörden zum KBA erfolgen zukünftig in einem Online-Verfahren. Um dies technisch abzusichern, soll auf Vorschlag des KBA ein bestimmtes Verschlüsselungsverfahren eingesetzt werden, welches, soweit wir feststellen konnten, dem heutigen Stand der Technik entspricht. Um die Daten nicht nur auf dem Übertragungswege, sondern auch im Bereich der Fahrerlaubnisbehörde gegen unbefugte Kenntnisnahme und Veränderungen zu sichern, haben wir zusammen mit dem Verkehrsministerium einen Maßnahmenkatalog für die Sicherung vor Ort erarbeitet.

11.8 Verfassungstreue Neubürger

Die Neuregelung des Staatsangehörigkeitsrechts im Jahr 1999 war politisch heftig umstritten. Unstreitig war, von den künftigen deutschen Staatsangehörigen zu verlangen, dass sie sich zur freiheitlich demokratischen Grundordnung des Grundgesetzes bekennen müssen. Ausschlussgründe für eine Einbürgerung sollten nur bestehen, wenn konkrete “Anhaltspunkte” die Annahme rechtfertigen, dass verfassungsfeindliche Bestrebungen verfolgt wurden. Im Gesetzgebungsverfahren wurde erreicht, dass die Einbürgerung auch möglich ist, wenn der Bewerber glaubhaft macht, sich von früheren Bestrebungen abgewandt zu haben. Die Wahrscheinlichkeit für Nichtdeutsche, von Ämtern für Verfassungsschutz erfasst zu werden, ist – nach Angaben in der Literatur – etwa zwanzigmal größer als für Deutsche. Angesichts dieser hohen Erfassungsquote und des teilweise nur wenig abgesicherten Erkenntnisstandes der Ämter für Verfassungsschutz besteht ein hohes Risiko, dass Einbürgerungswillige ungerechtfertigt mit dem Vorwurf einer verfassungsfeindlichen Bestrebung konfrontiert werden. Wir gehen davon aus, dass die gesetzliche Formulierung eine Regelanfrage der Einbürgerungsbehörden ausschließt.

11.9 Gerichtsakten in den Händen von Strafgefangenen

Im Frühjahr 1999 wurde berichtet, dass für die Umzugsarbeiten bei einem Amtsgericht Freigänger aus der nahe gelegenen Justizvollzugsanstalt eingesetzt worden waren. Ihre Aufgabe war es, die Gerichtsakten von einem Archivraum in einen anderen zu transportieren. Eine nennenswerte Aufsicht durch Justizpersonal fand dabei nicht statt. Die Nachfrage bei dem Amtsgericht ergab, dass zwar Justizbedienstete mit der Beaufsichtigung der Tätigkeit der Gefangenen betraut worden waren. Da diese Mitarbeiter aber nicht von anderen unaufschiebbaren Dienstgeschäften freigestellt wurden, mussten sie die Gefangenen immer wieder für nicht unerhebliche Zeiträume alleine lassen. In diesen Zeiten hätten die Strafgefangenen in den Gerichtsakten stöbern können. Wir haben dies als einen Verstoß gegen die Pflicht zu organisatorischen Maßnahmen der Datensicherheit förmlich beanstandet.

11.10 Die Organisation zahnärztlicher Abrechnungskontrolle

Die Kassenzahnärztliche Vereinigung (KZV) wollte einen großen Anteil der Karteikarten einer Zahnärztin zu Kontrollzwecken kopiert zugesandt bekommen. Diese weigerte sich mit dem berechtigten Argument, auf den Karteikarten stünden nicht nur die abrechnungsrelevanten Angaben, sondern auch sensible Daten aus der Behandlung, die sie nicht offenbaren dürfe. Das Gesetz erlaubt nur den Einblick in Befunde, nicht in sonstige Behandlungsunterlagen. Ein Schwärzen der Kopien hätte einen übermäßigen Aufwand verursacht. Im konkreten Fall schlugen wir vor, dass die Zahnärztin und die KZV in einem gemeinsamen Termin die relevanten Unterlagen sichten. Die Zahnärztin sollte nur Einblick in die prüfrelevanten Daten gewähren. Für die Zukunft formulierten wir gemeinsam mit der KZV eine Empfehlung über die Führung der Karteikarten durch die Zahnärzte, die derartige gemeinsame Sitzungen unnötig macht. Danach sollen die abrechnungsrelevanten Befunde quartalsweise auf einem getrennten Blatt erfasst werden. Für den Fall einer Überprüfung genügt es, dieses Blatt zu kopieren und der KZV zur Verfügung zu stellen. Die KZV erhält bei einer derartigen Datenorganisation keine Daten unbefugt zur Kenntnis, kann aber dennoch umfassend kontrollieren.

www.schleswig-holstein.datenschutz.de
(Rubrik: weitere Materialien/Bekanntmachungen)

11.11 Geplanter Erlaß einer neuen Telekommunikationsdatenschutzverordnung

Seit August 1996 ist der Bund in der Pflicht, eine Verordnung zum Datenschutz in der Telekommunikation zu schaffen. Ende des Jahres lag endlich ein Entwurf vor, der voraussichtlich in der ersten Jahreshälfte 2000 in Kraft tritt. Gegenüber den ursprünglichen Plänen stellt er eine Verbesserung dar. So war zunächst geplant, die Speicherungsdauer für Verbindungsdaten von bisher 80 Tagen nach Rechnungsversand auf künftig zwei Jahre auszudehnen. Auf Grund der Kritik vor allem aus dem Kreis der Datenschutzbeauftragten wurde die Zweijahresfrist wenigstens auf sechs Monate reduziert. Ein weiteres datenschutzrechtliches Problem sahen wir bezüglich der Absicht, eine so genannte Invers-Auskunft zuzulassen, bei der der Nachfragende lediglich die Telefonnummer kennt und dann dazu Name und eventuell Anschrift des Teilnehmers mitgeteilt bekommt. Hiervon wurde zwischenzeitlich abgesehen. Dies wirkt sich allerdings nur auf die Auskunftsdienste der Telekommunikationsunternehmen aus. Bei Daten, die auf CD-ROM gespeichert sind, kann technisch nicht verhindert werden, dass mithilfe frei verkäuflicher Software eine Invers-Suche stattfindet. Die Betroffenen müssen sich über diesen Umstand im Klaren sein. Wer eine solche Suchmöglichkeit verhindern will, sollte nicht in die Veröffentlichung seiner Anschlussdaten auf CD-ROM einwilligen. Dies kann durch eine entsprechende Erklärung gegenüber der Telekom erfolgen.

12 Rückblick

12.1 Neuorganisation des polizeiärztlichen Dienstes unter Dach und Fach

Im 20. Tätigkeitsbericht hatten wir unter Tz. 4.11.3 auf die Notwendigkeit einer Neuorganisation beim polizeiärztlichen Dienst hingewiesen, um eine ausreichende Trennung der Heilfürsorgeaufgaben von der Haus- sowie der Amtsarzttätigkeit zu erreichen. Eine entsprechende Regelung wurde vom Polizeiverwaltungsamt Anfang 1998 getroffen. Umstritten blieb allerdings zunächst das Verfahren zur amtsärztlichen Begutachtung von Polizeibeamten. Diese sollte grundsätzlich durch einen Polizeiarzt erfolgen, der den Betroffenen zuvor mindestens zehn Jahre nicht oder nur in geringem Umfang kurativ betreut hat. Eine Ausnahme sollte allenfalls mit schriftlicher Zustimmung des Betroffenen gemacht werden. Diese Frist ist datenschutzrechtlich geboten, um die Nutzung von Heilfürsorgedaten beziehungsweise hausärztlichen Behandlungsdaten für Zwecke der allgemeinen Personalverwaltung auszuschließen. Allerdings war auch vorgesehen, bei der Begutachtung durch einen anderen Polizeiarzt die Krankenkarte und gegebenenfalls auch die Krankenakte beizuziehen und für den Untersuchungszweck gezielt auszuwerten. Damit wäre der Zweck der personellen Abschottung unterlaufen worden. Nach eingehender Diskussion mit dem Polizeiverwaltungsamt wurde uns bestätigt, dass die Nutzung der Krankenkarten für amtsärztliche Begutachtungen zukünftig entfallen wird.

12.2 Evaluierung polizeilicher Befugnisse durch die Verwaltungsfachhochschule Altenholz

Aus dem Untersuchungsprojekt der Verwaltungsfachhochschule zur Praxis verdeckter Datenerhebungsbefugnisse in Strafverfahren (wir berichteten zuletzt im 21. TB, Tz. 4.2.8) wurden entgegen unserer Erwartung noch keine Ergebnisse vorgelegt. Sowohl in Mecklenburg-Vorpommern als auch in Hamburg haben die Innenressorts ihr Interesse an einer Beteiligung an der Untersuchung erklärt. Mittlerweile ist von anderer Seite Bewegung in die jahrelange Diskussion um eine unerlässliche Evaluierung verdeckter Datenerhebungsbefugnisse der Polizei gekommen. Im Zusammenhang mit der Veröffentlichung von Zahlen über die bundesweit durchgeführten Telekommunikationsüberwachungen durch die Bundesregierung im Jahr 1998, die einen weiteren sprunghaften Anstieg offen legen, vergab das Bundesjustizministerium ein Forschungsprojekt zur “Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO” an das Max-Planck-Institut für Straf- und Strafprozessrecht in Freiburg. Die wissenschaftliche Methodik des Instituts soll nach dem Willen des schleswig-holsteinischen Innenministers Eingang in das Evaluierungsprojekt der Verwaltungsfachhochschule Altenholz finden und auf die technischen Überwachungsmaßnamen übertragen werden, die vom Bundesprojekt nicht untersucht werden. Unter diesen Rahmenbedingungen und angesichts des bisherigen zeitlichen Vorlaufs sollte die hiesige Untersuchung in der Lage sein, im Jahr 2000 zu aussagekräftigen Ergebnissen zu gelangen.

12.3 Endlich “schlanke” Fahrtenbücher für Ärzte und Apotheken

Jahrelang wurde bundesweit zwischen den Finanzministerien, den Berufsverbänden der Ärzte und Apotheker sowie den Datenschutzbeauftragten darüber diskutiert, ob die Namen von Patienten bzw. Kunden in den aus steuerlichen Gründen zu führenden Fahrtenbüchern verzeichnet sein müssen (vgl. 19. TB, Tz. 4.10.3; 21. TB, Tz. 10.5). Endlich ist die Angelegenheit unter Dach und Fach. Zum Nachweis des Verhältnisses zwischen beruflicher/geschäftlicher und privater Nutzung der Kraftfahrzeuge muss im Fahrtenbuch nur "Patientenbesuch" bzw. "Kundenbesuch" vermerkt sein. Die Identität der einzelnen besuchten Personen ist in einer gesonderten Liste zu vermerken. Bei "normalen" Betriebsprüfungen werden die nunmehr anonymisierten Fahrtenbücher vorgelegt. Nur wenn in konkreten Einzelfällen Unstimmigkeiten aufzuklären sind, werden die Finanzämter Einblick in die personenbezogenen Listen verlangen. Auf diese gute Idee hätte man schon vor Jahren kommen können.

12.4 Sicherheitskonzepte nicht mehr umstritten

Die Datenschutzverordnung von 1994 hat sich rundherum bewährt. Die in ihr festgeschriebenen "Grundsätze einer ordnungsgemäßen automatisierten Verarbeitung personenbezogener Daten" werden durch die Bank von den Behörden als vernünftige Mindestanforderungen akzeptiert. Besonders hervorzuheben ist dabei die in den Grundsätzen enthaltene Verpflichtung zur Erarbeitung von Sicherheitskonzepten. Wenn Behörden in den vergangenen Jahren neue Computersysteme angeschafft und Datenbestände angelegt haben, ohne für die Verfahren Sicherheitskonzepte zu entwickeln, stand die rechtliche Fragwürdigkeit ihres Tuns stets außer Zweifel. Die Verantwortlichen mussten sich anlässlich unserer Prüfungen also nicht nur die tatsächlichen Sicherheitsdefizite vorwerfen lassen, sondern auch, dass sie Verstöße gegen die Datenschutzverordnung geduldet hatten. Soweit allerdings Sicherheitskonzepte erarbeitet worden waren, wurden die Verantwortlichen frühzeitig auf eventuelle Defizite aufmerksam. Die wenigen, die trotzdem auf entsprechende technische oder organisatorische Maßnahmen verzichteten, taten das für jeden erkennbar wider besseren Wissens. Das Sicherheitsniveau ist durch die Datenschutzverordnung zweifellos angehoben wurden (vgl. 18. TB, Tz. 6.1).

12.5 KomFIT gedeiht prima

Über Jahre hinweg haben wir die "kommunale Familie" (Städteverband, Landkreistag, Gemeindetag und deren Mitglieder) ermuntert, die Kooperation auf dem Gebiet des IT-Einsatzes zu verstärken, damit sicherheitsrelevante Fehlentwicklungen im kommunalen Bereich (insbesondere bei kleineren Organisationseinheiten) so weit wie möglich vermieden werden. Zunächst wurden unsere Anregungen nur zögerlich aufgenommen, dann hatte man ein Konzept, aber es fehlte am Geld. Noch vor zwei Jahren musste man befürchten, dass "die ganze Sache den Bach hinunter gehen würde" (vgl. 20. TB, Tz. 6.2). Als 1998 das "Kommunale Forum für Informationstechnik KomFIT" gegründet wurde, waren endlich die institutionellen Voraussetzungen geschaffen. Wiederum ein Jahr

später kann diese Institution eine durchaus beeindruckende Bilanz ihres Wirkens vorlegen. In Zusammenarbeit mit der Investitionsbank Schleswig-Holstein und einer Reihe anderer Institutionen sind z. B. Leitlinien für die IT-Infrastruktur der Kommunen, ein Standard-IT-Konzept, ein Standard-Beratungskonzept und ein Standard-Fortbildungskonzept erarbeitet worden. In Entwicklung befindet sich ein so genanntes "Verbandsforum", das auf der Basis des Internets den Informationsaustausch zwischen den kommunalen Landesverbänden und den Kommunen verbessern soll. Auch die Prüfung und Zertifizierung von Software für den kommunalen Markt zeigt erste Erfolge. Diese zunächst nicht zu erwartende positive Entwicklung rechtfertigt weiterhin unsere intensive unterstützende datenschutzrechtliche und sicherheitstechnische Beratung.

12.6 Rechtsgrundlagen für Studi-Chipkarten

Im letzten Tätigkeitsbericht (Tz. 4.9.3) haben wir von unserer beratenden Tätigkeit gegenüber einer Hochschule berichtet, die für ihre Studierenden universelle Berechtigungsausweise in Form von Chipkarten eingeführt hatte. Dabei war u.a. darauf hinzuweisen, dass es für die obligatorische Einführung eines solchen Ausweises einer bereichsspezifischen Rechtsgrundlage bedarf. Der von uns auf Wunsch formulierte Vorschlag wurde vom Bildungsministerium in modifizierter Form übernommen und in die Studierenden-Daten-Verordnung eingefügt. Es sind jetzt die zulässigerweise zu verarbeitenden Daten festgelegt und die einzelnen Funktionalitäten der Chipkarte innerhalb und außerhalb des Hochschulbetriebs beschrieben. Um die Datenverarbeitungsvorgänge so transparent wie möglich zu gestalten, ist weiter festgelegt, dass jede Kommunikation zwischen Chipkarte und Lesegerät für den Karteninhaber erkennbar sein muss. Außerdem steht ihm ein spezieller Auskunftsanspruch über die durch die Karte aktivierten Speicherungsvorgänge zur Seite. Schleswig-Holstein ist damit das erste Bundesland, das die Nutzung von Chipkarten als Studierendenausweis normenklar geregelt hat.

12.7 Telefondaten-CD-ROM in der öffentlichen Verwaltung

Im 19. Tätigkeitsbericht (Tz. 7.4) haben wir noch davor gewarnt, Produkte wie die **D-Info-CD-ROM** in der öffentlichen Verwaltung einzusetzen. Grund dafür war der Umstand, dass die Anbieter dieser und ähnlicher Produkte ihre Datensammlungen in unzulässiger Weise unmittelbar aus den Telefonbüchern abschreiben ließen. Die Widersprüche der Telefonkunden, die nicht in elektronischen Verzeichnissen erscheinen wollten, waren nicht berücksichtigt. Erst nach Einschaltung der Regulierungsbehörde für Telekommunikation und Post wurde von der Telekom der Preis für die Überlassung von Telefonverzeichnissen reduziert, womit dem legalen Erwerb der Veröffentlichungsrechte für die genannten Produkte nichts mehr im Wege steht. Bei einem legalen Erwerb der Daten bestehen damit keine datenschutzrechtlichen Bedenken mehr gegen die Nutzung derartiger Telefon-CDs in der öffentlichen Verwaltung. Die Betroffenen müssen sich darüber im Klaren zu sein, daß Daten in elektronischen Verzeichnissen, sei es auf CD-ROM oder im Internet, technisch bedingt einer erhöhten Verwertungsmöglichkeit unterworfen sind. Wer sich mit

der Nutzung seiner Daten nicht abfinden möchte, sollte der Veröffentlichung seiner Daten auf elektronischen Verzeichnissen nicht zustimmen bzw. seine Einwilligung zurückziehen.

13 Beispiele dafür, was die Bürger von unserer Tätigkeit haben

Datenschutzbeauftragte haben die Aufgabe zu kontrollieren und zu kritisieren, wenn sie Mängel bei der Verarbeitung personenbezogener Daten feststellen. Auch in diesem Bericht ist an vielen Stellen von “Kritik”, “Beanstandung” u. Ä.. die Rede. Dies könnte zu dem Schluss führen, Kritik und Behinderung seien unsere Hauptaufgaben. In Wirklichkeit geht es um Verbesserungen zu Gunsten des Grundrechtsschutzes der Bürgerinnen und Bürger. Hier einige Beispiele aus dem vergangenen Jahr, in denen dies gelungen ist. Aufgeführt sind nur Fälle, in denen generelle Verfahrensweisen verbessert wurden, keine Ergebnisse von Einzelpetitionen.

1. *Täglich nutzen **Sozialämter Vordrucke**, um Sozialdaten zu erheben, die sich oft nicht auf die erforderlichen Daten beschränken und unzureichende Erläuterungen für die Beteiligten enthalten. In Zusammenarbeit mit dem Deutschen Gemeindeverlag und dem Schleswig-Holsteinischen Landkreistag haben wir eine Vielzahl dieser Vordrucke datenschutzgerecht gestaltet – eine Initiative aus Schleswig-Holstein im Interesse der Datensparsamkeit mit Wirkung für viele andere Bundesländer.*

2. *In manchen Sozialämtern herrschte Unklarheit darüber, unter welchen Voraussetzungen **einmalige Beihilfen** als Bargeld oder in Form von Bestellscheinen bzw. Warengutscheinen zu gewähren sind. Viele Hilfeempfänger fühlten sich gegenüber den Kaufhäusern und Geschäften bloßgestellt. Wir veröffentlichten deshalb amtliche Hinweise, wie der Sozialdatenschutz bei der Gewährung von einmaligen Beihilfen zu berücksichtigen ist.*

3. *Ein Kreiskrankenhaus plante, zur Durchsetzung von Ansprüchen ein privates **Inkassobüro** zu beauftragen, wobei nicht nur Rechnungsdaten, sondern auch medizinische Angaben, z. B. über Art und Dauer der Behandlung, übermittelt werden sollten. Dies hätte zu einer unzulässigen Offenbarung ärztlicher Geheimnisse in einer Vielzahl von Fällen geführt. Das Inkassobüro hätte diese Daten überdies auch für von ihr durchgeführte Bonitätsbeurteilungen nutzen können. Auf Grund unserer Intervention sah das Krankenhau von seiner Planung ab.*

4. *Die bei der Durchführung des **Sozialentschädigungs- und des Schwerbehindertenrechts** vom Landesamt für Soziale Dienste verwendeten Vordrucke und Merkblätter waren fehlerhaft. Dies führte in vielen Fällen zu einem Übermaß an Datenerhebung sowie über Einwilligungserklärungen zu Blankettvollmachten, sich bei dritten Stellen hinter dem Rücken der Betroffenen Daten zu beschaffen. Auf Initiative des Sozialministeriums wurden diese in Kooperation mit uns gesetzeskonform gestaltet.*

5. *Bei der Durchführung eines **sozialmedizinischen Forschungsvorhabens** einer Fachhochschule sollten unter Einbeziehung einer Krankenkasse per Fragebogen, durch Einblick in Pflegegutachten und durch Interviews hochsensible Daten von vielen Pflegeversicherten erhoben werden. Diese Daten wären für missbräuchliche Verwendungen nutzbar gewesen. In Zusammenarbeit mit dem zuständigen Ministerium wurde ein Verfahren entwickelt, bei dem die Forschungsstelle nur anonymisierte Daten erhält.*

6. *In ambulanten **Suchtberatungsstellen** wird eine einheitliche **Basisdokumentation** mit dem Namen "Horizont" eingeführt. In der Grundkonzeption war keine ausreichende Aufklärung der Betroffenen und keine klare Datenabschottung vorgesehen, sodass Angaben über Straftaten und Drogenkonsum Nichtberechtigten zugänglich sein konnten. Durch die präzise Fassung der Einwilligungserklärung und eine Überarbeitung des EDV-Programms konnte die Voraussetzung geschaffen werden, dass das Risiko der illegalen Weitergabe der hochsensiblen Daten minimiert wurde.*

7. *Bei mehreren Forschungsprojekten im medizinischen Bereich mussten wir feststellen, dass die **Transparenz für die Betroffenen** und die vorgesehenen Einwilligungserklärungen unzulänglich waren. Dadurch konnte einerseits die Kooperationsbereitschaft der Betroffenen beeinträchtigt werden, zum anderen bestand die Gefahr, dass sensible medizinische Daten in falsche Hände gelangten. Im Berichtsjahr konnten wir durch Beratung bei mehreren Projekten darauf hinwirken, dass solche Mängel von vornherein vermieden wurden.*

8. ***Auskünfte** einer IHK über Kammermitglieder erfolgten bislang vielfach mündlich und wurden **nicht dokumentiert**. Bei solchen spontanen Datenübermittlungen schleichen sich leicht Fehler ein, die bei Betroffenen zu fatalen Folgen führen können und die sich mangels Dokumentation später nicht mehr oder nur unbefriedigend aufklären lassen. Auf unsere Beanstandung hin wird die Dokumentationspflicht in die entsprechende Dienstanweisung aufgenommen, ein entsprechendes Feld in der EDV eingerichtet und in Zweifelsfällen nur noch schriftlich Auskunft erteilt.*

9. *Die Bitte eines Studenten auf **Einsicht in seine Abiturklausuren** wurde von seiner ehemaligen Schule mit dem Hinweis auf einen Erlass des Bildungsministeriums, wonach dies erst nach 10 Jahren zulässig sei, zurückgewiesen. Dies widerspricht dem gesetzlich verankerten Akteneinsichtsrecht, da es hierzu weder eine entsprechende Aufbewahrungsfrist noch einen solchen Erlass gibt. Gemeinsam mit dem Bildungsministerium konnten wir erreichen, dass in Zukunft eine Einsichtnahme in schulische Abschlussarbeiten unverzüglich und*

unentgeltlich gewährt wird.

10. *Bislang wurde im Rahmen gaststättenrechtlicher Verfahren die persönliche Zuverlässigkeit eines Gastwirtes durch Nachfrage bei einer Vielzahl von Behörden und anderen Stellen überprüft. Dies führte nicht nur zu unzulässigen Datenübermittlungen und Zeitverzögerungen, sondern auch zu Mehrkosten, da sich die Höhe der Gebühren für eine Konzession nach dem Aufwand der Verwaltungsbehörde richtet. Die neue **Gaststättenverordnung**, die unsere diesbezüglichen Prüfungsergebnisse berücksichtigt, reduziert das **Konzessionsverfahren** auf das tatsächlich Erforderliche und vereinfacht und verkürzt es damit wesentlich.*

11. *Die **Beihilfeanträge** der Mitarbeiter einer kreisangehörigen Stadt wurden bislang in Eigenregie bearbeitet. Damit bestand das Risiko, dass auch Mitarbeiter der Personalverwaltung Kenntnis von den sensiblen Beihilfedaten erhielten und sie unzulässigerweise in Personalentscheidungen einfließen lassen konnten. Nach unserer Prüfung wurden die Beihilfeaufgaben auf die Versorgungsausgleichskasse übertragen.*

12. *In den Stationszimmern einer **Justizvollzugsanstalt** sind Hinweistafeln mit Informationen über die Namen sowie weiteren personenbezogenen Daten der Gefangenen angebracht. Da die Stationszimmer nicht nur von den Bediensteten der jeweiligen Abteilung, sondern auch von Gefangenen und Besuchern aufgesucht werden, konnten auf diesem Wege bislang Informationen über Gefangene, die nicht hätten offenbart werden dürfen, an Unbefugte gelangen. Auf unseren Vorschlag hin wurden die Hinweistafeln mit Klappen oder Rollos versehen, die nur bei Bedarf geöffnet werden.*

13. *Bei **Demonstrationen videografiert** die Polizei Teilnehmer zu Dokumentations- und Beweissicherungszwecken. Bislang wurden dabei offenbar nicht immer die gesetzlichen Vorgaben beachtet, wonach dies nur gegenüber Straftätern oder Störern geschehen darf. Diese Praxis kann Menschen von der Wahrnehmung ihres Demonstrationsgrundrechts abschrecken. Wir haben in Erörterungen mit Polizeipraktikern datenschutzgerechte Anforderungen an Bilderhebungen bei Versammlungen erarbeitet.*

14. *Im Zuge der Zentralisierung der Datensammlungen beim Kraftfahrt-Bundesamt in Flensburg werden die örtlichen **Fahrerlaubnisregister** aufgelöst und die Straßenverkehrsbehörden online mit dem zentralen Datenbestand verbunden. Ohne wirksamen technischen Schutz bestand bei der Übermittlung und auch im Bereich der Fahrerlaubnisbehörden die Gefahr, dass die Daten unterwegs von unbefugten Personen gelesen oder verändert werden. Wir erarbeiteten gemeinsam mit dem Verkehrsministerium einen*

Maßnahmenkatalog für die Fahrerlaubnisbehörden, der die Datensicherheitsstandards festlegt

15. *Im Landesbesoldungsamt wurden neue Regelungen über die Bearbeitung von **Beihilfeanträgen des eigenen Personals** erlassen. Für die 220 Mitarbeiter bedeutete dies, dass sowohl die eigenen Krankheitsdaten als auch die ihrer Familie je nach Vertretungsfall allen Mitarbeitern des Sachgebiets und unter Umständen sogar dem Vorgesetzten zugänglich geworden wären. Wir konnten eine verbesserte Abschottung erreichen: In Zukunft werden die Beihilfeanträge der Amtsangehörigen zentral in einem Sachgebiet und dort nur von einem Mitarbeiter bearbeitet.*

16. *Bei einer **Handwerkskamme** wurden über einen Zeitraum von 15 Jahren alle Informationen über Personen und Betriebe gesammelt, die in den Verdacht der Schwarzarbeit geraten waren. Dies führte zu einem umfangreichen Vorrat an belastenden Daten, für den sich weder ein konkreter Verwendungszweck noch eine Erforderlichkeit anführen ließen. Wir haben erreicht, dass dieser Bestand zunächst reduziert und anschließend erneut einer umfassenden Prüfung unterzogen wird.*

17. *Die Verarbeitung der Daten über die Nutzer von **gemeindlichen Büchereien** wurde bislang uneinheitlich und nicht immer gesetzeskonform gehandhabt. So bestand die Gefahr, dass unzulässige Informationssammlungen über die Nutzer und deren Leseverhalten entstanden. Wir haben die Büchereizentrale Schleswig-Holstein beraten und ihr Handreichungen zur datenschutzgerechten Verarbeitung der Ausleihdaten gegeben.*

18. *Bei vielen Ausländerbehörden war es Praxis, ausreisepflichtige Ausländer, deren Aufenthaltsort unbekannt war, im **Schengener Informationssystem** auszuschreiben, auch wenn die rechtlichen Voraussetzungen hierfür nicht vorlagen. Wenn nicht eine Ausweisung verfügt oder eine Abschiebung vollzogen wurde, können die betreffenden Ausländer jedoch nur in INPOL und im Ausländerzentralregister ausgeschrieben werden. Auf unsere Initiative hin wies das Innenministerium alle Ausländerbehörden per Erlass zu Änderungen der bisherigen Praxis an.*

19. ***Meldungen** von Arbeitgebern **über geringfügig Beschäftigte**, die von der AOK Schleswig-Holstein eigentlich nur an andere Sozialleistungsträger weiterübermittelt werden sollten, waren dort lange Zeit – teilweise unbefristet – gespeichert worden. Diese Daten waren zweckwidrig nutzbar und wurden auch für Werbezwecke von der Krankenkasse verwendet. Unsere Intervention führte nicht nur zur Löschung des umfangreichen Datenbestands, sondern auch zu einer datenschutzgerechten bundesweit einheitlichen Regelung.*

20. *In einer Augenklinik wurden immer mehrere **Patienten** gleichzeitig in einem Raum untersucht, sodass das Patientengeheimnis nicht mehr gewahrt war. Auf Grund unserer Beanstandung erfolgt nunmehr jeweils ein ausdrücklicher Hinweis auf die Möglichkeit einer Einzeluntersuchung; mittelfristig soll durch bauliche Änderungen in jedem Fall eine **separate Untersuchung** gewährleistet werden.*

21. *Bei der **Überprüfung ehelicher Lebensgemeinschaften** durch eine Ausländerbehörde wurde oft zu weitgehend ermittelt. Diese Vorgänge waren zudem ungenügend dokumentiert und wurden den Betroffenen nicht offen gelegt. Dies führte bei diesen zu Ängsten und Verunsicherung. Die Ausländerbehörde hat sich nun unsere Verfahrensvorschläge zu Eigen gemacht, bei deren Beachtung es nicht mehr zu unverhältnismäßigen Eingriffen kommen sollte.*

22. *Wenn oberste Landesbehörden auf dem Gebiet der Informationstechnik in der Vergangenheit **Dienstleistungen anderer Ministerien** in Anspruch genommen haben, gab es wegen des Grundsatzes der Ressortverantwortlichkeit und fehlender schriftlicher Vereinbarungen immer wieder sicherheitstechnische "Synchronisationsprobleme". Nicht selten verließ sich ein "Haus" auf das andere, ließ sich aber selbst nicht in die Karten schauen. Die Schwachstellen haben wir mehrfach kritisiert und Verbesserungen gefordert. Das neu entwickelte "**Landessystemkonzept**" wird hier Abhilfe schaffen.*

23. *Die "**Kundencenter**" **der AOK Schleswig-Holstein** sind bisher nach dem Prinzip "Offenheit" gestaltet worden, dem Diskretionsgedanken wurde kein besonderes Augenmerk geschenkt. So konnten in den Geschäftstellen und Filialien oft die Kundengespräche und Telefonate von wartenden bzw. an Nebentischen sitzenden Versicherten mitgehört werden. Auf Grund unserer Beanstandung werden alle Kundencenter so umgestaltet, dass von den Mitarbeitern das Sozialgeheimnis im täglichen Betrieb gewahrt werden kann.*

24. *Computerviren können u. a. auch dazu benutzt werden, die Sicherheitsmechanismen der Betriebssysteme lahm zu legen. Die Vertraulichkeit und Unversehrtheit der dort gespeicherten Daten ist außerdem gefährdet. Mit einigen Jahren Verzug setzen auf Grund unseres Drängens nun alle Ministerien in ihren Computersystemen **leistungsfähige Virenscanner** ein.*

25. *Die **Fernadministration von Rechnersystemen** durch Mitarbeiter der Datenzentrale erfolgte bislang häufig ohne Wissen der Kunden zur Nachtzeit. Dadurch war sie praktisch jeder Kontrolle entzogen. Auf Grund unserer Kritik hat die Datenzentrale ihr Fernwartungskonzept geändert und macht ihren Kunden die Abläufe und die Kontrollmöglichkeiten transparenter als bisher.*

Jetzt sind Überprüfungen der Arbeiten der Datenzentrale möglich.

26. *In den **Fahrtenbüchern der Ärzte und Apotheker** mussten bisher aus steuerlichen Gründen die Namen der besuchten Patienten bzw. Kunden vermerkt werden. Gelangte ein Fahrtenbuch in unbefugte Hände, war das z. B. gleichbedeutend mit dem Einblick in die Patientennamenskartei des Arztes. Nachdem die Datenschutzbeauftragten dies heftig kritisiert haben, gibt sich die Steuerverwaltung nunmehr mit pseudonymisierten Fahrtenbüchern zufrieden.*

27. *Die Mitarbeiter der AOK Schleswig-Holstein konnten bislang praktisch auf alle **Versichertendaten** zugreifen. Dadurch wurden sensible Krankheitsdaten auch solchen Mitarbeitern bekannt, die für den jeweiligen Fall nicht zuständig waren. Die **Zugriffsberechtigungen** wurden nach unserer Intervention erheblich eingeschränkt.*

14 DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN

Terminübersicht über die Kurse der DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN 2000

Kurse/Seminare/Workshops	Kurz-bez.	Zeit	Ort
Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung	SI 5	16.02.-18.02.2000	Leck
Technischer Datenschutz an Schulen	LT 2	02.03.2000	Kiel – IPTS
Datenschutz an der Schule	L 22	16.03.2000	Kiel – IPTS
Einführung in das Internet	E-INT	21.03.-22.03.2000	VerwFHS
Datenschutz an der Schule	L 23	04.05.2000	Kiel – IPTS
Schutz von Personaldaten	P 8	11.05.-12.05.2000	Bordesholm
Behördliche Datenschutzbeauftragte	D 11	15.05.-19.05.2000	Leck
Datenschutz bei der Internet-Nutzung	NET 1	23.05-24.05.2000	Kiel – KYC
Technik und Recht von Firewalls	FW 5	25.05.2000	Kiel – KYC
Datenschutz im Sozialamt	SOZ 1	07.06.2000	Kiel – KYC
Einstieg in das Datenschutzrecht	E 8	08.06.2000	Kiel – KYC
Einführungskurs Kommunalbereich	EK 7	15.06.2000	Kiel – KYC
Einführungskurs für Schulsekretärinnen und Schulsekretäre	ES 7	15.06.2000	Bordesholm
Führung von Personalakten	PA 8	11.09.-12.09.2000	Bordesholm
Behördliche Datenschutzbeauftragte	D 12	18.09.-22.09.2000	Leck
Einführungskurs für Schulsekretärinnen und Schulsekretäre	ES 8	21.09.2000	Bordesholm
Datenschutz an der Schule	L 24	28.09.2000	Kiel – IPTS
Beauftragte für Sozialdatenschutz	S 8	09.10.-13.10.2000	Leck
Workshop zur Datensicherheit	SIW 5	09.11.-10.11.2000	Leck
Datenschutz bei der Internet-Nutzung	NET 2	14.11-15.11.2000	Kiel – KYC
Technik und Recht von Firewalls	FW 6	16.11.2000	Kiel – KYC
Datenschutz an der Schule	L 25	23.11.2000	Kiel – IPTS
Modernisierung in der Verwaltung	MV 2	28.11.2000	Kiel – KYC
Einführungskurs Kommunalbereich	EK 8	30.11.2000	Kiel – KYC
Workshop für behördliche Datenschutzbeauftragte	DW 4	05.12.2000	Kiel – KYC
Technischer Datenschutz an Schulen	LT 3	07.12.2000	Kiel – IPTS
Einstieg in das Datenschutzrecht	E 9	12.12.2000	Kiel – KYC
Datenschutz im Sozialamt	SOZ 2	14.12.2000	Kiel – KYC

Im Rahmen der DATENSCHUTZAKADEMIE werden Sonderveranstaltungen speziell für die Behörden des Landes Schleswig-Holstein zum neuen Landesdatenschutzgesetz geplant. Die Veranstaltungen werden mit gesonderten Informationsblättern angekündigt.

Das Jahresprogramm 2000 der DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN mit näheren Informationen zu den Veranstaltungen und Anmeldeformularen kann kostenlos angefordert werden beim

Landesbeauftragten für den Datenschutz
Düsternbrooker Weg 82, 24105 Kiel
Telefon: 0431/988-1208, Telefax: 0431/988-1223
E-Mail: LDSH@netzservice.de
Homepage: http://www.schleswig-holstein.datenschutz.de

Das Programm ist auch im Internet auf unserer Homepage verfügbar:

www.schleswig-holstein.datenschutz.de
(Rubrik: DATENSCHUTZAKADEMIE)

15 Sommerakademie 2000

Die Sommerakademie 2000 findet am

28. August 2000

im Kieler Schloss statt. Dieses Mal treffen sich Fachleute und Interessierte zum Thema

E-Privacy
- Datenschutz im Internet -

E-Commerce, E-Business, E-Government ... – das vorangestellte "E" für "electronic" (manchmal auch schon weiterentwickelt zum "i" für "intelligent" oder "Internet") ist aus den Bezeichnungen inzwischen genauso wenig wegzudenken wie die Anwendungen, die sich dahinter verbergen. Alles "goes" Internet, auch der Datenschutz. Unter dem Titel E-Privacy wollen wir auf der Sommerakademie diskutieren, wie es mit der Privatsphäre im Internet bestellt ist und wie der Datenschutz aussehen muss, wenn er im Internet etwas bewirken will.

In der Veranstaltung kommen Praktiker aus der Internet-Community, Freaks und Privacy-Aktivisten, Diensteanbieter aus Wirtschaft und Verwaltung, Vertreter von Nutzerorganisationen, Wissenschaftler, Journalisten und nicht zuletzt auch die Datenschützer selbst zu Wort. Bei einem globalen Thema wie dem Internet werfen wir auch einen Blick über die nationalen Grenzen, wo auf Grund anderer Gesellschafts- und Rechtsstrukturen mit den entstehenden Problemen teilweise anders umgegangen wird. Interessante Fragestellungen betreffen den fortschreitenden Verlust der Privatsphäre im Netz und das Ende der staatlichen Einflussnahme. Welche Steuerungsinstrumente sind stattdessen wirkungsvoll? Wie viel Selbstschutz der Nutzer ist nötig und wie viel ist möglich? Was muss sich ändern, damit auch das "virtuelle Leben" im Internet lebenswert bleibt? Was gelten Demokratie und Menschenrechte im Internet?

Die diesjährige Sommerakademie will zur Diskussion über diese Fragen wieder Fachleute unterschiedlicher Disziplinen an einen Tisch bringen. Der *neue* Datenschutz, der sich mit seiner Ausrichtung auf datenschutzfreundliche Technologien zu einem Motor des technischen Fortschritts entwickelt, soll zeigen, was er den Bürgerinnen und Bürgern im Internet bieten kann.

In Vorträgen, Gruppenarbeit und Diskussionen werden die Perspektiven erörtert und konkrete Schritte erarbeitet. Auf der begleitenden Ausstellung werden Anwendungen zu Internet und E-Privacy vorgestellt. Praktische Tipps runden die Info-Börse der Veranstaltung ab. Wer sich an der Diskussion zu "E-Privacy" beteiligen will, kann dies übrigens im Vorfeld der Sommerakademie auch über das Internet machen.

An der Vorbereitung und Durchführung der Sommerakademie 2000 wirken u. a. mit:

Michael **Bobrowski,** Arbeitsgemeinschaft der Verbraucherverbände e. V.; Jason **Catlett,** Junkbusters Corp., Green Brook, USA; Dr. John **Borking,** Vice-President der Registratiekamer, Niederlande; Dr. Lorrie Faith **Cranor,** AT&T Labs-Research Shannon Laboratory, Florham Park, USA; Dr. Alexander **Dix,** Landesbeauftragter für den Datenschutz und das Recht auf Akteneinsicht, Brandenburg; Dr. Hannes **Federrath,** International Computer Science Institute (ICSI), Berkeley, USA; Prof. Dr. Hansjürgen **Garstka,** Berliner Beauftragter für Datenschutz und Akteneinsicht; Lukas **Gundermann,** Mitarbeiter beim Landesbeauftragten für den Datenschutz in Schleswig-Holstein; Dr. Rüdiger **Grimm,** GMD-Forschungszentraum Informationstechnik GmbH, Darmstadt; Prof**.** Dr. Thomas **Hoeren,** Institut für Informations-, Telekommunikations- und Medienrecht, Münster; Dipl.-Inform. Marit **Köhntopp,** Referentin beim Landesbeauftragten für den Datenschutz in Schleswig-Holstein; Prof. Dr. Herbert **Kubicek,** Universität Bremen; Nils **Löhndorf,** DG Bank Deutsche Genossenschaftsbank AG, Frankfurt am Main; **Jonas Luster,** Senior Security Engineer Exodus Communications, Santa Clara, USA; Prof. Dr. jur. Bernd **Lutterbeck,** Dozent de Aktion Jean Monnet der Europäischen Union Brüssel, Technische Universität Berlin, Institut für Angewandte Informatik; Erich **Moechel,** Österreich; Frank **Möller,** Mitarbeiter des Landesbeauftragten für den Datenschutz in Schleswig-Holstein; Prof. Dr. Dieter **Otten, M.A.,** Professor für Soziologie an der Universität Osnabrück; Prof. Dr. Andreas **Pfitzmann,** Technische Universität Dresden, Institut für Theoretische Informatik; Thomas **Roessler**, Bonn; Florian **Rötzer,** Publizist und Medientheoretiker; Chefredakteur beim Heise Verlag, München; Prof. Dr. Alexander **Roßnagel,** Universität Gesamthochschule Kassel; Ingo **Ruhmann,** Bundesministerium für Bildung und Forschung; Peter **Schaar,** Stv. Hamburgischer Datenschutzbeauftragter; Michael **Schneider,** Rechtsanwalt, Hennef; Bruce **Schneier,** Counterpane Systems, Mineapolis, USA; Christiane **Schulzki-Haddouti,** Korrespondentin, Koblenz; Leo **Schuster,** Erster Direktor des BKA, Wiesbaden; Prof. Dr. Dr. h.c. Spiros **Simitis,** Johann Wolfgang Goethe-Universität Forschungsstelle für Datenschutz, Frankfurt; Bettina **Sokol,** Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Düsseldorf; Hanno **Wagner**, Karlsruhe; Dr. Thilo **Weichert,** Stv. Landesbeauftragter für den Datenschutz in Schleswig-Holstein; Markus **Wiese,** Mitarbeiter beim Landesbeauftragten für den Datenschutz in Schleswig-Holstein; Dr. Helmut **Bäumler,** Landesbeauftragter für den Datenschutz in Schleswig-Holstein.

INFORMATION UND ANMELDUNG BEIM

Landesbeauftragten für den Datenschutz
Düsternbrooker Weg 82, 24105 Kiel
Telefon: 0431/988-1200, Telefax: 0431/988-1223
E-Mail: LDSH@netzservice.de

Beim **Landesbeauftragten für den Datenschutz** erhältliche Publikationen:

Datenschutz in Schleswig-Holstein
Text des Landesdatenschutzgesetzes, der Datenschutzverordnung und des Bundesdatenschutzgesetzes mit einer erläuternden Einführung

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

Broschüren
backUP – Magazin für IT-Sicherheit (Reihe)
Datenschutz leicht gemacht – Praxistipps zum Datenschutzrecht (Reihe)

Diverse Aufkleber
Der Mensch ist mehr als Null und Eins
Aufkleber zum Thema E-Mail-Verschlüsselung

DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN
- Broschüre
- Jahresprogramm 2000

Schleswig-holsteinische Datenschutzinformationen im Internet
Datenschutzinformationen aus Schleswig-Holstein sind natürlich auch im weltweiten Datennetz zugänglich: **http://www.schleswig-holstein.datenschutz.de** (Homepage des Landesbeauftragten für den Datenschutz Schleswig-Holstein). Zur Zeit sind das derzeit gültige Bundes- und Landesdatenschutzgesetz und die Datenschutzverordnung, das ab dem 01.07.2000 geltende neue Landesdatenschutzgesetz, das Informationsfreiheitsgesetz, das Programm der DATENSCHUTZAKADEMIE, Informationen zu den Sommerakademien, die Tätigkeitsberichte der letzten Jahre, Pressemitteilungen und weitere Publikationen im elektronischen Format abrufbar. Weiterhin ist dort der öffentliche Schlüssel des Landesbeauftragten für den Datenschutz und ein bedienfreundliches Verschlüsselungsprogramm PGP (Pretty Good Privacy) für vertrauliche E-Mail-Kommunikation 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. Als Systemvoraussetzung sind ein PC 386/486 oder höher, mindestens 18 MB Hauptspeicher, MS-DOS 5.0 aufwärts und Windows 3.1, Windows für Workgroups bzw. Windows 95/98/NT erforderlich. Die CD-ROM kann beim Landesbeauftragten für den Datenschutz kostenlos angefordert werden.