SCHLESWIG-HOLSTEINISCHER LANDTAG
15. Wahlperiode

Drucksache 15/2535
03-04-09

Bericht

des Unabhängigen Landeszentrums für den Datenschutz Schleswig-Holstein

Tätigkeitsbericht 2003

Tätigkeitsbericht 2003

des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

Berichtszeitraum: 2002, Redaktionsschluss: 19.02.2003
Landtagsdrucksache 15/2535

(25. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz)

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

Inhaltsverzeichnis **Seite**

1 Situation des Datenschutzes in Schleswig-Holstein

1.1 Datenschutz als Standortvorteil für Schleswig-Holstein

Es beginnt sich auszuzahlen, dass Schleswig-Holstein in Datenschutzfragen seit Jahren einen abgewogenen und zugleich konsequenten Kurs fährt. Die große Anfrage der SPD-Fraktion zur **Datenschutzpolitik in Schleswig-Holstein,** die Antwort der Landesregierung (Drucksache 15/2287) und die nachfolgende Parlamentsdebatte zeigten, dass es einen breiten Konsens quer durch alle Parteien gibt, was die grundlegenden Datenschutzfragen angeht. Alle Redner betonten, dass die Bürgerinnen und Bürger in Schleswig-Holstein sich auch in Zukunft darauf verlassen können, dass der Datenschutz eine wichtige Staatsaufgabe bleibt. Stammtischparolen über „zu viel Datenschutz“ hört man hier selten, stattdessen überwiegt die gemeinsame Anstrengung, den Datenschutz im Interesse der Bürgerinnen und Bürger kontinuierlich zu optimieren. Auch Schleswig-Holsteins Haltung im Bundesrat ist zumeist geprägt von der Absicht, den Grundrechtsschutz zu verbessern.

Das im Jahre 2000 umfassend modernisierte **Landesdatenschutzgesetz** (LDSG) erweist sich in der täglichen Praxis als vernünftiges und wirksames Handlungsinstrument. Das Parlament war mit seinem Ansatz, das Gesetz so weit wie möglich zu vereinfachen und zu verschlanken und auf der anderen Seite klare Konturen zu zeigen, wenn es um den Schutz der Bürgerinteressen geht, auf der Höhe der Zeit. Dass die Datenverarbeitung in bestimmten Fällen nunmehr direkt auf das LDSG gestützt werden kann, führt zunehmend zur Entlastung der Fachgesetze von allgemeinen Erhebungs- und Übermittlungsregelungen, ohne dass damit ein erkennbarer Nachteil für die Bürgerinnen und Bürger verbunden wäre.

Die Gründung des **Unabhängigen Landeszentrums für Datenschutz** (ULD) in der Form einer Anstalt des öffentlichen Rechts hat sich in den vergangenen zwei Jahren bewährt. Das ULD kann seine Aufgaben in der von der Europäischen Datenschutzrichtlinie verlangten Unabhängigkeit erfüllen. Die Anstaltsform erweist sich als geradezu ideal für die sinnvolle Verknüpfung der Verlässlichkeit und Korrektheit einer öffentlichen Behörde mit der aus der Privatwirtschaft gewohnten Flexibilität und Innovationskraft. Das ULD hat sich in den zwei Jahren seines Bestehens einen guten Ruf erworben, der weit über Schleswig-Holstein hinausreicht. Ein Beleg dafür ist die Vielzahl von Einladungen zu Vorträgen aus dem Bundesgebiet und aus europäischen Ländern, die gar nicht alle bewältigt werden können. Die Mitarbeiterinnen und Mitarbeiter sind auch als Autoren gefragt, wie ein Blick in die Datenschutz- und Datensicherheitsliteratur deutlich werden lässt. Die neuen Instrumente Datenschutzaudit und -gütesiegel sind so attraktiv, dass insbesondere überregional tätige Firmen nachfragen, welche Möglichkeiten es gibt, diese schleswig-holsteinischen Qualitätszeichen zu erlangen. Wenn diese Firmen Aufträge deshalb nach Schleswig-Holstein vergeben, weil sie nur so an ein Datenschutzaudit kommen können, dann ist „Datenschutz als Standortvorteil“ offenbar mehr als ein Schlagwort.

Auch das **Informationsfreiheitsgesetz**, das ein wesentlicher Baustein der schleswig-holsteinischen Informationspolicy ist, hat seine Bewährungsprobe bestanden.

Was anderswo gelegentlich von schrillen Tönen begleitet ist, hat sich in Schleswig-Holstein ohne viel Getöse etabliert. Eine Untersuchung des ULD (vgl. Tz. 13.1) zeigt, dass das Gesetz rege in Anspruch genommen wird. Bürgerinnen und Bürger, die dies tun, haben überwiegend Erfolg. Über 90 % aller Informationsanträge werden – zumeist binnen weniger Tage – positiv beschieden. Die Behörden, die das Gesetz keineswegs überall mit Begeisterung aufgenommen hatten, haben sich erstaunlich schnell mit den neuen Rechten der Bürger arrangiert. Die wenigen Streitfälle, die es in Schleswig-Holstein gibt, resultieren aus einer nur gelegentlich anzutreffenden engen, fast ängstlichen Gesetzesinterpretation.

1.2 Datenschutzaudit und -Gütesiegel im Praxistest

Im vergangenen Jahr wurden die ersten Audit- und Gütesiegelverfahren erfolgreich abgeschlossen (vgl. Tz. 10.1, 10.3). Ihre Zahl wird sich in diesem Jahr beträchtlich erhöhen. Zunehmend erkennen Firmen und Behörden, dass es ein Vorteil ist, bei ihren Kunden mit einem überzeugenden, von unabhängiger Seite geprüften Datenschutzkonzept zu werben. Die bisher durchgeführten Audits haben gezeigt, dass es allen Beteiligten Spaß machen kann, den Datenschutz einmal von einer ganz anderen Seite kennen zu lernen. Zwar ist es für eine abschließende Analyse noch zu früh, aber es ist aufgefallen, dass die Herangehensweise an das Thema Datenschutz von vornherein eine andere ist, wenn, wie beim Audit, Behörden von sich aus die Initiative ergreifen. Alle bisherigen Audits haben zu **datenschutzrechtlichen Verbesserungen** geführt, die eigener Einsicht entsprangen und nicht per Kontrolle und Kritik durchgesetzt werden mussten. Das im Rahmen eines Audits zu entwickelnde Datenschutzmanagementsystem gewährleistet, dass das erreichte Datenschutzniveau auf Dauer gehalten wird. Dafür kann auch die „Kontrolle“ durch die Kunden sorgen, die aufgrund eines zu Werbezwecken gezeigten Datenschutzauditzeichens vielleicht ein besonderes Augenmerk darauf richten, ob der Datenschutz in der jeweiligen Stelle tatsächlich so gut ist wie versprochen.

1.3 Die Ergebnisse bei Kontrollen

Datenschutzrechtliche Kontrollen sind neben Beratung, Audit und Gütesiegel weiterhin notwendig. Im Berichtszeitraum wurden insgesamt 26 systematische Kontrollen durchgeführt (vgl. Tz. 4.2.2, 4.2.4, 4.3.1, 4.8.8, 4.9.1, 4.11.1, 6.2.1, 7.4.1, 7.4.2, 7.4.3, 7.4.4, 7.6). Dabei wurden die Datenverarbeitungsprozesse sowohl bei öffentlichen Stellen als auch in der Privatwirtschaft analysiert. Kaum ein Prüfbericht kam ohne Beanstandung aus, aber die **Kontrollen** zeigen auch **tatsächlich Wirkung**. So ergab eine Nachschau in einer Justizvollzugsanstalt neun Jahre nach der ersten Querschnittsprüfung in diesem Bereich, dass tatsächlich einiges besser geworden ist (vgl. Tz. 4.3.1). Auch die Schwerpunktkontrollen im Bereich der Entsorgung von Akten und anderen Datenträgern im vergangenen Jahr (vgl. 24. TB, Tz. 7.6) haben ihre Wirkung nicht verfehlt. Bei einer systematischen Nachkontrolle in diesem Jahr gab es kaum Grund zu Beanstandungen (vgl. Tz. 7.6). Eine erstmals durchgeführte Kontrolle des Krebsregisters ergab, dass dort sehr sorgsam mit den Daten der Krebspatienten umgegangen wird (vgl. Tz. 7.4.3).

Im krassen Gegensatz dazu standen die Feststellungen im **Krankenhaus Itzehoe**. Die Mängel waren in einigen Punkten so gravierend, dass noch vor Beendigung der Prüfung „Eilbeanstandungen“ ausgesprochen werden mussten (vgl. Tz. 7.4.1).

Eine systematische Nachschau bei allen **Handels- und Wirtschaftsauskunfteien** in Schleswig-Holstein ergab diverse Mängel, die beim Umgang mit so sensiblen Daten nicht akzeptabel sind (vgl. Tz. 6.2.1).

Der Umgang der **Polizei** mit **genetischen Daten** in ihren Laboren ergab keinen Grund zur Beanstandung. Allerdings muss die Dokumentation der Entscheidungen über die Erhebung und Aufbewahrung genetischer Daten verbessert werden (vgl. Tz. 4.2.2). Bei der **Rasterfahndung** zeigte sich, dass ihre technische Durchführung bislang korrekt erfolgte. Im Gegensatz zum Innenministerium sind wir aber der Meinung, dass die Rolle des BKA bei dieser Rasterfahndung vom Gesetz nicht gedeckt ist und dass der Kreis der Personen, zu denen Anschlussermittlungen durchgeführt wurden, zu groß ist (vgl. Tz. 4.2.4).

Eine Anlasskontrolle bei der Christian-Albrechts-Universität (CAU) förderte erhebliche **Sicherheitslücken beim Internet-Anschluss** und eine Reihe konzeptioneller Mängel des Datenschutzes in der CAU zutage (vgl. Tz. 4.9.1).

1.4 Die Ausstattung des Unabhängigen Landeszentrums für Datenschutz

Das Unabhängige Landeszentrum für Datenschutz, das seine Räume nunmehr mitten in der Kieler Fußgängerzone hat, ist nicht nur dadurch **näher an die Bürgerinnen und Bürger** herangerückt. Mit mehreren Umfragen haben wir uns bemüht, die Meinung der Bürgerinnen und Bürger zu aktuellen Datenschutzfragen in Erfahrung zu bringen (vgl. Tz. 4.8.9, 6.1). Die konsequente Orientierung unserer Arbeit an den Interessen unserer „Kunden“ trägt dazu bei, dass die Bürger unsere Dienststelle als zentralen Anlaufpunkt für alle Fragen des Informationsrechts betrachten.

Allerdings ändern sich Struktur und Zielrichtung der Bürgereingaben in auffälliger Weise. Die Zahl der klassischen Petitionen, in denen sich Bürgerinnen und Bürger über datenschutzwidriges Verhalten einer speichernden Stelle beschweren, geht vor allem im Bereich der öffentlichen Verwaltung kontinuierlich zurück. Offenbar hat die jahrelange Kontroll-, Aufklärungs- und Überzeugungsarbeit ihre Wirkung nicht verfehlt. Die Behörden wollen sich in Datenschutzfragen möglichst keine Blöße mehr geben. Fälle, in denen das Datenschutzrecht der Bürger sehenden Auges missachtet wurde, kommen kaum noch vor. Dies werten wir als gutes Zeichen für das in **Schleswig-Holstein** erreichte **Datenschutzniveau**. Was bleibt, sind Streitfälle bei der Auslegung zweideutiger Gesetzesvorschriften oder Beschwerden über Nachlässigkeiten. Gleichwohl nimmt die Zahl der Eingaben seit Jahren überproportional zu. Immer mehr Menschen wollen von unseren Beratungsdienstleistungen profitieren. Auch außerhalb Schleswig-Holsteins wird es geschätzt, dass man sich bei uns kompetente Informationen und Ratschläge, z. B. zum Selbstdatenschutz, schnell und unbürokratisch holen kann. Täglich erreichen uns Dutzende von Anrufen und E-Mails, in denen die Bürger Hilfe und Orientierung im Informationsdschungel erbitten.

Die **Personalausstattung** der Dienststelle kann diese Nachfrage nach Datenschutz nur noch mit äußerster Mühe befriedigen. Zwar ist die Zahl der Mitarbeiterinnen und Mitarbeiter in den letzten Jahren immer wieder erhöht worden, aber mit der Entwicklung und Verbreitung der Informationstechnik und der Komplexität der sie steuernden Rechtsvorschriften konnte in keiner Weise Schritt gehalten werden. Besonders drastisch ist die Unterbesetzung im Bereich der **privaten Wirtschaft**, obwohl gerade dort die größten Steigerungsraten hinsichtlich der Nachfragen von Betrieben und Kunden zu verzeichnen sind. Als seinerzeit im Jahre 2000 die Aufgabe der Datenschutzkontrolle in der Privatwirtschaft vom Innenministerium auf das Unabhängige Landeszentrum für Datenschutz überging, wurde lediglich die im Innenministerium vorhandene Personalausstattung von zwei Mitarbeitern mit übertragen. Wegen der kurze Zeit später im Zuge der Novellierung des BDSG im Jahre 2001 in Kraft getretenen **erheblichen Aufgabenerweiterungen** bestand zwischen dem Innenministerium und uns Übereinstimmung, dass eine auch nur einigermaßen glaubwürdige Wahrnehmung der neuen Kontrollaufgaben mindestens die Einrichtung von vier weiteren Stellen notwendig machen würde. Obwohl diese Stellen im Rahmen der Haushaltsberatungen mehrfach beantragt wurden, ist bis heute keine einzige bewilligt worden. Bei allem Verständnis für die angespannte Haushaltssituation im Lande müssen wir darauf hinweisen: Mit der gegenwärtigen Personalausstattung im Bereich der Datenschutzaufsicht in der Privatwirtschaft kann man den Bürgerinnen und Bürgern nicht mit ruhigem Gewissen versichern, sie könnten sich auf die Kontrollen der Datenschutzaufsicht verlassen.

2 Der Weg in die Informationsgesellschaft

Wenn sich zu Überwachungseifer auch noch Regelungswut gesellt

Verschlankung, Verwaltungsmodernisierung, Deregulierung und Rückführung des staatlichen Sektors sind längst keine abstrakten Programmsätze mehr, sondern werden von Politik und Verwaltung auch tatsächlich zunehmend realisiert. In einem Bereich tobt sich dagegen die **staatliche Regelungswut**, unbeeindruckt vom Geschehen ringsherum, ungebremst aus: Wenn es um die Überwachung der Telekommunikation geht, spielen Kosten, Normenflut und fehlende Transparenz offenbar plötzlich keine Rolle. Die fixe Idee, es dürfe keine „abhörfreien", nicht überwachten Bereiche der Telekommunikation geben, hat in den vergangenen Jahren zu einer solchen Fülle von neuen Gesetzen, kurzatmigen Gesetzesnovellierungen und permanenten Anpassungen von untergesetzlichen Vorschriften geführt, dass sich in dem entstandenen Paragraphendschungel auch Fachleute nur noch schwer zurechtfinden. Die meisten Bürger haben längst den Versuch aufgegeben, durch einen einfachen Blick ins Gesetz klären zu wollen, ob ihre persönliche Telekommunikation abgehört oder sonst wie überwacht werden kann. Viele haben resigniert und rechnen vorsichtshalber damit, dass der Staat hemmungslos abhört und überwacht. Unternehmen der Telekommunikation beklagen sich darüber, dass ihnen durch permanente komplizierte Neuerungen in den gesetzlichen Vorschriften der Überblick und damit eine sichere Kalkulationsgrundlage entzogen wird.

Dabei fing alles so überschaubar an, als 1968 nach heftigen politischen Auseinandersetzungen im Zuge der **Notstandsgesetze** erstmals das Abhören von Telefongesprächen erlaubt wurde. Seitdem wurde der einschlägige § 100 a Strafprozessordnung (StPO) über ein Dutzend Mal geändert – immer wurden dabei die Abhörmöglichkeiten erweitert, niemals eingeschränkt. Ein neues Zeitalter der Überwachung begann 1997 mit dem In-Kraft-Treten des **Begleitgesetzes zum Telekommunikationsgesetz**, denn es ließ fortan nicht nur die Überwachung des „Fernmeldeverkehrs", sondern der gesamten Telekommunikation und damit aller Kommunikationsformen der neuen Medien zu. Infolge der Privatisierung der Telekommunikation wurden nicht nur der Post-Nachfolger Telekom, sondern alle geschäftsmäßigen Erbringer von Telekommunikationsdienstleistungen in die Pflicht genommen. Die Einzelheiten regelt die **Telekommunikationsüberwachungsverordnung**, die nach langwierigen Debatten im Windschatten des 11. September 2001 ohne viel Aufheben verabschiedet wurde (vgl. 24. TB, Tz. 8.3).

Zu Jahresbeginn 2002 traten die neuen §§ 100 g und 100 h StPO in Kraft, die den alten § 12 Fernmeldeanlagengesetz ablösten und die Nutzung von **Verbindungsdaten**, die im Rahmen der Digitalisierung nunmehr vollständig erfasst werden, neu regeln. Seitdem kann ein richterlicher Beschluss auch die Erfassung von Verbindungsdaten für die Zukunft anordnen. „Nebenbei" wird in der Gesetzesbegründung „klargestellt", dass die **IP-Nummern**, falls sie – in der Regel unzulässigerweise – bei den Access-Providern im Internet erfasst werden, nicht den neuen §§ 100 g und 100 h StPO unterliegen, sondern nach § 89 Abs. 6 Telekommunikationsgesetz zu beurteilen sind. Sie sind also auf Anforderung von Sicherheitsbehörden und ohne richterlichen Beschluss herauszugeben.

Schon 1996 wurde in § 90 TKG geregelt, dass Telekommunikationsanbieter **Kundendateien** zu führen haben, auf die die Sicherheitsbehörden unbemerkt von den Anbietern zugreifen können. Bei im Voraus bezahlten Telefonkarten für Handys brauchen die Anbieter eigentlich keine Kundendaten – im Gegenteil, die Bestimmungen zu Datenvermeidung und Datensparsamkeit verbieten ihnen das unnötige Datenspeichern in diesen Fällen. Das dachten zu Recht auch einige Telekommunikationsunternehmen und weigerten sich, dem Verlangen der Sicherheitsbehörden nach Speicherung von Kundendaten auch beim Kauf von Prepaid-Karten nachzukommen. Sie klagten gegen entsprechende Auflagen der Regulierungsbehörde für Telekommunikation und Post; sie wollten keine Kundendaten ohne Notwendigkeit speichern. Als sie beim Verwaltungsgericht Köln Recht bekamen (vgl. 23. TB, Tz. 8.1), wurde sofort der Bundesgesetzgeber aktiv und ließ verlautbaren, man werde diese „Lücke“ im TKG umgehend im Sinne der Sicherheitsbehörden schließen. Zwischenzeitlich hat das Oberverwaltungsgericht Münster entschieden, dass nach seiner Rechtsauslegung angeblich bereits der bestehende § 90 TKG die Anbieter verpflichtet, auch die Kundendaten von **Prepaid-Karten** im Interesse der Sicherheitsbehörden zu erheben und zu speichern. Gleichwohl will der Bundesgesetzgeber – sicher ist sicher – den § 90 noch einmal eindeutig in Richtung auf Datenerfassung und Weitergabe an die Sicherheitsbehörden „überarbeiten“. Bei dieser Gelegenheit soll dann auch gleich insgesamt der Katalog der von allen Kunden zu erfassenden Daten erweitert und die systematische Suche in den riesigen Kundendatenbanken perfektioniert werden (vgl. Tz. 8.4).

War noch ein Wunsch offen? In der Tat, Handys haben die schöne Nebenwirkung, dass man feststellen kann, wo sich der Besitzer gerade befindet. Das Handy als ein Peilsender, den inzwischen fast jeder mit sich herumträgt, das stand auf der Forderungsliste der Sicherheitsbehörden seit Jahren ganz oben. Der Einsatz des **IMSI-Catchers**, der die Ortung von mobilen Endgeräten wie Handys ermöglicht, war jahrelang umstritten. Nach dem 11. September 2001 wurde seine Nutzung im Rahmen der Antiterrorgesetzgebung zunächst den Geheimdiensten erlaubt, mit Gesetz vom 06.08.2002 nunmehr auch den Strafverfolgungsbehörden durch Einfügung eines neuen § 100 i in die StPO. Warnungen von Fachleuten, der IMSI-Catcher gehöre eigentlich strikt verboten, statt ihn bei den Sicherheitsbehörden hoffähig zu machen, weil er in den Händen von Kriminellen viel Unheil anrichten kann, wurden in den Wind geschlagen.

In all den Jahren wurden stets auch die Befugnisse der **Zollfahndung** nach § 39 Außenwirtschaftsgesetz, wonach die Telekommunikation sogar zur „**Verhütung**“ bestimmter Straftaten überwacht werden darf, „mitverbessert“. Ebenso wenig kamen die **Geheimdienste** bei den verschiedenen „Gesetzesoptimierungen“ zu kurz. Sie liefen bei den Gesetzesverschärfungen mehr oder weniger geräuschlos „mit“. Im Terrorismusbekämpfungsgesetz von 2002 erhielten sie erstmals direkten Zugriff auf Telekommunikationsverbindungsdaten und auf Nutzungsdaten. Der Einsatz des IMSI-Catchers wurde den Geheimdiensten sogar früher als der Polizei erlaubt.

Niemand sollte meinen, diese Aufzählung sei vollständig. Die vielen Einzelheiten und kleineren „Flurbereinigungen“ des **Überwachungsarsenals** können hier aus Platzgründen gar nicht dargestellt werden. Die gesamte Rechtslage der Überwachung der Telekommunikation ist **kompliziert** und **unübersichtlich**. Der perfek-

tionistische Anspruch, mit dem der Bund die Überwachungsgesetzgebung seit Jahren kontinuierlich betreibt, hat zu einem Flickenteppich von sich in Teilen überschneidenden, nicht sauber abgegrenzten Überwachungsbestimmungen geführt, den nur noch wenige überblicken. Aber er zeigt die gewünschte Wirkung: Die Überwachung der Telekommunikation nimmt jährlich gravierend zu. Selbst wenn man die allgemeinen Steigerungszahlen der Nutzung der Telekommunikation einkalkuliert, ergibt sich, dass die Überwachung schneller wächst als die Telekommunikation. In der Literatur ist davon die Rede, Deutschland habe sich in den vergangenen Jahren zu einem **Abhörparadies** entwickelt.

Fehlt noch etwas? Ja, im Teledienstedatenschutzgesetz haben sich bis heute ein paar Bestimmungen wacker gehalten, die, wenn sie beachtet würden, den Internet-Nutzern durchaus eine Chance auf Datenschutz ließen. Dort ist nämlich zum Beispiel geregelt, dass die Inanspruchnahme von Telediensten **anonym** oder unter **Pseudonym** möglich sein soll. Personenbezogene Daten dürfen von den Providern allenfalls dann gespeichert werden, wenn dies für Abrechnungszwecke erforderlich ist. Die Anbieter von Webseiten im Internet dürfen Daten ihrer Besucher also nicht speichern und die Zugangsprovider nur insoweit, wie dies für Abrechnungszwecke erforderlich ist. Nun weiß jeder Praktiker, dass dies keineswegs überall beachtet wird, sodass über Internet-Surfer an vielen Stellen heimlich und rechtswidrig Daten aufgezeichnet werden. Selbst wenn Kunden eine Flatrate haben, also die Zeit, in der sie im Internet surfen, gar nicht abrechnungsrelevant ist, speichern einige Provider das Surfverhalten ihrer Kunden. Andere Anbieter halten sich aber an das Gesetz und könnten mit den neuen Instrumenten Audit und Gütesiegel sogar um Kunden werben. Der von uns gemeinsam mit der TU Dresden betriebene Anonymisierungsdienst **AN.ON** (vgl. Tz. 9.2) erfreut sich nicht nur der Förderung durch das Bundeswirtschaftsministerium, sondern hat obendrein den Charme, durch und durch gesetzmäßig zu sein. Rechtswidrig ist nach dem Teledienstedatenschutzgesetz nämlich nicht das anonyme Nutzen des Internets, sondern das Speichern von Daten über das Surfverhalten.

Wer Systeme wie AN.ON nicht nutzt, muss damit rechnen, dass sein Surfverhalten aufgezeichnet und ausgewertet wird. Aber es geht eben nicht „nur“ um das Surfverhalten, sondern im Kern wird registriert, wofür die Bürgerinnen und Bürger sich interessieren, wie lange sie sich welche Seiteninhalte ansehen, welchen nächsten Klick sie vollziehen, woran sie also vermutlich als Nächstes gedacht haben usw. Da die Zahl der Internet-Nutzer in Deutschland ständig zunimmt, in Schleswig-Holstein sogar überproportional, wächst mit den im Internet protokollierten Surfdaten ein **Überwachungs- und Ausforschungspotenzial** heran, das seinesgleichen nirgendwo in der konventionellen Welt hat. In dieser Situation bräuchten die Bürger eigentlich Schutz und Hilfe vom Staat, damit die im Teledienstedatenschutzgesetz gesetzlich versprochene anonyme oder pseudonyme Nutzung des Internets überhaupt in Anspruch genommen werden kann.

Die Signale der Bundespolitik gehen leider genau in die entgegengesetzte Richtung. Statt den Sammlern rechtswidriger Protokolldatenbestände das Handwerk zu legen, soll das Protokollieren nicht nur gesetzlich erlaubt, sondern, wennschon – dennschon, gleich auch noch ausdrücklich vorgeschrieben werden. Die Vorstöße hierzu kommen aus den unterschiedlichsten Richtungen. Mal sind es Initiativen aus Brüssel, mal mahnt die Bundesratsmehrheit die Speicherung von **Vorrats-**

daten an. Noch hält das Teledienstedatenschutzgesetz; es wurde sogar im Berichtszeitraum in einer Novellierung, inklusive Anspruch auf anonyme oder pseudonyme Internet-Nutzung, bekräftigt. Aber die Begründungen der Bundesregierung bei der Ablehnung des Bundesratsentwurfs zur verpflichtenden Einführung der Vorratsspeicherung klingen nicht so, dass man allzu hohe Wetten darauf abschließen möchte, dass dies unter allen Umständen auch morgen noch gilt. Zu unerbittlich und konsequent sind in den vergangenen Jahren „Überwachungslücken" geschlossen worden, als dass man glauben könnte, der Gesetzgeber werde vor der Anordnung der Vorratsspeicherung dann doch zurückschrecken. Davon, dass die Politik ihr Augenmerk auf die ganz andere Seite richten könnte, nämlich den Datenschutz der Internet-Nutzer endlich auch in der Praxis durchzusetzen, mag man gar nicht mehr träumen ...

So sind wir denn, was die Einführung einer verpflichtenden Vorratsdatenspeicherung angeht, wieder einmal am **Scheideweg** angelangt: Traut der Staat seinen Bürgern, oder misstraut er ihnen von vornherein? Wer den Bürgern misstraut, der kann es auch nicht riskieren, ihnen eine anonyme Nutzung des Internets zuzugestehen. Er muss, ähnlich wie der griechische Philosoph Platon in der Geschichte vom Ring des Gyges, dafür plädieren, den Menschen nie, auch nicht für wenige Augenblicke, ohne Überwachung zu lassen, weil er dies sofort zu kriminellen Handlungen nutzen würde. Aus diesem abgrundtiefen Misstrauen gegen die Menschen resultiert bekanntlich ein Staatsideal Platons, das totalitären Regimen näher steht als unseren Vorstellungen von Demokratie. Bislang gingen wir immer davon aus, dass die Freiheit jedes Einzelnen das vorrangige Prinzip ist, in das der Staat nur ausnahmsweise und bei Vorliegen definierter Voraussetzungen eingreifen darf. Man muss allerdings einräumen, dass sich die Polizeirechts- und generell die Sicherheitsgesetzgebung seit Jahren auf einem Weg befindet, bei dem **rechtsstaatliche Sicherungen systematisch eingeebnet** werden. Wenn es nicht mehr darauf ankommt, ob jemand als Störer oder Verdächtiger eine objektive Ursache gesetzt hat, sondern Eingriffsmaßnahmen genauso gut gegen „andere Personen" zugelassen werden, kann letztlich jeder betroffen sein. Und wenn für Rechtseingriffe nicht mehr eine polizeirechtliche Gefahr vorliegen muss, sondern die Absicht der „Gefahrerforschung" ausreicht und im Rahmen der „vorbeugenden Bekämpfung von Straftaten" nicht einmal der Anfangsverdacht einer Straftat vorliegen muss, sondern dieselben Eingriffsinstrumente wie zur Straftatenaufklärung bereits unterhalb der Schwelle eines Anfangsverdachts eingesetzt werden dürfen, dann kann auch niemand mehr vorhersehen, in welchen Situationen er in Überwachungsmaßnahmen gerät. Die Einführung einer verdachtslosen Vorratsspeicherung im Internet würde die Überwachung noch weiter nach vorne verlagern. Absolut jeder wäre zunächst zu erfassen, die Unverdächtigen würden erst später ausgesondert.

Mit unserer Aktion „**Rote Karte für Internet-Schnüffler**" (vgl. Tz. 8.5) setzen wir uns dafür ein, dass auch im Internet das verfassungsrechtliche Verbot der Speicherung von Daten auf Vorrat zu unbestimmten Zwecken beachtet wird und Eingriffsmaßnahmen gegen die Nutzer des Internets nur beim Vorliegen des Anfangsverdachts einer strafbaren Handlung ergriffen werden dürfen. Mit unseren bescheidenen Mitteln haben wir im Berichtszeitraum untersucht, ob diejenigen, die mithilfe unseres AN.ON-Dienstes das Internet anonym nutzen, diese Freiheit missbrauchen. Nach unseren Feststellungen tut dies nur eine verschwindend klei-

ne Minderheit. Bei 1,2 Millionen Nutzungen im untersuchten Zeitraum konnten wir gerade einmal 17 Fälle feststellen, in denen möglicherweise der Anfangsverdacht einer Straftat vorlag (vgl. Tz. 9.2). Wenn eine derartig **niedrige Quote von Missbrauchsfällen** ausreichen würde, um daraufhin alle Nutzer vorsorglich zu überwachen, dann müssten z. B. alle Bundesautobahnen und Fernstraßen komplett per Video und mithilfe anderer elektronischer Hilfsmittel überwacht werden, denn die Dichte an Regelverstößen bis hin zum strafbaren Verhalten ist dort sicherlich ganz erheblich höher. Und niemand kann behaupten, Verkehrsverstöße seien harmlos. Tausende von Toten und Verletzten Jahr für Jahr auf den Straßen allein in Deutschland zeigen, dass die Nichtbeachtung von Verkehrsregeln schnell ganz schlimme Folgen haben kann.

Zurück zum **Internet**. Dass gerade dort die **Überwachungsfantasien** üppiger sind als in anderen gesellschaftlichen Bereichen, hat wahrscheinlich Gründe, die tiefer liegen. Das Internet verkörpert immer auch ein Stück Freiheit, insbesondere Gedanken- und Informationsfreiheit. Für manche scheint der Gedanke an Bürger, die sich über die Grenzen hinweg frei und unbeobachtet austauschen können, etwas Unheimliches, Bedrohliches zu haben. Was werden die Bürger ohne Kontrolle tun? Für Diktaturen ist diese Vorstellung offenbar besonders schwer zu ertragen. Sie behindern den Zugang ihrer Bürger zum Internet in unerträglicher Weise. China zum Beispiel hat die Nutzung unseres Anonymisierungsdienstes AN.ON unterbunden (vgl. Tz. 9.2). Zu Recht hat der Bundeskanzler vor kurzem in Peking ein freies Internet angemahnt. Wir sollten in Deutschland mit gutem Beispiel vorangehen.

3 Datenschutz im Landtag

3.1 Datenschutzgremium in Aktion

In Datenschutzfragen kontrolliert sich das Parlament selbst. Es hat zu diesem Zweck ein Datenschutzgremium gebildet. Die Vielzahl der behandelten Themen zeigt die Notwendigkeit einer solchen Einrichtung auf.

Im letzten Jahr konnten wir über die Bildung einer eigenständigen Datenschutzkontrollinstanz des Schleswig-Holsteinischen Landtags berichten. Inzwischen hat sich das Datenschutzgremium regelmäßig getroffen und einer Vielzahl aktueller Fragen gewidmet. So musste die Datenschutzordnung des Landtags an die Rechtslage nach Novellierung des LDSG angepasst werden. In einem Merkblatt wurden den Abgeordneten zusätzliche **Tipps und Hinweise** zum Umgang mit personenbezogenen Daten gegeben. Deren praktische Relevanz zeigten Einbrüche bei einem Landtagsabgeordneten, bei denen es offensichtlich darum ging, Notizen über die Arbeit eines Landtagsuntersuchungsausschusses zu entwenden.

In mehreren Sitzungen beschäftigte sich das Gremium auch mit der Sicherheit des **Telefonnetzes des Landtages** als Teil des Sprachnetzes des Landes. In einem Gutachten für das Datenschutzgremium legten wir die rechtlichen Rahmenbedingungen für die Weitergabe von Informationen aus Landtagsausschusssitzungen an Dritte, insbesondere an die Presse dar. Weitere Themen waren die Sicherheit der Postverteilung im Landtag und die datenschutzgerechte Ausgestaltung des Schließsystems des sich im Umbau befindlichen Landtagsgebäudes. Das Gremium achtete darauf, dass im Sicherheitskonzept des neuen Landtagsgebäudes der Datenschutz nicht zu kurz kommt.

Das ULD steht den Abgeordneten mit Rat und Tat in Datenschutzfragen zur Seite. Auf der **Webseite** des Landtages wurde eine besondere Rubrik zum Thema Datenschutz eingerichtet, in der die Tätigkeit des Datenschutzgremiums dokumentiert ist. Dort können das Merkblatt für Abgeordnete, das Gutachten über die Weitergabe von Informationen aus Landtagsausschüssen sowie sonstige Informationen zum Parlamentsdatenschutz abgerufen werden.

www.lvn.ParlaNet.de/parlament/datenschutz/

Was ist zu tun?
Die Tätigkeit des Datenschutzgremiums könnte Vorbild für die Realisierung des Datenschutzes auch in anderen Parlamenten sein.

3.2 Audits zum Petitionsverfahren und zum Internet-Angebot

Auf die Initiative des Datenschutzgremiums geht die Durchführung von zwei Datenschutzaudits in der Landtagsverwaltung zurück. Auditiert wurden die Durchführung von Petitionsverfahren und die anonyme Nutzung des über das ParlaNet bereitgestellten Internet-Informationsangebots.

Die Bürgerinnen und Bürger haben vielfältige Kontakte mit dem Landtag. Dabei handelt es sich durchgängig um sensible Informationsbeziehungen, egal ob politische Informationen eingeholt werden oder ob sich eine Person mit einem persönlichen Anliegen an ihre Volksvertretung wendet. Im Interesse der Stärkung des **Servicecharakters des Landtags** und zur Förderung des Bürgervertrauens in eine datenschutzgerechte Datenverarbeitung wollte der Landtag das neue Datenschutzinstrument „Audit“ nicht nur aktiv unterstützen, sondern war auch bereit, sich selbst beurteilen zu lassen. Bei der Durchführung der Audits arbeiteten die Leitungsebene des Landtags und die Abgeordneten ebenso aktiv mit wie die Landtagsbediensteten, die erkannten, dass ein Audit zur Qualitätsverbesserung der Datenverarbeitungsorganisation beiträgt. Die Ergebnisse beider Verfahren sind auf der Internet-Seite des ULD und der des Landtags veröffentlicht.

www.datenschutzzentrum.de/audit/register.htm
www.sh-landtag.de/parlament/datenschutz/index.html

Als Ergebnis der Auditierung des Internet-Informationsangebots im Rahmen des ParlaNet ist festzustellen, dass Bürgerinnen und Bürger getrost das Angebot des Landtags nutzen können. Sie müssen nicht befürchten, dass ihre Anfragen registriert oder sie als Anfragende identifiziert werden. Beim Surfen in diesem Informationsangebot wird also die **Anonymität der Anfragenden** gewährleistet. Mithilfe eines Datenschutzmanagementsystems wird auch sichergestellt, dass diese Gegebenheiten langfristig erhalten bleiben. Damit ist der Landtag als Anbieter im Internet eher eine große Ausnahme. Diesem Exempel sollten nicht nur Behörden, sondern auch private Anbieter folgen.

Die Sachverhaltsdarstellungen von Bürgerinnen und Bürgern im Rahmen von **Petitionsverfahren** lassen äußerst sensible Datenbestände entstehen. Daher ist in der Geheimschutzordnung und in der Datenschutzordnung des Landtags die besondere Vertraulichkeit der Petitionsdaten geregelt. Abgeordnete, die dem Eingabenausschuss nicht angehören, erhalten nur anonyme Informationen über das Petitionsverfahren. Der Abgleich ergab, dass bereits in der Vergangenheit ein recht hohes Vertraulichkeitsniveau bestanden hat. Durch Änderungen des Postlaufes, eine präzisere Information der Petenten, die Einführung von automatisierten Löschungsroutinen, die Verschlüsselung des Datenbestandes, weitere technische Sicherungsmaßnahmen und eine Festlegung der Datenschutzanforderungen in einer Dienstanweisung wurden während des Auditprozesses zusätzliche Verbesserungen erreicht. Es ist festzustellen, dass die vertrauliche Behandlung von Eingaben sichergestellt wird, sodass insoweit den Betroffenen durch die Wahrnehmung ihres verfassungsmäßigen Petitionsrechtes keine Nachteile entstehen.

Was ist zu tun?
Auch andere öffentliche Stellen sollten überlegen, ob die Durchführung eines Audits für sie interessant ist und ob sie den Datenschutz im Rahmen eines Auditverfahrens einmal von einer ganz anderen Seite kennen lernen wollen.

4 Datenschutz in der Verwaltung

4.1 Kommunalbereich

4.1.1 Vom Nutzen behördlicher Datenschutzbeauftragter

Die Bestellung behördlicher Datenschutzbeauftragter bei den Kommunen gewinnt zunehmend an Fahrt. Immer mehr Behörden nutzen die damit verbundenen organisatorischen Vorteile.

Durch die Bestellung eines Datenschutzbeauftragten entstehen den Behörden keine **Aufgaben**, die nicht ohnehin auf der Grundlage des allgemeinen und bereichsspezifischen Datenschutzrechts wahrzunehmen sind. Geändert wird durch die Bestellung nur die Art und Weise der Aufgabenerfüllung. Die Mitarbeiterinnen und Mitarbeiter in den Fachämtern müssen dann nicht mehr jeder für sich ihre Datenschutzprobleme lösen; sie können dafür auf eine entsprechend geschulte Fachkraft zurückgreifen. Die Aufgabe kann so in der Regel **schneller** und häufig auch **qualitativ besser** erledigt werden. Dem zeitlichen und personellen Aufwand für die Tätigkeit des Datenschutzbeauftragten steht also ein in der Regel sehr viel höherer Rationalisierungsfaktor in den Fachämtern gegenüber.

Schleswig-Holstein
DATENSCHUTZAKADEMIE

Kurse
DR, DT, R, T, DW, IFG

Weitere **Synergieeffekte** ergeben sich, wenn die Aufgabe des Datenschutzbeauftragten mit anderen Querschnittsaufgaben verknüpft wird (z. B. Aufgaben nach dem Informationsfreiheitsgesetz, Übertragung von Verwaltungscontrollingaufgaben). Gleiches gilt für die Bestellung gemeinsamer Datenschutzbeauftragter durch mehrere Behörden. Erfahrungen, die bei einer Kommune gesammelt werden, können mit reduziertem Aufwand auf andere Kommunen übertragen werden. Die notwendigen Fortbildungskosten fallen nur einmal an. Offensichtlich überzeugen diese Vorteile immer mehr Kommunen, denn die Zahl der kommunalen Datenschutzbeauftragten ist im vergangenen Jahr kontinuierlich gewachsen.

Auch wir sind bestrebt, zum Gelingen der Arbeit der Datenschutzbeauftragten beizutragen. Aus diesem Grund haben wir unsere Aktivitäten zur Unterstützung der Datenschutzbeauftragten deutlich ausgeweitet. Am häufigsten wurde die Möglichkeit genutzt, sich bei schwierigen Fragestellungen durch uns beraten zu lassen. Der „kleine Dienstweg“ hat sich in diesem Zusammenhang sehr bewährt. Daneben erfreut sich auch die neue **Mailinglist** für die Datenschutzbeauftragten großer Beliebtheit. Neben aktuellen Informationen werden darüber interessante datenschutzrechtliche Materialien verbreitet, die – vor Ort elektronisch abgelegt – jederzeit leicht erschließbare Antworten zu den unterschiedlichsten Fragestellungen geben können. Die Teilnehmer können die Mailinglist außerdem für den **Erfahrungsaustausch** und als **Diskussionsforum** nutzen. Weitere Interessenten werden gern in die Mailinglist aufgenommen.

Entsprechende Wünsche können an die Mailadresse
ld22@datenschutzzentrum.de gerichtet werden.

Was ist zu tun?
Behörden, die noch keinen Datenschutzbeauftragten bestellt haben, sollten sich über die damit verbundenen Vorteile informieren und anschließend von diesem Instrument Gebrauch machen. Wir sollten über die Bestellung unterrichtet werden, damit wir die Datenschutzbeauftragten betreuen können.

4.1.2 Hinweise zur Vorabkontrolle

Vor der Einführung von IT-Verfahren, mit denen besonders vertrauliche Daten verarbeitet werden, muss im Wege einer Vorabkontrolle geprüft werden, ob sie den Belangen des Datenschutzes genügen. Wenn ein Produkt bereits über ein Gütesiegel verfügt, kann dies die Vorabkontrolle abkürzen, aber nicht ganz ersetzen.

Das Instrument der Vorabkontrolle war aufgrund der EU-Datenschutzrichtlinie in das Landesdatenschutzgesetz (LDSG) aufzunehmen. Sie ist in zwei Fällen durchzuführen:

- Mehrere Daten verarbeitende Stellen führen gemeinsam die Verarbeitung durch, oder die Übermittlung personenbezogener Daten erfolgt durch ein Abrufverfahren, oder
- es wird ein Verfahren eingeführt, bei dem besondere Datenkategorien nach § 11 Abs. 3 LDSG verarbeitet werden. Dies sind z. B. Daten über die rassische oder ethnische Herkunft, die weltanschauliche oder religiöse Überzeugung, die Gesundheit und das Sexualleben sowie Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen.

Die Vorabkontrolle ist grundsätzlich von den behördlichen Datenschutzbeauftragten durchzuführen. Nur wenn ein solcher nicht bestellt ist, darf sie beim ULD beantragt werden. Wir haben deshalb **Hinweise zur Durchführung** von Vorabkontrollen erstellt und auf unserer Homepage veröffentlicht:

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

Kernstück ist eine **Checkliste**, nach der man vorgehen sollte, um die Vorabkontrolle einfach und effizient durchzuführen. Arbeitet man sie ab, so werden dadurch zugleich die gesetzlich geforderte Dokumentation nach § 7 Abs. 1 LDSG für das Verfahrensverzeichnis erstellt und die Anforderungen der Datenschutzverordnung berücksichtigt. Die wichtigsten Punkte sind:

- Grundangaben zum Verfahren wie Zweckbestimmung, Rechtsgrundlagen, Kreis der Betroffenen,
- Prüfung, ob die vorgesehene Datenverarbeitung von den Rechtsgrundlagen abgedeckt ist,
- Prüfung, ob die Rechte der Betroffenen gewahrt sind,
- Prüfung, ob eine Verfahrensdokumentation inklusive einer Verfahrensbeschreibung nach der Datenschutzverordnung vorliegt,

- Prüfung, ob ein Sicherheitskonzept gemäß Datenschutzverordnung vorliegt,
- Nachweis der Erprobung des Verfahrens durch einen Test,
- schriftliche Freigabe.

Auch für das **Haushalts-, Kassen- und Rechnungswesen** (HKR) ist eine Vorabkontrolle durchzuführen, wenn dort Steuer- und Sozialdaten verarbeitet werden. Damit sind Datenkategorien erfasst, die unter ein besonderes Berufs- oder Amtsgeheimnis fallen. Die Vorabkontrolle muss durchgeführt werden, bevor solche Verfahren zum Einsatz kommen. Nun bietet das Kommunale Forum für Informationstechnik (vgl. 22. TB, Tz. 12.5; 24. TB, Tz. 14.3) seit einiger Zeit ein Prüfzertifikat an, mit dem HKR-Verfahren nachweisen können, dass sie die fachlichen Vorgaben erfüllen. Zu den Eigenschaften, die nach einem Kriterienkatalog abgeprüft werden, gehören auch eine Reihe von datenschutzrechtlichen Anforderungen. Von verschiedenen Stellen wurde die Frage an uns herangetragen, ob nicht in den Fällen, in denen ein HKR-Verfahren eine solche Prüfung erfolgreich durchlaufen hat, auf die Vorabkontrolle verzichtet werden könne.

Dabei ist zu beachten, dass die datenschutzrechtliche Vorabkontrolle eine andere Ausrichtung hat als die Prüfung des IT-Produkts auf die Einhaltung der fachlichen Anforderungen. Während die Letztgenannte das Produkt sozusagen im Rohzustand begutachtet, beschäftigt sich die Vorabkontrolle mit dem konkreten Einsatz vor Ort. Daraus folgt, dass das Vorliegen eines **Zertifikats von KomFIT** zwar nachweist, dass das Produkt datenschutzrelevante Vorgaben umsetzen kann. Es ist allerdings nicht gesagt, dass die Einstellungen vor Ort auch tatsächlich vorgenommen worden sind. Aus diesem Grund kann die Vorabkontrolle auch bei Vorliegen eines Prüfsiegels nicht entfallen. Allerdings kann sie deutlich abgekürzt werden, wenn im Rahmen des Prüfverfahrens bereits wichtige datenschutzrechtliche Fragestellungen geklärt wurden. Hierzu muss anhand der Prüfkriterien, die KomFIT zugrunde legt, nachvollzogen werden, welche Eigenschaften des Produktes bereits positiv festgestellt wurden. Zusätzlich ist vor Ort die konkrete Implementierung zu überprüfen.

Was ist zu tun?
Öffentliche Stellen müssen bei bestimmten Verfahren zwingend eine Vorabkontrolle durchführen. Der Einsatz von Produkten, die ein Gütesiegel besitzen oder auf andere Art und Weise bezüglich der Einhaltung von fachlichen Anforderungen zertifiziert wurden, kann dies erleichtern.

4.1.3 Meldedaten an politische Parteien

Politische Parteien wenden sich vor Wahlen regelmäßig an die Meldeämter und ersuchen für Zwecke der Wahlwerbung um die Übermittlung von Wähleradressen. Obwohl die Bürgerinnen und Bürger ein Recht zum Widerspruch gegen die Weitergabe ihrer Daten an politische Parteien haben, kommt es nach den Werbeaktionen der Parteien immer wieder zu Beschwerden, weil die Bürger oftmals keine Kenntnis von ihrem Widerspruchsrecht gegen diese Datenübermittlungen haben.

Das Melderecht erlaubt die Übermittlung einiger weniger Daten (Vor- und Familienname, Doktorgrad, Anschriften) an Parteien, Wählergruppen und Wahlbewerber im Zeitraum von sechs Monaten vor der Wahl. Auch vor der jüngsten **Bundestagswahl** im September 2002 richteten politische Parteien entsprechende Anfragen an die Meldeämter.

In einem Fall ging es um die Anfrage einer Partei, die um Übermittlung der Daten von drei Gruppen von Personen ersuchte. Es handelte sich hierbei um die 18- bis 25-Jährigen, 26- bis 55-Jährigen sowie um Personen, die älter als 55 Jahre waren. Die einzelnen Personengruppen sollten jeweils mit bestimmten Punkten der parteilichen Programmatik besonders bekannt gemacht werden. De facto erstrebte die Partei damit die Übermittlung der **Daten sämtlicher Personen** im wahlberechtigten Alter. Es ist umstritten, ob eine derartig umfassende Auskunft noch vom Meldegesetz abgedeckt ist. Zwar scheint der Wortlaut der Vorschrift eine solche Art der Auskunftserteilung zu erlauben. Unzulässig wäre lediglich die pauschale Übermittlung der Daten aller Wahlberechtigten ohne Bildung von Gruppen. Aus der Gesetzesbegründung zum Landesmeldegesetz lässt sich jedoch schließen, dass nur die Übermittlung von Daten über Angehörige bestimmter (und nicht aller) Altersgruppen zulässig sein soll.

Das Landesmeldegesetz begründet allerdings **keinen absoluten Anspruch** der Parteien auf Übermittlung der Daten. Vielmehr obliegt die Entscheidung dem pflichtgemäßen Ermessen der Meldebehörden. Dies gilt auch, wenn von einer Partei nur die Auskunft über eine altersmäßig begrenzte Gruppe von Wahlberechtigten gefordert wird. Mehrere Oberverwaltungsgerichte haben entschieden, dass das Ermessen korrekt ausgeübt wird, wenn die Übermittlung der Daten mit dem Hinweis darauf verweigert wird, dass dem informationellen Selbstbestimmungsrecht ein hoher Rang zukomme und bei Übermittlung mit Protesten der Bürger zu rechnen sei. Zu beachten ist, dass die getroffene Ermessensentscheidung die Meldebehörde auch bei künftigen Anfragen anderer Parteien bindet, sodass sie in vergleichbaren Fällen in gleicher Weise zu entscheiden hat.

Was ist zu tun?
Die Meldebehörden haben ihrer im Landesmeldegesetz festgelegten Pflicht nachzukommen, die Meldepflichtigen bei der Anmeldung und bei jeder Ausstellung eines Personalausweises oder Reisepasses auf die Widerspruchsmöglichkeit hinzuweisen.

4.1.4 Wie detailliert dürfen Rechnungsprüfungsberichte sein?

Im Rahmen der kommunalen Rechnungsprüfung dürfen auch personenbezogene Daten verarbeitet werden. Werden Prüfberichte erstellt, so sollte mithilfe von Pseudonymisierungen der Grundsatz der Datensparsamkeit beachtet werden.

In mehreren Fällen nahmen Kommunalverwaltungen daran Anstoß, dass die Rechnungsprüfungsämter in **detaillierten Prüfberichten** Einzelangaben über bestimmte Beschäftigte gemacht hatten. Dazu gehörten Informationen über den Familienstand, die Vergütungsgruppe sowie über Krankheits- und Fehlzeiten.

Es fehlt an einer speziellen Befugnisnorm für die Datenverarbeitung zum Zwecke der Rechnungsprüfung. Daher ist auf die allgemeinen Zulässigkeitsvorschriften des Landesdatenschutzgesetzes zurückzugreifen. Danach ist die Datenverarbeitung dann zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Rechtsvorschrift zugewiesenen Aufgaben der Daten verarbeitenden Stelle erforderlich ist. Die Verwendung von Daten für Zwecke der Rechnungsprüfung ist ausdrücklich zugelassen. Nach den Vorschriften der Gemeindeordnung ist das Rechnungsprüfungsamt der **Gemeindevertretung** gegenüber unmittelbar verantwortlich. Daraus ergibt sich, dass die Prüfberichte an sie weitergegeben werden müssen. Allerdings ist zu beachten, dass die Gemeindevertreter ihrerseits nach den Vorschriften der Gemeindeordnung zur Verschwiegenheit über die personenbezogenen Daten aus den Berichten verpflichtet sind.

Werden **Berichte** (das gilt auch für Entwürfe) an die geprüfte Stelle gegeben, ist zu beachten, dass die Daten nicht über den Personenkreis hinaus bekannt werden, der ohnehin Zugriff auf die jeweils dargestellten Informationen hat. Es muss in jedem Fall ausgeschlossen werden, dass durch die Zirkulation der Berichte unbefugte Personen Kenntnis von Personaldaten erhalten. Die Rechnungsprüfungsämter sollten auf diesen Umstand hinweisen, wenn sie die Berichte an die geprüfte Stelle weitergeben.

Viele Kommunen möchten **Prüfberichte veröffentlichen**, um den sinnvollen Umgang mit Steuergeldern nachzuweisen. Dabei ist zu beachten, dass die vollständigen Prüfberichte inklusive der personenbezogenen Daten selbstverständlich nicht publik gemacht werden dürfen. Möglich ist die Verfahrensweise, dass der Prüfbericht in zwei Teile gegliedert wird. Der erste und ausführliche Teil bleibt unter Verschluss; der zweite, der eine abstrakte Zusammenfassung der Ergebnisse enthält, wird veröffentlicht. Diese Verfahrensweise wurde bereits im Jahre 1991 in einem Runderlass des Innenministeriums empfohlen.

Eine andere Alternative besteht darin, für die einzelnen Personen **Pseudonyme** im Sinne einer Referenz zu vergeben. Der Vorteil liegt darin, dass bei dieser Verfahrensweise in den Prüfberichten zunächst keine oder nur wenige personenbezogene Daten enthalten sind. Mithilfe der **Referenzliste** lässt sich die Identität feststellen, falls Unstimmigkeiten zwischen der geprüften Stelle und dem Rechnungsprüfungsamt geklärt werden müssen.

Was ist zu tun?
Sämtliche Stellen, die Berichte und Berichtsentwürfe der Rechnungsprüfungsämter erhalten, müssen sorgfältig prüfen, an wen sie welche Berichtsteile weitergeben. Die Rechnungsprüfungsämter sollten, wo immer dies möglich ist, durch Pseudonymisierung die Gefahren für die Datenschutzrechte der Betroffenen verringern.

4.1.5 Beauftragung eines Inkassodienstes

Die Einziehung privatrechtlicher Forderungen der Kommunen kann jetzt auch privaten Inkassobüros übertragen werden. Dabei sind die gleichen Maßgaben zu beachten, die auch für die Auftragsdatenverarbeitung gelten.

Von mehreren Städten und Gemeinden ist die Frage an uns herangetragen worden, ob gegen die Beauftragung eines Inkassounternehmens mit der Einziehung offener Forderungen von Kommunen datenschutzrechtliche Bedenken bestehen. Dabei handelte es sich ausschließlich um **privatrechtliche Forderungen**, die weder dem kommunalen Abgabengesetz noch der Abgabenordnung unterlagen.

Nach der Neufassung des LDSG ist die Übermittlung personenbezogener Daten zur Durchführung von beratenden oder begutachtenden **Tätigkeiten im Auftrag** der Daten verarbeitenden Stelle zulässig, wenn die übermittelnde Stelle die beauftragten Personen verpflichtet, die Daten nur für den Zweck zu verarbeiten, zu dem sie ihnen überlassen worden sind, und nach Erledigung des Auftrages die ihnen von der Daten verarbeitenden Stelle überlassenen Datenträger zurückzugeben und die bei ihnen gespeicherten Daten zu löschen, soweit nicht besondere Rechtsvorschriften entgegenstehen. Im Übrigen wird auf die Maßgaben der Auftragsdatenverarbeitung verwiesen.

Der im Gesetz genannte Begriff der **beratenden Tätigkeiten** ist in diesem Zusammenhang nicht zu eng auszulegen. Er umfasst nicht nur Tätigkeiten im Innenverhältnis zwischen Auftraggeber und beratender Stelle, sondern erlaubt auch nach außen wirkende, die Aufgabenerfüllung des Auftraggebers unterstützende Tätigkeiten im Namen des Auftraggebers. Im Hinblick auf den Schutzzweck der Norm würde es keinen Sinn machen, etwa nur eine Beratung der Kommune durch einen Rechtsanwalt oder einen Inkassodienst im Innenverhältnis zuzulassen und anschließend eine Prozessvertretung bzw. die Durchführung von Vollstreckungsmaßnahmen zu verbieten. Im Übrigen ist auch eine gutachterliche Tätigkeit häufig mit unmittelbarer Außenwirkung verbunden, soweit die Begutachtung die Ermittlung des jeweiligen Sachverhaltes einschließt.

Bei der Beauftragung des Inkassodienstes ist allerdings dafür Sorge zu tragen, dass die im LDSG genannten Maßgaben zur Auftragsdatenverarbeitung beachtet werden. Dies bedeutet, dass je nach Fallgestaltung weitere Auflagen notwendig sind. Die beauftragte Stelle muss bei der Abwicklung deutlich machen, dass sie im Auftrag der Behörde tätig ist.

Was ist zu tun?
Wenn Kommunen sich bei der Vollstreckung privatrechtlicher Forderungen eines Inkassodienstes bedienen, müssen sie dafür Sorge tragen, dass dabei die datenschutzrechtlichen Standards für Auftragsdatenverarbeitung eingehalten werden.

4.1.6 Wichtige Änderungen des Melderechts in Vorbereitung

Mit der Änderung des Melderechtsrahmengesetzes kündigen sich weitere wichtige Neuerungen im Melderecht des Landes an. Datenschutzrechtliche Verbesserungen drohen dabei auf der Strecke zu bleiben.

Mit der nunmehr dritten umfassenden Änderung des Melderechtsrahmengesetzes (MRRG) hat der Bundesgesetzgeber die Absicht verbunden, die erforderlichen Rahmenbedingungen für die Nutzung moderner **Informations- und Kommunikationstechnologien** zu schaffen. Tatsächlich gehen die Änderungen weit darüber hinaus. Als wichtigste Neuerungen sind zu nennen:

- die Speicherung der Seriennummer des Personalausweises und des Passes im Melderegister,
- der Wegfall der Abmeldepflicht,
- die Befugnis zum automatisierten Datenaustausch mit anderen Behörden,
- die automatisierte Erteilung einfacher Melderegisterauskünfte über das Internet,
- die Aufhebung der Auskunftssperre für Melderegisterauskünfte, wenn im Einzelfall eine entsprechende Gefährdung nachträglich ausgeschlossen werden kann.

Insbesondere die **Novellierung der Auskunftssperre** halten wir aus datenschutzrechtlicher Sicht für bedenklich. Werden Daten an private Stellen übermittelt, ist eine vertrauliche Behandlung dort nicht mehr zu gewährleisten. Es kann nicht ausgeschlossen werden, dass Personen, von denen eine Gefahr für den Meldepflichtigen ausgeht, sich die neuen Möglichkeiten zunutze machen, um an die aktuelle Anschrift des Meldepflichtigen zu kommen. Da bei einer Rechtsgüterabwägung dem Schutz von Leib und Leben der betroffenen Personen der absolute Vorrang eingeräumt werden muss, kann in diesem Sinne eine entsprechende Gefahr nur dann ausgeschlossen werden, wenn eine Datenübermittlung an private Stellen generell untersagt wird. Aus diesem Grund hätten wir es sehr begrüßt, wenn es bei der bisherigen Regelung geblieben wäre.

Was ist zu tun?
Der Landesgesetzgeber sollte zumindest durch eine Ergänzung der rahmenrechtlichen Regelung im Landesmeldegesetz dafür Sorge tragen, dass ein effektiver Schutz für gefährdete Personen geschaffen wird.

4.2 Polizeibereich

4.2.1 Überblick

Seit den Terroranschlägen des 11. September 2001 läuft auch in Schleswig-Holstein die **Rasterfahndung** nach so genannten „Schläfern". Dass die beteiligten Landesbehörden um eine datenschutzgerechte Durchführung der Rasterfahndung bemüht sind, hat eine im Sommer dieses Jahres durchgeführte Querschnittsprüfung ergeben. Rechtlich umstritten bleibt hingegen die Rolle des Bundeskriminalamtes (Tz. 4.2.4). Um eine datenschutzrechtlich korrekte Vorgehensweise waren die Polizeibehörden auch bei dem ersten so genannten **DNA-Massentest** bemüht, der aus Anlass des ungeklärten Mordes an einem Ehepaar durchgeführt worden war (Tz. 4.2.3). Erinnert werden muss an eine Forderung aus unserem 24. Tätigkeitsbericht: Die für das Jahr 2003 ins Haus stehende **Neukonzeptionierung der polizeilichen Datenverarbeitung** (COMPAS-Nachfolger) bedarf von Anfang an einer datenschutzrechtlichen Begleitung. Wie teuer hier Versäumnisse werden können, hat sich jüngst an der erforderlich gewordenen aufwändigen Nachrüstung des Lübecker Einsatzleitstellensystems gezeigt (Tz. 4.2.5).

4.2.2 Prüfung der Verarbeitung von DNA-Daten

Eine Querschnittskontrolle der Verarbeitung von DNA-Daten ergab im Landeskriminalamt keinen Grund zu Beanstandungen. Die Dokumentation der zugrunde liegenden Prognosenentscheidung muss allerdings verbessert werden.

In einer Querschnittsprüfung wurde bei Dienststellen der Landespolizei und der Staatsanwaltschaft Kiel die Erhebung, Untersuchung und Speicherung des **DNA-Identifizierungsmusters** von Personen für Zwecke eines laufenden Strafverfahrens oder künftiger Strafverfahren stichprobenhaft überprüft. Von Bedeutung war dabei insbesondere die Umsetzung der datenschutzrechtlichen Vorgaben der 1998 eingefügten Regelungen des § 81 g StPO und des DNA-Identifizierungsgesetzes (DNA-IFG) sowie der Gemeinsamen Richtlinien des Generalstaatsanwaltes und des Landeskriminalamtes.

Wir haben nämlich Zweifel, ob die in Schleswig-Holstein für so genannte Altfälle mit den Gemeinsamen Richtlinien

Im Wortlaut: § 81 g Abs. 1, 3 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) ...

(3) § 81 a Abs. 2 (Richtervorbehalt) und § 81 f (Richterliche Anordnung) gelten entsprechend.

in Kraft gesetzte „Freiwilligkeits“- bzw. „Einwilligungslösung“ mit der StPO und dem DNA-IFG vereinbar ist, da sie den vom Gesetzgeber festgelegten **Richtervorbehalt** nicht umsetzt (vgl. 23. TB, Tz. 4.3.2). Das Bundesverfassungsgericht hat in mehreren Beschlüssen in den vergangenen zwei Jahren die verfassungsrechtlichen Anforderungen an die Erhebung und Verarbeitung des „genetischen Fingerabdrucks“ präzisiert. Danach kommt den Gerichten eine sehr weitgehende Pflicht zur Prüfung sämtlicher für das Bestehen einer Wiederholungsgefahr aussagefähiger Unterlagen und Informationen zu. Die Entscheidungen müssen sich mit allen für oder gegen eine „Negativprognose“ sprechenden Umständen auseinander setzen und in der Begründung zu ihnen Stellung beziehen. Diese materiellrechtlichen Anforderungen können nicht durch die Einwilligung des Betroffenen ersetzt werden, da dieser nicht für sich selbst über das Vorliegen der erforderlichen Schwere der Anlasstat und der Wiederholungsgefahr (Negativprognose) entscheiden kann. Diese Prüf- und Begründungspflichten treffen die Polizei und die Staatsanwaltschaft.

Zunächst wurde beim **Landeskriminalamt** (LKA) die kriminaltechnische Untersuchung der DNA sowie die DNA-Sachbearbeitung der „Altfälle“ und sonstigen Fälle geprüft. In einem zweiten Schritt wurden anhand einer Stichprobe aus der DNA-Datei Kriminalakten zu den Betroffenen bei sieben Kriminalakten haltenden Dienststellen der Polizei gesichtet. Zuletzt wurden bei der **Staatsanwaltschaft** bei dem Landgericht Kiel die DNA-Vorgänge zu Personen aus der Stichprobe geprüft.

Hinsichtlich der **kriminaltechnischen Untersuchung** der DNA ergaben sich keinerlei Beanstandungen. Zum Zeitpunkt der Prüfung waren in der DNA-Analyse-Datei aufgrund bundesweiter Eingaben insgesamt 139.722 Datensätze gespeichert, davon 1901 aus Schleswig-Holstein. Auf bekannte Personen entfielen 125.166 Datensätze, davon 1616 aus Schleswig-Holstein. Die übrigen insgesamt 14.536 Datensätze, davon 285 aus Schleswig-Holstein, betrafen Spuren. Eine Eingabe von Datensätzen in die DNA-Analyse-Datei erfolgt in Schleswig-Holstein seit etwa Februar 1999. Eine Recherche in der DNA-Analyse-Datei wird lediglich mit **Allelwerten** und nicht mit anderen gespeicherten Daten durchgeführt.

> **?** ***Allelwert***
>
> *In der forensischen Spurenanalytik wird mit der PCR-Technik die gezielte Vervielfältigung definierter DNA-Abschnitte aus dem nicht codierenden Bereich vorgenommen. Die als Genorte bezeichneten Abschnitte der DNA weisen bei jeder Person zwei Allele auf, die durch einen Fragmentlängenpolymorphismus charakterisiert sind. Die Länge des jeweiligen Allels wird chromatographisch bestimmt und als Zahlenwert angegeben.*

Zur Realisierung einer einheitlichen Verfahrensweise hat das LKA geregelt, welche Teile eines abgeschlossenen DNA-Vorganges in die Kriminalakte aufzunehmen sind. Die Praxis entsprach bei den geprüften Stellen jedoch nicht immer dieser Regelung. Die Tatsache einer **unzureichenden Dokumentation** von Einträgen in die DNA-Datei in der Kriminalakte der Betroffenen ist datenschutzrechtlich wie folgt zu bewerten:

Bei der Eingabestelle im LKA werden keine Unterlagen geführt, die Aufschluss über die materiell-rechtliche Begründung für die Speicherung einer Person in der DNA-Datei und über das gewählte Verfahren geben. Diese Informationen verbleiben vielmehr bei den sachbearbeitenden Dienststellen. Um die Rechtmäßigkeit der Dateispeicherung nachvollziehen zu können, müssen die Polizeidirektionen als Daten verarbeitende Stellen Unterlagen führen, die belegen, dass die Voraussetzungen der Aufnahme in die Datei in materieller sowie in formeller Hinsicht vorliegen. Die bloße Möglichkeit, erforderlichenfalls die **Originalunterlagen** zur **Negativprognose** und zur Einwilligung, staatsanwaltschaftlichen Prognosebestätigung bzw. zur richterlichen Anordnung von der Staatsanwaltschaft anzufordern, reicht nicht aus, weil die Polizei auf die Aufbewahrung der Unterlagen der Staatsanwaltschaft keinen Einfluss hat. Die DNA-Akten werden dort als „AR-Vorgänge“ geführt und nach den Aufbewahrungsbestimmungen für die Staatsanwaltschaften fünf Jahre aufbewahrt. Für Speicherungen in der DNA-Datei vergibt die Polizei jedoch regelmäßig eine Frist von zunächst 10 Jahren, sodass die staatsanwaltschaftlichen Unterlagen bereits nach der Hälfte dieser Prüffrist als Aktenrückhalt nicht mehr zur Verfügung stehen. Hinzu kommt, dass bei der Entscheidung über eine Verlängerung der Speicherung in der DNA-Datei über die erste Prüffrist hinaus auch die ursprünglich erstellte polizeiliche Negativprognose eine Rolle spielt. Auch aus diesem Grunde muss sie in der Kriminalakte verfügbar sein. Die Prognose muss vollständig aus sich heraus verständlich sein.

Nach den vorgenannten Richtlinien des Generalstaatsanwaltes und des LKA hat die Staatsanwaltschaft die Einwilligungserklärung sowie auch anhand eigener Erkenntnisse die Begründetheit der polizeilichen Negativprognose zu prüfen und das Ergebnis ihrer Prüfung im positiven wie im negativen Fall der Polizeidienststelle schriftlich mitzuteilen. Hierdurch soll nach der Auffassung des Justizministeriums bei Altfällen mit Einwilligung des Betroffenen „die abschließende Prüfung, ob die Voraussetzungen einer molekulargenetischen Untersuchung vorliegen, in die Hand der Staatsanwaltschaft gelegt und damit durchgängig eine **justizielle Kontrolle** gewährleistet und die Position des Betroffenen gestärkt werden.

Ausführungen der Staatsanwaltschaft zur Wirksamkeit der Einwilligungserklärung fanden sich in lediglich einem der überprüften DNA-Vorgänge. Aus Sicht der Staatsanwaltschaft sind in der Praxis Zweifel an der Einwilligungsfähigkeit oder der Wirksamkeit der konkret abgegebenen Einwilligung kaum denkbar. Auch hinsichtlich der Annahme einer **Wiederholungsgefahr** (Negativprognose) konnte in den überprüften Akten zumeist lediglich das Ergebnis der staatsanwaltschaftlichen Überprüfung in Form eines Kurzvermerks (z. B. „Prognose bestätigt“) oder des Ankreuzens innerhalb eines Bearbeitungsformulars festgestellt werden. Begründungen für die staatsanwaltschaftliche Bestätigung waren durchweg nicht dokumentiert.

Wenn sich der polizeiliche Vermerk über das Bestehen einer **Negativprognose** mit den vom BVerfG angeführten Aspekten hinreichend auseinander setzt, kann sich die staatsanwaltschaftliche Bestätigung auf einen Verweis hierauf beschränken. Im Übrigen muss nach unserer Auffassung die inhaltliche Prüfung der entsprechenden Unterlagen aus der schriftlichen Entscheidung der Staatsanwaltschaft erkennbar sein. Diese ist der Polizeidienststelle zu übersenden und dort in der Kriminalakte des Betroffenen abzulegen. Gleiches gilt für die Prüfung der Wirk-

samkeit der Einwilligung, wenn sich aus dem konkreten Verfahrensablauf oder aus Umständen in der Person des Betroffenen Zweifel ergeben haben.

Die Generalstaatsanwaltschaft hat unsere datenschutzrechtlichen Bedenken aufgegriffen. Nach ihrer Auffassung obliegt die Darstellung der Voraussetzungen der Negativprognose der Polizei. In einem **Rundschreiben** wurde den **Staatsanwaltschaften** ein einheitlicher Verfahrensablauf vorgegeben. Danach prüft die jeweilige Staatsanwaltschaft, ob die Vermerke der Polizei zur Negativprognose und zur wirksamen Einwilligung ausreichend sind und die Entscheidung der Polizei rechtfertigen. Tritt sie nach eigener Prüfung dem Ergebnis bei, werden die Akten mit einem Zustimmungsvermerk an die Polizei zurückgesandt. Ist die Begründung der Polizei nicht ausreichend, sendet sie die Akten mit einem Hinweis auf die unzureichende Begründung zurück. Nur in Ausnahmefällen – z. B. bei Eilbedürftigkeit – kann die Staatsanwaltschaft ergänzende eigene Erwägungen anstellen.

Was ist zu tun?
Die Gründe für die Speicherung von Daten in der DNA-Analyse-Datei sind zu dokumentieren. Dies gilt auch für die staatsanwaltschaftliche Prüfung.

4.2.3 Erster DNA-Massentest in Schleswig-Holstein

Im Jahr 2002 fand in Schleswig-Holstein der erste DNA-Massentest statt. Obwohl das Vorgehen der Polizeibehörden in diesem Einzelfall nicht zu beanstanden war, müssen derartige Massentests die Ultima Ratio der strafprozessualen Ermittlungen bleiben.

Im Mai 2000 wurde in einem Hochhausblock einer schleswig-holsteinischen Kleinstadt ein älteres Ehepaar getötet. Ein Tatverdächtiger konnte trotz intensiver Ermittlungen nicht gefunden werden. Auch eine DNA-Täterspur war zunächst nicht zu isolieren. Erst Ende 2001 gelang es, an einem von dem Täter benutzten Tuch DNA einer männlichen Person festzustellen und nach acht Merkmalen aufzuschlüsseln. Von der Polizei und der Staatsanwaltschaft wurde entschieden, eine **DNA-Reihenuntersuchung** durchzuführen. Insgesamt wurden knapp 900 Personen zum Zwecke der Speichelprobenentnahme erfasst und durch eine Priorisierung den Gruppen A, B und C je nach „Tatnähe“ zugeordnet. Die Beschaffung der Speichelproben erfolgte dezentral über 123 polizeiliche Dienststellen, deren Mitarbeiter die Betroffenen ohne vorherige Benachrichtigung persönlich aufsuchten. Der Zweck der Reihenuntersuchung wurde erläutert. Nach Unterzeichnung eines Einwilligungsformulares wurde die Speichelprobe abgenommen und über die ermittelnde Dienststelle an das Landeskriminalamt übersandt. Nach Ermittlung des Täters, der der Gruppe A zugehörte, durch Abgleich mit der Tatortspur wurde die molekulargenetische Untersuchung der

? *DNA*

Die DNA (Desoxyribonukleinsäure) ist ein Molekül in jeder Körperzelle, das den gesamten genetischen Bauplan des Menschen enthält. Der so genannte 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.

übrigen Speichelproben eingestellt. Die Speichelproben sollen bis zur rechtskräftigen Verurteilung der Trefferperson bei der ermittelnden Dienststelle aufbewahrt werden.

Im vorliegenden Fall stellte sich die DNA-Reihenuntersuchung als **Ultima Ratio** der polizeilichen Ermittlungen dar, nachdem eineinhalb Jahre lang sämtliche Ermittlungsansätze ergebnislos ausgeschöpft worden waren. Es handelte sich um ein schweres, nicht anders aufklärbares Verbrechen, dessen Täter potenziell auch für weitere Personen gefährlich blieb, und es gab eine „Fahndungshypothese", die zumindest einen Ansatz für eine räumlich-sachliche Eingrenzung des Kreises der Probanden bot. Unabhängig von der Frage, unter welchen Voraussetzungen DNA-Reihenuntersuchungen ohne ausdrückliche gesetzliche Grundlage überhaupt zulässig sind, war das Vorgehen der Polizei in diesem Fall nicht zu beanstanden. Gleichwohl müssen gerade angesichts der Tatsache, dass Grundlagen für DNA-Reihenuntersuchungen derzeit in der StPO nicht vorhanden sind, **rechtsstaatliche Mindestanforderungen** definiert werden. Es wäre rechtsstaatlich bedenklich, wenn unabhängig von der Schwere der aufzuklärenden Tat und den sonstigen „herkömmlichen" Ermittlungsmöglichkeiten immer häufiger vom Instrument des Massengentests Gebrauch gemacht würde. Die Aufforderung an unverdächtige Personen, sich selbst zu entlasten, darf sich nicht zu einem Standardfall der Strafermittlungen abschleifen.

Das Positionspapier des ULD zur Durchführung molekulargenetischer Reihenuntersuchungen findet sich auf der Homepage des ULD:

www.datenschutzzentrum.de/material/themen/polizei/dna-reihe.htm

Was ist zu tun?
Die Politik sollte darüber entscheiden, ob sie DNA-Reihenuntersuchungen gesetzlich zulassen will.

4.2.4 Rasterfahndung

Die schleswig-holsteinische Polizei hat sich nach den Terroranschlägen des 11. September 2001 an der bundesweit koordinierten Rasterfahndung beteiligt. Ungeklärt ist nach wie vor die Rolle des Bundeskriminalamtes, weil es für präventive Rasterfahndungen nicht zuständig ist.

Nach den Terroranschlägen des 11. September 2001 schuf der Schleswig-holsteinische Landtag im Oktober 2001 eine Rechtsgrundlage für präventiv-polizeiliche Rasterfahndungsmaßnahmen (vgl. 24. TB, Tz. 4.2.2). Ziel der bundesweiten Rasterfahndung war und ist es, insbesondere anhand von Eigenschaften, die auf die Attentäter des 11. September 2001 zutrafen, bundesweit eine Personengruppe aus verschiedenen Datenbeständen herauszufiltern, bei der weitere polizeiliche Ermittlungen zur Abklärung von „**Schläfern**" im Netzwerk der Al-Kaida ansetzen sollen.

> ***Im Wortlaut: § 179 Abs. 2 a LVwG***
>
> *Wenn Tatsachen dafür sprechen, dass ein Verbrechen begangen werden soll, können personenbezogene Daten erhoben werden über Personen, bei denen Tatsachen dafür sprechen, dass sie solche Straftaten begehen oder sich hieran beteiligen werden.*

Das LKA hat die Rasterfahndung bislang im Großen und Ganzen rechtlich korrekt durchgeführt. Insbesondere die Datenerhebungen im Rahmen der Einzelfallermittlungen erfolgten in einem Umfang, der den Verhältnismäßigkeitsgrundsatz wahrte. An einer für die Gesamtbewertung der Rasterfahndung entscheidenden Weichenstellung war die Vorgehensweise der Landespolizei jedoch problematisch: Die **Anschlussermittlungen** sind zu einem wesentlich breiteren Personenkreis als zulässig durchgeführt worden. Bei den Personen, für die sich keine Treffer aus den Abgleichen beim BKA mit der Verbunddatei „Schläfer“ ergeben haben, hätten Anschlussermittlungen nicht durchgeführt werden dürfen, da die Voraussetzungen des hier mangels Vorliegens einer spezifischen Regelung allein in Betracht kommende § 179 Abs. 2 a LVwG nicht erfüllt waren. Denn die Tatsache, dass jemand ein bestimmtes Lebensalter hat, aus einem bestimmten Land kommt und islamischen Glaubens ist, spricht noch nicht dafür, dass er auch schwere Straftaten begehen möchte. Falls der Gesetzgeber sich im Rahmen der Evaluierung des Gesetzes zur Einführung des automatisierten Datenabgleichs (das Ende 2005 außer Kraft tritt) für eine Beibehaltung des Instruments der Rasterfahndung im Polizeirecht entscheiden sollte, muss die Frage geregelt werden, in welchen Trefferfällen nach einer Rasterfahndung konventionelle Ausschlussermittlungen durchgeführt werden dürfen.

Zum anderen ist der automatisierte Abgleich schleswig-holsteinischer Daten beim **BKA** mit den dort vorgehaltenen Abgleichsdateien nach unserer Auffassung der **Kern** der eigentlichen **Rasterfahndung** und nicht als reine „Informationsanreicherung“ anzusehen. Hierfür hat das BKA keine Befugnisgrundlage, und seine Vorgehensweise ist im Ergebnis auch nicht von den richterlichen Beschlüssen des Amtsgerichts Kiel gedeckt. Denn diese umfassen nur einen Abgleich mit bereits vorhandenen polizeiinternen Daten („Informationssystem des BKA“), nicht aber die Beschaffung von Informationen über Dateien aus polizeiexternen Quellen. Die Verarbeitung der schleswig-holsteinischen Daten beim BKA im Rahmen der Rasterfahndung kann nur **im Auftrag und nach Weisung Schleswig-Holsteins** geschehen, mit der Folge, dass die Abgleichs- und sonstigen Verarbeitungsvorgänge beim BKA den materiell- und formellrechtlichen Voraussetzungen des schleswig-holsteinischen Polizeirechts unterliegen.

Wie verdreht die Situation inzwischen ist, zeigt sich bei der **datenschutzrechtlichen Kontrolle** des Vorgehens des BKA: Während uns vom schleswig-holsteinischen Innenministerium mitgeteilt worden ist, dass die Daten auch nach Übermittlung an das BKA weiterhin der Sachherrschaft der schleswig-holsteinischen Polizei und unserer Kontrollbefugnis unterworfen bleiben, worüber Konsens zwischen dem BKA und den Ländern bestehe, will das BKA davon nichts wissen. Eine Kontrolle des Umgangs des BKA mit den schleswig-holsteinischen Daten durch uns wird vom BKA aus „grundsätzlichen Erwägungen der föderalen Kompetenzverteilung“ verweigert.

Was ist zu tun?
Das Innenministerium sollte erklären, wie die nach seiner Auffassung bestehende Sachherrschaft der schleswig-holsteinischen Polizei und unsere Kontrollbefugnisse beim BKA umgesetzt werden sollen.

4.2.5 Einsatzleitstellensystem Lübeck wird nachgebessert

Nach intensiven Erörterungen soll das Einsatzleitsystem der Polizeiinspektion Lübeck nachträglich technisch so umgerüstet werden, dass es den datenschutzrechtlichen Vorschriften entspricht. Einziges Hindernis für die Umsetzung der datenschutzgerechten Lösung ist die immer noch ausstehende Entscheidung hinsichtlich der Freigabe der erforderlichen finanziellen Mittel.

Da das neue System der Einsatzleitstelle der Polizeiinspektion Lübeck über **Speicher- und Recherchemöglichkeiten** verfügt, die in dieser Form deutlich über den datenschutzrechtlich zulässigen Rahmen hinausgehen, müssen die technischen Funktionalitäten an die rechtlichen Voraussetzungen angepasst werden (vgl. 24. TB, Tz. 4.2.4).

Die Polizeiinspektion Lübeck hat auf der Grundlage unserer Kritik Lösungen erarbeitet, nach denen nur Daten von **tatverdächtigen** oder **störenden Personen**, deren Taten die Anfertigung von Merkblättern für die Kriminalakte rechtfertigen, für den Zeitraum von sechs Monaten für Zwecke der Eigensicherung bei der Wahrnehmung von Einsätzen abrufbar vorgehalten werden. Darüber hinaus sollen bei **besonderen Deliktsgruppen**, welche unterhalb der Kriminalaktenrelevanz einzustufen sind, im Rahmen einer „Erinnerungsfunktion“ die Daten für die Dauer von vier Wochen auswertbar sein.

Durch die Implementierung entsprechender **technischer Tools** soll sichergestellt werden, dass lediglich die als erforderlich angesehenen und gesetzlich zugelassenen personenbezogenen Daten für die Dauer des zulässigen Zeitraumes recherchiert werden können. Eine systemseitige Protokollierung der Abfragen sowie des Abfragenden gewährleisten die nachträgliche Überprüfbarkeit im Rahmen von Kontrollen.

Was ist zu tun?
Die Umsetzung der zugesicherten technischen Korrekturen sollte umgehend erfolgen. In künftigen Fällen ist eine rechtzeitige Prüfung der Rechtsvorschriften im Rahmen der Vorabkontrolle nicht nur gesetzlich vorgeschrieben, sondern aus Effizienzgesichtspunkten dringend geboten.

4.2.6 Neues Vorgangsbearbeitungssystem bei der Landespolizei installiert (COMPAS-Nachfolger)

Zum Jahresende 2002 ist die Polizei mit 1500 vernetzten Computern ausgestattet worden, die auch den Zugriff auf das bundesweite Fahndungs- und Informationssystem INPOL-neu ermöglichen sollen. Eine Vorabkontrolle wurde bislang nicht durchgeführt.

Das polizeiliche Vorgangsbearbeitungssystem @RTUS eröffnet für die polizeiliche Arbeit völlig neue Möglichkeiten, z. B. die Nutzung der **Office-Anwendung** aus dem Landessystemkonzept. Daneben sollen E-Mail und Intranet zur Anwendung gelangen. Damit beinhaltet @RTUS im Zusammenhang mit seiner Einbettung in das Landessystemkonzept ein deutliches Mehr gegenüber dem COMPAS-Vorgangsbearbeitungssystem.

Unverständlich bleibt, warum die Inbetriebnahme der 1500 PC ohne rechtzeitige Erfüllung der rechtlichen Vorgaben so schnell erfolgen musste. **Versäumnisse**, die bei der Einführung der Vorgängersoftware (COMPAS) und von weiteren 1000 unvernetzten PC zutage getreten sind, sollten sich jetzt nicht wiederholen. Gerade in Bezug auf die Verzahnung mit dem Landessystemkonzept muss sich die Landespolizei fragen lassen, was technisch zwischen den einzelnen Systemen machbar und was im Einzelfall zur jeweiligen Aufgabenerfüllung erforderlich ist.

Was ist zu tun?
Die Landespolizei sollte unverzüglich die rechtlich vorgeschriebene Verfahrensdokumentation erstellen und zur Begutachtung vorlegen.

4.2.7 Auskunft der klinischen Ambulanz an die Polizei

Die Frage der Polizei, ob sich eine von ihr gesuchte Person zur ambulanten Behandlung im Klinikum aufhält, darf vom Klinikpersonal nicht beantwortet werden. Eine Zuwiderhandlung verstößt gegen die ärztliche Schweigepflicht.

Eine Bürgerin schilderte uns folgenden Vorfall: Sie sei anlässlich ihrer Vorstellung in der Ambulanz des Klinikums wegen einer nicht bezahlten Geldstrafe von der Polizei verhaftet worden. Ihr Aufenthalt sei der Polizei zuvor durch das Klinikpersonal mitgeteilt worden. Anschließend sei sie **erkennungsdienstlich behandelt** worden. Unsere Nachfragen bei der Polizei und dem Klinikum bestätigten den Sachverhalt: Tatsächlich war zwischen dem Klinikpersonal und der Polizei ein Telefonat geführt und der Polizei mitgeteilt worden, dass die Petentin sich im Krankenhausbereich aufhielt.

Wir haben die Klinikleitung davon in Kenntnis gesetzt, dass das Vorgehen des Klinikpersonals einen Verstoß gegen die **ärztliche Schweigepflicht** darstellt. Nach der Rechtsprechung erstreckt sich die Vertrauensbeziehung zwischen Arzt und Patient auch auf die Anbahnung eines Beratungs- und Behandlungsverhältnisses. Weder der Arzt noch seine Hilfspersonen dürfen die Identität und die Tat-

sache der Behandlung einer Person Dritten offenbaren. Dies gilt auch dann, wenn die Polizei nach der Person sucht. Auch wer einer Straftat verdächtig ist oder aus anderen Gründen von der Polizei gesucht wird, muss einen Arzt aufsuchen können, ohne dabei befürchten zu müssen, sich selbst der Strafverfolgung auszuliefern.

Dieser Grundsatz gilt nicht schrankenlos. Bei stationärer Aufnahme gibt das Melderecht der Polizei einen Auskunftsanspruch. Außerdem kann eine Mitteilung an die Polizei in Betracht kommen, wenn der Arzt konkrete Anhaltspunkte dafür hat, dass der Patient weitere schwere Straftaten begehen wird und keine anderen Möglichkeiten zur Gefahrenabwehr bestehen. Diese **Ausnahme** kam hier jedoch nicht zum Tragen. Die Beschäftigten der Ambulanz wurden von der Klinikleitung noch einmal ausdrücklich auf die bestehende Rechtslage hingewiesen.

4.3 Justizverwaltung

4.3.1 Daten über Strafgefangene

Die Verarbeitung von Daten über Strafgefangene war Gegenstand einer Querschnittskontrolle in der Justizvollzugsanstalt Neumünster. Einige der in früheren Prüfungen festgestellten Mängel sind inzwischen abgestellt. Gleichwohl enthält auch der neue Prüfbericht eine Reihe von Kritikpunkten.

Der Vollzugsalltag bringt es mit sich, dass über die Gefangenen detaillierte Informationen bis hin zum Intimbereich anfallen. Wer unter welchen Voraussetzungen Zugang zu diesen Unterlagen bekommt, ist nicht nur für die Gefangenen und ihre Angehörigen von größter Bedeutung. Daneben müssen die Interessen der Anstaltsbediensteten sowie der Allgemeinheit unter dem Aspekt des Opferschutzes und der Verhütung künftiger Straftaten berücksichtigt werden. In einigen Punkten hat sich die **Situation** seit der letzten Querschnittsprüfung in Schleswig-Holstein vor zehn Jahren deutlich **verbessert**:

- So ist positiv anzumerken, dass die undifferenzierte Weitergabe von Gefangenendaten unabhängig von der Erforderlichkeit im Einzelfall mittels einheitlich gestalteter „**A-Bögen**“ an alle Organisationsteile der JVA sowie an externe Behörden (z. B. Polizei, Staatsanwaltschaften sowie Jugend- bzw. Ausländerbehörden) nicht mehr praktiziert wird.
- Auch die frühere Praxis, auf den für viele zugänglichen **Stationstafeln** umfangreiche Informationen über Gefangene bereitzustellen, die jeder zur Kenntnis nehmen konnte, der sich im Stationszimmer aufhielt, wurde eingestellt.
- Der Zugriff auf die **Gefangenenpersonalakten**, die häufig auch über die Familien der Gefangenen oder über die Opfer ihrer Straftaten Informationen enthalten, wurde auf das jeweils erforderliche Maß beschränkt. Die an der Vollzugsplankonferenz beteiligten Personen erhalten nur in dem Umfang Einsicht in die Akte, wie es notwendig ist, um sich ein Bild über den einzelnen Gefangenen sowie seine persönlichen Verhältnisse und sein familiäres Umfeld zu verschaffen. Die Einsichtnahme durch externe Stellen (wie z. B. die Gewalttäter- bzw. Sexualtätertherapie der CAU Kiel) wird nur noch mit Einwilligung des betroffenen Gefangenen gewährt.

In anderen Bereichen gab es Anlass zu **datenschutzrechtlicher Kritik** und **Beanstandungen**. Einiges hat sich offenbar in den letzten zehn Jahren nicht verbessert, einiges ist neu:

- In einigen Fällen werden umfangreiche **medizinische Gutachten** in Gefangenenpersonalakten aufbewahrt, die ursprünglich im Strafverfahren für die Feststellung der Schuld und der Persönlichkeit des Beschuldigten erstellt wurden. Sie enthalten Informationen nicht nur über den Gefangenen, sondern auch über die Familienmitglieder und über das Opfer der Tat (z. B. über eine sexuell missbrauchte Ehefrau, die den Gefangenen jetzt noch in der JVA besucht). Nur in einem Teilbereich der JVA wird mit diesen Gutachten sachgerecht in der Weise umgegangen, dass sie getrennt von der Akte in einem gesonderten Schrank aufbewahrt und nur unter besonderen Voraussetzungen herausgegeben werden. Dieses Verfahren sollte allgemeiner Standard in der JVA werden.
- Im Lazarettbereich werden ausnahmslos alle Gefangenen auf mögliche Infektionen und Erkrankungen wie Hepatitis und **HIV** ohne Hinweis auf die Freiwilligkeit der Untersuchung getestet. Die Gefangenen werden über ihr Recht, der Untersuchung nicht zuzustimmen, im Unklaren gelassen. Ein Erlass des Justizministeriums aus dem Jahre 1996 sieht vor, dass allen Gefangenen im Rahmen der Aufnahmeuntersuchung u. a. auch eine Untersuchung auf **AIDS** auf freiwilliger Basis anzubieten ist. Hierüber ist der Gefangene unter Aushändigung einer schriftlichen Belehrung und vor der Blutentnahme nochmals mündlich zu unterrichten. Stimmt ein Gefangener trotz Belehrung nicht zu, muss von der Blutentnahme abgesehen werden. Der routinemäßige AIDS-Test ohne ausdrückliche Einwilligung ist rechtswidrig.
- Der **Hinweis** auf den Personalakten der Gefangenen mit positivem **HIV-Befund** sowie Vermerke im elektronischen Datenverarbeitungssystem BASIS und an den Stationstafeln der einzelnen Abteilungsbüros erfolgte ohne die Prüfung, ob für die Empfänger der Information überhaupt ein Infektionsrisiko in Betracht kam.

- Im Bereich der **automatisierten Datenverarbeitung** fehlten für das Windows **NT-Netz** mit den darauf betriebenen Microsoftanwendungen, für das Verfahren **BASIS** (Buchungs- und Abrechnungssystem im Strafvollzug) und für die in diversen Organisationsteilen vorhandenen **Einzelplatzrechner** die nach der Datenschutzverordnung vorgeschriebenen Dokumentationen. Ebenso fehlten Sicherheitskonzepte sowie die Test- und Freigabeunterlagen. Insbesondere beim Betrieb von Einzelplatzrechnern gab es keine klare Trennung zwischen der System- und der Anwenderebene und dementsprechend auch keine klare Differenzierung der Befugnis- und Zugriffsrechte. In einem Fall legten Mitarbeiter an einem Stand-Alone-PC selbst Hand an, um ihn „leistungsfähiger“ zu machen. In einem anderen Fall bestand ein Zugang zum Internet ohne geeignete Schutzvorkehrungen, obwohl auf dem Rechner zugleich Gefangenendaten verarbeitet wurden.
- **Ungestörte Gespräche** mit dem **Anwalt** können im Besucherraum aufgrund der räumlichen Bedingungen, und weil der Raum gleichzeitig zu anderen Zwecken genutzt wird, nicht geführt werden. Das Strafvollzugsgesetz sieht vor, dass Besuche von Verteidigern nicht überwacht werden dürfen. Durch die bloße Anwesenheit der Anstaltsbediensteten entsteht der Anschein einer Über-

wachung, auch wenn dies nicht beabsichtigt sein mag. Das Mithören von Gesprächsinhalten durch die Mitarbeiter oder andere Gefangene oder deren Besucher kann nicht ausgeschlossen werden. Ein freies und vertrauensvolles Gespräch zwischen dem Gefangenen und seinem Rechtsanwalt ist so nur schwer möglich.

- Die **Aufbewahrungsfristen** für abgeschlossene Unterlagen und Buchwerke werden zum Teil erheblich überschritten, weil die Buchwerke mehrere Jahre umfassen.

Insgesamt wurden 60 Punkte aufgelistet, bei denen datenschutzrechtliche Verbesserungen angezeigt sind. Die aufgezeigten Schwachpunkte werden im Wesentlichen vom Justizministerium eingeräumt. In Abstimmung mit der JVA Neumünster wird eine Arbeitsgruppe zur zügigen Aufarbeitung der von uns vorgelegten Empfehlungen eingerichtet.

Was ist zu tun?
Die im Prüfbericht aufgezeigten Schwachstellen sollten umgehend nicht nur in Neumünster, sondern in allen JVA'en beseitigt werden.

4.3.2 MESTA mit Mängeln

Die Errichtungsanordnung für MESTA wurde erlassen, obwohl wir auf eine Reihe von rechtlichen Mängeln hingewiesen hatten. Deren Beseitigung ist unter Verweis auf die notwendige Abstimmung mit den anderen Ländern, die die Software einsetzen, bislang unterblieben.

Die Datenverarbeitung bei den Staatsanwaltschaften ist in Schleswig-Holstein im Gesetz über die **staatsanwaltschaftlichen Verfahrensregister** (StARegG) geregelt. Das Gesetz wurde vom Parlament 1996 als Ausgleich zwischen den Bedürfnissen der Strafverfolgung und den datenschutzrechtlichen Belangen geschaffen. Zwar enthält seit kurzem auch die Strafprozessordnung eine Rechtsgrundlage für Dateien der Staatsanwaltschaft. Die Einzelheiten können die Länder aber per Errichtungsanordnung selbst klären. Das StARegG enthält im Wesentlichen die Regelungen, die die StPO den Ländern überlässt. Deshalb ist dieses Gesetz keineswegs obsolet geworden. Zwar dürfte nach der StPO die Exekutive selbst die Einzelheiten der staatsanwaltschaftlichen Dateien festlegen. Dass in Schleswig-Holstein diese Regelungen sogar in Gesetzesform bestehen, darf die Justizverwaltung bei der Formulierung der Errichtungsanordnung für MESTA nicht einfach ignorieren.

Jetzt soll ein **landesweites Verfahrensregister** der Staatsanwaltschaften eingerichtet werden, obwohl die Staatsanwaltschaften schon bisher gegenseitig auf die Verfahrensdaten gemäß dem Gesetz über die staatsanwaltschaftlichen Verfahrensregister (StARegG) zugreifen konnten. Eine Erforderlichkeit für ein gemeinsames Verfahrensregister in Schleswig-Holstein ist also nicht zu erkennen.

Die jetzt vom Generalstaatsanwalt in Kraft gesetzte Errichtungsanordnung senkt den datenschutzrechtlichen Standard bei den Staatsanwaltschaften in Schleswig-

Holstein ohne Rücksicht auf die Regelungen des StARegG deutlich ab. So haben wir vor allem wegen des erheblich **erweiterten Personenkreises** Bedenken. Warum z. B. Daten von Geschädigten und Anzeigenden in Straf- und Bußgeldverfahren bis zur Aktenaussonderung gespeichert werden sollen, ist nicht nachvollziehbar. Hier müssen die Regelungen des StARegG berücksichtigt werden. Die StPO lässt Spielraum für eine Beibehaltung der bislang in Schleswig-Holstein zugunsten der Persönlichkeitsrechte von Geschädigten und Anzeigenden praktizierten Beschränkung. Auch sind die Gründe dafür nicht ersichtlich, dass künftig über MESTA in Erfahrung gebracht werden können soll, in welcher Eigenschaft eine Person an einem Verfahren beteiligt ist.

Daneben sollten **Zugriffsberechtigungen** eindeutig definiert werden. Die Prüffristen sollten den Wertungen des StARegG Rechnung tragen. Ferner muss die **Speicherungsdauer** der Daten in der Errichtungsanordnung selbst festgelegt werden.

Was ist zu tun?
Die Errichtungsanordnung muss mit dem StARegG in Einklang gebracht werden.

4.3.3 Einblick in die Krankenakten auch für psychisch kranke Straftäter

Das Akteneinsichtsrecht ist ein wichtiges Datenschutzrecht, das grundsätzlich auch psychisch Kranken und Straftätern zusteht. Der restriktive Kurs einer Fachklinik führte zu Konflikten mit fragwürdigem therapeutischem Nutzen.

Von einer Anwältin wurden wir gleich auf eine ganze Palette von Problemen bei der Einsicht in die Patientenakten von nach dem Maßregelvollzugsgesetz (MVollzG) oder dem Strafvollzugsgesetz (StVollzG) in der Fachklinik Neustadt untergebrachten Straftätern hingewiesen. Im MVollzG wird den wegen einer Straftat psychiatrisch Untergebrachten sowohl ein Auskunfts- wie auch ein Akteneinsichtsanspruch gewährt. Verweigert werden darf die Auskunft nur, soweit der Zweck des Maßregelvollzugs wesentlich gefährdet würde. Die Einsicht ist ausgeschlossen, soweit eine wesentliche **Gefährdung des Gesundheitszustandes** des Untergebrachten oder des Vollzugszweckes droht.

Mit letzterem Argument wurde nun der Anwältin immer wieder Akteneinsicht verweigert. Dabei **wechselten** die **Begründungen**. Nachdem sie den Fall eines Untergebrachten in die öffentlichen Medien gebracht hatte, sah die Klinik Gesundheit und Aufgabenerfüllung in Gefahr. Auch das sehr engagierte Auftreten der Anwältin und die Verwendung ihrer Kenntnisse gegenüber den Untergebrachten betrachtete die Klinik als Anlass, Beeinträchtigungen bei den Probanden zu befürchten. Bei nach dem StVollzG Untergebrachten wurde die Akteneinsicht zunächst mit der Begründung verweigert, dass die Anwältin nicht präzise angegeben habe, für welche Zwecke sie die Auskunft nutzen wolle. Der Konflikt beschäftigte nicht nur uns, sondern auch die Gerichte. Eine Aufweichung der Fronten ist bisher nicht zu erkennen.

Zwar verlangt das StVollzG zur Begründung der Akteneinsicht für einen Gefangenen, dass „eine Auskunft für die **Wahrnehmung seiner rechtlichen Interessen** nicht ausreicht und er hierfür auf die Einsichtnahme angewiesen ist“. Diese muss bei verfassungskonformer Auslegung so verstanden werden, dass es genügt, dass der Gefangene als rechtliches Interesse die Wahrnehmung seines Grundrechtes auf informationelle Selbstbestimmung anführt. Will z. B. ein Betroffener prüfen, ob ein Rechtsstreit gegen die aktenführende Anstalt oder einen behandelnden Arzt Aussicht auf Erfolg haben würde, so muss eine Akteneinsicht möglich sein. Bei medizinischen Unterlagen ergibt sich der Anspruch auf Akteneinsicht bereits aus dem ärztlichen Standesrecht.

Beim **Maßregelvollzug** gibt es eine dem StVollzG entsprechende rechtliche Einschränkung der Akteneinsicht nicht. Da die Auskunfts- oder Einsichtsverweigerung jedoch medizinisch begründet werden darf, eröffnen sich einer Fachklinik Ablehnungsgründe, die juristisch nur eingeschränkt auf ihre Plausibilität hin überprüft werden können. Dies bedeutet aber nicht, dass mit dem Argument des Gesundheitsschutzes jedes Begehren zurückgewiesen werden dürfte. Vielmehr müssen **konkrete Gesundheitsgefahren** dargelegt werden.

Zwar geht das Recht eines **bevollmächtigten Anwaltes** nicht weiter als das der betroffenen Person, doch ist der Umstand, dass ein Begehren von einem Anwalt vorgebracht wird, besonders zu gewichten, weil durch ihn Erkenntnisse gegenüber dem Betroffenen gefiltert werden und Gefahren für Sicherheit und Gesundheit abgewendet werden können. Es geht nicht an, dass selbst eine rechtliche Prüfung der Akten durch den Anwalt wegen einer vermuteten Falschbehandlung mit dem Argument sabotiert wird, dies könne dem Patienten gesundheitlich schaden. Der Umstand, dass ein Anwalt mit Zustimmung seines Mandanten einen Konflikt mit der Klinik öffentlich gemacht hat oder vor Gericht streitig austrägt, ist für sich noch kein Grund für eine Einsichtsverweigerung.

Was ist zu tun?
Die Fachklinik wäre gut beraten, ihre restriktive Praxis bei der Akteneinsicht durch ein flexibleres Vorgehen abzulösen. Es ist nicht auszuschließen, dass dies auch positive therapeutische Wirkungen hätte.

4.4 Verfassungsschutz

In Schleswig-Holstein sollen Regelungen über Sicherheitsüberprüfungen zu Zwecken des personellen Sabotageschutzes eingeführt werden. Das A und O ist die Auslegung des Begriffes „personeller Sabotageschutz“.

Wie das Sicherheitsüberprüfungsgesetz des Bundes sieht der Gesetzentwurf des Landes eine Überprüfung für Personen vor, die an **sicherheitsempfindlichen Stellen** bestimmter **lebens- oder verteidigungswichtiger Einrichtungen** tätig sind. Die vorgeschlagene Regelung ist grundsätzlich nachvollziehbar und im Verhältnis zu den Gefahren durch den extremistischen Terrorismus prinzipiell angemessen. Der Kreis der lebenswichtigen Einrichtungen sowie der darin befindlichen sicherheitsempfindlichen Stellen sollte in einer Verordnung der Landesregierung präzise bestimmt werden, weil die dort geregelten Fragen von Bedeutung für alle Ressorts sein können.

Eine wesentliche Verschärfung gegenüber dem Bundesgesetz bedeutet die Absicht, für Beschäftigte an sicherheitsempfindlichen Stellen von lebens- oder verteidigungswichtigen Einrichtungen regelmäßig die **erweiterte Sicherheitsüberprüfung** durchzuführen. Hierfür ist kein sachlicher Grund erkennbar. Das Bundesgesetz lässt die einfache Sicherheitsüberprüfung genügen. Auf eine Einbeziehung von Ehe- und Lebenspartnern in eine Überprüfung sollte in Anbetracht der Tatsache, dass sicherheitsbeeinträchtigende Einwirkungen des Partners kaum vorstellbar sind, gerade im Sabotageschutz verzichtet werden.

Was ist zu tun?
Der Gesetzentwurf sollte unter diesen Gesichtspunkten verbessert werden.

4.5 Ausländerverwaltung

4.5.1 Überblick

Im 24. Tätigkeitsbericht (Tz. 4.5.1 und 4.5.2) stellten wir die nach den Terroranschlägen vom 11. September 2001 erfolgten Änderungen des Ausländerrechts dar, die zu verfassungsrechtlich fragwürdigen **Erfassungsmöglichkeiten von Nichtdeutschen** führen. Inzwischen liegen die ersten Erfahrungen mit der Umsetzung des neuen Ausländerrechts vor. Wir konnten feststellen, dass von vielen gesetzlichen Möglichkeiten bislang nicht oder nur sehr zurückhaltend Gebrauch gemacht worden ist.

Dies ändert nichts an dem Umstand, dass die Vorgaben des Terrorismusbekämpfungsgesetzes eine nach der anderen umgesetzt werden, auch wenn deren Sinnhaftigkeit angesichts der inzwischen eingetretenen zeitlichen Distanz zu den auslösenden Ereignissen zunehmend bezweifelt wird. Ein Beispiel hierfür ist die Durchführung der Rasterfahndung (vgl. Tz. 4.2.4). Ein anderes ist eine Verwaltungsvorschrift, nach der bei **Anträgen für ein Visum oder für eine Aufenthaltserlaubnis** von Staatsangehörigen bestimmter Länder pauschal eine Anfrage bei allen drei Bundesgeheimdiensten, beim Bundeskriminalamt und beim Zollkriminalamt vorgenommen wird. In Einzelfällen ging die Praxis selbst über die ausufernden neuen Regelungen hinaus.

4.5.2 „Verdächtige“ Ausländer

In bundesweit verteilten Merkblättern werden Ausländerbehörden aufgefordert, „verdächtige“ Ausländer anhand vager, zur Geheimsache erklärter Kriterien an die Polizei zu melden. Eine Rechtsgrundlage für derartige Meldungen besteht nicht.

Im Rahmen einer Prüfung beim Landeskriminalamt entdeckten wir bundesweit einheitliche **Merkblätter für Ausländerbehörden**, die „Handreichungen zum Erkennen von potenziellen islamistischen Gewalttätern“ geben und im Trefferfall dazu auffordern, die Polizei zu benachrichtigen. Ähnlich wie bei den Merkmalen zur Rasterfahndung werden als Indizien neben der (vermuteten) Herkunft aus bestimmten Staaten, häufige Reisetätigkeit, Passverlust, Namensänderung, Verbes-

serung des Aufenthaltsstatus z. B. auch die anwaltliche Vertretung als auffällig bewertet. Als entlastende Kriterien werden genannt: Analphabetismus, fehlende Fremdsprachenkenntnisse und körperliche Behinderungen. Als Legitimation für diese besondere „Verdachtsschöpfung“ wurde auf das Terrorismusbekämpfungsgesetz verwiesen. Auf unsere Nachfrage, ob diese Merkblätter in Schleswig-Holstein zu Meldungen durch Ausländerbehörden geführt haben, konnte uns das Innenministerium keine Antwort geben, „weil darüber keine zentralen Aufzeichnungen vorhanden sind“.

Wir haben dem Innenministerium mitgeteilt, dass für die in den Merkblättern empfohlenen Übermittlungen an die Polizei **keine Rechtsgrundlage** besteht. Auch wenn das Terrorismusbekämpfungsgesetz sehr weite Tatbestände enthält, so erlaubt es nicht alles. Für die Rechtfertigung der Übermittlung eines Terrorismusverdachtes genügt kein Merkblatt, das zudem als „Verschlusssache“ erklärt wird, sondern es bedarf einer förmlichen Rechtsvorschrift, in der die Kriterien für die für verdächtig erklärten Personengruppen präzise benannt werden. Besonders problematisch ist die Aufforderung in den Merkblättern, unabhängig von einem Anlass, z. B. der Beantragung einer Aufenthaltserlaubnis, tätig zu werden.

Was ist zu tun?
Bei der Fahndung nach Terroristen ist Augenmaß zu wahren. Die Ausländerbehörden sollten die bundesweit genutzten Merkblätter im Schredder entsorgen.

4.6 Wirtschafts- und Verkehrsverwaltung

Wirtschaftsnummer führt zur versteckten Einführung eines Personenkennzeichens

Durch das Wirtschaftsnummern-Erprobungsgesetz droht die Einführung eines behördenübergreifenden Personenkennzeichens im Bereich der Wirtschafts- und Sozialverwaltung.

Gesetze werden manchmal sehr schnell verabschiedet. Der Katzenjammer wegen nicht bedachter Konsequenzen folgt dann oft erst viel später. Dies könnte auch für ein Gesetz zur Vorbereitung einer **bundeseinheitlichen Wirtschaftsnummer** gelten, das Anfang 2002 in Kraft trat. Darin ist vorgesehen, dass die Bundesanstalt für Arbeit, die Finanzämter, die Gewerbebehörden, die Statistikämter sowie eventuell die Industrie- und Handelskammern, sonstige berufliche Kammern, die Berufsgenossenschaften, die Sozialversicherungsträger und die Monopolkommission für alle im Wirtschaftsleben selbstständig Tätigen eine einheitliche Nummer vergeben, mit der der Behördenverkehr mit den Betroffenen sowie untereinander erleichtert werden soll. Erfasst werden dadurch nicht nur große Kapitalgesellschaften, sondern auch die Angehörigen freier Berufe, Klein- und Kleinstbetriebe und sogar private Haushalte, die eine Haushaltshilfe beschäftigen. Angesichts der weit verbreiteten Tendenz zu „Ich-AGs“ laufen die Pläne darauf hinaus, den formal nicht abhängig Beschäftigten eine Kennziffer zu verpassen.

Daran wäre nichts zu kritisieren, wenn die Kennziffer ausschließlich im Kontakt zwischen Bürger und Verwaltung genutzt würde, da dadurch manch bürokratischer Aufwand reduziert werden könnte. Heikel sind die Pläne aber, weil sie auch den Datenabgleich und -austausch zwischen Behörden bezwecken und damit eindeutig die Funktion eines Personenkennzeichens erfüllt wird. Solche **Personenkennzeichen** (PKZ) wurden von den ersten Anfängen der modernen Datenverarbeitung in den 70er-Jahren an als verfassungswidrig angesehen, weil mit ihnen umfassende Persönlichkeitsprofile erstellt werden können. Aus diesem Grunde wurde eine in der früheren **DDR** genutzte PKZ nach der Vereinigung der beiden deutschen Staaten sofort abgeschafft. Verblüffend war nun, dass solch eine PKZ ohne Getöse und im Schnelldurchgang durch die Gesetzgebung eingeführt werden konnte. In einem Aufwasch soll auch ein einheitlicher behördlicher Stammdatensatz eingeführt werden. Nutzungsbeschränkungen sieht das Gesetz nicht vor, obwohl die zugelassenen Übermittlungen und Datenabgleiche Finanz- und Sozialbehörden einbeziehen, die besonderen Amtsgeheimnissen unterworfen sind. Die Gesetzesbegründung enthält keine Aussagen zur Erforderlichkeit und Verhältnismäßigkeit – allein schon dies ist ein Indiz für dessen wenig durchdachte Ausarbeitung.

Das Problem wird allerdings dadurch gemildert, dass durch das Gesetz nicht gleich eine bundesweite Einführung, sondern nur eine **Erprobung** in einer Region ermöglicht wird. So besteht die Möglichkeit, die Funktionsweise einer sehr weit verbreiteten PKZ und die damit verbundenen Risiken zuvor zu untersuchen und öffentlich zu debattieren. Zur Prüfung der Grundrechtsverträglichkeit ist allerdings keine Evaluation des Erprobungsgesetzes vorgesehen.

Was ist zu tun?
Die grundrechtlichen Konsequenzen des Vorhabens müssen bei der Erprobung untersucht und vor einer bundesweiten Einführung der Wirtschaftsnummer berücksichtigt werden.

4.7 Sozialverwaltung

4.7.1 Kreissozialämter haben das Heft in der Hand

In den letzten Jahren tauchte immer wieder die Frage auf, wer eigentlich für die Sozialhilfegewährung zuständig ist. Der Landkreistag, der Gemeindetag und der Städtebund vertreten die Auffassung, dass in zehn von elf Kreisen des Landes die Kreise die Herren des Verfahrens sind und somit auch die Verantwortung für die Datenverarbeitung tragen.

Das Ausführungsgesetz zum Bundessozialhilfegesetz Schleswig-Holstein (AG BSHG SH) sieht die Besonderheit vor, dass die Kreise ihre Gemeinden per Satzung zur **generellen Aufgabenerfüllung heranziehen** können, ohne dass die Verantwortung für die Datenverarbeitung an diese übergeht, sodass die Gemeinden „nur“ im Namen des Kreises tätig werden. Von dieser Möglichkeit haben zehn von elf Kreisen in Schleswig-Holstein Gebrauch gemacht. Soweit bekannt, ist diese Form der Heranziehung bundesweit einmalig.

Was bedeutet dies für die Gemeinden der zehn Kreise in der täglichen Praxis? Wird die Gemeinde **im Namen des Kreises** tätig, so kann er u. a. bestimmen, welche Sozialhilfesoftware eingesetzt werden soll, dass die Sozialhilfedaten auf einem Server des Kreises verwaltet werden oder dass innerhalb eines Kreises nur noch eine gemeinsame Sozialhilfeakte geführt wird.

Der **Kreis** trägt andererseits die **Verantwortung** für die datenschutzgerechte Verarbeitung der Sozialdaten in den Gemeinden. Er ist daher bei Verstößen innerhalb der Sozialämter der Gemeinden Adressat unserer Beanstandungen. Um dieser Verantwortung gerecht zu werden, gehören zu den Aufgaben des Kreises u. a.

- die datenschutzgerechte (einheitliche) Gestaltung von Vordrucken,
- die korrekte Gestaltung der Briefköpfe in den Schreiben und Bescheiden der Gemeinden sowie
- die Anordnung technischer und organisatorischer Sicherheitsmaßnahmen einschließlich des Erlasses von Dienstanweisungen zur Wahrung des Sozialgeheimnisses in allen gemeindlichen Sozialämtern.

Um seine Aufgaben effektiv zu erfüllen, hat der Kreis

- ein unbeschränktes Zugriffsrecht auf alle Sozialhilfedaten in seinem Kreisgebiet,
- ein umfangreiches Kontrollrecht und
- ein durchgreifendes Weisungsrecht gegenüber den Gemeinden.

In einem „offenen Brief“ an alle Kreise haben wir auf diese Rechtslage sowie auf die hieraus resultierenden **Konsequenzen** hingewiesen. Einige Kreise zeigten sich wegen dieser Verantwortung erst einmal erschrocken. Die „Zentralisierung“ bei den Kreisen kann unter Datenschutzaspekten zweifellos auch positive Effekte für Hilfe suchende Bürgerinnen und Bürger haben, denn nunmehr müssen die Kreise für ein einheitliches Datenschutzniveau bei allen Gemeinden sorgen.

Was ist zu tun?
Es liegt nun an den Kreisen, ihre gewollte Verantwortung für die Gemeinden auch tatsächlich wahrzunehmen.

4.7.2 Hilfeplan und Leistungskontrolle

Die Eingliederungshilfe für psychisch Kranke wird auf der Grundlage des Sozialhilferechts von den Kreisen finanziell unterstützt. Dies bedeutet jedoch nicht, dass die Behandlungseinrichtungen den Sozialämtern sämtliche persönlichen Umstände und insbesondere den genauen seelischen Zustand der Patienten mitteilen dürfen. Für deren Begutachtung ist das Gesundheitsamt zuständig.

Zum Zweck der Optimierung der Rehabilitationsplanung bei psychisch Erkrankten und Behinderten und um „den personellen und finanziellen Aufwand so gering

wie möglich zu halten“ forderte das Sozialamt eines Kreises von einem Träger vieler Einrichtungen der stationären Versorgung von psychisch Kranken die Vorlage fast sämtlicher **Informationen aus dem internen Dokumentationssystem.** Der Träger bezweifelte deren Notwendigkeit und die Zulässigkeit einer solchen pauschalen Datenübermittlung.

Dies führte zu einem Diskussionsprozess der Beteiligten, der erst durch unsere rechtliche Beratung und Vermittlung zu einer alle zufrieden stellenden **Klärung des Verfahrensablaufes** führte. Zu Recht monierte der Kreis, dass die bisher praktizierte Vorlage von standardisierten Begründungsschreiben keine objektive und zielorientierte Begutachtung des Hilfebedarfs ermögliche. Statt aber nun umfangreiche Dokumentationen über Seelenzustand und Lebensbedingungen der Betroffenen beim örtlichen Sozialamt zu sammeln, das für die Bewertung der Unterlagen ohnehin nicht den medizinischen Sachverstand vorhält, soll mit Einwilligung der Betroffenen ein Datensatz, der von einem Betroffeneninteressenverband definiert worden ist, als „Arztsache“ an das Gesundheitsamt des Kreises weitergegeben werden. Die Amtsärzte nehmen eine Begutachtung vor, bei der der Proband und die unterbringende Einrichtung aktiv einbezogen werden.

Durch Übersendung dieses Gutachtens, das sich auf die für die Hilfegewährung notwendigen Daten beschränkt, wird das Sozialamt informiert. Es wird auch zur Grundlage für die **Erstellung des Gesamtplanes** für die Eingliederungshilfe verwendet. Bei der Fortschreibung des Gesamtplanes erfolgt die Antragstellung, Begutachtung und Hilfegewährung nach dem gleichen Verfahren. Im Konfliktfall wird zunächst eine Klärung mit dem Gutachter gesucht, bevor das Sozialamt direkt auf den Betroffenen und die Einrichtung zugeht.

Was ist zu tun?
Die gemeinsam gefundene Vorgehensweise kann landesweit als Vorbild für die Bewertung der Hilfemaßnahmen zur Eingliederung von psychisch Kranken dienen.

4.7.3 Wenn der Schwerbehindertenbescheid beim Vermieter landet

Ein als schwerbehindert anerkannter Mieter einer Wohnung war nicht wenig erstaunt, als sein Vermieter ihm wortwörtlich aus seinem Anerkennungsbescheid zitierte.

Der Bescheid enthielt nicht nur Angaben zur Behinderung selbst, sondern in der Begründung auch viele medizinische Details. Der Petent hatte zuvor einen Antrag auf Ausstellung eines allgemeinen Parkausweises gestellt und gehofft, einen Parkplatz auf der Stellplatzanlage des Vermieters zu bekommen. Um diesen Antrag zu unterstützen, hatte die Gemeinde **ohne Wissen des Betroffenen** Teile des Anerkennungsbescheides an den Vermieter gesandt. Die Gemeinde meinte, der Petent habe diese Unterlagen doch zur Verfügung gestellt und einer eventuellen Weitergabe nicht widersprochen.

Die Datenweitergabe haben wir beanstandet. Für diese Datenübermittlung gab es keine Rechtsgrundlage, sie war schlicht überflüssig und zugleich eine Beeinträchtigung des Persönlichkeitsrechtes des Betroffenen. Bürgerfreundlichkeit darf nicht so verstanden werden, dass **am Bürger vorbei** sensible Daten über ihn ausgetauscht werden. Der Bitte des Betroffenen, die unzulässig erhaltenen Unterlagen zu vernichten, kam der Vermieter umgehend nach.

Was ist zu tun?
Vor der Weitergabe von Gesundheits- und Sozialdaten an Private durch öffentliche Stellen sollte eine Einbeziehung des Betroffenen erfolgen, je nach Rechtslage in Form einer Benachrichtigung oder durch die Einholung einer Einwilligung.

4.8 Schutz des Patientengeheimnisses

Überblick

Der Datenschutz im Medizinbereich befindet sich schon seit Jahren im Spannungsfeld der Interessen der „Player" im Gesundheitswesen. Dabei geht es nicht immer nur um hehre Grundsätze einer qualitativen Verbesserung der medizinischen Versorgung, sondern zumeist auch um sehr viel Geld. Wir verstehen uns in diesen Konflikten als **Interessenvertreter der Patientinnen und Patienten**, deren Stimme im Getöse der Lobbyvertreter sonst noch weniger Gehör finden würde. Dabei fällt „dem Datenschutz" oft die Rolle eines Moderators zu; eine Aufgabe, der wir uns nicht entziehen können und wollen.

Allerdings beschränken wir uns nicht darauf, auf externe Anforderungen zu reagieren. Mit unserer Aktion „**Datenschutz in meiner Arztpraxis**" haben wir gemeinsam mit den Kammern eine auf Dauer angelegte Kampagne begonnen, die im gesamten Gesundheitsbereich gestaltend und überzeugend wirken soll. Die Resonanz und die praktischen Erfolge geben uns mit unserem Ansatz Recht (s. Tz. 4.8.9).

Wir konnten dabei feststellen, dass gerade der Gesundheitssektor das ideale Anwendungsgebiet für die neuen Instrumente **Datenschutzaudit und Gütesiegel** ist, weil das Vertrauen in die ärztliche Verschwiegenheit einer der zentralen Akzeptanzfaktoren für technische und organisatorische Innovationen ist. Der Patientendatenschutz darf nicht zwischen widerstreitenden wirtschaftlichen Interessen zerrieben werden. Er muss zum wirtschaftlich nutzbaren Faktor werden.

4.8.1 Disease-Management-Programme

Der Versuch, die Gesundheitsversorgung effektiv zu gestalten, läuft zumeist über das Sammeln von noch mehr Patientendaten. Nur intelligente Pseudonymisierungsprogramme können negative Auswirkungen auf den Schutz des Patientengeheimnisses vermeiden.

Im Sommer 2002 hätten gemäß einer Entscheidung des Bundesgesetzgebers die besonderen Behandlungsprogramme für chronisch Kranke umgesetzt werden sollen. Mit diesen „Disease-Management-Programmen“ (DMP) will man bei langwierigen und kostenintensiven Krankheiten – zunächst geht es um Brustkrebs, koronare Herzkrankheiten, Asthma und Diabetes – eine gezielte, standardisierte und zugleich qualitätskontrollierte Behandlung und Anleitung der Patienten bewirken. Zweck ist eine **Verbesserung des Behandlungserfolges**, aber natürlich auch die Reduzierung der außer Kontrolle geratenen **Krankenkassenkosten**. Für das Disease Management sind Patientendaten über die Behandlung und das Patientenverhalten erforderlich. Daher haben sich die Datenschutzbeauftragten von Anfang an in die Entwicklung der Programme eingeschaltet. Leider konnten wir nicht verhindern, dass die „Lotsenfunktion“ für die chronisch Kranken den Krankenkassen übertragen wurde. Diese Aufgabenzuweisung birgt nämlich die Gefahr, dass neben dem Ziel einer effektiven Behandlung zu sehr die Kostengesichtspunkte in die Anleitung von Ärzten und Patienten einfließen. Insbesondere aus der Ärzteschaft erntete DMP wegen des möglichen Kontrolleffekts viel Kritik und Abwehr.

Da wir das politische und medizinische Ziel des DMP nicht zu bewerten hatten, haben wir versucht, die datenschutzrechtlichen Gefahren einer zentralen Langzeitpatientendatenspeicherung durch flankierende Sicherungen zu minimieren. Wir sehen z. B. in der Einführung einer pseudonymen Patientendatenverarbeitung eine Chance, auch in weiteren Bereichen der gesetzlichen Krankenversicherung einen Ausgleich zwischen dem Schutz des Patientengeheimnisses und dem Datenbedarf im Gesundheitswesen zu schaffen und dabei zugleich einen **Interessenausgleich** zwischen den sich gegenüberstehenden **Kassen und der Ärzteschaft** zu erleichtern.

www.datenschutzzentrum.de/material/themen/gesund/kkdmp.htm

Um der Gefahr des Eingriffs in die Autonomie von Patient und Arzt zu begegnen, wurde im Regelwerk – der Risikostruktur-Ausgleichsverordnung – ein ausgeklügeltes Datenmanagement vorgesehen: Die besonders sensiblen medizinischen Daten sollten **in einer unabhängigen Stelle pseudonymisiert** werden und nicht patientenbezogen für Zwecke der Qualitätssicherung ausgewertet werden. Ein weniger sensibler Datensatz soll an die Krankenkassen weitergegeben werden, der dazu dient, den Patienten über Untersuchungs-, Behandlungs- und Trainingsangebote zu einem optimalen medizinischen Erfolg zu verhelfen.

Leider zeigte sich die Kassenärztliche Vereinigung (KV) des Landes zunächst wenig an einem konstruktiven Dialog interessiert. In einer von ihr ausgehenden Anzeigenkampagne wurde kurz vor der Bundestagswahl – aus unserer Sicht in

unsachlicher Weise – die **Angst vor dem gläsernen Patienten geschürt**. Erst einige Zeit nach der Wahl setzten sich Ärzte und Kassen auch in Schleswig-Holstein zusammen, um gemeinsam eine Lösung zu finden. Dabei geht es insbesondere darum, dass die Patientendaten, die sich bei den Krankenkassen befinden, einer strengen Zweckbindung unterworfen werden und nicht dazu missbraucht werden, Patienten und Ärzte zu gängeln.

Was ist zu tun?
Nachdem der Theaterdonner zum DMP verklungen ist, müssen Kassen, Ärzte und Datenschützer gemeinsam verfahrensbegleitend darauf achten, dass bei der Verwirklichung der berechtigten gesundheitspolitischen Ziele das Patientengeheimnis und die Patientenautonomie nicht auf der Strecke bleiben.

4.8.2 Gesundheitskarte Schleswig-Holstein

Das Projekt einer multifunktionalen medizinischen Chipkarte wird als „Gesundheitskarte Schleswig-Holstein" in der Pilotregion Flensburg vorangetrieben. Die Initiatoren haben die Absicht, dabei das Patientengeheimnis zu wahren.

Bewegten sich die Überlegungen zur Weiterentwicklung der „alten" Karte der gesetzlichen Krankenversicherungen zu einem elektronischen Kommunikations- und Datenverarbeitungsinstrument im letzten Jahr noch im Bereich politischer Willensbekundungen (vgl. 24. TB, Tz. 4.8.2), so macht man sich nun an die praktische Umsetzung. Im Rahmen der von der Landesregierung gestarteten „**Gesundheitsinitiative Schleswig-Holstein**" wurde auf der Grundlage des Flensburger Praxisnetzes begonnen, eine elektronische Gesundheitschipkarte zu realisieren, auf der neben den Versichertenangaben weitere medizinische Daten (Organspende, Allergien, Impfungen, Notfalldaten, Implantate) und vor allem auch weitere Funktionen (Arzneimittelausweis, elektronischer Arztbrief) sukzessive realisiert werden sollen. Flensburg ist eine Pilotregion für die Erprobung einer Karte, die später bundesweit eingesetzt werden soll. Die einheitlichen Vorgaben hierfür wurden im Mai 2002 von allen beteiligten Interessengruppen unter Einbeziehung eines „Aktionsforums Telematik im Gesundheitswesen" in einer gemeinsamen Erklärung zusammengefasst, in der abweichend von früheren Plänen die **Patientenautonomie** eine zentrale Rolle spielt. Für die Chipkarte wurden Wahlfreiheit und Patientengeheimnis als zentrale Konzeptbestandteile anerkannt.

Bei dem vom Gesundheitsministerium des Landes koordinierten Flensburger Projekt sitzen neben ambulanten und stationären Einrichtungen Apotheker, Krankenkassen und Vertreter aus der Medizintechnik in einem Boot. Wir begleiten das Projekt beratend. Als eines der ersten Module soll das **elektronische Rezept** realisiert werden. Dabei ist vorgesehen, dass die verschreibenden Ärzte ihre Medikation in elektronischer Form auf einem zentralen Server ablegen und zugleich auf der Chipkarte des Patienten dazu einen eindeutigen „Pointer" abspeichern. Dieser Pointer kann in einer Apotheke elektronisch ausgelesen werden und den Zugriff auf die zentral gespeicherten Rezeptdaten eröffnen. Der Apotheker kann durch Abgleich der Rezeptdaten mit einer zentralen Medikamentendatenbank feststellen, ob bei dem Medikamentenmix für den Patienten Risiken bestehen oder Kontra-

indikationen beachtet werden müssen; er kann den Patienten entsprechend beraten. Die Einlösung des Rezeptes wird vom Apotheker vermerkt: Die Daten werden an die Krankenkassen elektronisch zur Abrechnung weitergegeben. Solange es für die Nutzung des elektronischen Rezeptverfahrens noch keine gesetzliche Verpflichtung gibt, muss das bisherige Papierrezeptverfahren selbstverständlich parallel dazu weiter betrieben werden.

Bei dem Projekt ist eine **Vielzahl datenschutzrechtlicher Fragen** (z. B. welche Einwilligungen bei den Patienten einzuholen sind) zu beantworten. Bei aller Offenheit der weiteren Projektentwicklung muss dem Patienten durch eine präzise Information klar sein, wozu er seine Zustimmung gibt und welche personenbezogenen Datenflüsse vorgesehen sind. Bei der technischen Umsetzung muss durch Verschlüsselungs- und Signaturmechanismen gewährleistet werden, dass nur befugte Personen im notwendigen und zugelassenen Umfang auf Patientendaten zugreifen können. Die technische Machbarkeit eines datenschutzgerechten Datenmanagements ist dabei wohl das kleinste Problem.

Was ist zu tun?
Bei der Weiterentwicklung der Gesundheitskarte muss zu jedem Stadium ein Datenschutzcheck erfolgen. Es bietet sich an, das Verfahren bereits einem Datenschutzaudit zu unterziehen, bevor mit der Realisierung begonnen wird.

4.8.3 Das Verfallsdatum von Einwilligungen

Die Wirksamkeit von einmal erteilten Schweigepflichtsentbindungserklärungen für private Krankenversicherungen dauert nicht ewig.

Bei Abschluss eines Versicherungsvertrages fordern private Krankenversicherer von ihren Kundinnen und Kunden oft routinemäßig die Unterschrift unter eine umfangreiche Schweigepflichtsentbindungserklärung. Während der Datenfluss zwischen Ärzten und gesetzlichen Krankenkassen nämlich gesetzlich geregelt ist, bedarf es für eine Offenbarung von Patienteninformationen an private Krankenversicherungen einer wirksamen Einwilligungserklärung des Patienten. Die privaten Krankenversicherungsunternehmen bedienen sich einer im Jahre 1989 entworfenen **Mustererklärung**. Darin erklärt sich der Versicherte per Unterschrift damit einverstanden, dass die Mitarbeiter der privaten Krankenversicherung seine Patientendaten abfragen dürfen, und zwar

- für einen Zeitraum von 5 Jahren ab Antragstellung zur **Beurteilung eines möglichen Versicherungsrisikos** bei allen Ärzten, Zahnärzten usw., bei denen sich der Antragsteller in den letzten 10 Jahren in Behandlung befand,
- bzw. unbefristet ab Antragstellung zur **Beurteilung der Leistungspflicht** der privaten Krankenversicherung bei den Ärzten, Zahnärzten usw.

Manche private Versicherungen wollen auch noch **20 und mehr Jahre** nach Vertragsabschluss ärztliche Auskünfte erhalten, ohne dass der Versicherte zuvor eingeschaltet wird. Wer weiß aber noch, was er vor vielen Jahren einmal unterschrieben hat, und rechnet mit entsprechenden Datenweitergaben? Ärzte bezweifelten

uns gegenüber in vielen Einzelfällen, dass die Patienten bei Kenntnis der Sachlage der abverlangten Offenbarung der äußerst sensiblen Patientendaten zugestimmt hätten. Sie äußerten ihre Angst vor strafrechtlichen Konsequenzen, wenn sie Auskünfte erteilen und sich im Nachhinein erweist, dass die uralten Schweigepflichtsentbindungen ungültig sind.

Die problematisierten Erklärungen – „Blankovollmachten“ mit unbegrenzter Gültigkeit – sind wahre Muster für unbegrenzte Pauschalität. Sie verstoßen gegen die datenschutzrechtliche Forderung, dass Einwilligungserklärungen **inhaltlich ausreichend bestimmt** sein müssen. Der Versicherte muss zum Zeitpunkt seiner Unterschrift erkennen können, welche seiner Patientendaten von welchen Ärzten an die Versicherung übermittelt werden sollen. Dieses Patientenrecht wurde durch die aktuelle Rechtsprechung des Bundesgerichtshofes und die Europäische Datenschutzrichtlinie bekräftigt. Insbesondere bezüglich der Prüfung der Leistungsverpflichtung durch die Versicherung wird diesen Anforderungen mit dem Mustertext nicht (mehr) genügt. In einem ausführlichen Gutachten haben wir diese Rechtsauffassung begründet und den Aufsichtsbehörden bundesweit zur Kenntnis gegeben.

www.datenschutzzentrum.de/material/themen/gesund/versentb.htm

Zu Beginn des Versicherungsverhältnisses sollte demnach nur noch eine Schweigepflichtentbindung verlangt werden, mit der Auskünfte über mögliche Versicherungsrisiken eingeholt werden können. Reicht ein Versicherter später eine Rechnung ein und entstehen hierzu Fragen beim Versicherungsunternehmen, so sind diese an den Versicherten zu richten. Soweit erforderlich, kann von ihm, bezogen auf diese aktuelle Frage, eine **konkrete Schweigepflichtentbindungserklärung** gefordert werden. Der Patient kann sich in genauer Kenntnis der Umstände entscheiden, ob er diese Erklärung abgibt, und der behandelnde Arzt kann sich sicher sein, dass er befugt Patientendaten übermittelt.

Was ist zu tun?
Die Versicherungen sollten nicht länger mit antiquierten Pauschalerklärungen arbeiten, sondern sich bei ihren Kunden jeweils aktuell vergewissern, ob sie mit der Weitergabe ihrer Krankheitsdaten einverstanden sind.

4.8.4 Anforderung von Kurzberichten durch Krankenkassen

Die AOK Schleswig-Holstein hat in nahezu allen Fällen, in denen Patienten kürzer als vier Tage stationär aufgenommen wurden, Kostenübernahmeanträge des Krankenhauses so lange zurückgewiesen, bis das Krankenhaus einen Kurzbericht über den behandelten Patienten abgab.

Das Sozialgesetzbuch V definiert, welche Daten Krankenhäuser über ihre Patienten an die Krankenkassen übermitteln dürfen. Wenn darüber hinaus z. B. die Erforderlichkeit einer kurzen stationären Behandlung überprüft werden muss, ist dafür der Medizinische Dienst der Krankenversicherungen (MDK) zuständig, da für diese Beurteilung medizinischer Fachverstand nötig ist. Den Krankenkassen steht diese Prüfung nicht zu. Die **AOK Schleswig-Holstein** machte jedoch für

sich ein **Vorprüfungsrecht** geltend und berief sich dabei auf die Rechtsprechung der Sozialgerichte. Sie meinte, einen Anspruch auf Kurzberichte der Krankenhäuser zwecks Prüfung ihrer Leistungspflicht zu haben. Bei ambulant behandelbaren Diagnosen sei es generell erforderlich, von den Krankenhäusern nachvollziehbare medizinische Begründungen für die Notwendigkeit der stationären Behandlung anzufordern. Zudem sei die Anforderung von Kurzberichten im Vertrag zwischen der Deutschen Krankenhausgesellschaft und den Spitzenverbänden der Krankenkassen zur Überprüfung der Notwendigkeit und Dauer der Krankenhausbehandlung ausdrücklich geregelt. Dieser Vertrag wurde jedoch zum Jahresende 2002 gekündigt.

Damit spitzte sich der Streit auf die Frage zu, ob der nach dem Sozialgesetzbuch zu übermittelnde Datensatz abschließend ist – so die Sicht der Krankenhäuser – oder nicht – so die Sicht der Krankenkassen. „Kurzberichte", in denen die medizinische Notwendigkeit der Dauer der stationären Behandlung begründet wird, enthalten Daten, die weit über den im Sozialgesetzbuch genannten Umfang hinausgehen. Grundsätzlich muss die Frage der Notwendigkeit durch ein MDK-Gutachten anhand von Daten entschieden werden, die Aussagen zu „Art, Schwere, Dauer und Häufigkeit der Erkrankung" erlauben. Diese Entscheidung muss **im Einzelfall** erfolgen; eine pauschale Vorprüfung sämtlicher Kurzaufenthalte im Krankenhaus ist im Gesetz nicht vorgesehen. Dies wurde nunmehr auch durch eine Entscheidung des Bundessozialgerichtes ausdrücklich bestätigt.

Was ist zu tun?
Bei der Neuregelung der „Kurzberichte" oder ähnlicher medizinischer Kurzgutachten in den Verträgen zwischen Krankenhaus- und Kassenverbänden ist darauf zu achten, dass den Kassen keine pauschalen medizinischen Prüfkompetenzen zugewiesen werden und die Rechtsprechung des Bundessozialgerichtes berücksichtigt wird.

4.8.5 Wenn sich das Pflegeheim für den Lebenslauf interessiert

Der Medizinische Dienst der Krankenversicherungen in Schleswig-Holstein (MDK) rät den Pflegeheimen zur Erhebung von biografischen Daten über ihre Pflegefälle, um eine aktivierende und zielgerichtete Pflege durchführen zu können. Diese nachvollziehbare Empfehlung – nur wer seine Pflegefälle wirklich kennt, kann effektiv betreuen – darf aber nicht zu einer Sammlung sensibler Daten führen und zum Selbstzweck werden.

Ein Sohn bekam von dem Pflegeheim seiner Mutter einen **umfangreichen Fragebogen** zugesandt und wurde aufgefordert, Angaben zu machen über

- Kindheit/Jugend,
- schulische und berufliche Ausbildung,
- Eheschließung und Familiengründung,
- prägendes Zeitgeschehen und besondere Ereignisse,
- Wohn-/Lebensverhältnisse vor dem Heimaufenthalt,

- Umzüge,
- soziale Kontakte, Bezugspersonen,
- Hobbys/Interessen/Aktivitäten und Gewohnheiten.

Auf Nachfrage erklärte das Pflegeheim, der MDK benötige diese biografischen Angaben für eine „Sonderaktion". Der MDK widersprach: Nicht er benötige diese Daten, sondern das Heim selbst, welches ja die Pflege durchführe. Es stellte sich die Frage: Warum wurden die Betroffenen nicht über den Zweck der Datenerhebung informiert? Unsere Prüfung ergab, dass der Fragebogen eine reine **Feigenblattfunktion** hatte: Bei MDK-Prüfungen wurden die Fragebögen vorgezeigt; bei der täglichen Pflege spielten sie jedoch keine Rolle. Noch während unserer Prüfung erklärte das Heim, zukünftig auf die Erhebung der biografischen Daten vollständig zu verzichten.

Was ist zu tun?
Der Umfang der zum Zwecke der zielgerichteten und aktivierenden Pflege benötigten biografischen Daten richtet sich nach den Besonderheiten des einzelnen Pflegefalles. Umfangreiche standardisierte Datenerhebungen produzieren oft nur sensiblen Datenschrott, aber keine bessere Versorgung.

4.8.6 Die Grenzen des Outsourcing

„Outsourcing" gilt für viele als Zauberformel für Kosteneinsparungen. Erhoffte Einsparungen lassen sich aber oft nicht realisieren; teuer kann dagegen der Vertrauensverlust bei den Bürgerinnen und Bürgern kommen.

Eine von mehreren Aufgaben des Medizinischen Dienstes der Krankenversicherungen Schleswig-Holstein (MDK) ist die Begutachtung im Rahmen der Pflegeversicherung. Dabei werden oft besonders sensible medizinische Daten der Versicherten erhoben. Dem Pflegegutachten ist z. B. zu entnehmen, ob der Betroffene noch in der Lage ist, sich selbst zu verpflegen, zu waschen, zur Toilette zu gehen, welche Medikamente er benötigt, ob er geistig noch auf der Höhe ist, inwieweit Verwandte bei der Pflege helfen usw. Die Pflegegutachten werden generell von Mitarbeiterinnen des hauseigenen Schreibdienstes geschrieben. In Spitzenzeiten kann es jedoch dort zu Engpässen kommen. Da man zusätzliche Schreibkräfte nicht einstellen wollte, wurde vom MDK ein **externes privates Schreibbüro** beauftragt. Dadurch erfuhren die Mitarbeiter der privaten Firma nicht nur Namen und Anschrift der Pflegeversicherten, sondern auch die vollständigen Ergebnisse der Begutachtung. Die Betroffenen selbst wurden weder gefragt noch unterrichtet.

Der MDK erklärte uns, dieses Verfahren diene der Einsparung von Zeit und Geld; es sei daher im Interesse der Betroffenen. Als Sozialleistungsträger sei man nach den Vorschriften des Sozialgesetzbuches rechtlich befugt, im Rahmen einer **Auftragsdatenverarbeitung** auch ohne Einwilligung der Pflegeversicherten die Daten der Gutachten an eine private Firma im Rahmen des Outsourcing zu übermitteln.

Nach unserer Auffassung unterliegen die Daten eines Pflegegutachtens nicht nur dem Sozialdatenschutz, sondern auch der **ärztlichen Schweigepflicht**. Die Übermittlung von Pflegegutachten ist daher nur zulässig, wenn der Versicherte zuvor unterrichtet wird und schriftlich einwilligt. Unsere Rechtsauffassung wird zwar nicht von allen Datenschutzbeauftragten in Deutschland geteilt. Im Interesse der Pflegeversicherten halten wir jedoch an ihr fest. Medizinische Daten in einem MDK-Pflegegutachten dürfen nicht weniger geschützt sein als solche in der Patientenakte eines Arztes. Die Einschaltung einer privaten Firma als Schreibdienst bedarf der Einwilligung der Pflegeversicherten (vgl. zum MDK auch Tz. 7.4.4).

Ein positives Beispiel für einen verantwortungsvollen Umgang mit medizinischen Daten zeigte eine große Krankenkasse in Schleswig-Holstein: Um Kosten zu sparen, hatte man überlegt, die **ein- und ausgehende Post** zukünftig von einer privaten Firma verwalten zu lassen. Nach einer Beratung durch uns nahm man davon Abstand. Es sei nicht im Interesse der Krankenkasse, wenn die Versicherten bei der Übersendung ärztlicher Unterlagen ein unbehagliches Gefühl haben, weil die Briefe von einer privaten Firma geöffnet werden.

Was ist zu tun?
Dem Outsourcing der Bearbeitung von Patientendaten hat der Bundesgerichtshof zu Recht enge Grenzen gesetzt. Der MDK bleibt ungeachtet der rechtlichen Interpretationsspielräume aufgefordert, darüber nachzudenken, ob es nicht im Interesse an dem Erhalt des nötigen Vertrauens zu den Pflegeversicherten läge, auf die Weitergabe von Pflegegutachten an externe Schreibbüros zu verzichten.

4.8.7 Über den Kopf der Versicherten hinweg

Gesetzliche Rentenversicherer benötigen zur Prüfung von Rentenansprüchen ärztliche Gutachten. Die Begutachtung erfolgt in vielen Fällen durch externe Ärzte. Vor deren Einschaltung und der Übersendung von Gutachten und Attesten bedarf es des Einverständnisses des Betroffenen.

Das Thema ist ein „Dauerbrenner“ (vgl. 24. TB, Tz. 4.8.5). Zum wiederholten Male erhielten wir eine Beschwerde darüber, dass ein Rentenantragsteller **Post** von einem ihm **nicht bekannten Arzt** aus Hamburg erhielt. Darin wurde ihm kurz und knapp erklärt, dass die Landesversicherungsanstalt Schleswig-Holstein (LVA) den Arzt mit einer medizinischen Begutachtung beauftragt habe. Die Informationen, die er bisher von der LVA erhalten habe, genügten für eine vollständige ärztliche Begutachtung nicht. Der Rentner war nicht damit einverstanden, dass ohne sein Wissen medizinische Daten an einen ihm unbekannten Arzt übermittelt wurden. Zudem erwies sich, dass im konkreten Fall die Begutachtung entbehrlich war, weil ein aktuelles Attest seines Hausarztes vorlag.

Wir schlugen der LVA vor, zukünftig vor der Einschaltung externer Gutachter den betroffenen **Antragsteller** zu **unterrichten**. Dieser könne so offene Fragen durch die Vorlage vorhandener Atteste beantworten und dadurch unter Umständen schmerzhafte und teure Untersuchungen vermeiden. Sei er mit einem vorgeschlagenen Gutachter nicht einverstanden, könne gemeinsam eine Alternative gesucht werden.

Die LVA teilte nur mit, man sehe sich nicht in der Lage, Rentnerinnen und Rentner derart zu unterrichten, da dieser **Verwaltungsaufwand** zu hoch sei. Ebenso wenig wolle man Rentenbeziehern eine Möglichkeit geben, zwischen verschiedenen Gutachtern zu wählen oder gar solche selbst zu benennen. Die aktive Beteiligung könnte zu Verzögerungen in der Rentenbewilligung führen. Zudem wähnte man sich in guter Gesellschaft: Die Bundesversicherungsanstalt für Angestellte (BfA) und etliche Landesversicherungsanstalten bedienten sich eines ähnlichen Verfahrens.

Wir haben den Bundesbeauftragten und die Landesbeauftragten für Datenschutz über das Problem unterrichtet. Bis zu einer **bundesweiten Klärung** haben wir von einer Beanstandung des Verfahrens abgesehen, doch vertreten wir die Auffassung, dass es nicht akzeptabel ist, wenn „hinter dem Rücken“ der Rentner zum Teil äußerst sensible medizinische Daten an externe Gutachter übermittelt werden.

Was ist zu tun?
Auf Bundesebene müssen sich die Rentenversicherungsträger auf ein einheitliches Verfahren einigen, das nicht nur einen „reibungslosen Verwaltungsablauf“ sichert, sondern auch den Interessen der betroffenen Rentner an umfassender Unterrichtung und Beteiligung gerecht wird.

4.8.8 Patientenakten auf dem Bürgersteig

Von einem Bürger wurden wir darauf aufmerksam gemacht, dass mitten in der Innenstadt von Kiel auf dem Bürgersteig ein offener Bauschuttcontainer herumstand, in dem sich für jedermann frei zugänglich hunderte von Patientenakten befanden.

Eine Nachschau bestätigte die Angaben. Offensichtlich war eine Arztpraxis ausgeräumt worden, wobei nicht nur **hochsensible Patientenakten**, sondern auch Abrechnungs-, Personal- und Bewerbungsunterlagen **entsorgt** wurden. So konnte jeder vorbeikommende Passant eine Patientenakte seiner Wahl mitnehmen oder vielleicht sogar nachstöbern, ob unter den Patienten ein Bekannter sei und welche Blutwerte und welchen Befund aus einer Stuhluntersuchung dieser aufzuweisen hatte. Wir mobilisierten umgehend den verantwortlichen Arzt und baten die Polizei um Sicherung des Containers.

Es zeigte sich, dass der Arzt sich bewusst auf diese Weise der Akten entledigen wollte. Leider mussten wir feststellen, dass er selbst nach der Konfrontation mit dem Umstand, dass hier offensichtlich ein Verstoß gegen die strafbewehrte ärztliche Schweigepflicht erfolgt war, nicht erkennbar ein Problem-, geschweige denn ein Unrechtsbewusstsein entwickelte. Daher informierten wir eine größere Zahl von betroffenen Patienten, von denen viele **Strafanzeige** bei der Staatsanwaltschaft stellten. Es bedurfte auch einiger Schreiben an die Staatsanwaltschaft, bis dort die strafrechtliche Relevanz des Vorgangs richtig eingeschätzt wurde und immerhin der Straftatbestand ermittelt wurde. Das Verfahren gegen den Arzt wurde dann nach Zahlung einer Geldbuße eingestellt.

Kurse
AR, AR-I, AR-II

Sicherlich ist der Vorgang ein ungewöhnlicher „**Ausreißer**“. Den meisten Ärzten dürfte die hohe Bedeutung des Patientengeheimnisses bewusst sein. Doch ist das Ganze auch ein Beleg dafür, dass wir mit unseren umfangreichen Informations- und Sensibilisierungsbemühungen wie mit unserer Aktion „Datenschutz in meiner Arztpraxis“ offenbar bei vielen Ärzten noch auf Nachholbedarf treffen.

Was ist zu tun?
Erweisen sich Ärzte im Einzelfall im Hinblick auf ihre Pflichten zur Wahrung des Patientengeheimnisses als beratungsresistent, so muss die Staatsanwaltschaft ihren gesetzlichen Strafverfolgungspflichten nachkommen.

4.8.9 Zwischenbilanz zur Aktion „Datenschutz in meiner Arztpraxis“

So ungewöhnlich unsere Aktion, so differenziert die Reaktionen: Zurückhaltung bei vielen Ärzten, Zustimmung bei vielen Patienten und sonstigen Beteiligten – nicht nur in Schleswig-Holstein. In einem nächsten Schritt soll die Aktion auf Krankenhäuser ausgeweitet werden.

Im letzten Tätigkeitsbericht stellten wir die Aktion „Datenschutz in meiner Arztpraxis“ vor (vgl. 24. TB, Tz. 4.8.8), die wir im Berichtsjahr fortführten. Sämtlichen Ärzten und Zahnärzten in Schleswig-Holstein wurde ein „Selbstcheck“ übersandt. Anhand dieser **Checkliste** konnten sie ihre Praxis unter die Lupe nehmen: Reicht die Diskretionszone am Empfang? Kann kein wartender Patient vertrauliche Gespräche mithören? Sind die Behandlungstüren geschlossen? Befinden sich Patientenakten oder Karteikarten stets unter Verschluss? Erhält der Patient auf Anfrage Einsicht in seine Akte? Sind die Patientendaten in der EDV auch wirklich gegen den Zugriff Unberechtigter ausreichend geschützt?

Einige Ärzte stellten zwischenzeitlich infrage, ob dem Patientengeheimnis die von uns betonte Bedeutung zukommt. Dies veranlasste uns in diesem Jahr zu einer **Passantenbefragung** in der Kieler Innenstadt. Das Ergebnis war deutlich: 95 % der Befragten erklärten, dass ihnen die Sicherstellung des Patientengeheimnisses in der Arztpraxis wichtig sei. 88 % der Patienten würden sogar den Arzt wechseln, wenn sie der Meinung wären, dass das Patientengeheimnis nicht gewahrt wird. Viele Patientinnen und Patienten konnten von eigenen Erfahrungen mit Fällen ärztlicher Indiskretion berichten. Das Umfrageergebnis hat uns hinsichtlich der Notwendigkeit der Aktion „Datenschutz in meiner Arztpraxis“ bestärkt.

Die Aktion läuft auch 2003 weiter. Ständig wird unser **Informationsangebot im Internet** unter

www.datenschutzzentrum.de/medizin/arztprax/

Kurse
AR, AR-I, AR-II

erweitert. Für interessierte Ärzte und ihr Personal bietet die DATENSCHUTZAKADEMIE Schleswig-Holstein auch in diesem Jahr wieder Fortbildungen an. Zu unserer Aktion hat es bereits eine Reihe von Anfragen von Ärztekammern und Kassenärztlichen Vereinigungen aus anderen Bundesländern gegeben. Zum Teil wurden unsere Texte in den dortigen Publikationen veröffentlicht.

In einem weiteren Schritt wurden in Kooperation mit den **Berufsschulen** in Schleswig-Holstein die Auszubildenden zum Beruf der Arzthelferin mit den Problemen und Lösungsmöglichkeiten vertraut gemacht. Die Auszubildenden wurden eingeladen, ihren eigenen Arbeitsplatz nach Schwächen zu untersuchen und Vorschläge zu entwickeln, wie die Beachtung des Patientengeheimnisses optimiert werden kann.

Unsere Aktion „Datenschutz in meiner Arztpraxis“ ist zunächst nicht mehr als ein Angebot. Letztendlich muss jeder Arzt und jeder Zahnarzt selbst erkennen, wie wichtig der Datenschutz bzw. das Patientengeheimnis für ihn und für seine Patienten ist. Wir sind der Überzeugung, dass das **Vertrauen der Patienten** in die ärztliche Verschwiegenheit Grundlage für eine erfolgreiche Behandlung ist. Mit Datenschutz kann eine Arztpraxis für sich werben. Die ärztliche Schweigepflicht ist aber auch ein rechtliches Gebot, dessen Einhaltung wir im Rahmen von datenschutzrechtlichen Kontrollen überprüfen. Niemand kann davon ausgehen, dass wir durch die Aktion „Datenschutz in meiner Arztpraxis“ auf Dauer auf unsere Kontrollbefugnisse verzichten.

Was ist zu tun?
Zahnärzte und Ärzte sollten sich auch weiterhin an unserer Aktion beteiligen. Wer den Patientendatenschutz in seiner Praxis gut organisiert hat, sollte dies nicht verbergen, sondern z. B. durch den Aushang unserer Plakate oder die Aushändigung der Patientenflyer bekannt machen.

4.9 Kultur und Bildung

4.9.1 Via Internet in die Hochschulrechner

Hochschulen sind keine streng hierarchisch organisierten Betriebe. Die Freiheit von Lehre und Forschung steht im Vordergrund. Dies darf aber nicht dazu führen, dass Datensicherheitsstandards missachtet werden, sonst könnten einzelne Schwachstellen zum Einfallstor für die gesamte Hochschule werden.

Unsere Prüftätigkeit beschränkt sich in Zeiten des Internets nicht mehr darauf, den Verschluss von personenbezogenen Daten in Schränken und hinter Türen zu kontrollieren. Bei der Prüfung von Rechnern, die an öffentliche Netze angeschlossen sind, müssen wir nicht einmal vor Ort tätig sein und können über **Angriffstests von der Dienststelle aus** wichtige Erkenntnisse sammeln. Bei einer solchen Online-Kontrolle von Kieler Universitätsrechnern stießen wir auf „offene Scheunentore“. Zugangsversuche zu zwei Internet-Adressbereichen ergaben, dass 62 Rechnersysteme angeschlossen waren. Auf sechs dieser Rechner konnte ohne

eine Passworteingabe auf die Netzlaufwerke zugegriffen werden. Völlig ungeschützt und weltweit für jeden Internet-Nutzer waren so Unterlagen aus der Rechnungsprüfung (z. B. Abrechnungen mit Professoren), aus der Personalführung (z. B. Abmahnungen, Stellenpläne mit Geburts- und Verfügungsdaten), Prüfungsergebnisse, persönliche Beurteilungen, private und dienstliche E-Mails zugänglich.

Nachdem in der Universität zunächst Empörung über unsere Prüfmethode herrschte, wurden die **notwendigen Schritte** dann doch eingeleitet: Passwortprozeduren wurden eingerichtet. Die Freischaltungen wurden auf das Notwendige reduziert. Die nicht benötigten Ports bei den Rechnern wurden geschlossen. In einer Dienstanweisung wurden die Anforderungen an die Gestaltung von Passwörtern verschärft. Mit dem Rechenzentrum der Universität wurde vereinbart, die Zugriffe von außen auf die Rechner der betroffenen Fakultät zu unterbinden.

Kurse
NET, FW, NT,
WIN-I

Wir wiesen die Universität ergänzend darauf hin, dass unabhängig vom Schließen der Sicherheitslöcher in diesem Einzelfall angesichts ca. 5000 eingesetzter Rechner und ca. 80 logisch getrennter Teilnetze eine **nachhaltige Sicherheitsstrategie** zwingend erforderlich ist. Tatsächlich wurde eine Arbeitsgruppe eingerichtet, deren Aufgabe es ist, Anweisungen zum Datenschutz auf allen Ebenen, von der Leitung bis zur Anwendung, auszuarbeiten. Die nach knapp einem Jahr vorgelegten Vorschläge der CAU sind noch in starkem Maße verbesserungsbedürftig.

Was ist zu tun?
Auch in großen wissenschaftlichen Einrichtungen ist trotz aller Wünsche nach individuellen Freiheiten durch technische, aber vor allem organisatorische Maßnahmen sicherzustellen, dass die Leitung die Übersicht und die Kontrolle über die Datenverarbeitung und deren Ordnungsmäßigkeit behält. Dies gilt insbesondere bei einer Anbindung an öffentliche Netze wie z. B. das Internet.

4.9.2 Kindergartenbeiträge

Die Regelungen des Kindertagesstättengesetzes zur Gebührenermäßigung im Rahmen der Sozialstaffelung von Beiträgen führt bei den Kreisen und Gemeinden wie bei den Betroffenen offensichtlich zu Unsicherheiten.

Mehrere Eingaben zeigen, dass Kreise und kreisangehörige Gemeinden offensichtlich Schwierigkeiten bei der Umsetzung der neuen Vorschriften im Kindertagesstättengesetz zur einheitlichen Gestaltung von Sozialstaffelungen bei den Beiträgen und der damit verbundenen Datenverarbeitung haben. In einigen Kreisen war die **Konfusion über Aufgaben und Zuständigkeiten** beträchtlich.

So beantragten Eltern in einem Fall eine Gebührenermäßigung für den Kindertagesstättenbeitrag bei der kreisangehörigen Stadt. Als diese abschlägig entschied, legten die Eltern Widerspruch gegen den – wie sie meinten – Verwaltungsakt der Stadt ein. Daraufhin wurden die kompletten Antragsunterlagen, aus denen sich die Einkommens- und Vermögensverhältnisse und die Familienverhältnisse der Betroffenen ergaben, zunächst an die Kindertagesstätte selbst, von dort an den Kindertagesstättenträger und nach Protesten der Petenten letztendlich an die Kreis-

verwaltung als örtlichen Träger der öffentlichen Jugendhilfe übermittelt. Die kreisangehörige Stadt meinte gar keinen Bescheid erlassen zu haben, sondern lediglich im Auftrag des privaten Kindertagesstättenträgers zu handeln. Deshalb hatte sie den kompletten Vorgang einfach an die Kindertagesstätte weitergeleitet. Dabei berücksichtigte sie nicht, dass der Kreis den kreisangehörigen Städten mit öffentlich-rechtlichem Vertrag die Aufgabe über die Gebührenermäßigungen zugewiesen hatte, es sich also hier um eine **öffentlich-rechtliche Aufgabe** handelte. Die Daten hatten also weder beim Kindergarten selbst noch bei dessen Träger etwas zu suchen.

Was ist zu tun?
Den Jugendhilfeträgern im Lande muss klar sein, dass sie unabhängig von der Trägerschaft der Kindertagesstätte das Ermäßigungsverfahren in ihrem Zuständigkeitsbereich zu erledigen haben und damit auch ihre kreisangehörigen Gemeinden beauftragen können. Ein Vagabundieren von Sozialdaten muss vermieden werden.

4.10 Steuerverwaltung

4.10.1 Neues zur Steuerdatenabrufverordnung

Bereits vor Jahren hat der Gesetzgeber den Bundesfinanzminister aufgefordert, für automatisierte Abrufe von Steuerdaten Sicherheitsvorschriften in einer Rechtsverordnung festzulegen. Im Jahr 2003 wird die Verordnung endlich in Kraft treten. In der amtlichen Begründung wird dieser Verzug mit keinem Wort begründet. Stattdessen wird das gesamte Datenschutzrecht für den Bereich der Steuerverwaltung für nicht anwendbar erklärt.

Im Jahr 1986 ist der Schutzbereich des Steuergeheimnisses durch eine Änderung der Abgabenordnung erweitert worden. Bis dahin verbot das Steuergeheimnis lediglich, ihm unterliegende Daten Dritten gegenüber unbefugt zu offenbaren oder sie unbefugt zu verwerten. Die damalige Neuregelung im **Steuerbereinigungsgesetz** postulierte zusätzlich einen Schutz gegen den unbefugten Abruf von Daten im Rahmen automatisierter Verfahren (§ 30 Abs. 2 Nr. 3 AO). Zugleich ermächtigte der Gesetzgeber das Bundesfinanzministerium, durch eine Rechtsverordnung zu bestimmen, welche technischen und organisatorischen Maßnahmen gegen einen unbefugten Datenabruf zu treffen sind. Insbesondere sollten Regelungen getroffen werden über die Art der zum Abruf bereitgehaltenen Daten sowie über die abrufberechtigten Amtsträger.

Im Wortlaut:
§ 30 Abs. 2 Nr. 3 Abgabenordnung (AO)

Ein Amtsträger verletzt das Steuergeheimnis, wenn er ... geschützte Daten in automatisierten Verfahren abruft, wenn sie ... in einer Datei gespeichert sind.

Die ersten Entwürfe der so genannten **Steuerdatenabrufverordnung** stammten aus den 80er-Jahren und waren wegen ihrer Restriktionen aus sicherheitstechnischer Sicht durchaus vorbildlich. In dem Maße, in dem in der Verwaltung die Möglichkeiten der automatisierten Abrufverfahren erkannt wurden, regte sich der

Widerstand gegen die Art der Regulierung. Immer neue Versionen der Verordnungsentwürfe wurden erarbeitet, stets mit dem Ergebnis, dass sich das Sicherheitsniveau nach unten und die Handlungsfreiheit der Verwaltung nach oben orientierten. Als zehn Jahre nach In-Kraft-Treten der gesetzlichen Neuregelung endlich alles in „trockenen Tüchern“ schien, regte sich Protest aus den Reihen der Kommunen. Sie hatten zwischenzeitlich festgestellt, dass die Verordnung auch von ihnen zu beachten war, und sahen dies als unmöglich an. Daraufhin wurde aus der Verordnung eine Verwaltungsanweisung ausschließlich für den Bereich der Finanzämter und des Bundesamtes für Finanzen; die Kommunen bewegten sich weiter in einem regelungsfreien Raum.

Dies wäre eigentlich unproblematisch gewesen, da in den Datenschutzgesetzen der meisten Bundesländer die Einrichtung automatisierter Abrufverfahren generell nur aufgrund spezieller Rechtsverordnungen zulässig ist. Auch diese Klippe wurde jedoch „geschickt“ umschifft. Kurz und bündig stellte man seitens des Bundesfinanzministeriums fest, dass die gesamte **Abgabenordnung** „eine eigene **Datenschutzvorschrift mit abschließendem Charakter**“ sei. Auch soweit sie für ihren Anwendungsbereich keine konkreten Regelungen treffe, sei für andere Datenschutzvorschriften kein Raum. Der Hinweis der Datenschutzbeauftragten des Bundes und der Länder, dass diese sonst von niemandem geteilte Auffassung der AO-Referenten der Finanzministerien den Intensionen des Gesetzgebers ganz offenbar zuwiderlaufe und das gesamte Datenschutzrecht infrage stelle, bleibt bis heute unbeachtet.

Zurzeit liegt ein **neuer Entwurf** zur Steuerdatenabrufverordnung vor, der nach vielen „kosmetischen“ Korrekturen auch den Segen der Kommunen gefunden hat. Anfang 2003 gibt es also endlich die seit Jahren überfälligen bundeseinheitlichen bereichsspezifischen Regelungen. Sie entsprechen zwar nicht in allen Punkten den Vorstellungen der Datenschutzbeauftragten, man kann aber mit ihnen leben – wäre da nicht der Text der amtlichen Begründung, in dem völlig überflüssig und offenbar nur um die Position der Steuerverwaltung zu zementieren, der alte Rechtsstandpunkt bezüglich der Nichtanwendbarkeit des Datenschutzrechts in der Steuerverwaltung noch einmal ausdrücklich wiederholt wird.

Was ist zu tun?
Der Finanzminister sollte sich im Bundesrat der Rechtsposition des Bundesfinanzministeriums nicht anschließen. Der Wirksamkeit der Verordnung täte dieses keinen Abbruch, dem Ansehen der Steuerverwaltung stünde ein solcher Schritt gut zu Gesicht.

4.10.2 Konsequenzen aus der Steuerdatenübermittlungsverordnung

Steuerpflichtige werden ihre Steuererklärungen künftig mit der fortgeschrittenen elektronischen Signatur unterschreiben können, obwohl dies kein vollwertiger Unterschriftsersatz im Sinne des Signaturgesetzes ist. Die Steuerverwaltung meint durch flankierende Maßnahmen eine ausreichende Sicherheit gewährleisten zu können.

Die EU-Richtlinie zur Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Umsatzsteuern, die Abgabenordnung (§ 150 AO), das Einkommenssteuergesetz (§ 45 a EStG) und auch das Umsatzsteuergesetz (§ 18 a UStG) erlaubt es dem Bundesfinanzminister, durch eine Rechtsverordnung zu bestimmen, dass die Inhalte der **Steuererklärungen** von den Steuerpflichtigen auch **auf elektronischem Wege** an die Finanzämter übermittelt werden können. Was der Gesetzgeber als regelungsbedürftig ansieht, ist in der Abgabenordnung katalogmäßig dargestellt. Es sind dies

- die Voraussetzungen für die Anwendung der Verfahren,
- Näheres über die Form, den Inhalt, die Verarbeitung und die Sicherung der Daten,
- die Art und Weise der Übermittlung der Daten,
- die Zuständigkeit für die Entgegennahme der Daten,
- die Haftung von Dritten bei der unrichtigen Übermittlung oder Verarbeitung der Daten,
- der Umfang und die Form der besonderen Erklärungspflichten der Steuerpflichtigen,
- die Verweise auf die Veröffentlichung sachverständiger Stellen.

Der unübliche Konkretisierungsgrad in einer Verordnungsermächtigung hat dem Bundesfinanzministerium enge Zügel angelegt. Der Ende 2002 vorgestellte Entwurf der „**Steuerdatenübermittlungsverordnung**“ **(StDÜV)** reflektiert den vorgenannten Katalog und entspricht im Wesentlichen auch den datenschutzrechtlichen Anforderungen.

Der „zukunftsweisende“ Aspekt dieser Verordnung besteht darin, dass für elektronische Steuererklärungen statt einer an sich erforderlichen „qualifizierten elektronischen Signatur“ (umfassender Unterschriftsersatz im Sinne des Signaturgesetzes) nur die **fortgeschrittene elektronische Signatur** vorge-

> **?** ***Fortgeschrittene Signatur***
>
> *Hierbei handelt es sich um einen Begriff aus dem Signaturgesetz. Er besagt, dass eine elektronische Signatur auch auf der Basis eines Schlüssels erteilt werden kann, der nicht von einer Institution ausgegeben wurde, die durch die Regulierungsbehörde zertifiziert worden ist. Außerdem ist nicht erforderlich, dass die Signaturerstellungseinheit (z. B. das Chipkartenterminal) sehr hohen Sicherheitsanforderungen genügt. Die fortgeschrittene Signatur wurde geschaffen, um auch bei rechtlich und wirtschaftlich nicht so gravierenden Geschäftsvorfällen elektronisch unterschreiben zu können.*

schrieben wird. Diese Entscheidung soll demnächst durch eine Neuregelung an anderer Stelle in der Abgabenordnung legitimiert werden. Sie wird u. a. damit begründet, dass die bei einer qualifizierten elektronischen Signatur erforderliche kostenpflichtige Einschaltung einer Zertifizierungsstelle sowie die unzureichende Verbreitung und Nutzung der dafür erforderlichen Signaturerstellungseinheit zumindest in der nahen Zukunft einen zügigen Ausbau der elektronischen Kommunikation zwischen den Steuerpflichtigen und der Steuerverwaltung behindern würde. Neben den Signaturen der qualifizierten Trustcenter sollen auch die z. B. durch Banken und Arbeitgeber herausgegebenen Signaturen genutzt werden können. Welche Anforderungen des Signaturgesetzes in diesen Fällen nicht erfüllt werden müssen, wird in der geplanten Verordnung akribisch festgelegt. Das Bundesfinanzministerium meint, dass die Verwendung derartiger fortgeschrittener Signaturen trotzdem „für eine Übergangszeit technisch weitgehend die gleichen Sicherheiten bieten wie die qualifizierten Signaturen“.

Ob diese Verfahrensweise die Verfügbarkeit, die Integrität und insbesondere die Vertraulichkeit der elektronischen Kommunikation zwischen den Steuerpflichtigen und den Finanzämtern hinreichend gewährleistet, wird sich zeigen. Besonders gravierend ist, dass durch diese Verordnung die fortgeschrittene elektronische Signatur in einem der größten Verwaltungsbereiche zum „**Industriestandard**“ gemacht wird. Wer als Zertifikatsanbieter die Bedingungen der Steuerdatenübermittlungsverordnung erfüllt, bekommt praktisch einen „Ritterschlag“, der ihn qualifiziert, auch in anderen, im Hinblick auf die Sensibilität der Daten möglicherweise weniger bedeutsamen Verwaltungsbereichen eingesetzt zu werden. Es dürfte an der Zeit sein, in einer umfassenden Sicherheitsanalyse zu ermitteln, welche Konsequenzen sich für Wirtschaft und Verwaltung ergeben, wenn die fortgeschrittene elektronische Signatur auf der Basis einer Vielzahl „privater“ Zertifikate zum Standard und die qualifizierte Signatur zum Exoten wird bzw. in der Versenkung der Kostenvermeidung verschwindet.

Was ist zu tun?
Die Verwaltung, die Wirtschaft, die Software- sowie die Zertifikatsanbieter, die Datenschutzbeauftragten und das Bundesamt für Sicherheit in der Informationstechnik sollten gemeinsam analysieren, ob und gegebenenfalls unter welchen Bedingungen das Sicherheitsniveau der fortgeschrittenen elektronischen Signatur künftig als ausreichend anzusehen ist.

4.10.3 ELSTER soll sicherer werden

Mängel in einer Software, die bundesweit in der Steuerverwaltung eingesetzt wird, können rechtlich und sicherheitstechnisch gravierende Folgen haben. Vor ihrem Echteinsatz sind daher ganz besonders sorgfältige Tests durchzuführen. Wenn nicht jedes Bundesland eigene Prüfungen vornehmen soll, bedarf es hierfür einer bundeseinheitlichen Infrastruktur und entsprechender Audit- und Zertifizierungsprozeduren.

Als im März 2001 die Stiftung Warentest eine Sicherheitslücke in dem Verfahren ELSTER, mit dem man seine Steuererklärungen auf elektronischem Wege über das Internet bei seinem Finanzamt abgeben kann, entdeckte (vgl. 24. TB, Tz. 4.10.2),

standen die Länderfinanzbehörden ziemlich ratlos da. Sie empfingen die für sie bestimmten Datensätze zwar über eine **Clearingstelle in München**, die systemtechnischen Details des Verfahrens waren ihnen jedoch nicht bekannt. Es ist von der bayerischen Steuerverwaltung entwickelt und den anderen Ländern zur Verfügung gestellt worden. Diese haben sich, ohne selbst zu prüfen, auf die Korrektheit der Software und die Sicherheit bei deren Verteilung verlassen, nach der Devise: „Was für Bayern gut ist, kann für uns nicht schlecht sein." Der Fehler wurde schleunigst behoben. Neue Schwachstellen wurden bislang nicht entdeckt, obwohl zwischenzeitlich weit mehr als eine Million Steuererklärungen und 12 Millionen Steueranmeldungen elektronisch abgegeben wurden. So könnte es eigentlich nur positiv bewertet werden, dass das bestehende Grundmodul um neue Komponenten und Funktionen erweitert werden soll.

Zunächst soll eine **elektronische Lohnsteuerkarte** eingeführt werden. Die Arbeitgeber vermerken dabei nicht mehr die Daten über das Bruttoeinkommen, die einbehaltenen Steuern und die Zeitdauer des Arbeitsverhältnisses auf der Rückseite der Karteikarte, sondern übermitteln diese Daten direkt an das zuständige Finanzamt, das sie bei der Abgabe der Steuererklärung durch den Arbeitnehmer automatisch berücksichtigt. Dazu bedarf es natürlich eines unverwechselbaren Ordnungsbegriffes für jeden Arbeitnehmer, der aus bestimmten Teilen des Namens, des Geburtsdatums und des Wohn- und Geburtsortes gebildet wird. Außerdem braucht man eine technische Infrastruktur, an die die Planer u. a. folgende Anforderungen stellen:

- höchste Datensicherheit,
- systemunabhängige Client-Software,
- elektronische Signatur,
- optimale Lastverteilung,
- zentrale Datenverfolgung,
- revisionssichere Ablage und Archivierung und
- einheitliche Schnittstellen.

Darüber hinaus wird in der Steuerverwaltung an der Umsetzung der elektronischen Signatur unter Verwendung von beliebigen Signaturkomponenten gearbeitet. Hierzu wird ein Verfahren entwickelt, welches dynamisch die beim Anwender installierten **Signaturkomponenten** erkennt und verwendet. Seit Juli 2002 ermöglichen es mehrere große Banken und Sparkassen, deren Signaturkarte auch bei ELSTER einzusetzen. Einer raschen Verbreitung der elektronischen Signatur für die elektronische Steuererklärung steht dann nichts mehr im Wege (vgl. auch Tz. 4.10.2).

Ein weiterer zentraler Punkt ist die Schaffung von Online-Diensten über das Internet. Vorgesehen sind die Möglichkeiten der Online-Steuerkontoabfrage und die Abfrage des Bearbeitungszustandes der Steuererklärung. Schließlich zeichnet sich die Schaffung eines zentralen und unveränderbaren **Identitätskennzeichen** für alle steuerlich relevanten Personen ab. Ähnlich wie im Bereich der Wirtschaftsverwaltung (vgl. Tz. 4.6) gäbe es dann auch in den Besteuerungsverfahren

ein Personenkennzeichen, das die Verknüpfung aller elektronischen Datenbestände, die zu einer Person angelegt worden sind, ermöglicht.

Zurzeit ist allerdings noch ungeklärt, wer all diese bundesweit eingesetzten Projekte entwickelt, sie testet und zum Einsatz freigibt. Obwohl mit der FISCUS-GmbH ein zentrales Softwarehaus der Steuerverwaltungen des Bundes und der Länder gegründet worden ist, laufen, wie bei dem Verfahren ELSTER, parallel auch weiterhin Länderentwicklungen. Auch ist noch unklar, ob die **FISCUS-GmbH** ihre Produkte eigenständig entwickelt und auf dem Markt anbietet oder ob sie nur Auftragsentwicklungen tätigt. In diesem Fall stellt sich die Frage, wer Auftraggeber und Abnehmer der Software ist. Eine entsprechende „Infrastruktur" auf Bundes- und Länderebene ist jedenfalls noch nicht geschaffen. Sie ist allerdings Voraussetzung für die Gewährleistung eines hinreichenden Standards für Datenschutz und Datensicherheit auf Produktebene sowie für die gebotene Transparenz der entsprechenden Funktionen für die Behörden, die die Produkte in der täglichen Praxis handhaben.

Was ist zu tun?
Die Landesregierung sollte sich für eine steuerrechtliche und datenschutzrechtliche Auditierung und Zertifizierung aller Softwareprodukte einsetzen, die für den bundesweiten Einsatz konzipiert werden.

4.10.4 Irritationen über die öffentliche Nutzung der Steuernummern

Kleine Ursache, große Wirkung – diese Aussage passt im besonderen Maße zu einer neuen Regelung im Umsatzsteuergesetz, nach der Unternehmer ihre Steuernummer auf den Rechnungen zu vermerken haben. Die Finanzämter müssen bei Auskunftserteilungen viel vorsichtiger sein als bisher. Die Steuerpflichtigen sind trotzdem besorgt, dass das Steuergeheimnis nicht mehr so sicher ist wie bisher. Außerdem bestehen Zweifel, ob das Ziel der Maßnahme überhaupt erreicht wird.

> ***Im Wortlaut:***
> ***§ 14 Abs. 1 a Umsatzsteuergesetz***
>
> *Der leistende Unternehmer hat in der Rechnung die ihm vom Finanzamt erteilte Steuernummer anzugeben.*

Steuernummern waren einerseits nie geheim, sie wurden aber andererseits auch nicht veröffentlicht. Teilweise konnte man aus ihnen nämlich Rückschlüsse auf steuerliche Verhältnisse ziehen. Fälle mit bestimmten Besteuerungstatbeständen waren in **abgegrenzten Nummernkreisen** zusammengefasst, sodass jemand, der einer solchen Gruppe angehörte, aus dem Wissen um seine eigene Steuernummer Rückschlüsse ziehen konnte, wenn ihm die Steuernummer einer anderen Person mit gleichen Merkmalen bekannt wurde. Deshalb ist die Steuernummer auch nicht im Anschriftenfeld eines Briefes des Finanzamtes sichtbar, obwohl Rückläufe leichter der absendenden Stelle innerhalb des Finanzamtes zuzuordnen wären. Bis zu einem gewissen Grad wurde die Steuernummer als Identitätsnachweis bei telefonischen Anfragen bei einem Finanzamt genutzt. Dies muss seit Mitte 2002 der Vergangenheit angehören. Das Umsatzsteuergesetz verpflichtet den Rechnungssteller, seine **Steuernummer** auf der Rechnung anzugeben. Damit ist sie ebenso **öffentlich** wie die Telefonnummer und die Kontoverbindung.

Ziel dieser Maßnahme ist es, Steuerhinterziehungen durch Manipulationen beim Vorsteuerabzug zu erschweren. Im Ergebnis sollen Scheinrechnungen dadurch aufgedeckt werden, dass bei Überprüfungen im Bereich des Rechnungsempfängers anhand der Steuernummer die Existenz und die korrekte Besteuerung des Rechnungsstellers überprüft wird. Es bestehen bei Fachleuten zwar erhebliche Zweifel, ob dies ein praktikables Verfahren ist. Die gesetzliche Regelung ist gleichwohl bindend.

Bei den Steuerpflichtigen haben die Zweifel an der Sinnhaftigkeit der Regelung und die Furcht vor dem Missbrauch der nunmehr öffentlichen Steuernummer zu Irritationen geführt, die sich in einer Vielzahl von schriftlichen und mündlichen Anfragen niederschlugen. Auf die Frage, ob durch die Maßnahme tatsächlich Fälle der Steuerhinterziehung aufgedeckt werden, konnten wir keine Antwort geben. Zu der Frage des möglichen **Missbrauchs** haben wir uns allerdings von der Oberfinanzdirektion bestätigen lassen, dass die Finanzämter angewiesen sind, künftig keinerlei Auskünfte zu erteilen, wenn als Authentifikationsmerkmal des Auskunftsersuchenden nur die Steuernummer genannt wird. Hieran scheinen sich die Mitarbeiter zu halten, obwohl es die Kommunikation mit Steuerberatern und Steuerpflichtigen im Einzelfall durchaus behindert.

Nicht ganz so eindeutig ist die Problematik mit den „sprechenden“ Steuernummern. Die **Oberfinanzdirektion** ist zwar der Auffassung, dass aufgrund der in Schleswig-Holstein für den Bereich Umsatzsteuer genutzten Systematik aus ihnen keine Informationen abgeleitet werden können, die dem Steuergeheimnis unterliegen. Man hat aber wohl eine gewisse Großzügigkeit bei den entsprechenden Überprüfungen walten lassen, denn der Verwaltungsaufwand für die Änderung tausender von Steuernummern, nur um für einige wenige „Wissende“ nicht erkennbar werden zu lassen, dass z. B. jemand beschränkt steuerpflichtig ist, erscheint ihr zu hoch. Generell kann die Steuernummer nur noch sehr begrenzt als Organisationsmittel eingesetzt werden. Hierauf haben wir die Oberfinanzdirektion und die Steuerpflichtigen hingewiesen; konkrete Missbrauchsfälle sind uns allerdings bisher nicht bekannt geworden.

Was ist zu tun?
Die Finanzämter können die Steuernummern nicht mehr als Authentifikationsmerkmal nutzen. „Sprechende“ Steuernummern müssen zügig ersetzt werden.

4.10.5 Forderungen der Datenschutzbeauftragten zur Änderung der Abgabenordnung

Die Abgabenordnung ist trotz der Regelungen über das Steuergeheimnis ein Verwaltungsverfahrensgesetz mit einem niedrigen Datenschutzniveau. Bisher hat sich die Steuerverwaltung erfolgreich gegen Änderungswünsche gewehrt. Selbst das allgemeine Datenschutzrecht hält sie im Steuerbereich nicht für anwendbar, obwohl dies dem Wortlaut des Bundesdatenschutzgesetzes und der Länderdatenschutzgesetze widerspricht.

Die Grundzüge des steuerlichen Verfahrensrechts sind in der Reichsabgabenordnung von 1919 festgelegt worden. Sie war mit vielen Änderungen und Ergänzungen fast 60 Jahre in Kraft und wurde im Jahr 1977 durch die derzeit geltende

Abgabenordnung modernisiert. Auch diese hat vielfältige Änderungen erfahren, ohne dass die **obrigkeitsstaatlich geprägte Grundstruktur** des steuerlichen Verfahrensrechts korrigiert worden ist. Dies hatte zur Folge, dass zwar das Steuergeheimnis (§ 30 AO) eine der zentralen bereichsspezifischen Datenschutzvorschriften darstellt, dass die Abgabenordnung aber das inhaltliche Spektrum des Datenschutzrechts nicht widerspiegelt. Selbst eine Ergänzung und Anpassung der Normen an das im Volkszählungsurteil manifestierte informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger ist nicht erfolgt.

Hieraus folgt, dass für viele Datenverarbeitungsprozesse in den Finanzämtern das allgemeine Datenschutzrecht anzuwenden ist. In vielen anderen Verwaltungsbereichen führt das zu keinen besonderen Schwierigkeiten. Das Datenschutzrecht wird dort als ein Bestandteil des Verwaltungsverfahrensrechts betrachtet. Die Steuerverwaltung vermochte sich diesen vom Gesetzgeber gewollten Gegebenheiten bislang nicht anzupassen. Einerseits bestreitet man generell die Gültigkeit der Datenschutzgesetze für den Anwendungsbereich der Abgabenordnung, weil alle Datenschutzfragen dort abschließend geregelt seien (vgl. Tz. 4.10.1). Andererseits sperrt man sich dagegen, die Abgabenordnung um Regelungen zu erweitern, die dem **gängigen Datenschutzstandard** entsprechen. Alle Initiativen der Datenschutzbeauftragten sind bisher im Sande verlaufen.

Dies haben sie zum Anlass genommen, den Bundesfinanzminister nunmehr **konkrete Formulierungsvorschläge** für einzelne Regelungen zu unterbreiten und diese im Detail zu begründen. In dem umfangreichen Katalog sind folgende Komplexe von besonderer Bedeutung:

- Konkretisierung der gesetzlichen Regelungen zum Umfang und zur Absicherung automatisierter Datenabrufe,
- Zweckbindung der gespeicherten Daten und Begrenzung der Speicherung von Daten für „künftige Zwecke“ (Vorratsspeicherung),
- Definition der Akteneinsichts- und Auskunftsansprüche der Steuerpflichtigen,
- Festlegung des Umfangs und der Voraussetzungen für die Erhebung, Verarbeitung und Nutzung von Daten durch Auftragnehmer (entsprechend den Regelungen im Sozialgesetzbuch X),
- Konkretisierung der Regelungen über die zwischenstaatliche Rechts- und Amtshilfe in Steuersachen,
- Klarstellung der Befugnisse zum Erstellen von Kontrollmitteilungen,
- Festlegung von Fristen für die Sperrung und Löschung von Daten,
- Schaffung einer Berichtigungspflicht von Daten, insbesondere in steuerlichen Informationssystemen (z. B. in den Bereichen „Auslandsbeziehungen“ und „Steuerfahndung“),
- Neuregelung des Schadensersatzes bei unzulässigen oder unrichtigen Datenverarbeitungsprozessen.

Das Bundesfinanzministerium hat immerhin signalisiert, dass diese Vorleistung der Datenschutzbeauftragten anerkannt wird. Es ist zu erwarten, dass es nunmehr

zu konstruktiveren Erörterungen kommen wird als in der Vergangenheit. Die Zeit der **Totalverweigerung** ist hoffentlich vorüber.

Was ist zu tun?
Die Landesregierung sollte sich im Bundesrat und in den Beratungen der AO-Referenten dafür einsetzen, dass durch die Übernahme der Vorschläge der Datenschutzbeauftragten die Abgabenordnung auf das Datenschutzniveau anderer Verwaltungsverfahrensgesetze gehoben wird.

4.10.6 Fehler bei der automatischen Identitätsprüfung

Um Doppelspeicherungen zu vermeiden, wird in den automatisierten Besteuerungsverfahren versucht, identische Personen, die in mehreren Steuerfällen von Bedeutung sind, zu erkennen und die Namens- und Adressdaten nur einmal zu speichern. Wenn dabei etwas schief geht, ist es möglich, dass Steuerbescheide einer falschen Person zugestellt werden. Das ist bei einigen Finanzämtern passiert, weil die entsprechenden Programme nicht miteinander synchronisiert waren.

Wenn jemand innerhalb weniger Tage insgesamt **acht Steuerbescheide** von drei unterschiedlichen Steuerbehörden bekommt und keiner ihn selbst, sondern andere Steuerpflichtige betrifft, dann stimmt etwas nicht. Das musste auch die Oberfinanzdirektion dem Rundfunksender gegenüber eingestehen, der Anfang 2002 diesen Sachverhalt der Öffentlichkeit darstellte. Auch wir wurden über diese eklatante Verletzung des Steuergeheimnisses informiert.

Die Ursache der Panne zu finden war schwieriger als erwartet, weil sie nicht im Bereich des „menschlichen Versagens“ lag. Vielmehr handelte es sich um einen Mangel im Zusammenspiel verschiedener Softwarekomponenten, die in den automatisierten Besteuerungsverfahren eingesetzt werden. Dazu muss man Folgendes wissen: Viele Menschen stehen in unterschiedlichen Rollen in Beziehungen zu einer Mehrzahl von Steuerfällen. Das gilt z. B. für Personen, die mehrere Autos oder Grundstücke besitzen, die als Steuerberater tätig sind oder – wie im vorliegenden Fall – von den eigentlichen Steuerpflichtigen als Zustellungsbevollmächtigte für Steuerbescheide benannt worden sind. Damit man deren Namen und Anschrift nicht etliche Male speichert, wird bei jeder Neuaufnahme einer Person programmgesteuert geprüft, ob sie schon registriert ist. Ist dies der Fall, wird bei den Daten des betreffenden Steuerobjektes **nur eine Nummer** als Verweis auf den ausgelagerten Adressdatensatz abgelegt. Das hat den Vorteil, dass Adressänderungen, einmal eingegeben, für alle Steuerfälle automatisch wirksam werden. Steht eine Person zu keinem Steuerobjekt mehr in Beziehung, wird sie im Bestand gelöscht, die Verknüpfungsnummer wird also frei. Anstatt die vielen frei gewordenen Nummern auf Dauer frei zu lassen, hat man aus Gründen eines besseren Datenbankmanagements damit begonnen, sie neu zu belegen und dabei übersehen, dass in einigen Datenbeständen noch Hinweise gespeichert waren, die nunmehr auf eine falsche Person „zielten“. Im vorliegenden Fall wurde ein „normaler“ Steuerpflichtiger fälschlicherweise zum Zustellungsvertreter mehrerer anderer Personen und bekam somit deren Steuerbescheide zugestellt.

Der Oberfinanzdirektion war dieser Effekt offensichtlich sehr peinlich, zeigte er doch auf, dass hier ein **konzeptioneller Fehler** vorlag, der zudem durch alle Tests „gerutscht“ war. Die Wiederbelegung interner Verknüpfungsmerkmale wurde unverzüglich beendet. Für eine Reihe von Konstellationen der Verwendung bereits gespeicherter Daten in anderen Fällen wurden manuelle Prüfroutinen angeordnet.

Was ist zu tun?
Die Synchronisation der verschiedenen Komponenten der automatisierten Besteuerungsverfahren und die Testprozeduren sollten optimiert werden, damit derartige Effekte künftig nicht erneut auftreten.

4.10.7 Wer trägt die Verantwortung für die Arbeit der Steuerfahnder?

Die Steuerfahnder der Finanzämter sind Diener zweier Herren. Einerseits sind sie Steuerbeamte und unterliegen damit den Weisungen der Finanzamtsvorsteher, andererseits sind sie Hilfsbeamte der Staatsanwaltschaften. Wenn bei ihrer Arbeit das Steuergeheimnis nicht ausreichend beachtet wird, ist es deshalb schwierig, die dafür Verantwortlichen zu ermitteln.

Wer einer „normalen“ Straftat verdächtigt wird, gegen den ermitteln die Polizei und die Staatsanwaltschaften. Wer dagegen in den Verdacht gerät, Steuern hinterzogen zu haben, bekommt es mit einer „**Spezialpolizei**“, der **Steuerfahndung**, zu tun. In Schleswig-Holstein sind derartige Dienststellen, in denen keine Polizisten, sondern speziell ausgebildete Steuerbeamte tätig sind, bei vier Finanzämtern eingerichtet. Ihre Aufgaben und Befugnisse werden durch § 208 AO festgelegt.

Im Wortlaut:
§ 208 Abgabenordnung (AO)

Aufgabe der Steuerfahndung ist:

Die Erforschung von Steuerstraftaten und Steuerordnungswidrigkeiten, die Ermittlung der Besteuerungsgrundlagen in den in Nr. 1 bezeichneten Fällen, die Aufdeckung und Ermittlung unbekannter Steuerfälle. Die mit der Steuerfahndung betrauten Dienststellen haben außer den Befugnissen nach § 404 S. 2 1. Halbsatz auch die Ermittlungsbefugnisse, die den Finanzämtern zustehen.

Danach haben sie eine **Doppelfunktion**: Sie haben einerseits dafür zu sorgen, dass die Besteuerungsgrundlagen richtig ermittelt und unbekannte Steuerfälle aufgedeckt werden. Insoweit werden ihr Handeln und ihre Befugnisse durch das steuerliche Verfahrensrecht (Abgabenordnung) geregelt. Andererseits haben sie auf der Grundlage der Strafprozessordnung Steuerstraftaten und Steuerordnungswidrigkeiten zu erforschen, und zwar sowohl in eigener Zuständigkeit als auch auf Weisung der Staatsanwaltschaft. Den Steuerfahndungsstellen sind nämlich auch Strafsachenstellen angegliedert, die Strafbefehle aussprechen können, ohne dass Staatsanwaltschaften und Gerichte eingeschaltet werden müssen. Hat eine Staatsanwaltschaft ein Steuerstrafverfahren eingeleitet oder von der Steuerfahndung übernommen, sind die Mitarbeiter des Finanzamtes insoweit Hilfsbeamte der Staatsanwaltschaft.

Bei den Ermittlungen der Steuerfahndungsstellen müssen im Rahmen der Datenerhebungen bei Dritten (Befragungen, schriftliche Auskunftsersuchen, Beiziehung von Unterlagen usw.) in einem gewissen Umfang steuerliche Verhältnisse offenbart werden, die grundsätzlich dem Steuergeheimnis unterliegen. Der Umfang der bekannt gegebenen Einzelheiten hat sich strikt an dem Erforderlichkeitsgrundsatz zu orientieren. Unabhängig von den notwendigen Ermittlungen zur **Abklärung eines Anfangsverdachtes** ist eine Steuerhinterziehung erst dann eine solche und nicht nur ein geschicktes Ausnutzen von Schlupflöchern im hochkomplizierten Steuerrecht, wenn der Strafbefehl oder das Urteil rechtskräftig ist. Bis dahin gilt die Unschuldsvermutung bzw. der Grundsatz „in dubio pro reo".

Die Problematik der Abgrenzung der Zuständigkeitsbereiche zeigte sich in einem Fall, in dem der Beschuldigte in zweiter Instanz von dem Vorwurf der Steuerhinterziehung **rechtskräftig freigesprochen** worden war. Als er im Rahmen des Strafverfahrens Einblick in die Ermittlungsakte erhielt, stellte er fest, dass die Steuerfahnder des Finanzamtes Datenerhebungen bei einer größeren Anzahl von Behörden und Unternehmen vorgenommen hatten und dabei in jedem Falle mitgeteilt hatten, dass gegen den Betroffenen wegen Steuerhinterziehung ermittelt werde. Dies hätte der Steuerpflichtige noch akzeptiert, nicht einverstanden war er aber damit, dass z. B. der Genehmigungsbehörde für Fluglizenzen Folgendes mitgeteilt wurde (Zitat): „Im Zuge der Ermittlungen wurde festgestellt, dass Herr ... Inhaber einer Lizenz ist, die ihn zum Führen eines Sportflugzeuges berechtigt. Herr ... macht gegenüber der Finanzbehörde geltend, aufgrund einer asthmatischen Erkrankung erwerbsunfähig zu sein. Ich möchte Sie bitten, mir mitzuteilen, ... ob die von Herrn ... angegebene, zum Erwerb einer Erwerbsunfähigkeitsrente führende Erkrankung (Asthma) den Entzug der Fluglizenz zur Folge hätte." Der Steuerpflichtige betrachtete diese Formulierung als **Denunziation**, da der Hinweis auf die Möglichkeit des Lizenzentzugs für das anhängige Steuerstrafverfahren völlig unerheblich sei. Auch in anderen Zusammenhängen habe die Steuerfahndung zu viele steuerliche Informationen über ihn preisgegeben.

Im Verlauf der Sachverhaltsaufklärung erwies sich dieser Fall als ein **Vorgang von grundsätzlicher Bedeutung**, bei dem bis heute ein Dissens zwischen der Oberfinanzdirektion und uns besteht. Bereits die Sachverhaltsaufklärung war schwierig, weil sich das Finanzamt zunächst darauf berief, nur im Auftrag der Staatsanwaltschaft gehandelt zu haben und somit datenschutzrechtlich nicht verantwortlich zu sein. Erst als die Staatsanwaltschaft uns mitteilte, dass sich aus der Ermittlungsakte keine Anhaltspunkte ergaben, ob die Nachforschungen auf eigene Initiative der Steuerfahndungsstelle oder auf Anforderung der Staatsanwaltschaften erfolgt waren, bezog das Finanzamt Position und schaltete die Oberfinanzdirektion ein. Letztlich blieb es aber bei der Feststellung (Zitat): „Die handelnden Beamten der Steuerfahndung sind in ihrer Eigenschaft als Hilfsbeamte der Staatsanwaltschaft (§ 404 AO) tätig geworden. Die Ermittlungsmaßnahmen der Steuerfahndung sind deshalb nicht dem Finanzamt, sondern der Staatsanwaltschaft zuzurechnen." Dennoch nahmen das Finanzamt und später die Oberfinanzdirektion zur Sache Stellung und hielten alle Offenbarungen der steuerlichen Verhältnisse für rechtmäßig.

Wir haben die Verfahrensweise dem Finanzamt gegenüber gleichwohl **beanstandet**, weil wir der Auffassung sind, dass

- trotz der Funktion seiner Mitarbeiter als „Hilfsbeamte der Staatsanwaltschaft" das Finanzamt für den Teilaspekt „Wahrung des Steuergeheimnisses" als im datenschutzrechtlichen Sinne verantwortliche Stelle anzusehen ist und
- im konkreten Fall die Ermittlungsmaßnahmen an sich gerechtfertigt gewesen sein mögen, in ihrem Verlauf tatsächlich aber zu viele steuerliche Verhältnisse offenbart worden sind.

Da die **Oberfinanzdirektion** den Beanstandungen widersprochen hat, ist die verfahrensrechtliche Grauzone nach wie vor nicht beseitigt. Es kann nicht befriedigen, dass für den Inhalt eines Schreibens, das den Briefkopf „Gemeinsame Steuerfahndungsstelle beim Finanzamt ..." und die Anschrift des betreffenden Finanzamtes enthält, ein Staatsanwalt und nicht der Finanzamtsvorsteher die Verantwortung tragen soll. Desgleichen ist nicht nachzuvollziehen, dass die Steuerfahndung das Steuergeheimnis in diesem Zusammenhang sehr weit ausgelegt hat, während sie Erkenntnisse über sonstige Straftaten nur dann an die Staatsanwaltschaft weitergeben darf, wenn ein zwingendes öffentliches Interesse besteht (§ 30 Abs. 4 Nr. 5 AO).

Im Wortlaut:
§ 30 Abs. 4 Nr. 5 Abgabenordnung (AO)

Die Offenbarung der ... erlangten Erkenntnisse ist zulässig, soweit für sie ein zwingendes öffentliches Interesse besteht; ein zwingendes öffentliches Interesse ist namentlich gegeben, wenn Verbrechen und vorsätzliche schwere Vergehen gegen Leib und Leben oder gegen den Staat und seine Einrichtungen verfolgt werden oder verfolgt werden sollen oder wenn Wirtschaftsstraftaten verfolgt werden und verfolgt werden sollen, die nach ihrer Begehungsweise oder wegen des Umfangs des durch sie verursachten Schadens geeignet sind, die wirtschaftliche Ordnung erheblich zu stören oder das Vertrauen der Allgemeinheit auf die Redlichkeit des geschäftlichen Verkehrs oder auf die ordnungsgemäße Arbeit der Behörden und der öffentlichen Einrichtungen erheblich zu erschüttern ...

Was ist zu tun?
Aus Gründen der Rechtssicherheit sollte das Finanzministerium den Steuerfahndungsstellen im Erlasswege klare Handlungsanweisungen zum Umgang mit dem Steuergeheimnis geben.

4.11 Personalverwaltung

4.11.1 Führung von Personalnebenakten bei einer Universität

Die Führung von doppelten Personalakten innerhalb einer Behörde verletzt die Rechte der Betroffenen. Personalnebenakten, die außerhalb der Personalabteilung geführt werden, sind in der Regel weder erforderlich, noch ist die notwendige Transparenz gegenüber dem Betroffenen gewährleistet. Daneben wird häufig auch die besondere Vertraulichkeit von Personalaktendaten verletzt.

Auf entsprechende Hinweise von Betroffenen haben wir festgestellt, dass im Büro des Verwaltungsleiters eines Fachbereiches der Christian-Albrechts-Universität zu Kiel über alle Mitarbeiterinnen und Mitarbeiter eine **doppelte Personalakte** geführt wurde. Darüber hinaus waren auch über bereits ausgeschiedene Mitarbeiter noch Akten vorhanden. Ein Hinweis auf diese Akten war in den Personalgrundakten der Personalabteilung nicht enthalten. Tatsächlich benötigte der Verwaltungsleiter für seine Aufgabenerfüllung nur wenige aktuelle Personalaktendaten wie z. B. Name, Anschrift, Geburtsdatum und Vergütungsgruppe.

Nach dem Personalaktenrecht dürfen **Personalnebenakten** nur geführt werden, wenn die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist oder wenn mehrere personalverwaltende Behörden für einen Mitarbeiter zuständig sind; sie dürfen nur solche Unterlagen enthalten, deren Kenntnis zur rechtmäßigen Aufgabenerledigung der betroffenen Behörde erforderlich ist. Als Nebenakten werden solche Unterlagen bezeichnet, die sich auch in der Grundakte oder in Teilakten befinden.

Bei der **Fachabteilung der Universität** handelte es sich um eine unselbstständige Organisationseinheit der Behörde. In einem solchen Fall ist die Führung von doppelten Personalakten unzulässig. Wie der vorliegende Fall zudem gezeigt hat, war im Fachbereich weder eine ausreichende vertrauliche Behandlung der Personalakten gewährleistet, noch war für die Mitarbeiter hinreichend transparent, dass solche Akten über sie geführt wurden. Die festgestellten Verstöße wurden deshalb von uns beanstandet. Nach Mitteilung der Universität wurden die Akten inzwischen im von uns geforderten Umfang vernichtet. Darüber hinaus wurden auch die anderen Fachabteilungen auf die bestehende Rechtslage hingewiesen.

Was ist zu tun?
Behörden müssen dafür Sorge tragen, dass bei ihnen keine doppelten Personalakten geführt werden. Die Fachbereiche sollten auf die Rechtslage in einer schriftlichen Weisung ausdrücklich hingewiesen werden.

Schleswig-Holstein DATENSCHUTZAKADEMIE
Kurse P, PA

4.11.2 Weitergabe von Personalakten im Rahmen eines Betriebsüberganges

Werden öffentliche Unternehmungen privatisiert, geht auch das Eigentum an den vorhandenen Personalakten der Mitarbeiter auf die private Stelle über. Voraussetzung ist allerdings, dass der Inhalt der Akten dem geltenden Personalaktenrecht entspricht.

Eine Stadt beabsichtigte, ihr städtisches Freibad im Zuge der geplanten Privatisierung einer **Betriebsführungs-GmbH** zu übertragen. Mehrheitsgesellschafter sollte die Stadt sein. In diesem Zusammenhang wurde die Frage an uns gerichtet, wie mit den vorhandenen Personalakten der Bediensteten zu verfahren sei.

Ein solcher Betriebsübergang richtet sich nach den Vorschriften des Bürgerlichen Gesetzbuches (BGB). Danach tritt der Rechtsnachfolger in die Rechte und Pflichten aus den im Zeitpunkt des Überganges bestehenden Arbeitsverhältnissen ein. Sachenrechtlich waren also die Personalakten der Mitarbeiterinnen und Mitarbeiter des städtischen Freibades diesem Betrieb zuzurechnen. Mit dem **Betriebsübergang** ging auch das Eigentum an den Personalakten an die GmbH über. Sie trat als Daten verarbeitende Stelle in die bisherige Rechtsposition der Stadt ein.

Eine Rechtsvorschrift aus dem Bereich des öffentlichen Rechts, die einem solchen Übergang von Personalakten generell entgegensteht, besteht nicht. Der Inhalt der Personalakten musste lediglich daraufhin überprüft werden, ob sie Unterlagen enthielten, die aufgrund **besonderer öffentlich-rechtlicher Vorschriften** erhoben wurden (z. B. Bundeszentralregisterauskünfte für Behörden, besoldungsrechtliche Vergleichsmitteilungen nach dem Bundesbesoldungsgesetz) und damit einem speziellen den Regelungen des BGB vorgehenden Schutz unterlagen. Solche Unterlagen waren in jedem Fall zurückzuhalten.

Angesichts der besonderen Situation, die sich aus dem Betriebsübergang für die Mitarbeiter ergab, haben wir der Stadt empfohlen, dafür Sorge zu tragen, dass die Personalakten zum Zeitpunkt des Überganges den aktuellen Maßgaben des Personalaktenrechts entsprachen. Dies bedeutete insbesondere, dass die Akten **nur solche Unterlagen** enthalten durften, die auch als materielle Bestandteile der Personalakte zu qualifizieren waren, und dass die Mitarbeiter über die Möglichkeit, belastende Unterlagen auf Antrag nach Ablauf von drei Jahren entfernen und vernichten zu lassen, aufgeklärt wurden. In diesem Zusammenhang lag es nahe, den Mitarbeiterinnen und Mitarbeitern vor Abgabe der Personalakten die Möglichkeit zur Einsichtnahme in ihre Personalakten einzuräumen. Die Stadt hat unseren Empfehlungen entsprochen.

Was ist zu tun?
Im Falle einer Privatisierung öffentlicher Unternehmungen sollten vorhandene Personalakten vor Abgabe an die private Stelle nach den Maßgaben des Personalaktenrechts überprüft werden. Die Mitarbeiterinnen und Mitarbeiter sollten aus diesem Anlass nochmals über die ihnen zustehenden Rechte aufgeklärt werden.

4.11.3 Verarbeitung von Zeiterfassungsdaten

Auch die Daten über die Arbeitszeiterfassung der Mitarbeiter gehören zu den besonders geschützten Personalaktendaten. Sie sind vertraulich zu behandeln und vor unbefugter Einsicht zu schützen. Fachvorgesetzte dürfen solche Daten allerdings für Zwecke einer Plausibilitätsprüfung zur Kenntnis erhalten.

Bei einer Behörde war ein **elektronisches Zeiterfassungssystem** im Einsatz, bei dem am Ende eines jeden Monats Listen mit dem jeweiligen Stand der Zeitkonten für die einzelnen Mitarbeiter ausgedruckt und von der Personalabteilung den jeweils zuständigen Fachvorgesetzten mit der Bitte um eine Schlüssigkeitsprüfung zugeleitet wurden. Im konkreten Fall wurden die Daten von einem Fachvorgesetzten nach Prüfung nicht an die Personalabteilung zurückgegeben, sondern vor Ort so aufbewahrt, dass es anderen Mitarbeitern möglich war, diese Daten zur Kenntnis zu nehmen.

Wir haben die geprüfte Stelle darauf hingewiesen, dass es sich bei den Zeiterfassungsunterlagen um Personalaktendaten im Sinne des Landesbeamtengesetzes handelt und folglich diese Daten vor dem Zugriff Unbefugter zu schützen sind. Die Kenntnisnahme der Daten durch den **Fachvorgesetzten** ist in diesem Zusammenhang zulässig, soweit dies für eine Plausibilitätsprüfung der vom Betroffenen vorgenommenen Zeiterfassung erforderlich ist. Es muss aber dafür Sorge getragen werden, dass diese Daten bei den Fachvorgesetzten nicht dauerhaft gespeichert werden. Die geprüfte Stelle hat angekündigt, künftig entsprechend verfahren zu wollen.

Was ist zu tun?
Die Personalabteilungen in den Behörden müssen dafür Sorge tragen, dass Zeiterfassungsdaten bei der Plausibilitätsprüfung durch Fachvorgesetzte vertraulich behandelt und nach Abschluss der Prüfung vollständig an sie zurückgegeben werden.

5 Datenschutz bei den Gerichten

Namen auf Terminsbestimmungen zu Zwangsversteigerungen

Ein Amtsgericht veröffentlichte in einem Zwangsversteigerungsverfahren Name und Geburtsdatum der betroffenen Grundstückseigentümerin. Zumindest auf das Geburtsdatum soll künftig verzichtet werden.

Nach den Regelungen des Zwangsversteigerungsgesetzes (ZVG) wird für jede Zwangsversteigerung ein öffentlich bekannt zu machender Versteigerungstermin bestimmt. Die Terminsbestimmung soll auch die Bezeichnung des zur Zeit der Eintragung des Versteigerungsvermerkes eingetragenen Eigentümers enthalten. Wir haben das Amtsgericht darauf hingewiesen, dass es sich um eine reine **Ordnungsvorschrift** handelt, und angeregt zu prüfen, ob jedenfalls dann auf die Namensnennung des Eigentümers verzichtet werden kann, wenn das betreffende Grundstück auch ohne dieses Datum eindeutig identifiziert werden kann. Im Regelfall dürfte dies bereits durch die Adressangabe der Fall sein. Das Amtsgericht hat dies unter Hinweis auf die gesetzlichen Bestimmungen und den damit verfolgten Zweck, potenzielle Bieter bestmöglich zu erreichen, verneint. Immerhin wird auf die Angabe des Geburtsdatums künftig bei amtlichen Veröffentlichungen verzichtet.

Was ist zu tun?
Amtsgerichte sollten überlegen, ob die Namensangabe wirklich in jedem Fall erforderlich für eine eindeutige Identifizierung des betroffenen Grundstückes ist.

6 Datenschutz in der Wirtschaft

6.1 Werbung, die die Verbraucher nicht wollen

Den Verbrauchern ist keineswegs egal, was mit ihren Daten geschieht. Eine Umfrage belegt, dass die große Mehrheit den Adresshandel ohne Zustimmung der Kunden ablehnt.

Mehr als 80 % der Bürgerinnen und Bürger ärgern sich mehr oder weniger über unaufgefordert übersandte kommerzielle Werbezuschriften, die sie in ihren Briefkästen vorfinden. Das ergab eine Umfrage, die wir in der Fußgängerzone Kiels und auf dem Schleswig-Holstein-Tag in Bad Segeberg durchgeführt haben. Befragt wurden insgesamt 388 zufällig ausgewählte Personen. Eine **überwältigende Mehrheit** der Befragten forderte den Gesetzgeber auf, die Situation der Verbraucherinnen und Verbraucher zu verbessern. Im Einzelnen sehen die Ergebnisse wie folgt aus:

Auf die Frage: „Haben Sie sich schon einmal über an Sie adressierte **Werbesendungen in Ihrem Briefkasten** geärgert?“ wurde wie folgt geantwortet:

Ja.	270	= 69,6 %
Ja, aber nicht sehr.	56	= 14,4 %
Nein.	62	= 16,0 %

Offensichtlich wissen viele Bürgerinnen und Bürger nicht, ob und wie man sich effektiv gegen unerwünschte Werbezusendungen zur Wehr setzen kann. Zwar gaben 46,9 % der Befragten an zu wissen, wie man Werbezuschriften unterbinden kann (39,9 % nein, 13,2 % unentschieden). Aus der im Anschluss gestellten Frage ergibt sich jedoch, dass die Unsicherheit groß ist. Auf die Frage nämlich, ob bekannt sei, dass man gegen unerwünschte Werbezuschriften ein gesetzlich garantiertes **Widerspruchsrecht** hat, wurde geantwortet mit:

Ja.	111	= 29,0 %
Ja, aber ich weiß nicht, wie ich davon Gebrauch machen soll.	74	= 19,3 %
Nein, aber ich hätte gerne mehr Informationen darüber.	148	= 38,6 %
Nein, ist mir egal.	50	= 13,1 %

Von allen Befragten, die angaben zu wissen, wie man sich gegen Werbezuschriften wehrt, wusste nur knapp die Hälfte (49 %), dass es ein gesetzlich garantiertes Widerspruchsrecht gibt, immerhin 57,1 % der anderen Hälfte hatten Interesse an weitergehenden Informationen.

Die große Mehrheit der Befragten wünscht eine **Verbesserung der derzeitigen Gesetzeslage**. Auf die Frage, ob der Gesetzgeber die Verwendung der Adressdaten zu Werbezwecken künftig so regeln solle, dass zuvor der Betroffene um Einwilligung zu bitten ist, ergaben sich folgende Antworten:

Ja, Gesetzesänderung ist erforderlich.	312	= 80,6 %
Nein, kann so bleiben.	57	= 14,7 %
Ist mir egal.	18	= 4,7 %

Auffallend ist, dass sogar die Befragten, die zuvor angegeben hatten, sich nicht über unverlangt zugesandte Werbezuschriften zu ärgern, gleichwohl überwiegend die Schaffung einer Einwilligungslösung befürworteten.

Wir ziehen aus den Ergebnissen dieser Umfrage den Schluss, dass die **gegenwärtige Rechtslage**, die die Verwendung von Adressdaten für Werbezwecke erlaubt, solange der Betroffene ihr nicht widersprochen hat, für die große **Mehrzahl der Bürger unbefriedigend** ist. Der Unmut über unverlangt zugesandte Werbesendungen ist weit verbreitet. Die Verbraucherinnen und Verbraucher sehen sich regelrecht hintergangen, wenn ihre Adressen hinter ihrem Rücken weitergegeben und zur Direktwerbung genutzt werden.

Informationen über die Reaktion des Deutschen Direktmarketingverbandes auf unsere Umfrage unter

www.datenschutzzentrum.de/material/wirtscha/ddvumfra.htm

Kurs DB

Was ist zu tun?
Wir werten die Umfrageergebnisse als einen Auftrag, die Bürgerinnen und Bürger noch intensiver als bisher über ihre Schutzmöglichkeiten zu informieren. Parallel dazu sollte der Bundestag endlich das Selbstbestimmungsrecht der Verbraucher im Zusammenhang mit der Direktwerbung stärken.

6.2 Handels- und Wirtschaftsauskunfteien/Inkassowesen

Wer einen Kredit aufnehmen möchte oder Waren auf Rechnungsbasis bestellt, ahnt nicht, dass seine Vertragspartner häufig in erheblichem Umfang Informationen über seine Kreditwürdigkeit einholen. Solche **Bonitätsdaten** werden von **Handels- und Wirtschaftsauskunfteien** systematisch gesammelt, ausgewertet und Kunden auf Anfrage zur Verfügung gestellt.

6.2.1 Ergebnisse von Kontrollen

Das erhebliche Risiko, das von Auskunfteien für die Bürgerinnen und Bürger ausgeht, war Anlass, dort flächendeckend die Einhaltung von wichtigen Datenschutzvorschriften zu überprüfen. Dabei offenbarten sich teilweise erhebliche Mängel.

Kurse BDSG-I, DWBT

Nach dem Bundesdatenschutzgesetz (BDSG) müssen alle Handels- und Wirtschaftsauskunfteien die Verfahren, die sie zum Zweck der Übermittlung geschäftsmäßig verwenden, der Aufsichtsbehörde melden. Diese **Meldepflicht** dient sowohl dem betrieblichen Datenschutzbeauftragten als auch der Aufsichtsbehörde als Grundlage für Rechtmäßigkeitsprüfungen. Dementsprechend soll die Meldung

einen Überblick über die Verarbeitungsvorgänge bei der meldenden verantwortlichen Stelle ermöglichen.

Die Kontrollen haben gezeigt, dass die überprüften Stellen **überwiegend Unsicherheiten** mit der Erstellung der Meldeunterlagen hatten. So meldeten einige Auskunfteien statt einer Beschreibung der betroffenen Personengruppen die Quellen, die sie zur Datenerhebung nutzten. Nahezu sämtliche Auskunfteien gaben statt der tatsächlichen Fristen für die Löschung die gesetzlichen Bestimmungen an, nach denen sie zur Löschung verpflichtet waren.

Im Wortlaut: § 4 e Satz 1 BDSG

Inhalt der Meldepflicht:

Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind folgende Angaben zu machen:

1. *Name oder Firma der verantwortlichen Stelle,*
2. *Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,*
3. *Anschrift der verantwortlichen Stelle,*
4. *Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,*
5. *eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten und Datenkategorien,*
6. *Empfänger oder Empfängerkategorien, denen die Daten mitgeteilt werden können,*
7. *Regelfristen für die Löschung der Daten,*
8. *eine geplante Datenübermittlung in Drittstaaten,*
9. *eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.*

Bereits im 24. Tätigkeitsbericht (Tz. 6.2.6) berichteten wir über einen Einzelfall, in dem eine Auskunftei die von den Amtsgerichten herausgegebenen Listen über vorzeitige **Löschungen aus dem Schuldnerverzeichnis** (so genannte Löschlisten) nicht gesetzeskonform nach der Auswertung unverzüglich vernichtet hatte, sondern für die Dauer von drei Jahren speicherte. Die weiteren Kontrollen zeigten, dass nahezu alle anderen Auskunfteien, die die genannten Löschlisten in Papierform bezogen, auch gegen die gesetzlichen Bestimmungen verstießen. Angesichts des hohen Gefährdungspotenzials für das Persönlichkeitsrecht der Betroffenen hat der Gesetzgeber den Auskunfteien bei der Anordnung der unverzüglichen Löschung keinen Ermessensspielraum gelassen. Dass es auch richtig geht, bewies die Creditreform Kiel Isert KG, die als **einzige überprüfte Wirtschaftsauskunftei** in Papierform erhaltene Änderungsmitteilungen unverzüglich nach Auswertung der Daten vernichtete.

Die Überprüfung zeigte allerdings auch, dass sich das datenschutzrechtliche Problem der Löschlisten verlagert. Mittlerweile sind einige Amtsgerichte dazu übergegangen, die Löschungsmitteilungen auf **Diskette** zu übergeben, sodass die Beweisfunktion der schriftlichen Änderungsmitteilungen nicht mehr besteht. Damit fällt das Hauptargument der Auskunfteien für die fortdauernde Speicherung weg. Neben der oben genannten gab es weitere Auskunfteien, die aufgrund dieses Tatbestandes keine Änderungsmitteilungen mehr vorhielten. Es ist zu hoffen, dass sich deshalb das Problem der Behandlung von Löschlisten langfristig entschärfen wird.

Eine **Vorratsspeicherung zu unbestimmten Zwecken** ist **datenschutzrechtlich grundsätzlich unzulässig**. Für die Auskunfteien lässt das Datenschutzrecht ausnahmsweise eine Art geschäftsmäßige Vorratsspeicherung „zum Zwecke der Übermittlung“ zu. Eine Auskunftei darf personenbezogene Bonitätsdaten nur übermitteln, wenn der Datenempfänger zuvor ein berechtigtes Interesse an ihrer Kenntnisnahme glaubhaft dargelegt hat. Die Übermittlung von personenbezogenen Daten trotz fehlender oder unzureichender glaubhafter Darlegung eines berechtigten Interesses ist datenschutzrechtswidrig. Bereits im 24. Tätigkeitsbericht (Tz. 6.2.6) wurde bei einer Handels- und Wirtschaftsauskunftei die Verwendung von zu **unbestimmten Anfragegründen** und eine unzureichende Überprüfung des berechtigten Interesses durch die Auskunftei kritisiert. Genau diese Kritikpunkte fanden wir leider bei sämtlichen überprüften Auskunfteien vor.

Was ist zu tun?
Begriffe wie „Bonitätsprüfung“ und „Geschäftsanbahnung“ sind nichts sagend und müssen deshalb konkretisiert werden. Handels- und Wirtschaftsauskunfteien müssen auch weiterhin mit Wiederholungsprüfungen rechnen.

6.2.2 Benachrichtigung nach Aufhebung einer längerfristigen Datensperrung

Ist die Richtigkeit von gespeicherten Daten streitig, so sind sie zu sperren. Die Sperrung kann erst aufgehoben werden, wenn die Daten korrigiert sind. Über ihre Aufhebung sollte der Betroffene unterrichtet werden.

Ein Petent hatte einer Auskunftei gegenüber das Verbot ausgesprochen, seine personenbezogenen Daten an Dritte zu übermitteln. Nach seiner Auffassung waren die **gespeicherten Daten unrichtig**. Die Auskunftei hatte daraufhin ihm zugesichert, dass sein Datensatz mit sofortiger Wirkung gesperrt werden würde. Entgegen dieser Zusicherung erhielt eine Firma kurze Zeit später trotzdem eine Auskunft mit kreditrelevanten Daten über den Betroffenen. Wir haben erreicht, dass der Datensatz des Petenten tatsächlich gesperrt wurde. Die Auskunftei hat uns versichert, den Betroffenen rechtzeitig zu informieren, wenn sie diese Sperrung aufzuheben gedenkt.

Über den Einzelfall hinaus hat der Fall grundsätzliche Bedeutung. Wenn ein Betroffener die Richtigkeit der gespeicherten Daten substanziiert bestreitet, sind seine Daten zu sperren. Diese **Sperrung** stellt ein Verwertungsgebot dar, das so lange aufrechtzuerhalten ist, bis die Richtigkeit der gespeicherten personenbezogenen Daten geklärt ist. Hinzu kommt, dass der Betroffene bei einer längerfristigen Sperrung des gesamten Datensatzes nicht mehr mit einer Übermittlung durch die verantwortliche Stelle rechnen muss. Eine „heimliche“ Aufhebung der Sperrung dieser Daten verstößt gegen das Datenschutzrecht.

Deshalb haben wir von der Auskunftei verlangt, in den Fällen der längerfristigen Sperrung eines gesamten Datensatzes die jeweils **Betroffenen künftig** generell vor der geplanten Aufhebung der Sperrung zu **benachrichtigen**, um ihnen die Prüfung zu ermöglichen, ob die gespeicherten Daten richtig sind. Die Auskunftei hat eine Überprüfung dieses Vorschlages auf Verbandsebene zugesichert; eine Reaktion des Verbandes steht noch aus.

Was ist zu tun?
Macht ein Betroffener begründet geltend, dass seine bei einer Auskunftei gespeicherten Daten unrichtig sind, und wird sein Datensatz deshalb längerfristig gesperrt, haben die Auskunfteien den Betroffenen zeitlich vor der geplanten Aufhebung zu benachrichtigen.

6.3 Industrie, Handel, Handwerk

6.3.1 Abberufung eines betrieblichen Datenschutzbeauftragten

Der kaufmännische und Personalleiter eines Betriebes nahm zusätzlich auch die Funktion des Datenschutzbeauftragten wahr. Er konnte wegen der zu erwartenden Interessenkollisionen nicht als unabhängiger Kontrolleur im Amt bleiben.

Die Aufsichtsbehörde für den Datenschutz kann die Abberufung eines Beauftragten für den Datenschutz verlangen, wenn dieser die zur Erfüllung seiner Aufgaben erforderliche **Fachkunde** und **Zuverlässigkeit** nicht besitzt. Die Funktion des betrieblichen Datenschutzbeauftragten besteht darin, auf die Einhaltung der datenschutzrechtlichen Bestimmungen durch die Geschäftsführung hinzuwirken. Eine effektive Kontrolle ist jedoch dann nicht gegeben, wenn der Kontrolleur sich selbst kontrollieren müsste. Das ist typischerweise bei Personen der Fall, die Aufgaben der Geschäftsführung wahrnehmen. Dementsprechend sieht das Bundesdatenschutzgesetz vor, dass der Beauftragte für den Datenschutz **dem Leiter** der nichtöffentlichen Stelle **unmittelbar zu unterstellen** ist. Dies bedeutet im Umkehrschluss, dass Personen, die innerhalb der Stelle eine Geschäftsleitungsfunktion wahrnehmen, nicht für die Bestellung eines betrieblichen Datenschutzbeauftragten in Betracht kommen. Darüber hinaus sind bei Personen mit Leitungsfunktionen erhebliche Interessenkollisionen zu befürchten.

Wie das Unternehmen selbst darlegte, beeinflusste der betreffende Datenschutzbeauftragte als kaufmännischer Leiter nahezu sämtliche Geschäftsvorgänge des Hauses. Damit mochte eine effektive datenschutzrechtliche Kontrolle der Arbeitnehmer stattfinden, es bestand jedoch zugleich die Gefahr, dass **eine Kontrolle der Firmenleitung selbst nicht** stattfand. Diese Kontrollaufgabe hat das BDSG für den betrieblichen Datenschutzbeauftragten aber vor allem vorgesehen. Das Unternehmen kam unserem Abberufungsverlangen zuvor und berief einen geeigneteren Datenschutzbeauftragten.

Was ist zu tun?
Geschäftsführer oder Personalleiter können nicht die Funktion des betrieblichen Datenschutzbeauftragten ausüben, weil aufgrund der Interessenkollisionen eine effektive Kontrolle im betrieblichen Datenschutzmanagement fraglich ist.

6.3.2 Offene Weitergabe von Lohnsteuerkarten durch Arbeitgeber

Auch innerhalb der Betriebe dürfen Personaldaten nicht unbefugten Personen zugänglich gemacht werden.

Verschiedene Eingaben betrafen den Umgang mit Lohn- und Gehaltsabrechnungen, insbesondere dann, wenn die Unternehmen die Lohnbuchhaltung durch Dritte abwickeln lassen. So waren z. B. die **Lohnsteuerkarten** in einigen Betrieben einer Büroangestellten ausgehändigt worden, die dann die Verteilung der Karten erledigte. Da sich die Lohnsteuerkarten nicht in geschlossenen Kuverts befanden, konnte sie die Steuerdaten der betroffenen Beschäftigten ohne weiteres zur Kenntnis nehmen.

Es versteht sich von selbst, dass die Höhe des Gehalts andere Kolleginnen und Kollegen nichts angeht. Auf unsere **Beanstandungen** hin versicherten die betroffenen Unternehmen, die Lohnsteuerkarten künftig in verschlossenen Umschlägen an die Betroffenen weiterzuleiten.

Was ist zu tun?
Ausgefüllte Lohnsteuerkarten gehören in einen geschlossenen Umschlag, bevor sie an Dritte ausgehändigt werden!

6.3.3 Zirkulation von Personaldaten im Weltkonzern

Die einzelnen Teile eines Konzernes gelten datenschutzrechtlich als selbstständige Unternehmen, auch dann, wenn sie technisch ein einheitliches Personalinformationssystem betreiben.

Ein ausgeschiedener Mitarbeiter eines Unternehmens war erbost, als er in Erfahrung brachte, was sein ehemaliger Arbeitgeber über ihn in seiner Personaldatei gespeichert hatte. Wegen schwacher Arbeitsleistung sei er nicht zur Wiedereinstellung geeignet. Das Arbeitszeugnis des Betroffenen besagte hingegen, dass seine Leistungen gut bis zufrieden stellend einzuschätzen seien. Besonders problematisch war die Speicherung, weil die verantwortliche Stelle das Tochterunternehmen eines weltweit operierenden Konzerns ist. Die Informationen wurden im Rahmen des **Personalinformationssystems** auch an die **Konzernmuttergesellschaft in den USA** und an andere Stellen in Drittstaaten übermittelt. Für eine solche Übermittlung gab es keine Rechtsgrundlage. Auch gesetzliche Ausnahmegründe, welche die Übermittlung von personenbezogenen Informationen über den Betroffenen rechtfertigen könnten, waren nicht gegeben.

Wir haben die **Praxis** des Unternehmens **beanstandet** und es aufgefordert, dafür Sorge zu tragen, dass die unzulässig übermittelten personenbezogenen Daten des Betroffenen bei sämtlichen ausländischen Stellen des Konzerns zeitnah gelöscht werden. Dies wurde uns zugesichert. Der Vorfall spiegelt die Schwierigkeiten mancher Konzernunternehmen wider, die rechtlichen Rahmenbedingungen für die Übermittlung von personenbezogenen Daten einzuhalten. Dabei mag es nachvollziehbar sein, dass andere Konzernunternehmen einen bequemeren Datenzugriff

wünschen. Datenschutzrechtlich ist dies jedoch nicht zulässig. Entscheidet ein Konzern, sich in rechtlich eigenständige Stellen zu untergliedern, muss er auch die rechtlichen Folgen tragen. Datenübermittlungen zwischen den Konzernteilen sind nicht anders zu beurteilen als zwischen selbstständigen Unternehmen.

Was ist zu tun?
Konzernunternehmen haben bei der Übermittlung von personenbezogenen Daten an andere Unternehmen ihres Konzerns die gleichen Rechtmäßigkeitsbedingungen zu beachten wie bei der Datenübermittlung an dritte Stellen.

6.3.4 Was nicht in Personalfragebögen stehen darf

Die in einem Personalfragebogen zulässigen Fragen sind bereits seit geraumer Zeit durch die Rechtsprechung festgelegt worden. Auf vielen Fragebögen finden sich allerdings nach wie vor unzulässige Fragen.

Mehrere Eingaben und ein Zufallsfund im Internet führten dazu, dass wir uns eingehender mit der Frage befassten, welche personenbezogenen Daten im Rahmen eines so genannten **Personalfragebogens** erhoben werden dürfen. Hierzu gibt es eine Fülle von arbeitsgerichtlicher Rechtsprechung, die von Unternehmen leider nicht immer beachtet wird. Hier einige Beispiele:

- Die Frage nach dem **Gesundheitszustand** des Bewerbers ist nicht generell unzulässig. Gerade in einem Fall der Bewerbung als Koch war diese Frage nicht zu kritisieren. Dabei sind insbesondere in einer Großküche die erforderliche Hygiene und die Gefahr der Infizierung der übrigen Belegschaft zu berücksichtigen.
- Fragen nach dem Verlauf des vorherigen bzw. nach dem Bestehen eines gegenwärtigen Arbeitsverhältnisses werden von der Rechtsprechung als zulässig erachtet. Konkrete Fragen nach den Modalitäten der Kündigung des **letzten Arbeitsverhältnisses** sowie nach dem Grund des Stellenwechsels sind hingegen nicht zulässig.
- Die Frage nach einer bestehenden **Schwangerschaft** muss von einer Bewerberin nur in seltenen Ausnahmefällen beantwortet werden, z. B. wenn eine befristete Tätigkeit erhebliche gesundheitliche Auswirkungen auf die Schwangere haben würde.
- Die Zulässigkeit der Frage nach der **finanziellen Situation des Bewerbers** (z. B. Gehalt in der letzten Stellung, Darlehensverpflichtungen oder Gehaltspfändungen) ist abhängig von der Art des Arbeitsplatzes, um den es bei der Bewerbung geht. Nur wenn die finanzielle Zuverlässigkeit für die konkrete Tätigkeit eine Rolle spielt (z. B. als Kassierer oder Geldbote), ist die Frage zu akzeptieren.

In den meisten Problemfällen haben wir nach dem bestehenden BDSG leider keine direkten Einwirkungsmöglichkeiten, wenn die in den Personalfragebögen erfassten Informationen nicht in der EDV oder in einer nichtautomatisierten Datei gespeichert werden.

Was ist zu tun?
Die Arbeitgeber müssen diese Grundsätze bei Personaleinstellungen beachten.

6.3.5 Kontrolle der Internet-Nutzung durch den Arbeitgeber

Wenn ein Arbeitgeber seinen Beschäftigten die Nutzung des Internets nur zu dienstlichen Zwecken erlaubt, darf er grundsätzlich die Korrektheit der Internet-Nutzung stichprobenartig überprüfen. Ist die Internet-Kontrolle durch eine Betriebsvereinbarung geregelt, ist der Arbeitgeber an deren Vorgaben gebunden. Bei allen Kontrollen der Internet-Nutzung ist der Datenschutzbeauftragte zu beteiligen.

Mehrere Mitarbeiter eines Unternehmens wandten sich an uns, weil der Arbeitgeber die Internet-Nutzung regelmäßig kontrolliert hatte, obwohl eine **Betriebsvereinbarung** hierfür eine Kontrolle nur bei konkreten Verdachtsfällen gestattete. Dabei wurde die Firewall des Unternehmens auf angewählte Internet-Seiten mit pornografischen Inhalten und auf Internet-Auktionsseiten überprüft. Die betroffenen Nutzer wurden über die Identifizierung der IP-Adressen der Arbeitsplatzrechner ermittelt.

Unsere Ermittlungen ergaben, dass die Unternehmensleitung aufgrund von Hinweisen des Betriebsrates tätig geworden war. Bei diesem hatten sich einige Mitarbeiter beschwert, dass sich Kollegen während der Pausen pornografische Internet-Seiten ansehen würden. Geschäftsführung und Betriebsrat hoben mithilfe von so genannten „**Anlassvereinbarungen**“ den Schutz der Betriebsvereinbarung rückwirkend auf und schlossen dabei auch die Mitwirkung des Datenschutzbeauftragten aus.

Soweit dabei Nutzer ermittelt wurden, die pornografische Seiten besucht hatten, war dies von der Betriebsvereinbarung gedeckt, weil konkrete Hinweise für Missbräuche vorlagen. Im Übrigen haben wir die **Vorgehensweise** des Unternehmens als rechtswidrig **beanstandet**:

- Die **Kontrollbefugnisse des Datenschutzbeauftragten** sind gesetzlich festgelegt und unterliegen nicht der Disposition des Unternehmens und des Betriebsrates. Die so genannten „Anlassvereinbarungen“ widersprachen diesen gesetzlichen Befugnissen des Datenschutzbeauftragten.
- Soweit die Kontrollen den Besuch von Internet-Auktionsseiten betrafen, hatte der Arbeitgeber keinen konkreten Anlass zur Kontrolle. Die Tatsache der Nutzung von Internet-Auktionsseiten wurde erst durch das systematische Auswerten der Firewall ermittelt; vor dieser Kontrolle lag kein Verdacht gegen Mitarbeiter vor. Derartige **rasterfahndungsähnliche Ermittlungsmethoden** sollte die Betriebsvereinbarung ausschließen. Die rückwirkende Aufhebung der Betriebsvereinbarung bedeutete einen Verstoß gegen Grundsätze des Vertrauensschutzes.

Obwohl das betreffende Unternehmen unsere Rechtsauffassung nicht in allen Punkten teilte, hat es zugesichert, bei Kontrollen der betrieblichen Internet-Nutzung künftig seinen Datenschutzbeauftragten angemessen und rechtzeitig einzubinden. Darüber hinaus strebt es eine Änderung der Betriebsvereinbarung an, um die Durchführung von Kontrollen klar und unmissverständlich zu regeln.

6.3.6 Datenübermittlungen zwischen Autohändlern und Automobilherstellern

Zur Abwicklung von Garantie- und Kulanzanträgen kann es zulässig sein, dass ein Autohaus Kundendaten an den Hersteller übermittelt.

Dem Kunden eines Autohauses war zu Ohren gekommen, dass sowohl die **Deutschland-Zentrale** in Nordrhein-Westfalen als auch die **Konzernmutter** in Frankreich ungehinderten Zugriff auf alle seine im Autohaus gespeicherten Daten hatten. Dazu zählten nicht nur Name, Geburtsdatum und Adresse, sondern auch sämtliche Fahrzeugdaten vom Kennzeichen über Fahrgestellnummer bis hin zum Tag der ersten Zulassung und Kilometerstand sowie durchgeführte Reparaturen. Auf unsere Nachfrage stellte sich heraus, dass der umfassende Zugriff des Herstellers lediglich der papierlosen Abwicklung von Garantie- und Kulanzanträgen diente, über die bekanntermaßen nicht der Händler vor Ort, sondern der Fahrzeughersteller entscheidet.

Im Endeffekt war die Übermittlung der Kundendaten datenschutzrechtlich nicht zu beanstanden, da sie noch im Rahmen der Zweckbestimmung des zwischen dem Autohaus und dem Kunden bestehenden Vertragsverhältnisses lag. Die **Abwicklung von Garantie- und Kulanzanträgen** steht in enger Beziehung mit dem Reparatur- oder Servicevertrag und liegt überdies auch im Interesse des Kunden. Allerdings haben wir dem Autohaus empfohlen, in den Allgemeinen Geschäftsbedingungen (AGB) oder in den Reparaturaufträgen auf diese Datenübermittlungen im Zusammenhang mit etwaigen Garantie- oder Kulanzleistungen hinzuweisen. Hierdurch könnte die Transparenz des eingesetzten EDV-Verfahrens für die Kunden erheblich verbessert werden. Der Hersteller kündigte an, die Allgemeinen Geschäftsbedingungen zu ändern. Es bestehe außerdem die Absicht, dem einzelnen Kunden durch eine Modifizierung der Software die Möglichkeit zu geben, seine Daten individuell sperren zu lassen.

In einem weiteren Fall übermittelte ein Autohändler über einen Autohersteller Kundendaten an ein **Callcenter**, das dann bei den betroffenen Kunden eine „Zufriedenheitsbefragung“ durchführte. Dieser aufgedrängte „Service“ erzeugte bei einigen Kunden erheblichen Ärger. Wir konnten den Autohändler davon überzeugen, dass die Formulierung einer klaren Einwilligungserklärung zur Förderung der Akzeptanz führen würde.

Was ist zu tun?
Autohändler und Automobilhersteller sollten durch entsprechende Hinweise in den vertraglichen Unterlagen für mehr Transparenz ihrer Datenflüsse sorgen. Dies dient letztendlich auch der Kundenzufriedenheit.

6.4 Kreditinstitute

6.4.1 Auch Banken haben ein Müllproblem

Vertrauliche Bankunterlagen über Kunden müssen so entsorgt werden, dass Unbefugte sie nicht zur Kenntnis nehmen können.

Auf ein Müllproblem der besonderen Art machte uns die Polizei aufmerksam. Sie fand auf einer **Mülldeponie** Ausdrucke von Rücklastschriftmitteilungen einer Bank. Unsere Ermittlungen ergaben, dass die Bank eine große Aktenvernichtungsaktion unternommen hatte. Dabei wurden Altakten in Säcke eingefüllt, die von einem externen Aktenvernichter entsorgt wurden. Ein Mitarbeiter der Bank gab allerdings mindestens eine Akte ins normale Altpapier, anstatt sie ordnungsgemäß von dem beauftragten Unternehmen abholen zu lassen.

Pikanterweise hatte wenige Tage zuvor eine **Mitarbeiterschulung** stattgefunden, die unter anderem Datenschutzbelange betraf. Ganz offenbar hatte die Schulung noch nicht die notwendige Sensibilisierung für das Thema Persönlichkeitsrechtsschutz erbracht. Wir haben die Vorgehensweise der Bank als Verstoß gegen die gesetzlichen Vertraulichkeitspflichten beanstandet und angeregt, den Vorfall in der Hauszeitschrift der Bank als abschreckendes Beispiel zu veröffentlichen.

Was ist zu tun?
Datenschutzschulungen müssen Mitarbeiter auch tatsächlich sensibilisieren und zur Anwendung von Datenschutzprinzipien im Alltag befähigen.

6.4.2 Um welche Bank geht es eigentlich?

Das Datenschutzrecht verlangt eine korrekte Bezeichnung der Daten verarbeitenden Stelle.

Einige Petenten wandten sich an uns, weil ein Konzernunternehmen gegenüber seinen Kunden unter sage und schreibe acht **verschiedenen Firmennamen** auftrat. Das Datenschutzrecht besagt jedoch, dass eine verantwortliche Stelle die Betroffenen einer Datenverarbeitung auch über ihre Identität zu unterrichten hat.

Das Problem erwies sich aufgrund einer bevorstehenden Fusion als kurzlebig. Um einerseits den Interessen der Betroffenen, andererseits die bevorstehende **Fusion** zu berücksichtigen, forderten wir von der verantwortlichen Stelle, dass sie für die Zeit der rechtlichen Selbstständigkeit in die vertraglichen Unterlagen eine konkrete Belehrung aufnahm und die Mitarbeiter die Identität ihrer Firma bis zur erfolgten Fusion ordnungsgemäß angeben sollen.

Was ist zu tun?
Auch Unternehmen, die Leistungen eines Konzernverbundes anbieten, müssen berücksichtigen, dass Kunden nach dem Datenschutzrecht einen Anspruch darauf haben zu erfahren, mit wem sie es zu tun haben.

6.5 Vereine

6.5.1 Sponsoring und Datensammeln im Vereinswesen

Vereine dürfen die Daten ihrer Mitglieder an Sponsoren nur in eingeschränktem Umfang übermitteln. Pauschale „Überlassungsverträge“ sind unzulässig.

Weit verbreitet sind Partnerschaften zwischen Sportvereinen und großen Wirtschaftsunternehmen. Die Partner erhoffen sich eine **win-win-Situation**: Die Vereine werden durch Sach- und Geldmittel in ihrer Tätigkeit unterstützt, der Sponsor erhält Gelegenheit zur Eigendarstellung und Werbung. Datenschutzrechtlich problematisch kann eine solche Partnerschaft allerdings werden, wenn der Sponsor personenbezogene Mitgliederdaten als Gegenleistung für seine Unterstützung verlangt.

Wir haben mehrere Eingaben erhalten, in denen ein Sponsorenvertrag die Übermittlung aller Mitgliederdaten an den Sponsor vorsah. Eine solche Datenübermittlung ist nur zulässig, wenn sie berechtigten Interessen des Sponsors dient und keine schutzwürdigen Interessen der Betroffenen beeinträchtigt werden. Durch eine pauschale Verpflichtung des Vereins zur Übermittlung werden bestehende **schutzwürdige Interessen** der Mitglieder **missachtet**, wenn diesen nicht zuvor Gelegenheit zum Widerspruch eingeräumt worden ist.

Auch der inhaltliche Umfang der weitergegebenen personenbezogenen Daten ging in den Beschwerdefällen über das rechtlich Erlaubte hinaus. Besonders „beliebt“ war das Verlangen nach den genauen Geburtsdaten. Verständlich wäre vielleicht noch die Mitteilung der Altersgruppe, etwa um zu beurteilen, ob die Betroffenen einer Zielgruppe des Unternehmens entsprechen. Das genaue Geburtsdatum hingegen ist jedoch ein wichtiges Identifizierungsmerkmal und oft Grundlage für umfassendere Datenprofile. Eine Weitergabe des Geburtsdatums an Sponsoren ist nur erlaubt, wenn die Betroffenen in sie **einwilligen**. In allen Fällen konnten wir datenschutzgerechte Lösungen erzielen, sei es über Einwilligungen oder über eine Beschränkung der übermittelten Datenkategorien.

Was ist zu tun?
Vereine sollten personenbezogene Mitgliederdaten schon aus Transparenzgründen nur dann an mögliche Sponsoren weitergeben, wenn die Betroffenen mit einer solchen Übermittlung einverstanden sind. Mögliche Sponsoren sollten berücksichtigen, dass regelmäßig nur dann eine Produktinformation auf Akzeptanz stößt.

6.5.2 Wettkampfergebnisse am schwarzen Brett

Die Mitteilung von Wettkampfergebnissen an Vereinsfremde ist ohne Zustimmung der Betroffenen nicht ohne weiteres zulässig. Die Vereine sollten in ihren Satzungen die Verarbeitung von Mitgliederdaten präzise und für die Mitglieder nachvollziehbar regeln.

Bei einem Sportverein war es üblich, personenbezogene Ergebnisse auch von **internen Wettkämpfen** am schwarzen Brett im Vereinsheim auszuhängen. Vielleicht hätte man damit noch leben können, aber die Räumlichkeiten wurden ab und zu zur Aufbesserung der Vereinskasse für öffentliche Veranstaltungen (z. B. Geburtstage oder Ehejubiläen) vermietet. So konnten Dritte, die nicht Vereinsmitglieder waren, von den Wettkampfergebnissen Kenntnis erhalten. Nachdem uns Beschwerden erreichten, veranlassten wir die Entfernung der Aushänge vom schwarzen Brett. Bei dieser Gelegenheit wurde zusammen mit dem Vereinsvorstand eine Datenschutzklausel formuliert, die in die Satzung des Vereins aufgenommen werden soll. Diese Klausel ist in anonymisierter Form auch auf der Homepage des ULD veröffentlicht:

www.datenschutzzentrum.de/wirtschaft/praxis.htm

In der vom Sportverein ebenfalls neu formulierten Beitrittserklärung wird künftig explizit auf diese Klausel verwiesen.

Was ist zu tun?
Vereine sollten dazu übergehen, die Verarbeitung ihrer Mitgliederdaten eindeutig zu regeln und die Mitglieder entsprechend zu informieren.

6.6 Geschäftsidee mit unerwarteten Akzeptanzproblemen

Im Rahmen von Preisausschreiben, Verlosungen u. Ä. muss bei der Datenerhebung eine ausreichende Aufklärung der Teilnehmer erfolgen.

Gleich mehrere Eingaben betrafen die Geschäftsidee eines Diskothekenbetreibers. Er hatte die Rückseite seiner **Eintrittskarten als Verlosungsschein** gestaltet. Um an der Tombola teilnehmen zu können, sollten die Teilnehmer Angaben zu Name, Beruf, Wohnadresse, Telefon, Mail und Geburtstag machen. Einige nahmen das Angebot jedoch nicht an, weil sie einen Datenmissbrauch vermuteten. Das lag insofern nahe, als der Diskothekenbetreiber seine Kundinnen und Kunden weder

Im Wortlaut: § 4 Abs. 3 S. 1 BDSG

Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. *die Identität der verantwortlichen Stelle,*
2. *die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und*
3. *die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss, zu unterrichten.*

über den Zweck der erhobenen Daten aufklärte noch eine Adresse für Rückfragen angab.

Wir haben dies als Verstoß gegen das BDSG gewertet. Die Reaktion des Betreibers erfolgte prompt: Er sagte nicht nur zu, entsprechende Eintrittskarten nicht mehr zu verwenden und künftige Verlosungen nur unter Beachtung der entsprechenden **Unterrichtungspflichten** durchzuführen, sondern teilte uns mit, dass er andere Kollegen seiner Branche über den Sachverhalt und seine rechtliche Bewertung informiert habe.

Was ist zu tun?
Bei Preisausschreiben, Verlosungen und Gewinnspielen sollten die Bürgerinnen und Bürger fair über die Verwendung ihrer personenbezogenen Daten informiert werden.

7 Systemdatenschutz

7.1 Praxisprobleme bei der Systemadministration

Nahezu alle Behörden im Land betreiben zwischenzeitlich komplexe IT-Systeme in eigener Regie und streben mutig ins Workflow-Management und E-Government. In vielen Fällen kann die Qualität der Systemadministration diesen Anforderungen nicht standhalten, weil an der Ausbildung der betreffenden Mitarbeiter gespart wird und ihre Kompetenzen nicht definiert sind.

Kaum ein sicherheitstechnisches Thema musste in den vergangenen Jahren so häufig in den Tätigkeitsberichten behandelt werden wie die Probleme im Zusammenhang mit der Systemadministration. Es ging dabei z. B. um Mängel bei der Überwachung von Fernwartungen (vgl. 20. TB, Tz. 6.7.5), um fehlende Ausbildungsmöglichkeiten für Verwaltungsinformatiker (vgl. 21. TB, Tz. 6.3), um die Grenzen des Outsourcing der Systemadministration (vgl. 23. TB, Tz. 7.2) und um die richtige aufbauorganisatorische Einbindung der Administratoren in das Verwaltungsgefüge (vgl. 24. TB, Tz. 7.5.1, 7.5.3 und 7.5.4). Trotzdem ist nicht erkennbar, dass die Praxisprobleme geringer geworden sind. Das Gegenteil ist der Fall. Vor dem Hintergrund, dass zwischenzeitlich jede auch noch so kleine Behörde ihr eigenes Client-Server-System installiert hat und sich zielstrebig auf systemtechnisch höchst anspruchsvolle Applikationen des Workflow-Management und des E-Government über das Internet zubewegt, wird bei unseren Prüfungen und Beratungen immer deutlicher, dass die **Systemadministration** eine **Achillesferse** der automatisierten Datenverarbeitung in kleinen und mittleren Verwaltungseinheiten ist.

In den meisten Behörden haben selbst die Dienststellenleiter nicht so viele Eingriffsmöglichkeiten in die Datenverarbeitungsprozesse wie die Systemadministratoren. In dem Maße, wie die personenbezogenen Datenbestände in elektronischen Dateien gespeichert werden, verfügen sie als „**Herren über die Festplatten**“ über Zugriffsmöglichkeiten auf praktisch alle Informationen einer Behörde.

Zu ihren Aufgaben gehört es zudem, die Software zu verwalten, sie zu ändern und neue Programme in das System zu integrieren. Ob die Ergebnisse der Verarbeitungsprozesse richtig oder falsch sind oder ob „Schad-Software“ (Viren, Trojaner, Würmer usw.) in das System gelangt, hängt ganz wesentlich von der korrekten Arbeitsweise der „**Softwaremanager**“ ab.

Die transaktionsgesteuerte Nutzung von IT-Systemen führt schließlich dazu, dass der Benutzerverwaltung (Anlegen von Benutzerkonten, Zuteilung von Zugriffsrechten auf Software und Daten) eine zentrale Bedeutung zukommt. Die in vielen Fällen rechtlich gebotene Abschottung bestimmter Datenverarbeitungsprozesse gegenüber anderen automatisierten Verfahren (z. B. bei der Personaldatenverarbeitung, bei Daten, die dem Arzt-, Steuer- oder Sozialgeheimnis unterliegen, bei Daten nichtöffentlicher Sitzungen kommunaler Gremien) bedingt, dass die Rechte jedes einzelnen Benutzers des IT-Systems exakt definiert sein müssen. Erteilt ein Administrator zu weit gehende Rechte, ist dies von der Behördenleitung in der Regel nicht festzustellen. Die Administratoren sind mithin auch „**Garanten der**

Vertraulichkeit“ der Datenverarbeitung. Dabei gibt es derzeit faktisch kein Betriebssystem auf dem Markt, das die Administrationsarbeiten revisionsfest protokolliert. Es können zwar vielfach umfassende Protokolle erzeugt werden, diese befinden sich aber wie alle Datenbestände in der Verfügungsgewalt der Administratoren. Eine nachträgliche verlässliche Überprüfung ihrer Arbeiten ist weder möglich, um Fehler aufzudecken, noch um im Sinne einer Entlastung ihnen die Korrektheit ihrer Maßnahmen zu bestätigen.

Es macht keinen Sinn, diese Fakten dadurch zu relativieren, dass man die persönliche Integrität der betreffenden Mitarbeiter hervorhebt und sich dagegen verwahrt, dass ihnen (vermeintlich) unlauteres Handeln unterstellt wird. Viel wichtiger ist es, ihre **Sonderstellung** offensiv zu akzeptieren und sie auch im Interesse der Betroffenen zu „entschärfen“. Dass Banktresore in der Regel nur von zwei Mitarbeitern gleichzeitig geöffnet werden können, ist kein Misstrauen, sondern ein Schutz der Bank und der Geldverwaltung.

Der **schwarze Peter** liegt eindeutig in der Hand des **Verwaltungsmanagements**. Die ständig steigenden Teilnehmerzahlen bei den Sicherheitskursen für Systemadministratoren in der DATENSCHUTZAKADEMIE machen deutlich, dass der Anteil der „freischaffenden Administrationskünstler“ rapide zurückgeht. Überwiegend treffen wir auf Mitarbeiterinnen und Mitarbeiter, die darüber klagen, dass ihr Bemühen um eine sichere und ordnungsgemäße automatisierte Datenverarbeitung durch fehlende Finanzmittel, unklare organisatorische Regelungen und zu geringe Zeitkontingente bei gleichzeitiger Erhöhung der Anforderungen durch neue Projekte konterkariert wird. Neben der Vermittlung von Fachwissen auf dem Gebiet des Systemdatenschutzes müssen wir uns daher immer häufiger mit ihrer Frage auseinander setzen: „Wie erklärt man Vorgesetzten die Sinnhaftigkeit einer effektiven Sicherheitsorganisation?“

Die Erfahrungen zeigen, dass die nachfolgenden, auf den Regelungen des Landesdatenschutzgesetzes und der Datenschutzverordnung basierenden **Grundanforderungen** an eine ordnungsgemäße Systemadministration von vielen Kursteilnehmern zwar als vernünftig, aber bezogen auf ihre Behörde als „reale Utopie“ angesehen werden:

- **Mindestens zwei** (weisungsgebundene) Mitarbeiter der Daten verarbeitenden Stelle müssen die Befähigung besitzen, die erforderlichen **Administrationsarbeiten** durchzuführen. Mindestens ein weiterer (entscheidungsbefugter) Mitarbeiter muss in der Lage sein, das Ergebnis dieser Arbeiten plausibel zu überprüfen.
- Die **Verantwortung** für die richtige Verarbeitung der personenbezogenen Daten muss in der jeweiligen Fachabteilung verbleiben. Veränderungen an der Hard- oder Software dürfen erst wirksam werden, nachdem ihre Korrektheit überprüft worden ist.
- **Aufbauorganisatorisch** ist die Systemadministration „nur“ als Dienstleistungseinrichtung für die einzelnen Fachbereiche anzusehen. Die Verantwortungsabgrenzungen sind daher in Dienstanweisungen festzulegen.

- Sofern **externe Dienstleister** die Administratoren unterstützen, ist zu gewährleisten, dass sie eigenständig keine Systemveränderungen vornehmen können.
- Die Mitarbeiter, die die Arbeit des externen Administrationsunternehmens zu überwachen haben, müssen so ausgebildet sein, dass sie stets das „**Heft des Handelns**“ in der Hand behalten. Erforderlich ist also zumindest ein Basis-Know-how. Eine Administration durch Externe (z. B. durch Fernwartung) kann daher zwar den personellen Aufwand der Daten verarbeitenden Stelle reduzieren, das Administrationsmanagement muss aber bei ihr verbleiben.
- Die Administration durch Externe darf in keinem Fall so weit gehen, dass die Daten verarbeitende Stelle nicht einmal überprüfen kann, mit welcher Software unter welchen Bedingungen welche Datenbestände angelegt werden, für wen sie verfügbar sind und welche Sicherheitsmechanismen wirken. Diese **Systemparameter** müssen durch sie auslesbar sein.

Behördenleiter unterliegen einem Irrtum, wenn sie glauben, ihre Verwaltung modernisieren, die Arbeitsabläufe effektiver gestalten und den Bürgerservice erhöhen zu können, ohne in das **IT-Wissen** ihrer Mitarbeiter zu **investieren**. Investitionen in Hard- und Software sind sicher wichtig, ihre Wirkung verpufft aber, wenn die Menschen fehlen, die ihren Einsatz sachgerecht steuern.

Was ist zu tun?
Die Investitionen in die Ausbildung von qualifizierten Systemadministratoren sind Grund- und keine Zusatzkosten. Kleine Organisationseinheiten werden nicht umhinkommen, durch Kooperation mit anderen diesen Aufwand zu reduzieren, z. B. durch Bildung von Administrationsverbünden.

7.2 Konsequenzen aus der Umstellung der Betriebssysteme

Wenn die Firma Microsoft demnächst ihr Betriebssystem Windows NT 4.0 nicht mehr unterstützt, müssen mehr als tausend Systemadministratoren der Behörden im Lande umgeschult und Sicherheitskonzepte den neuen Gegebenheiten angepasst werden. Noch ist vielen Stellen nicht klar, wie das neue Betriebssystem Windows 2000/XP sicherheitstechnisch sinnvoll zu konfigurieren ist.

Man mag die Geschäftsstrategie der Firma Microsoft bezüglich der kurzen Produktzyklen noch so sehr kritisieren. Fakt ist, dass in absehbarer Zeit alle IT-Systeme, die heute noch auf der Basis des Betriebssystems Windows NT 4.0 arbeiten, auf Windows 2000/XP oder auf Konkurrenzprodukte wie Linux oder UNIX umgestellt werden müssen. Das bedeutet, dass in der öffentlichen Verwaltung im Lande weit **mehr als tausend Systemadministratoren** umgeschult werden müssen. Dies scheint auf den ersten Blick eher ein Kosten- als ein Datenschutzproblem zu sein. Bei genauerer Betrachtung stellt sich aber heraus, dass mit der Umstellung auch eine Vielzahl von Sicherheitsproblemen verbunden ist.

Mit Ausnahme einiger Open-Source-Produkte sind alle derzeit auf dem Markt gängigen **Betriebssysteme** zum Zeitpunkt ihrer Auslieferung „**offen**“, d. h., sie offerieren ein Maximum an Funktionalität. Bisher hat sich aus Marketingüberle-

gungen noch kein Anbieter getraut, ein Betriebssystem auf dem Markt zu platzieren, dessen sicherheitskritische Funktionalitäten zunächst alle ausgeschaltet sind und von den Käufern erst entsprechend ihrer Sicherheitsanforderungen freigeschaltet werden müssen. Das gilt auch für die neuen Produkte Windows 2000 und Windows XP, die sich in sicherheitstechnischer Hinsicht nicht wesentlich unterscheiden.

Die Firma Microsoft rühmt sich zwar, dass dem Betriebssystem Windows 2000 die „Common Criteria“ Certification zuerkannt worden sei. Aus ihrer Presseverlautbarung ergibt sich, dass die Produkte Windows 2000 Professional, Server und Advanced Server jeweils mit dem Service-Pack 3 und dem Hotfix Q326886 getestet wurden. Über die **Testkriterien** schweigt sich die Firma allerdings aus. Es steht also nach wie vor die Frage im Raum, ob die Tests ergeben haben, dass das Produkt generell als hinreichend sicher anzusehen ist, oder ob lediglich die Möglichkeit besteht, durch eine geschickte Ausnutzung bestimmter Konfigurationsmöglichkeiten das erforderliche Maß an Sicherheit zu erreichen.

Die Problematik wird durch zwei Presseveröffentlichungen deutlich:

- Der Produktsicherheitschef von Microsoft wird mit den Worten zitiert: „Sicherheit ist aufwändig wie die Mondlandung ..., ich würde Trustworthy Computing mit Kennedys Versprechen gleichsetzen, Menschen auf den Mond zu senden. Beides braucht einige Zeit.“ Bei Microsoft könne es Jahre dauern.
- Auf ihren Internet-Seiten bietet die US-Spionagebehörde (NSA) einen öffentlich zugänglichen „Windows-XP-Sicherheitsguide“ an. Auf immerhin 141 Seiten werden zahlreiche Konfigurationsprofile beschrieben, die Mitarbeiter des Verteidigungsministeriums und anderer sicherheitsrelevanter US-Behörden anwenden sollen, um potenzielle Schwachstellen in XP-Systemen abzuschotten.

In der schleswig-holsteinischen Landesverwaltung müsste dieses Problem eigentlich weitgehend geklärt sein. Der von der IT-Kommission als verbindlich festgelegte **IKOTECH III-Standard** basiert nämlich auf dem Betriebssystem Windows 2000/XP. Da z. B. alle 1500 neu installierten IT-Arbeitsplätze in der Landespolizei ein hohes Sicherheitsniveau auf der Betriebssystemebene erfordern, müssten die dort festgelegten Parameter als Musterkonfiguration für andere Verwaltungsbereiche genutzt werden können. Leider ist der IKOTECH III-Standard bisher noch keiner Vorabkontrolle und keinem Sicherheitscheck unterzogen worden (vgl. auch 22. TB, Tz. 7.4, und Tz. 4.2.6 und Tz. 7.3 dieses Berichtes).

Dass die dabei zu behandelnden Fragestellungen alles andere als trivial sind, lässt sich an dem Beispiel des Verzeichnisdienstes (Active Directory Service) darstellen. Bei Windows 2000/XP handelt es sich um ein Netzwerkbetriebssystem, das alle Ressourcen miteinander verknüpft. Was sich relativ harmlos anhört, bedeutet, dass an einer Stelle, nämlich im Verzeichnisdienst, alle Dateien, **Verzeichnisse**, Softwarekomponenten, Hardwarekomponenten, aber auch alle Benutzer und ihre Zugriffsrechte zentral verwaltet werden. Es mag schon in einer kleinen Amtsverwaltung bedenklich sein, dass ein einzelner Mitarbeiter über eine solche „Machtfülle“ verfügt (vgl. Tz. 7.1 dieses Berichtes). Wenn aber alle IT-Arbeitsplätze der

Landesverwaltung unter der Regie **eines einzigen Active Directory** laufen, damit z. B. eine E-Mail-Kommunikation über Behörden- und Ressortgrenzen hinaus möglich ist, dann stellt sich die Frage, wer die Arbeit dieses Superadministrators kontrolliert, umso mehr, wenn sie durch Mitarbeiter eines externen Dienstleisters (in diesem Fall der Datenzentrale) erledigt wird.

Wie zu dem Betriebssystem Windows NT 4.0 werden wir auch zu dem Betriebssystem Windows 2000/XP im Rahmen unserer **backUP-Magazine** Handreichungen für die Praxis herausgeben (vgl. Tz. 11.2).

Was ist zu tun?
Der Innenminister als Betreiber des Verzeichnisdienstes für alle IKOTECH III-Arbeitsplätze sollte die Wirksamkeit der konfigurierten Sicherheitsparameter kurzfristig durch eine unabhängige Stelle, z. B. im Rahmen eines Behördenaudits, überprüfen lassen.

7.3 Wer beim behördlichen Datenschutzbeauftragten spart ...

Bei den Beratungen der EU-Datenschutzrichtlinie war man sich insbesondere in Deutschland einig, dass in allen Behörden und Wirtschaftsunternehmen behördliche bzw. betriebliche Datenschutzbeauftragte tätig sein sollten. Schleswig-Holsteinische Behörden, die diese Erkenntnisse bisher ignoriert und keinen Datenschutzbeauftragten bestellt haben, merken insbesondere bei den Vorabkontrollen, dass sie sich damit einen Bärendienst erweisen.

Die überwiegende Mehrzahl der Behörden im Lande hat zwischenzeitlich behördliche Datenschutzbeauftragte bestellt und fährt offensichtlich recht gut damit (vgl. 24. TB, Tz. 4.1.1, und Tz. 4.1.1 dieses Berichtes). Aber in einigen Verwaltungsbereichen und insbesondere auf der Ebene der **Ministerien** meint man nach wie vor die Kannregelung des Landesdatenschutzgesetzes in Anspruch nehmen zu sollen (vgl. 23. TB, Tz. 1.1 und Tz. 4.1.1). Sie **verzichten auf behördliche Datenschutzbeauftragte**. Das führt bei ihnen zunehmend zu „Problemlagen“, wenn automatisierte Verfahren in Betrieb genommen werden sollen, in denen besonders sensible Daten (z. B. Steuer-, Sozial-, Personal- und medizinische Daten) zu verarbeiten sind.

In diesen Fällen ist nämlich eine **Vorabkontrolle gesetzlich vorgeschrieben**. Diese wird standardmäßig von den behördlichen Datenschutzbeauftragten durchgeführt. Da diese Mitarbeiter einer Behörde in der Regel bereits während des gesamten Planungsprozesses einer Verfahrensneuentwicklung bzw. gravierenden Verfahrensänderung beteiligt werden, können sie die datenschutzrechtlichen und sicherheitstechnischen Fragestellungen sehr früh in die Überlegungen und Entscheidungen einfließen lassen. Die Vorabkontrolle stellt sich auf diese Weise als ein selbstverständlicher dynamischer Prozess für alle automatisierten Verfahren dar. Bei Verfahren, mit denen die oben angeführten „besonderen“ Datenkategorien verarbeitet werden, ist der Prüfungsaufwand für den Datenschutzbeauftragten lediglich etwas größer als bei „normalen“ automatisierten Verwaltungsabläufen.

Ist kein behördlicher Datenschutzbeauftragter bestellt, entfällt das Datenschutzfeed-back während der Entwicklungsphase. Erst kurz vor der beabsichtigten Inbetriebnahme des betreffenden Verfahrens kann die ersatzweise durch das ULD vorzunehmende Vorabkontrolle veranlasst werden. Es müssen uns dann alle Unterlagen, die das Verfahren dokumentieren, übersandt und um Erläuterungen ergänzt werden, die für das Verständnis der Abläufe erforderlich sind. Unseren Mitarbeitern sind nämlich die Einzelheiten und Hintergründe der ihnen zur Vorabkontrolle vorgelegten Verfahren nicht bekannt. Dies führt in der Regel zu **zeit-** und **arbeitsaufwändigen Rückkopplungen**. Außerdem ist unsere Personalkapazität nicht darauf ausgelegt, dass wir stets auf den jeweiligen Verfahrensgegenstand spezialisierte Mitarbeiter zur Verfügung haben. Da die Anträge auf Vorabkontrolle ohne Vorankündigung und in zufälliger Anzahl bei uns eingehen, sind längere Bearbeitungszeiten unvermeidbar. Das ist insbesondere der Fall, wenn unsere Überprüfungen die Notwendigkeit von Änderungen an der Software oder den Abläufen ergeben. All das geht zulasten der Daten verarbeitenden Stelle, die mit dem Echtbetrieb erst nach unserem Okay starten kann.

Deshalb nehmen einige Behörden ein **rechtswidriges Vergehen** in Kauf. Entweder sie verzichten ganz auf eine Vorabkontrolle (vgl. Tz. 4.2.6 dieses Berichtes) oder aber sie starten bereits mit dem Echtbetrieb, bevor die Kontrolle erfolgt ist (vgl. 24. TB, Tz. 7.3). Damit sind die Probleme aber nicht behoben, sondern nur aufgeschoben, wenn sich nachträglich datenschutzrechtliche oder sicherheitstechnische Mängel herausstellen. Einige Behördenleiter werden offenbar erst aus einem Schaden klug.

Was ist zu tun?
Man kann nicht alles auf einmal haben: Wer bei der Bestellung behördlicher Datenschutzbeauftragter spart, zahlt bei der Vorabkontrolle drauf. Deshalb sollten auch die letzten Behörden lieber gleich einen Datenschutzbeauftragten bestellen.

7.4 Ergebnisse von Prüfungen

7.4.1 Offenes Krankenhausinformationssystem

Die medizinischen Daten in Krankenhäusern gehören zu den Datenbeständen, die im besonderen Maße vor unbefugten Zugriffen geschützt sein müssen. Wer zulässt, dass deren Vertraulichkeit nicht gewährleistet ist, macht sich unter Umständen strafbar. Weil ein Krankenhausinformationssystem offen wie ein Selbstbedienungsladen war, mussten wir bei einer Prüfung die „Notbremse“ ziehen.

In den letzten Jahren sind die technischen und organisatorischen Sicherheitsmaßnahmen in mehr als einem Dutzend Krankenhäuser im Lande überprüft worden. Es hat zwar regelmäßig Beanstandungen gegeben, weil das Sicherheitsniveau im Hinblick auf den Schutzbedarf der medizinischen Daten nicht ausreichend war. Teilweise sind auch durchaus erhebliche Mängel festgestellt worden. Keine der bisherigen Prüfungen hat aber mit einem solchen **Paukenschlag** begonnen wie die beim Zweckverbandskrankenhaus Itzehoe.

Bereits in den ersten Tagen der Nachschau stellten wir fest, dass die Mitarbeiter mehrerer **externer Softwarehäuser** und **Fernwartungsunternehmen** seit geraumer Zeit einen unkontrollierten und unkontrollierbaren Zugriff auf alle bzw. auf wesentliche Teile der Patientendaten hatten. Nicht einmal die genaue Zahl der Personen mit Zugriffs- und Änderungsmöglichkeiten konnte ermittelt werden, weil die entsprechenden Terminals in Räumen installiert waren, die zwar zum Krankenhaus gehörten, deren Nutzung aber nicht von ihm überwacht wurde. Besonders problematisch war, dass vielen Mitarbeitern externer Firmen sogar das Recht zugestanden wurde, neue Benutzerkonten mit eigenen Rechten anzulegen und die Rechte bestehender Benutzerkonten zu verändern. Das Attribut „**Selbstbedienungsladen**“ war mithin keineswegs übertrieben.

Die Prüfung hat zwar keine Anhaltspunkte dafür ergeben, dass die betreffenden Personen diese Möglichkeit tatsächlich missbräuchlich genutzt haben. Da aber die **ärztliche Schweigepflicht** grundsätzlich auch durch ein Unterlassen gebrochen werden kann, bestand jederzeit die Gefahr, dass die verantwortlichen Ärzte sich dadurch strafbar machten, dass sie entsprechende Zugriffe nicht durch technische und organisatorische Maßnahmen verhinderten. Die Situation war vergleichbar mit einer unverschlossenen und unbeaufsichtigten Lagerung von papierenen Patientenakten in Räumen, die Unbefugten zugänglich sind. Eine mögliche strafrechtliche Verantwortung traf auch die kaufmännische Leitung des Krankenhauses.

Auch aus Fürsorgegründen haben wir in diesem Fall noch während der laufenden Kontrolle eine **Beanstandung** ausgesprochen und den Zweckverband als Träger des Krankenhauses aufgefordert, die unkontrollierten Zugriffe externer Dienstleister kurzfristig zu unterbinden. Die Reaktion folgte prompt, und der uns übersandte Maßnahmenkatalog liest sich wie ein Auszug aus einem Sicherheitshandbuch zur Fernadministration, wie folgende Beispiele deutlich machen:

- Alle offenen Fernwartungsverbindungen wurden getrennt und werden fortan nur nach vorheriger Absprache für gezielte Maßnahmen zeitlich begrenzt freigeschaltet. Alle Zugriffe werden protokolliert.
- Zur Kontrolle der Fernwartungszugänge über Routerverbindungen hat die EDV-Abteilung ein eigenes Know-how aufgebaut und ist nun in der Lage, die Routerverbindungen gezielt zu steuern und zu überwachen.
- Der Fernwartungszugriff auf die Laborsysteme wird nur noch bei Bedarf durch eine Steckerverbindung hergestellt. Dadurch ist die Laborabteilung in der Lage, die Verbindung selbst zu aktivieren und zu unterbrechen.
- Für Arbeiten vor Ort wird den Mitarbeitern der externen Dienstleister ein Arbeitsplatz zur Verfügung gestellt, der eine Überwachung ihrer Arbeiten ermöglicht.
- Die Benutzerkonten der externen Administratoren werden nur auf Anforderung freigeschaltet und nach Beendigung der notwendigen Arbeiten wieder deaktiviert.

Die Risiken für die **Vertraulichkeit der elektronischen Patientendatenbestände** des Krankenhauses dürften damit deutlich vermindert sein. Die gesamte Prüfungsmaßnahme, in der neben technischen insbesondere auch rechtliche Fragestellungen behandelt werden sollen, war bis zum Redaktionsschluss dieses Tätigkeitsberichtes noch nicht abgeschlossen.

Was ist zu tun?
Die Abschottung von Krankenhausinformationssystemen gegenüber Unbefugten muss in allen Krankenhäusern gewährleistet sein.

7.4.2 Problemfall Firewall

Verwaltungen, die sich eine Firewall „von der Stange" zulegen, ohne sich zu vergewissern, dass deren Filterregeln auch ihren Anforderungen entsprechen, erlangen nur eine Scheinsicherheit. Diesem Trend kann durch eine Auditierung der Produkte entgegengewirkt werden. Kleinere Verwaltungen sind mit den entsprechenden Analysen selbst dann überfordert, wenn sie sich zu Kooperationen zusammenschließen.

Bei der Bestimmung der Behörden, die wir im jeweiligen Jahr einer Prüfung vor Ort unterziehen wollen, legen wir Wert auf einen Mix aus Daten verarbeitenden Stellen, bei denen wir Standardkonfigurationen und -anwendungen vermuten, und solchen, bei denen von vornherein Besonderheiten zu erwarten sind. Auf diese Weise erreichen wir eine **Flächendeckung** und gleichzeitig eine **exemplarische Aufbereitung von Spezialproblemen**. Wie schnell aus einer Standardprüfung ein Fall von grundsätzlicher Bedeutung werden kann, zeigte sich bei einer kleinen Amtsverwaltung in Angeln. Sie war nämlich zur Realisierung ihres Internet-Anschlusses eine Kooperation mit 16 anderen Verwaltungen eingegangen. Auf diese Weise waren mehrere hundert Arbeitsplätze in gleicher Weise mit dem Internet verknüpft.

Während über die Behebung der auch in anderen Verwaltungen häufig zu verzeichnenden sicherheitstechnischen Schwachstellen schnell Einvernehmen erreicht werden konnte, bereitete die Analyse der **Filterregeln der Firewall** erhebliche Schwierigkeiten. Sie konnte bis zum Redaktionsschluss dieses Berichtes nicht abgeschlossen werden, obwohl die Prüfung bereits im Januar 2002 stattgefunden hat. Die 17 kooperierenden Verwaltungen betreiben nämlich nicht jede für sich eine spezielle Firewall, sondern bedienen sich aus Kostengründen eines Providers, der für sie ein zentrales Filtersystem konfiguriert hat. Da die Verwaltungen dem Provider kein von ihnen entwickeltes Anforderungsprofil für die ein- und ausgehende Internet-Kommunikation übergeben hatten, war zu ermitteln, welche Filterungen der Provider von sich aus realisiert hatte.

Die Auswertung der uns übergebenen Dokumentation ergab einen Erläuterungsbedarf bei immerhin 15 Filterregeln. Die Amtsverwaltung konnte unsere Fragen nicht beantworten und bemühte sich ihrerseits bei dem Provider um Auskunft. Dies war ein mühsames Unterfangen, da das betreffende Unternehmen mehrfach den Namen bzw. den Besitzer gewechselt hatte. Die ersten Antworten waren so wenig aussagekräftig, dass man den Eindruck gewinnen musste, dass dort selbst

niemand mehr den „**Durchblick**“ hatte. Erst nach massivem Druck durch die Verwaltungen, Drohungen mit einer Vertragskündigung und einer klaren Definition der Defizite durch uns ist Anfang 2003 ein Papier übergeben worden, das eine substanziierte Analyse ermöglicht. Dabei werden wir den Fragestellungen nachgehen, ob das, was generiert worden ist, überhaupt einen Sinn macht und ob weitere Filterungen erforderlich sind. Dies ist ein zeit- und personalaufwändiges Unterfangen. Das Ergebnis ist völlig offen. Es kann sein, dass es am Ende von unserer Seite ein Okay geben wird, es ist aber auch möglich, dass wir signifikante Sicherheitslücken entdecken.

Dieser Fall zeigt, dass viele Verwaltungen im Lande, die sich einer **Firewall „von der Stange**“ bedienen, mit dem Risiko leben, nur über eine Scheinsicherheit zu verfügen. Die wenigsten Behörden dürften selbst in der Lage sein, die richtige Umsetzung der von ihnen formulierten Vorgaben (wenn es denn solche gibt) zu kontrollieren. Darauf zu hoffen, dass wir demnächst zu einer Prüfung erscheinen und ihnen dadurch die Arbeit abnehmen, ist keine Lösung. Die kann ganz offensichtlich nur darin liegen, dass nur Firewalls eingesetzt werden, die sich zuvor einem Produktaudit unterzogen haben. Dass außerdem eine Wartung der Firewalls und eine Anpassung der Filterregeln an neue Bedrohungen erfolgen muss, sollte selbstverständlich sein.

Was ist zu tun?
Die Behörden des Landes sollten nur Firewalls einsetzen, die ein datenschutzrechtliches Gütesiegel besitzen oder auditiert worden sind.

7.4.3 Vertrauensstelle für das Krebsregister

Zur Bekämpfung von Krebserkrankungen kann die epidemiologische Forschung einen wichtigen Beitrag leisten. Deshalb werden in Schleswig-Holstein Krebserkrankungen von Ärzten an ein zentrales Register gemeldet und dort erfasst. Wegen der Sensibilität des Datenbestandes sind besonders wirksame Sicherheitsmaßnahmen erforderlich. Die Ärztekammer ist dieser Pflicht vorbildlich nachgekommen.

Nachdem wir in den vergangenen Jahren die gesetzlichen (Neu-)Regelungen zum Krebsregister begleitet hatten (vgl. 19. TB, Tz. 3.1. und 4.8.1, und 21. TB, Tz. 4.8.1), haben wir nun deren praktische Umsetzung beleuchtet und eine sicherheitstechnische Überprüfung bei der **Ärztekammer** vorgenommen.

Das Krebsregister besteht aus zwei Abteilungen: der Vertrauensstelle und der Registerstelle. Die **Vertrauensstelle** hat den gesetzlichen Auftrag, alle Meldungen über Krebserkrankungen von den Ärzten entgegenzunehmen. Diese bestehen aus einem epidemiologischen und einem identifizierenden Teil, der je nach Entscheidung des Patienten Identitätsdaten (wie Name und Anschrift) oder nur einen Namenscode enthält. Die Aufgabe der Vertrauensstelle besteht darin, den epidemiologischen Teil zu pseudonymisieren und an die Registerstelle des Krebsregisters (Institut für Krebsepidemiologie, Lübeck) weiterzuleiten. Dabei ist von Bedeutung, dass alle medizinischen Stellen, die nacheinander eine Krebserkrankung behandeln, meldepflichtig sind (z. B. Hausärzte, Krankenhäuser und Patho-

logen), sodass oft mehrere Meldungen über die gleiche Erkrankung bei der Vertrauensstelle eingehen. Deshalb ist allen Meldungen, die einen bestimmten Patienten betreffen, dasselbe patientenorientierte Pseudonym zuzuordnen.

Die Meldungen über Krebserkrankungen erreichen die Vertrauensstelle in papierener und elektronischer Form. Nach der Erfassung werden sie auf Plausibilität und Vollständigkeit überprüft und zwischengespeichert. Der pseudonymisierte epidemiologische Teil der korrekten Datensätze wird monatlich an die Registerstelle übertragen. Ergeben auch deren Plausibilitätsprüfungen keine Fehler, werden diese Daten nach drei Monaten in der Vertrauensstelle gelöscht. Bei ihr verbleiben nur die **Referenzdateien über die Pseudonyme**.

Die **Registerstelle** kann anhand ihres Datenbestandes keine personenbezogenen Informationen gewinnen. Nur in ganz besonderen Ausnahmefällen ist eine Repersonifizierung von Datensätzen zu wissenschaftlichen Zwecken unter Einschaltung der Vertrauensstelle und gegebenenfalls auch des Arztes und nur mit Einwilligung des Patienten zulässig und möglich. Derartige Projekte sind uns nach den Regeln des Krebsregistergesetzes anzuzeigen. Es werden dann genaue Vorgaben zur Datensicherheit gemacht.

Unsere Prüfung hat keine Anhaltspunkte dafür ergeben, dass die Vertraulichkeit der personenbezogenen Daten während des Zeitraumes der Zwischenspeicherung in der Vertrauensstelle und die Datenbestände der Referenzdateien konkret beeinträchtigt werden. Gleichwohl gab es Anlass, die **Verfahrensweise aus Sicherheitsgründen zu optimieren**. Bestehende Zugriffsmöglichkeiten der Administratoren auf Echtdaten während des Tests von Software und auch im Produktionsbetrieb konnten weitestgehend eingeschränkt werden. Die verbleibenden Zugriffe unterliegen stets der Kontrolle der verantwortlichen Ärztin der Vertrauensstelle. Das Ergebnis der Prüfung ist insgesamt positiv zu bewerten.

Was ist zu tun?
Die Ärztekammer sollte das positive Ergebnis der sicherheitstechnischen Prüfung dadurch nach außen dokumentieren, dass sie sich einem formellen Behördenaudit unterwirft. Das Zertifikat würde die Akzeptanz des Krebsregisters bei Ärzten und Patienten weiter erhöhen.

7.4.4 Wie geht der MDK mit medizinischen Daten um?

Der Medizinische Dienst der Krankenversicherungen (MDK) erstellt jährlich etwa 120.000 Gutachten. Die dabei erfassten Daten beziehen sich detailliert auf physiologische und psychische Leiden sowie auf die häusliche Intimsphäre der Betroffenen. Die getroffenen Datensicherheitsmaßnahmen waren im Großen und Ganzen ausreichend, Verbesserungen wurden in Angriff genommen.

Die gesetzlichen Kranken- und Pflegekassen können Leistungen oft erst dann erbringen, wenn zuvor durch einen medizinischen Gutachter festgestellt worden ist, welche Art von Behandlung oder Unterstützung wie lange erforderlich ist. Diese Arbeit erledigen sie nicht durch eigenes Personal. Durch das Sozialgesetz-

buch V ist geregelt, dass hierfür der **Medizinische Dienst der Krankenversicherungen** zuständig ist.

Der MDK ist in Schleswig-Holstein eine eigenständige Daten verarbeitende Stelle, die **jährlich** etwa **120.000 Gutachten** in 13 Beratungsstellen erstellt und an die gesetzlichen Krankenkassen weitergibt. Bei einem Datenbestand dieser Größenordnung und Sensibilität – immerhin erhält der MDK im Bereich Krankenversicherung detaillierte Daten über physiologische und psychische Leiden einzelner Personen sowie im Pflegebereich auch Angaben über die häusliche Intimsphäre – ist es nahe liegend, dass die Sicherheitsmaßnahmen mindestens das Niveau eines Krankenhauses oder einer Arztpraxis erreichen müssen.

> **?** ***Medizinischer Dienst der Krankenversicherungen***
>
> *Der Medizinische Dienst der Krankenversicherungen (MDK) ist eine Körperschaft des öffentlichen Rechts, die an die Stelle des früheren Vertrauensärztlichen Dienstes getreten ist. Es ist eine Arbeitsgemeinschaft der Krankenkassen, die Gutachter-, Beratungs- und Prüfungstätigkeiten ausübt. So hat der MDK u. a. die Aufgabe, Gutachten zur Pflegebedürftigkeit zu erstellen, Vorschläge zur Sicherung des Heilerfolges und zur Einleitung von Rehabilitationsmaßnahmen zu machen und Gutachten bei Zweifeln an der Arbeitsunfähigkeit zu erstatten. Die MDK der Bundesländer sind in einer bundesweiten Arbeitsgemeinschaft organisiert, die Begutachtungsrichtlinien und die verwendete Software abstimmt.*

Mit dem Ergebnis unserer stichprobenweisen Kontrollen in der Hauptverwaltung und in zwei Beratungsstellen kann man im Großen und Ganzen zufrieden sein, wenngleich doch eine **ganze Reihe kleinerer Beanstandungen** ausgesprochen werden mussten. Im Wesentlichen ging es dabei um

- die tatsächliche Einhaltung der im eigenen Sicherheitskonzept festgelegten (durchaus sinnvollen) Kriterien,
- die bessere technische Absicherung des Schreibdienstes durch externe Mitarbeiter (vgl. hierzu Tz. 4.8.6 dieses Berichtes),
- die Verbesserung der Abschottung der papierenen Datenbestände gegenüber Besuchern, Reinigungspersonal usw.,
- die Deaktivierung nicht benötigter Diskettenlaufwerke,
- die Anpassung der Datenlöschung in den elektronischen Datenbeständen an die papierenen Bestände,
- die bessere Absicherung der elektronischen Datenbestände auf den Festplatten,
- das Unterbinden von Downloads von Programmen aus dem Internet,
- die Begrenzung der Einsichtsrechte der Systemadministratoren,
- die Vervollständigung der Dokumentation,
- die Wahrung der Vertraulichkeit medizinischer Daten bei der Altpapierentsorgung und
- die Verbesserung der Anonymisierung statistischer Datensätze.

Der MDK hat unsere Beanstandungen weitestgehend akzeptiert und Abhilfe zugesagt. Teilweise sind bereits entsprechende Maßnahmen ergriffen worden.

Was ist zu tun?
Wegen ihrer Sensibilität sind die Datenbestände, die bei den Begutachtungen anfallen, nur einem möglichst kleinen Personenkreis zugänglich zu machen und gegen unbefugte Zugriffe wirksam zu schützen.

7.5 Datenschutzrechtliche Begleitung bundesweiter Automationsprojekte

In den nächsten drei bis vier Jahren werden bundesweit an mehreren hunderttausend IT-Arbeitsplätzen der Polizei, der Steuerverwaltungen und der gesetzlichen Krankenversicherungen neue automatisierte Verfahren eingesetzt, die zwar auf Bundesebene entwickelt werden, für die aber die Daten verarbeitenden Stellen der Länder die Verantwortung tragen. Da die fertigen Verfahren von den Landesbeauftragten für den Datenschutz zu kontrollieren sind, macht es Sinn, dass sie sich bereits in der Entwicklungsphase mit den rechtlichen und sicherheitstechnischen Problemen befassen.

In drei großen Verwaltungsbereichen, die in die Zuständigkeit der Länder fallen, werden auf Bundesebene derzeit neue automatisierte Verfahren entwickelt. Es sind dies die Polizei mit dem Projekt **INPOL-neu** (vgl. 24. TB, Tz. 4.2.3), die Steuerverwaltungen mit dem Projekt **FISCUS** (vgl. 24. TB, Tz. 4.10.2 sowie auch Tz. 4.10.3 dieses Berichtes) sowie seit kurzem die Sozialverwaltung mit dem Projekt **AOK-SAM**. Das Besondere daran ist, dass die fertigen Produkte von Landesbehörden eingesetzt werden und somit die rechtliche und sicherheitstechnische Korrektheit von den Landesbeauftragten für den Datenschutz kontrolliert wird. Die einzelnen Daten verarbeitenden Stellen haben aber zum Zeitpunkt dieser Prüfungen gar keinen unmittelbaren Einfluss mehr auf die Gestaltung der Verfahrensabläufe, Datenbestände und Sicherheitskomponenten. Sie setzen vorkonfektionierte Verfahren ein, bei denen Änderungen erst nach langwierigen Abstimmungsprozessen auf Bundesebene möglich sind. Insgesamt hat diese Problematik Auswirkungen auf mehr als 12.000 IT-Arbeitsplätze in Schleswig-Holstein.

Deshalb hat sich die Konferenz der Datenschutzbeauftragten entschlossen, über Arbeitsgruppen frühzeitig Einfluss auf die datenschutzrechtliche und sicherheitstechnische Gestaltung der neuen Verfahren zu nehmen. Dies erweist sich zumindest in Teilbereichen als ein schwieriges und vor allem arbeitsaufwändiges Unterfangen, weil zunächst die Bereitschaft der Gremien auf Bundesebene bestehen muss, sich **bereits in der Entwicklungsphase** in die Karten schauen zu lassen. Ist dies erreicht, müssen oft noch fragmentarische Unterlagen auch dann sorgfältig unter datenschutzrechtlichen und sicherheitstechnischen Aspekten analysiert werden, wenn die Möglichkeit besteht, dass sie am Ende keine Relevanz erlangen, weil andere Lösungsoptionen ins Auge gefasst worden sind.

Ein „klassisches“ Beispiel hierfür ist das Projekt **INPOL-neu**. Nachdem jahrelang die zentrale Speicherung auch der Länderdatenbestände beim Bundeskriminalamt mit all den technischen und organisatorischen Abschottungsschwierigkeiten in der Diskussion gestanden und uns viel Arbeit gemacht hat, scheint sie nunmehr vom

Tisch zu sein. Ähnlich hat es sich beim Projekt **FISCUS** verhalten, bei dem das neue Softwarehaus der Steuerverwaltung offensichtlich wesentliche Teile der sicherheitstechnisch besonders „sensiblen“ Verarbeitungssteuerungskomponenten „gekippt“ hat. Bei dem Projekt **AOK-SAM** handelt es sich um eine Kooperation des Bundesverbandes der Ortskrankenkassen mit der Firma SAP mit dem Ziel, die Teilbereiche „Leistungen für Versicherte“, „Beitragseinzug“ und „Betriebswirtschaft“ zu optimieren und zu verbinden. Deshalb bedarf es hier einer Synchronisation der Sicherheitskomponenten der Software „SAP/R3“ mit den Anforderungen aus den Sozialgesetzbüchern V und X.

Gleichwohl gibt es keine Alternative zu dieser Vorgehensweise. Das umso mehr, als es sich um eine **Vorstufe eines Datenschutzaudits** handelt, für das außer in Schleswig-Holstein in den anderen Bundesländern noch keine Rechtsgrundlage besteht. Deshalb sind wir auch in allen drei Arbeitsgruppen vertreten und haben die Koordinierung der Arbeitsgruppe für das Projekt FISCUS übernommen; bezüglich der Arbeitsgruppe für das Projekt AOK-SAM teilen wir uns diese Aufgabe mit den Kollegen aus Hamburg.

Was ist zu tun?
Auch ohne dass bereits überall gesetzliche Grundlagen hierfür bestehen, sollte die Zusammenarbeit zwischen den Arbeitsgruppen der Datenschutzbeauftragten und den jeweiligen Projektmanagementgruppen so ausgestaltet werden, dass sie zu einer Art Datenschutzaudit führt.

7.6 Akten in Müllcontainern: Kontrollen zeigen Wirkung

„Ärztliche Gutachten, medizinische Stellungnahmen, Patientenlisten, Beihilfeanträge, Listen von Sozialhilfeempfängern ... offen in Müllcontainern gefunden“. So lautete eine von vielen Schlagzeilen im vorangegangenen Jahr. Was ist seitdem geschehen?

Bei fünfzig privaten und öffentlichen Stellen prüften wir 2001, ob in frei zugänglichen und unverschlossenen Müllcontainern Papiere und **Unterlagen mit personenbezogenen Daten** zu finden waren. Bei zehn Stellen fanden wir zum Teil hochsensible Unterlagen.

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

Die Behördenleiter gelobten durchweg Besserung. So etwas werde nie wieder passieren. Ein Jahr später wurde bei den gleichen Stellen eine **unangemeldete Nachkontrolle** durchgeführt. Und tatsächlich: Wir haben nichts Beanstandenswertes gefunden. Viele Behörden hatten in der Zwischenzeit Schredder angeschafft, einschlägige Dienstanweisungen erlassen und das Personal geschult. Unsere Kontrollen hatten offenbar den gewünschten Effekt: Mit Bürgerdaten wurde ordentlich umgegangen, auch nachdem sie fachlich nicht mehr benötigt wurden.

Wir kontrollierten zusätzlich fünfzehn Behörden bzw. private Stellen, die wir 2001 nicht besucht hatten. Hier war das Prüfungsergebnis nicht so positiv: Bei drei Stellen wurden wir fündig. Wieder waren es besonders sensible **Sozial- und Medizindaten** oder Daten, die dem „**Bankgeheimnis**“ unterlagen. Bei einer Behörde fanden wir sogar einen ganzen Container bis zum Rand gefüllt mit Unterlagen zu brisanten Informationen über die wirtschaftlichen Verhältnisse von Bürgerinnen und Bürgern. Ursächlich für diese Verstöße waren sowohl die Nachlässigkeit oder Überlastung einzelner Mitarbeiter, als auch die von den Behördenleitungen zu vertretende fehlende Ausstattung mit Aktenvernichtern bzw. die fehlende Existenz von Organisationsregelungen. Wieder wurde Besserung gelobt. Aber weiter gilt: Vertrauen ist gut, unangekündigte Kontrollen sind manchmal besser ...

Was ist zu tun?
Papiere und Unterlagen mit personenbezogenen Daten müssen datenschutzgerecht entsorgt werden. Die Verantwortung dafür liegt bei der Behördenleitung. Also: Aktenvernichtung regeln, Schredder anschaffen, sich regelmäßig vom ordentlichen Ablauf überzeugen.

8 Recht und Technik der neuen Medien

8.1 Selbstregulierung durch den deutschen Presserat

Die Pressefreiheit ist ein hohes Gut. Daher gelten für Presseorgane nicht die allgemeinen Datenschutzvorschriften. Im Wege der Selbstregulierung soll jetzt dafür gesorgt werden, dass die Rechte der Betroffenen gleichwohl nicht auf der Strecke bleiben.

> ***Im Wortlaut: § 41 Abs. 1 BDSG***
>
> *Die Länder haben in ihrer Gesetzgebung vorzusehen, dass für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken den Vorschriften der §§ 5, 9 und 38 a entsprechende Regelungen einschließlich einer hierauf bezogenen Haftungsregelung entsprechend § 7 zur Anwendung kommen.*

Mit dem 2001 in Kraft getretenen neu gefassten Bundesdatenschutzgesetz (BDSG) hat der Bundesgesetzgeber eine **Rahmenregelung** geschaffen, die den Ländern vorgibt, wie sie das Presserecht im Bereich des Datenschutzes zu gestalten haben. Das BDSG enthält für die Presse und ihre Hilfsunternehmen lediglich wenige Vorschriften. Dies sind insbesondere die Verpflichtung zur Wahrung des Datengeheimnisses sowie die Vorgaben zu den technischen und organisatorischen Maßnahmen. Außerdem wird auf ein Instrument verwiesen, das durch die Europäische Datenschutzrichtlinie aus dem Jahr 1995 neu eingeführt wurde: Die Möglichkeit, dass die beteiligten Verbände selbst für ihre Mitgliedsunternehmen bestimmte Vorgaben für den Datenschutz aufstellen. Einige Länder haben bereits ihre Pressegesetze entsprechend angepasst; in Schleswig-Holstein steht dies noch aus.

Auf dieser Grundlage hat der **Deutsche Presserat** nun seine Tätigkeit auf die Selbstkontrolle bei der Einhaltung des Redaktionsdatenschutzes ausgeweitet. Der Deutsche Presserat ist ein privat gegründetes Gremium, das seit 1959 dafür sorgen soll, dass Missstände im Pressewesen abgestellt werden. Damit soll eine staatliche Regulierung in dem sensiblen und durch das Grundrecht der Pressefreiheit besonders geschützten Bereich abgewendet werden. Zu den Trägern des Presserates gehören Verbände der Zeitungs- und Zeitschriftenverleger, Journalistenverbände sowie die Gewerkschaft. Um einheitliche Standards vor allem für die Art und Weise der Berichterstattung zu definieren, werden Empfehlungen und Richtlinien für die publizistische Arbeit herausgegeben (der so genannte Pressekodex). Danach sollen z. B. keine Veröffentlichungen erfolgen, die das sittliche oder religiöse Empfinden einer Personengruppe nach Form und Inhalt verletzen, und es soll auf eine unangemessen sensationelle Darstellung von Gewalt und Brutalität verzichtet werden. Die Verlage periodischer Druckwerke sind aufgefordert, sich zu den Vorgaben des Presserates zu bekennen und eventuell ausgesprochene Sanktionen zu befolgen.

Im Herbst des Jahres 2001 nahm der Deutsche Presserat den Redaktionsdatenschutz in seine Statuten auf. Dazu wurde ein besonderer **Beschwerdeausschuss** gegründet, der aus sechs Personen besteht. Nach der Beschwerdeordnung des

Presserates ist jeder berechtigt, sich bei diesem über Veröffentlichungen oder Vorgänge zu beschweren. Dies kommt insbesondere dann in Betracht, wenn jemand der Auffassung ist, dass die Verarbeitung von personenbezogenen Daten zu journalistisch-redaktionellen Zwecken im Rahmen der Recherche oder Veröffentlichung das Recht auf Datenschutz verletzt. Daneben kann der Presserat von sich aus ein Verfahren einleiten. Der Beschwerdeausschuss kann, falls eine Beschwerde begründet ist, einen Hinweis, eine Missbilligung oder eine Rüge aussprechen. Kommt es zu einer Rüge, so muss diese nach den Statuten des Presserates von dem betroffenen Presseorgan veröffentlicht werden.

Der Presserat hatte bereits im Jahr 2002 Gelegenheit, wegen eines Verstoßes gegen Datenschutzprinzipien eine **Rüge** auszusprechen. Ein Reporter der BILD-Zeitung hatte sich ein Foto eines Unfallopfers erschlichen, das später unter voller Namensnennung veröffentlicht wurde. Dabei hatte er vorgegeben, ein ehemaliger Mitschüler des Opfers gewesen zu sein.

Betroffene, die sich über die Missachtung der oben dargestellten Grundsätze beschweren wollen, können sich an folgende Adresse wenden:

Deutscher Presserat
Gerhard-von-Are-Str. 8, 53111 Bonn
Postfach 7160, 53071 Bonn

Tel: 0228/9 85 72-0
Fax: 0228/9 85 72-99

Homepage: www.presserat.de
E-Mail: info@presserat.de

Es ist abzuwarten, ob diese Mechanismen der Selbstregulierung ausreichend sind, um auch im Bereich der Presse den Bürgerinnen und Bürgern einen ausreichenden Datenschutz zu garantieren.

Was ist zu tun?
Der Presserat sollte bei der Kontrolle des Redaktionsdatenschutzes die selbst gesetzten Ziele und Vorgaben konsequent umsetzen, um nicht die an sich begrüßenswerte Selbstregulierung zu diskreditieren. Das Land Schleswig-Holstein wird eine Regelung zum Datenschutz bei Presseorganen in das Landespressegesetz einfügen müssen.

8.2 Neues vom E-Government

E-Government bleibt ein aktuelles Thema. Beispiele aus der Praxis zeigen, dass Vorhaben ohne Berücksichtigung von Datenschutz auf Dauer keine Chance auf Akzeptanz haben.

Auch im Jahr 2002 war das Thema E-Government in Verwaltung, Politik und Wissenschaft sehr populär. Allerdings sind die im Rahmen dieses Schlagworts verfolgten Initiativen zum Teil recht unterschiedlich. Während einige ihre Bemühungen vollständig auf das Internet ausrichten und den Idealzustand darin sehen, dass sämtliche **Verwaltungsleistungen** ausschließlich **online** abgewickelt werden, sind andere zunächst am Ausbau und an der Vereinheitlichung der im Hintergrund bei der Verwaltung laufenden Datenverarbeitung interessiert. Mit beiden Aspekten konnten wir auch im Berichtsjahr Erfahrungen sammeln.

> ***? E-Government***
>
> *ist die Abwicklung geschäftlicher Prozesse im Zusammenhang mit Regieren und Verwalten mithilfe von Informations- und Kommunikationstechniken über elektronische Medien und insbesondere des Internets. Oft werden drei Stufen unterschieden:*
>
> 1. *Information: Es werden die für die Bürger wichtigen Informationen bereitgestellt,*
> 2. *Kommunikation: Zwischen Verwaltung und Bürger werden Informationen ausgetauscht,*
> 3. *Transaktion: Ganze Verwaltungsvorgänge werden online abgewickelt.*
>
> *Bei dieser Betrachtung stehen die Außenbeziehungen der Verwaltung im Vordergrund; E-Government hat aber auch weit reichende Auswirkungen auf die internen Geschäftsprozesse.*

Virtuelles Rathaus

Beim Datenschutzaudit der Gemeinde Büchen (vgl. Tz. 10.1) war u. a. die Komponente „Virtuelles Rathaus“ zu auditieren. Dabei zeigte sich, dass es nicht einfach ist, eine größere Zahl von Verwaltungsdienstleistungen online abzuwickeln. Wenn Informationen aus dem Bereich der Verwaltung nach außen fließen können, muss sichergestellt sein, dass kein Unbefugter Informationen über Betroffene erhält. Zu diesem Zweck muss eine **Authentisierung** der anfragenden Person vorgenommen werden. Als Mittel dafür werden regelmäßig elektronische Signaturen genannt. Bereits im 24. TB (Tz. 8.1) hatten wir darauf hingewiesen, dass die Benutzung qualifizierter Signaturen im Sinne des Signaturgesetzes aufgrund der sich daran anknüpfenden Rechtsfolgen (Gleichstellung zur Schriftform) mit einer nicht unbedeutenden Gefährdung verbunden ist, die von den meisten Nutzern nicht vollständig beherrscht werden kann.

Unterhalb der Schwelle der qualifizierten Signaturen gibt es so genannte **fortgeschrittene Signaturen**. Diese können ein geeignetes Instrument darstellen, um eine Authentisierung zu realisieren. Allerdings haben sich in der Praxis Probleme gezeigt, wenn diese auf Programmkomponenten aufsetzen, die ihrerseits nicht sicher sind. So unterstützt z. B. der weit verbreitete Microsoft Internet Explorer ab Version 5.5 das Einbinden von Softwarezertifikaten im Browser. Die Möglichkeiten, die Sicherheitseinstellungen vorzugeben, sind jedoch unzureichend.

In einigen Fällen stellte sich heraus, dass ein Zertifikat, das durch die Kommune, die ein E-Government-Portal betreibt, selbst herausgegeben wird, nicht praxisgerecht ist. So sollte z. B. in Büchen den Nutzern die Möglichkeit eröffnet werden, über das Internet **Personenstandsurkunden**, wie etwa die Geburtsurkunde, zu bestellen. Dieses Angebot darf nicht dazu führen, dass es Dritten ermöglicht wird, solche Urkunden ohne Berechtigung abzurufen. Wird mit einem Softwarezertifikat gearbeitet, so muss der Antragsteller zunächst zum Rathaus der Kommune, bei der die Urkunden vorliegen, um sich ein Zertifikat ausstellen zu lassen, mit dem er dann von seinem Wohnort aus über das Internet die Papiere online bestellen kann. Dieses Szenario ist offensichtlich nicht besonders wirklichkeitsnah.

Die Probleme mit der Authentisierung fallen weg, wenn nicht versucht wird, um jeden Preis die Verwaltung vollständig über das Internet abzuwickeln. **Informationen über die Verwaltungsleistungen** wie Verfügbarkeit und Kosten, die über das Internet abgerufen werden können, sind oft schon eine erhebliche Verbesserung für die Bürger. Diese Angebote werfen in der Regel keine besonderen datenschutzrechtlichen Probleme auf. Dies gilt auch für Formulare, die zum Download oder Ausdruck angeboten werden.

Verwaltung 2000 und Kreisnetz Nordfriesland

Ein Ansatz, der den Bürgerbedürfnissen eher entgegenkommen dürfte, wird unter dem Stichwort „**Verwaltung 2000**“ von unterschiedlichen kommunalen Körperschaften verfolgt, deren Koordination beim Kreis Segeberg liegt. Deren Idee ist es, den Bürgerinnen und Bürgern die wichtigsten Verwaltungsleistungen an einer Stelle anzubieten. Zwar müssen diese dafür noch das Rathaus bzw. das Bürgerbüro aufsuchen. Dort werden sie jedoch umfassend bedient, sodass sie in einer bestimmten **Lebenslage** keine weiteren Amtsgänge mehr erledigen müssen. Zu diesem Zweck soll beispielsweise die Ummeldung von Kraftfahrzeugen nach einem Umzug auch bei dem Bürgerbüro der Gemeinde möglich sein. Damit wird der oft lästige Besuch in der nächsten Kreisstadt entbehrlich. Außerdem soll es möglich sein, die Ummeldung nicht nur bei der Zuzugsgemeinde, sondern auch bei einer sonstigen dem Verbund angeschlossenen Gemeinde zu tätigen. So könnte z. B. künftig eine Person, die im an eine größere Stadt angrenzenden Kreisgebiet von einer Gemeinde im Kreis in eine andere umzieht, die Ummeldung in der kreisfreien Stadt tätigen. Anstatt ganze oder halbe Tage auf den Ämtern zu verbringen, könnte dies oft in der Mittagspause vom Arbeitsplatz aus erledigt werden. Verwaltung 2000 wird derzeit im Rahmen eines Auditverfahrens datenschutzrechtlich überprüft.

Ein ähnliches Konzept verfolgt der Kreis Nordfriesland, der unter dem Projektnamen „**Von Inseln zu Netzen**“ ebenfalls zunächst für den internen Verwaltungsbereich (Back-Office) ein einheitliches Datennetz zusammenstellt. Nordfriesland ist auch im Hinblick auf die an die Bürger gerichtete Homepage vorbildlich. Der Kreis wurde in der Vergangenheit ausgezeichnet für seinen bürgerfreundlichen, informativen und umfassenden Internet-Auftritt.

Änderung des Verwaltungsverfahrensgesetzes

Im 24. Tätigkeitsbericht (vgl. Tz. 8.1) haben wir auf eine Initiative hingewiesen, durch die auch im **Verwaltungsverfahrensrecht** eine weitgehende Gleichstellung der elektronischen Signaturen zur Schriftform erreicht werden sollte. In diesem Zusammenhang hatten wir gemeinsam mit anderen Datenschutzbeauftragten auf verschiedene Risiken hingewiesen, die aus der Formulierung des Gesetzentwurfes folgen. Dazu gehört, dass die Bürger nicht gegen ihren Willen und ohne Kenntnis des Risikos in das Verfahren der qualifizierten elektronischen Signatur gedrängt und möglichst nur nach Einwilligung auf elektronischem Wege kontaktiert werden dürfen.

Leider hat der Bundesgesetzgeber diese Anregungen nicht umgesetzt. Die Änderungen des Verwaltungsverfahrensgesetzes, das allerdings nur auf Bundesebene gilt, traten im Februar 2003 in Kraft. In Schleswig-Holstein wird das Verwaltungsverfahren durch das **Landesverwaltungsgesetz** geregelt. Es ist davon auszugehen, dass dies in Kürze in ähnlicher Weise angepasst wird.

Informationsbroschüre „Datenschutzgerechtes E-Government“

Die Datenschutzbeauftragten des Bundes und der Länder haben sich im Berichtszeitraum der Fragestellungen der Schnittstellen von Datenschutz und E-Government in konzentrierter Form angenommen. Unter der Federführung des Niedersächsischen Datenschutzbeauftragten wurde in einer gemeinsamen Arbeitsgruppe eine umfassende Handreichung erstellt. Diese wurde im Dezember 2002 veröffentlicht und kann im Internet unter

www.lfd.niedersachsen.de

abgerufen oder in Schriftform bei uns bestellt werden. Es werden auf 120 Seiten die einschlägigen Fragen beantwortet und vor allem viele Beispiele für **mustergültige Lösungen** im Sinne einer Übersicht über „best practice“ vorgestellt. Wir haben dazu u. a. mit einem Beispiel aus der Stadt Norderstedt beigetragen.

Kurs EG

Was ist zu tun?
Die öffentlichen Stellen in Schleswig-Holstein, die E-Government einführen wollen, müssen die datenschutzrechtlichen Vorgaben beachten. Dazu können sie sich an der vorliegenden Broschüre der Datenschutzbeauftragten orientieren.

8.3 Der ständige Ärger mit 0190- und 0180-Nummern

Unverlangte Werbezusendungen per Fax, SMS oder E-Mail nehmen immer mehr überhand. Sie kosten nicht nur Nerven, sondern teilweise auch bares Geld. Der Gesetzgeber sollte in diesem Bereich endlich wirksame Möglichkeiten zur Abwehr schaffen.

Im Berichtszeitraum gab es sehr viele Eingaben, die sich auf unverlangt zugesandte Werbung bezogen (vgl. auch Tz. 6.1). Neben vielen unverlangten **Werbe-E-Mails** ärgerten sich die Betroffenen vor allem über **Werbefaxe** und **Werbe-**

SMS, die Ressourcen wie Papier und Zeit übermäßig beanspruchen. Gerade in den Medien Fax und SMS wird häufig nicht für den Kauf eines Produktes, sondern für die Inanspruchnahme einer bestimmten Telekommunikationsdienstleistung geworben. So wird man aufgefordert, eine bestimmte Nummer anzurufen oder einen Faxabruf über eine Nummer zu tätigen. Dabei handelt es sich häufig um Nummern, die mit dem Nummernblock 0190 oder 0180 beginnen.

0190-Dialer

Mittlerweile ist vielen Verbrauchern bekannt, dass insbesondere die Anwahl der 0190-Nummern zu enormen Kosten führen kann. Dies machen sich **Betrüger** zunutze, die sich auf besonders perfide Weise **Zugang zu den Rechnersystemen** der Betroffenen verschaffen. Sie versprechen den Zugang zu bestimmten Websites im Internet zu besonders günstigen Bedingungen. Voraussetzung sei allerdings, dass ein bestimmtes Programm installiert wird. Nimmt der Nutzer die Installation vor, so wird die Einwahl ins Internet künftig nicht mehr über den regulär voreingestellten Internet-Provider vollzogen, sondern über eine teure 0190-Verbindung. Dabei werden teilweise regelrechte „Mondpreise“ verlangt. So sollte für eine einzige Einwahl (die dann allerdings beliebig lange dauern konnte) ein dreistelliger €-Betrag fällig werden.

Wurden diese so genannten 0190-Dialer in der Vergangenheit vor allem in Verbindung mit pornografischen Webseiten beobachtet, so sind die Betrüger mittlerweile raffinierter und verschicken z. B. entsprechende Programme getarnt als Microsoft-Windows-Update. **Gutgläubige Nutzer** installieren diese und entnehmen oft erst der nächsten Telefonrechnung, welche horrenden Kosten angefallen sind.

Mittlerweile gibt es eine Reihe von technischen Schutzmaßnahmen, um die unerwünschten Dialer abzuwehren. Gelangt trotzdem ein solches schädliches Programm auf den eigenen Rechner, sollte es nicht sofort gelöscht werden. Es empfiehlt sich vielmehr, um die überhöhten Gebührenansprüche abzuwehren, möglichst die **Beweise** zu **sichern**, aus denen sich ergibt, dass ein solches Programm ohne bewusstes Zutun des Nutzers auf den Rechner gelangt ist. Kann dies bewiesen werden, so dürfte in der Regel die Gebührenforderung nicht durchsetzbar sein.

Mehrwertdienste

Eines der Probleme bei der Abwehr der überhöhten Ansprüche besteht darin, dass die Rechnungen nicht unmittelbar von den Stellen, die von diesen so genannten Mehrwertdiensten profitieren, gestellt werden. Vielmehr ermöglicht die Rechtslage es den Anbietern dieser Dienste, die Telekommunikationsnetzbetreiber als Inkassostellen zu verwenden. Dies bedeutet, dass z. B. auf der **Rechnung der Telekom** die entsprechenden Verbindungen auftauchen und von dieser abgerechnet werden. Dabei wird für die Telekommunikationsnetzbetreiber die Rufschädigung, die für sie entsteht, dadurch versüßt, dass sie an den überhöhten Gebühren mitverdienen. Im Berichtszeitraum sollte eine Rechtsänderung erfolgen, wonach der Kunde Einspruch beim Netzbetreiber (wie z. B. der Telekom) gegen die überhöhten Gebührenanteile aus den 0190-Nummern einlegen könnte. Daraufhin hätte der eigentlich rechnungsstellende Betreiber des Mehrwertdienstes unmittelbar bei

dem Kunden abzurechnen gehabt. Diese aus Verbrauchersicht erfreuliche Änderung ist leider am Widerstand der **Lobby der Mehrwertdiensteanbieter** gescheitert. Damit gerät eine ganze Branche ins Zwielicht, weil es schwarzen Schafen gelingt, die Kunden hinters Licht zu führen.

Werbung für die Inanspruchnahme der Mehrwertdienste

Ein anderer Bereich, der von Betrügern ausgenutzt wird, ist die unverlangte Werbung für die Nutzung der Mehrwertdienste, die über die 0190- und 0180-Rufnummern zu erreichen sind. In diesen Fällen wird zwar nicht wie bei dem Problem der 0190-Dialer hinter dem Rücken und ohne Wissen des Betroffenen eine kostenpflichtige Verbindung hergestellt. Allerdings ist auch die Versendung von Werbung für die Nutzung solcher Dienste nur dann erlaubt, wenn der Betroffene zuvor eingewilligt hat. Angesichts der klaren Rechtslage könnte man annehmen, es sei ein Leichtes, gegen die häufig auch aus Deutschland operierenden Versender der Werbefaxe oder SMS, die für die Inanspruchnahme der Mehrwertdienste werben, vorzugehen. Tatsächlich tun sich allerdings einige praktische Probleme auf. Häufig verschleiern die Absender dieser Werbung durch technische Tricks ihre Rufnummer. Es gibt allerdings einen Weg, die absendende Rufnummer festzustellen, auch wenn diese vom Sender unterdrückt wird. Dazu muss eine so genannte **Fangschaltung** beim Netzbetreiber beantragt werden. Dies ist unter bestimmten, in § 10 Abs. 1 und 2 der Telekommunikations-Datenschutzverordnung genannten Voraussetzungen zulässig. Diese Maßnahme ist auf künftige Anrufe gerichtet und hat dann Sinn, wenn mit der wiederholten Zusendung unverlangter Sendungen zu rechnen ist. Zwar wäre es den Netzbetreibern technisch auch möglich, aus ihren vorhandenen Datenbeständen die Absender bestimmter Kommunikationen im Nachhinein herauszufiltern, ohne dass eine spezielle Fangschaltung installiert wird. Dies verursacht aber erhebliche Kosten und wird daher nicht für private Zwecke, sondern lediglich für die Zwecke der Strafverfolgungs- und Sicherheitsbehörden vorgenommen.

Im Wortlaut:
§ 10 Abs. 1 und 2 Telekommunikations-Datenschutzverordnung (TDSV)

(1) Trägt ein Kunde in einem zu dokumentierenden Verfahren schlüssig vor, dass bei seinem Anschluss bedrohende oder belästigende Anrufe ankommen, hat der Diensteanbieter auf schriftlichen Antrag auch netzübergreifend Auskunft über die Anschlüsse zu erteilen, von denen die Anrufe ausgehen. Die Auskunft darf sich nur auf Anrufe beziehen, die nach dem Antrag durchgeführt werden. (...)

(2) Die Bekanntgabe nach Absatz 1 Satz 3 darf nur erfolgen, wenn der Kunde zuvor die Verbindungen nach Datum, Uhrzeit oder anderen geeigneten Kriterien eingrenzt, soweit ein Missbrauch der Überwachungsmöglichkeit nicht auf andere Weise ausgeschlossen werden kann. (...)

Kann die absendende Rufnummer nicht ermittelt werden, liegt es nahe, den Anbieter des Mehrwertdienstes, für dessen Inanspruchnahme geworben wird, als Quelle der Zusendung zu vermuten. Schon der gesunde Menschenverstand spricht dafür, dass die massenhafte Werbung für die Inanspruchnahme bestimmter Mehrwertdienste nicht ohne Zutun der Anbieter in die Welt gesetzt worden ist. Also

müsste der Inhaber der beworbenen Mehrwertdienstenummer eigentlich als so genannter **Störer im Sinne des Wettbewerbsrechts** angesehen werden können. Noch fehlen allerdings Gerichtsurteile, die dies bestätigen.

Schwierigkeiten bei der Auskunft über zugeteilte Mehrwertdienstenummern

Wird entweder die absendende Rufnummer festgestellt oder unterstellt, dass der beworbene Mehrwertdiensteanbieter selbst Störer ist, muss ermittelt werden, wer hinter der beworbenen Rufnummer steht. Dies ist nicht ohne weiteres möglich. Handelt es sich um **0190-Rufnummern**, so gilt Folgendes: Diese Rufnummern werden blockweise von der zuständigen Regulierungsbehörde für Telekommunikation und Post (RegTP) an Telekommunikationsnetzbetreiber weitergegeben. Diese überlassen aus den Blöcken einzelne Rufnummern an Dritte, die diese wiederum weiterverkaufen können. Zwar lässt sich bei der RegTP klären, welchem Telekommunikationsnetzbetreiber eine bestimmte 0190-Nummer zugewiesen wurde. Dieser hat jedoch nur unter sehr eingeschränkten Voraussetzungen darüber Auskunft zu erteilen, an wen er sie weitergegeben hat.

Fehlte bis vor kurzem noch überhaupt ein Anspruch, so hat der Gesetzgeber mittlerweile reagiert und immerhin bestimmten Stellen die Möglichkeit eingeräumt, Auskunft bei den Telekommunikationsnetzbetreibern über die Stellen zu erhalten, denen die fraglichen Nummern weiterverkauft wurden. Anspruchsberechtigt sind nach dem **Unterlassungsklagegesetz** qualifizierte Verbraucherschutzverbände, die in eine entsprechende Liste aufgenommen wurden, sowie Industrie- und Handelskammern und Handwerkskammern. Dies bedeutet umgekehrt, dass der einzelne Nutzer, der sich gegen die unverlangte Zusendung von Werbesendungen wehren will, zurzeit keinen Anspruch hat. Allerdings prüft die Bundesregierung, ob der Kreis der Anspruchsberechtigten auf die Betroffenen erweitert werden muss. Die genannten Organisationen könnten also dann, wenn sie sich der Missbrauchsfälle annehmen, die Störer erfahren und wettbewerbsrechtlich gegen sie vorgehen. Den Betroffenen bleibt derzeit lediglich, sich mit konkreten Beschwerden an die Telekommunikationsunternehmen zu wenden, denen die 0190-Nummer von der RegTP zugewiesen wurden.

Der Netzbetreiber könnte, ohne dazu verpflichtet zu sein, den Betroffenen mitteilen, welcher Mehrwertdiensteanbieter hinter einer bestimmten Nummer steht. Allerdings werden, jedenfalls dann, wenn diese Dienstbetreiber keine juristischen Personen (z. B. GmbH, AG), sondern natürliche Personen sind, ausgerechnet datenschutzrechtliche Gründe dafür angeführt, dass eine solche Auskunft nicht erteilt wird. Der Gesetzgeber ist hier aufgefordert, möglichst schnell einen entsprechenden **Auskunftsanspruch auch für Nutzer** so auszugestalten, dass sich die Störer nicht länger hinter dem Datenschutz verstecken können.

Wenig effektive Sanktionsmöglichkeiten

Die Telekommunikationsunternehmen haben nach einer weiteren Rechtsänderung aus dem Berichtszeitraum die Pflicht, gegenüber den Stellen, denen sie die Nummern weiterverkaufen, darauf hinzuweisen, dass keine unverlangte Werbung zugesandt werden darf. Bei **Verstößen** haben sie **geeignete Maßnahmen** gegenüber den nachgeordneten Mehrwertdienstebetreibern zu erwägen. Dazu kann auch

eine Sperrung der Nummern gehören. Diese ist allerdings erst bei wiederholter und schwerer Zuwiderhandlung vorgesehen. Der einzelne Betroffene wird also davon ausgehen müssen, dass seine konkrete Beschwerde gegenüber dem Telekommunikationsunternehmen lediglich dazu führt, dass vielleicht die Gesamtheit der Nachfragen dieses irgendwann zum Handeln veranlasst. Werden die Telekommunikationsunternehmen nicht tätig, kann die **RegTP** ihrerseits Maßnahmen gegen diese verhängen. Allerdings sind derartige Fälle bisher noch nicht bekannt geworden.

Etwas anders verhält sich die Sache bei 0180-Nummern, die auch häufig über **unverlangte Faxe** beworben werden. Deren Vergabe regelt die RegTP selbst. In diesen Fällen sollen sich die Nutzer nach einer Auskunft der Regulierungsbehörde an diese wenden und den Sachverhalt möglichst unter Beifügung von Beweismitteln darlegen. Sie ist zu erreichen unter der Adresse:

Regulierungsbehörde für Telekommunikation und Post
Referat 118
Postfach 8001
55003 Mainz

Was ist zu tun?
Das Land sollte darauf hinwirken, dass durch entsprechende Rechtsänderungen endlich die Rechte der Betroffenen ernster genommen werden als die Einwände der Betreiber von Mehrwertdiensten.

8.4 Statt Datenvermeidung neue Vorratsspeicherung

Das Verwaltungsgericht (VG) Köln hat in einem Urteil die Verpflichtung zur Speicherung von Kundendaten beim Kauf von Prepaid-Handys mit guten Gründen für unzulässig erklärt. Daraufhin wurde im zuständigen Bundesministerium sofort ein Entwurf zur Änderung des Telekommunikationsgesetzes (TKG) vorbereitet, um eine Rechtsgrundlage für diese Vorratsspeicherung zu schaffen. Das Oberverwaltungsgericht (OVG) Münster hat überraschenderweise die Entscheidung des VG Köln aufgehoben.

Im 23. Tätigkeitsbericht (Tz. 8.1) hatten wir darüber berichtet, wie nach derzeit gängiger Praxis die Telekommunikationsprovider beim Verkauf von Handys mit Prepaid-Karten gesetzeswidrig zu **Außenstellen der Sicherheitsbehörden** gemacht werden. Ausschließlich für Zwecke eventueller künftiger Strafverfolgung müssen die Unternehmen bestimmte Daten ihrer Kunden in eine Datenbank aufnehmen. Um die Identifizierung der Kunden zu überprüfen, muss sogar der Ausweis vorgelegt werden. Die Unternehmen selbst haben an dieser Datenverarbeitung kein Interesse. Sie würden es vorziehen, ihre vorausbezahlten Produkte in Warenhäusern, Tankstellen usw. anonym und ohne Formalitäten vertreiben zu können.

Auf eine Klage verschiedener Mobilfunkunternehmen hin hat das **VG Köln** im Herbst des Jahres 2000 die entsprechende Anordnung der Regulierungsbehörde für unzulässig erklärt. Dabei wurde vor allem darauf abgestellt, dass die einschlägige Vorschrift im Telekommunikationsgesetz sich nur auf solche Daten bezieht, die die Unternehmen ohnehin für eigene Zwecke verarbeiten. Die Entscheidung wurde allgemein für gut begründet und kaum angreifbar gehalten. Gleichwohl wurde die bisherige Praxis der Datenerhebung auch beim Verkauf von Prepaid-Handys zunächst fortgesetzt, da Berufung eingelegt worden war und die Entscheidung des Verwaltungsgerichtes keine aufschiebende Wirkung hatte.

Da die Strafverfolgungsbehörden und sonstige Sicherheitsbehörden einen erheblichen Bedarf bei der Nutzung der in diesen Verzeichnissen gespeicherten Bestandsdaten sahen, wurde vonseiten des **Bundesministeriums für Wirtschaft und Technologie** umgehend eine Änderung des TKG auf den Weg gebracht. Diese sollte sicherstellen, dass die Vorschrift so gefasst wird, dass sie eine ausreichende Rechtsgrundlage für die Erhebung und Speicherung der Bestandsdaten auch bei Prepaid-Karten darstellt, die anschließend im Interesse der Sicherheitsbehörden erfolgen.

Der im Frühjahr 2002 vorgelegte Gesetzentwurf enthielt nicht nur entsprechende Änderungen im TKG, sondern sollte bei dieser Gelegenheit auch die Abfrage vonseiten der Sicherheitsbehörden in den Datenbanken der Handelsverkäufer erleichtern (vgl. zu den Risiken, die diese Datenbanken mit sich bringen, 19. TB, Tz. 7.3.1). So sollte gesetzlich geregelt werden, dass nicht nur mit vollständigen Teilnehmerdaten, sondern auch mit so genannten Jokerzeichen für einen oder mehrere unbekannte Buchstaben oder Ziffern

Im Wortlaut:
§ 90 Telekommunikationsgesetz (TKG), Abs. 1-3 (Auszug)

Auskunftsersuchen der Sicherheitsbehörden

(1) Wer geschäftsmäßig Telekommunikationsdienste anbietet, ist verpflichtet, Kundendateien zu führen, in die unverzüglich die Rufnummern (...) sowie Name und Anschrift der Inhaber von Rufnummern (...) aufzunehmen sind, auch soweit diese nicht in öffentliche Verzeichnisse eingetragen sind.

(2) Die aktuellen Kundendateien sind von dem Verpflichteten nach Absatz 1 verfügbar zu halten, sodass die Regulierungsbehörde einzelne Daten oder Datensätze in einem von ihr vorgegebenen automatisierten Verfahren abrufen kann. Der Verpflichtete hat durch technische und organisatorische Maßnahmen sicherzustellen, dass ihm Abrufe nicht zur Kenntnis gelangen können.

(3) Auskünfte aus den Kundendateien nach Absatz 1 werden
1. *den Gerichten, Staatsanwaltschaften und anderen Justizbehörden sowie sonstigen Strafverfolgungsbehörden,*
2. *den Polizeien des Bundes und der Länder für Zwecke der Gefahrenabwehr,*
3. *den Zollfahndungsämtern für Zwecke eines Strafverfahrens sowie dem Zollkriminalamt zur Vorbereitung und Durchführung von Maßnahmen nach § 39 des Außenwirtschaftsgesetzes und*
4. *den Verfassungsschutzbehörden des Bundes und der Länder, dem Militärischen Abschirmdienst und dem Bundesnachrichtendienst jederzeit unentgeltlich erteilt, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist.*

regelrecht gerastert werden kann. Außerdem sollte es möglich sein, nach Daten zu suchen, die lediglich phonetisch aufgenommen wurden und deren Schreibweise daher nicht vollständig geklärt ist. Es liegt auf der Hand, dass diese Art der Abfrage den Sicherheitsbehörden auch eine Vielzahl personenbezogener Daten unbeteiligter Dritter zugänglich machen würde, ohne dass diese Daten für die Aufgabenerfüllung erforderlich wären. Als Reaktion auf den vorliegenden Gesetzentwurf kritisierte die **Konferenz der Datenschutzbeauftragten des Bundes und der Länder**, dass ein weiterer Grundrechtseingriff im Bereich der Telekommunikationsdaten vorgenommen werde. Während Straftätern, die gezielt mehrere Karten verwendeten oder die Karten untereinander tauschten, mit diesem Vorhaben nicht Einhalt geboten werden könne, würde über Unbescholtene unnötigerweise eine Vielzahl von Daten auf Vorrat erhoben, anstatt die datenschutzrechtlichen Vorteile der Prepaid-Verfahren zu nutzen, die in der Datenvermeidung durch Anonymität des Bezahlens bestehen.

Im Mai 2002 überraschte das **OVG Münster** mit der Aufhebung des Urteils des VG Köln. Dabei übernahm das OVG vollständig die Argumentation der Regulierungsbehörde und ließ sich damit offenbar von den Begehrlichkeiten der Sicherheitsbehörden leiten. In dem Urteil finden sich Formulierungen wie z. B.: „Das Führen von Kundendateien (...) setzt zwingend die Erhebungen dieser Kundendaten (...) voraus. Die Erhebung (...) der Daten ist daher eine Selbstverständlichkeit, die keiner wörtlichen Erwähnung in § 90 Abs. 1 und 2 TKG bedürfte."

Diese und vergleichbare Formulierungen lassen Zweifel aufkommen, ob das Gericht das **Volkszählungsurteil** des Bundesverfassungsgerichtes bei seiner Entscheidung berücksichtigt hat. Dort heißt es, Beschränkungen des Grundrechts auf informationelle Selbstbestimmung bedürften „einer (verfassungsmäßigen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht. (...) Ein Zwang zur Abgabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren."

Das OVG Münster hat trotz der offensichtlichen Abweichung von den Vorgaben des Bundesverfassungsgerichts eine **Revision** zur nächsthöheren Instanz, dem Bundesverwaltungsgericht, **nicht zugelassen**, da es sich nicht um eine Angelegenheit von grundsätzlicher Bedeutung handele. Allerdings hat dem Vernehmen nach einer der betroffenen Telekommunikationsprovider bereits das in dieser Situation einschlägige Rechtsmittel, die **Nichtzulassungsbeschwerde**, eingelegt. Im Übrigen aber bleibt es zunächst bei der wenig befriedigenden Rechtslage. Die Bundesregierung hat nach dem Bekanntwerden der Entscheidung die weiteren Arbeiten an der kurzfristigen Novellierung des TKG eingestellt. Es ist aber damit zu rechnen, dass die Pläne zur Verpflichtung der Provider zur Vorratsspeicherung im Interesse der Sicherheitsbehörden weiterverfolgt werden.

Was ist zu tun?
Statt über ständig neue Überwachungsmöglichkeiten nachzudenken, sollte die Politik das von ihr selbst im Bundesdatenschutzgesetz verankerte Prinzip der Datenvermeidung endlich ernst nehmen.

8.5 Rote Karte für Internet-Schnüffler

Auf deutscher und europäischer Ebene werden die Bemühungen forciert, eine Verpflichtung zur vollständigen Speicherung von Nutzungsdaten im Internet einzuführen. Mit unserer Kampagne „Rote Karte für Internet-Schnüffler" wenden wir uns entschieden gegen diese Bestrebungen.

Bereits im letzten Tätigkeitsbericht (vgl. 24. TB, Tz. 8.2) haben wir uns ausführlich mit unterschiedlichen Vorhaben zur Einführung einer Pflicht zur Speicherung der Nutzungsdaten in der klassischen Telekommunikation und im Internet auseinander gesetzt. Nach der **bisherigen Rechtslage** wird im Bereich der klassischen Telekommunikation und des Internets die Speicherung von Verbindungs- bzw. Nutzungsdaten lediglich dann zugelassen, wenn diese zur Abrechnung erforderlich sind. Die Sicherheitsbehörden drängen nun darauf, diese Rechtslage um 180 Grad zu wenden und eine Verpflichtung für die Provider zur Speicherung dieser Daten einzuführen. In manchen Fällen könnten sämtliche Informationen über alle Nutzungsvorgänge für einen Zeitraum von bis zu zwei Jahren gespeichert werden.

Auf nationaler Ebene wurde über den **Bundesrat** eine entsprechende Initiative in der Folge des 11. September 2001 von den Ländern **Bayern** und **Thüringen** angestoßen. Der vorgelegte Gesetzentwurf fand dort zwar zunächst keine Mehrheit. Nach der Wahl in Sachsen-Anhalt änderten sich jedoch die Mehrheitsverhältnisse im Bundesrat zugunsten der unionsregierten Länder. Daraufhin ergriffen die Länder Thüringen und Bayern erneut die Initiative und brachten den schon einmal vorgelegten Text als Ergänzung eines im Übrigen nicht mit dem Thema unmittelbar zusammenhängenden Gesetzentwurfs des Landes Niedersachsen ein. In dieser Fassung wurde der Vorschlag zur Einführung einer Speicherpflicht vom Bundesrat mit der neuen Mehrheit im Mai 2002 verabschiedet. Die **Bundesregierung** legte den Entwurf mit ihrer Stellungnahme versehen dem Bundestag vor. Dort konnte er aber wegen der Neuwahl des Bundestages nicht weiter behandelt werden und fiel der Diskontinuität anheim.

Bei den Abstimmungen im Bundesrat ist positiv hervorzuheben, dass sich das Land **Schleswig-Holstein** als einziges mehrfach explizit gegen die Einführung einer Speicherpflicht ausgesprochen und die Bundesregierung aufgefordert hat, einer solchen Initiative auf europäischer Ebene nicht zuzustimmen.

Auch wenn die erste Initiative nicht unmittelbar zum Erfolg führte, ist dennoch Wachsamkeit geboten. Die **Stellungnahme der Bundesregierung** ist leider **keineswegs eindeutig ablehnend**. Zwar wird darauf hingewiesen, die Bundesregierung sei bestrebt, „*einen angemessenen Interessenausgleich herbeizuführen, der das wichtige öffentliche Interesse an einer effektiven Strafverfolgung (...) mit den Grundrechten der Betroffenen in ein ausgewogenes Verhältnis bringt*". Kann diese Äußerung, die im Hinblick auf die Änderung des Telekommunikationsrechts abgegeben wurde, noch so verstanden werden, dass die Einführung der Speicherpflicht dort als unverhältnismäßig anzusehen wäre, fällt die Stellungnahme im Hinblick auf die Speicherpflicht im Internet weniger klar aus. Dazu wird lediglich vorgebracht, der Entwurf des Bundesrates lasse die „erforderliche Abwägung" vermissen. Dies muss wohl so verstanden werden, dass bei Vornahme der entsprechenden Abwägung die Bundesregierung eine Speicherpflicht nicht für ausgeschlossen hält.

Im Wortlaut:
Erklärung der schleswig-holsteinischen Justizministerin im Bundesrat

„Schleswig-Holstein nimmt den Entwurf der Schlussfolgerungen des Rates zur Kenntnis. Er begegnet hinsichtlich der Aufforderung, Telekommunikationsbetreiber zu verpflichten, Telekommunikationsdaten aufzubewahren, erheblichen datenschutzrechtlichen Bedenken. Eine damit verbundene Vorratsspeicherung von sensiblen personenbezogenen Daten zum Zwecke möglicher strafrechtlicher Ermittlungen wäre abzulehnen.

Schleswig-Holstein bittet daher die Bundesregierung, im Rat der Europäischen Union diese Bedenken deutlich zu machen und darauf hinzuwirken, dass es keinen unverhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung gibt."

Die Initiative des Bundesrates kann nicht losgelöst vom **europäischen Kontext** betrachtet werden. Dort sind zwei Entwicklungslinien zu erkennen. Die bisherige Richtlinie zum Datenschutz in der Telekommunikation wurde durch eine Nachfolgeregelung abgelöst, die den Datenschutz in der gesamten elektronischen Kommunikation zum Gegenstand hat (vgl. dazu Tz. 12.1). Nach kontroversen Diskussionen wurde in die Richtlinie schließlich eine Öffnungsklausel aufgenommen, wonach die grundsätzlich bestehende Verpflichtung, Daten im Wesentlichen nur zu Abrechnungszwecken zu speichern und ansonsten umgehend zu löschen, unter bestimmten Voraussetzungen aufgegeben werden kann. Wörtlich heißt es dort: *„Zu diesem Zweck (gemeint ist u. a. Herstellung der öffentlichen Sicherheit, Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten und des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen) können die Mitgliedstaaten u. a. durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden."* Damit ist zwar keine eigenständige Verpflichtung zur Datenspeicherung geschaffen. Die Vorschrift bewirkt jedoch klar, dass die Datenschutzrichtlinie kein europarechtliches Hindernis mehr bildet, wenn eine solche Regelung in nationales Recht gegossen werden soll.

Noch problematischer als diese im Sommer 2002 erfolgte Änderung des europäischen Rahmenrechts sind mehr oder weniger **verborgene Initiativen** verschiedener Akteure in der EU, eine europaweite Speicherpflicht verbindlich einzuführen. So wurde im August 2002 zunächst ein vertraulicher Entwurf eines so genannten

Rahmenbeschlusses bekannt, den Belgien, das die Ratspräsidentschaft der EU im zweiten Halbjahr 2001 innehatte, eingebracht hat. Danach sollte eine Pflicht zur Vorratsspeicherung aller Verbindungs- bzw. Nutzungsdaten für mindestens 12 und höchstens 24 Monate europaweit eingeführt werden. Zwar versuchte die im zweiten Halbjahr 2002 amtierende dänische Ratspräsidentschaft, die aufkeimenden Besorgnisse zu zerstreuen, allerdings konnte dies nicht überzeugend gelingen. Ausweislich der Unterlagen der dänischen Ratspräsidentschaft, die im Internet abrufbar sind, gehörte es zu den vorrangigen politischen Vorgaben Dänemarks, für eine solche europaweite Speicherpflicht zu sorgen.

Als konkrete Maßnahme hat eine Arbeitsgruppe des Rates mit dem Namen „Multidisciplinary Group on Organised Crime (MDG)“ eine **Befragung der Mitgliedstaaten** der Europäischen Union durchgeführt. Dabei wurde ermittelt, ob bereits entsprechende nationale Regelungen bestehen, ob deren Einführung geplant ist oder unmittelbar bevorsteht. Weiterhin wurde abgefragt, ob die Mitgliedstaaten Vorteile in einer europaweiten einheitlichen Regelung sehen würden.

Während die Fragen dieses Fragebogens noch öffentlich abrufbar waren, sollte dies nicht für die Antworten gelten. Diese wurden allerdings **durch** verschiedene **Bürgerrechtsorganisationen an die Öffentlichkeit gebracht**. Danach zeigt sich, dass in den meisten Ländern der EU entweder bereits eine Speicherpflicht für Verbindungs- und Nutzungsdaten existiert oder deren Einführung unmittelbar bevorsteht. Lediglich in Österreich, Griechenland, Portugal, Schweden und Deutschland fehlt bisher noch eine solche Überwachungsregelung. Die allermeisten Länder äußern sich positiv zu der Idee einer Überwachung der Internet-Nutzer. Zurückhaltender sind lediglich Schweden und Deutschland. Dabei bringt die deutsche Bundesregierung im Wesentlichen dieselben Aspekte vor, die sie auch gegenüber der Bundesratsinitiative zur Vorratsspeicherung erwähnte.

Angesichts dieser Lage sind wir der Auffassung, dass den vielfältigen Tendenzen zur Aufhebung des Grundrechts auf informationelle Selbstbestimmung für Internet-Nutzer, die eine neue Qualität der Überwachung bedeuten würden, mit einer eigenen **Kampagne** entgegengetreten werden muss. Diese wurde als Reaktion auf die Bundesratsinitiative im Juni 2002 gestartet und ist unter der Adresse

www.datenschutzzentrum.de/material/themen/rotekarte/

oder über diese Grafik auf anderen Webseiten abrufbar.

Ziel der Seite ist es, die Bürgerinnen und Bürger mit den Organisationen, die die Vorhaben ablehnen, zusammenzuführen und sie mit allen wichtigen Informationen zu versorgen. Damit wurde ein **Forum** geschaffen, das dem **Informationsaustausch** dient und auch dem Einzelnen die Möglichkeit eröffnet, seine Meinung und Diskussionsbeiträge einzubringen. Darüber hinaus werden weitere Aktionsmöglichkeiten aufgezeigt und den Bürgern die Kontaktadressen der Ministerien und Bundestagsabgeordneten an die Hand gegeben, die in diesen Politikfeldern agieren. Wir haben in der Zwischenzeit viele E-Mails mit Äußerungen bekommen und einige auf der Seite veröffentlicht. Sie verweist mittlerweile auch auf eine Vielzahl von Stellungnahmen anderer Organisationen, Unternehmen und sonstiger Interessengruppen, die die Vorratsspeicherung ablehnen. Wir werden prüfen, wie wir diese Initiative künftig noch effektiver fortführen können.

Was ist zu tun?
Sämtliche interessierten und betroffenen Kreise sollten ihre Aktivitäten gegen die Einführung einer Speicherpflicht verstärken. Das Land Schleswig-Holstein sollte weiterhin eine klare Position gegen die Speicherpflicht beziehen.

9 Modellprojekte zur Weiterentwicklung des Datenschutzes

9.1 Virtuelles Datenschutzbüro ausgebaut

Das Virtuelle Datenschutzbüro bleibt auf Erfolgskurs. Im deutschsprachigen Raum dürfte es mittlerweile die erste Anlaufadresse sein, wenn es um Datenschutzfragen geht. Dies soll auch nach dem Auslaufen der Förderung im Jahr 2003 so bleiben.

Das Virtuelle Datenschutzbüro ist eine gemeinsame Einrichtung der meisten Landesbeauftragten und des Bundesbeauftragten für den Datenschutz in Deutschland sowie verschiedener nichtstaatlicher und ausländischer Datenschutzkontrollinstanzen. Es wurde bis zum Ende des Jahres 2002 gefördert durch die **Initiative Informationsgesellschaft Schleswig-Holstein**. Zu dem Service gehört vor allem die Portalseite www.datenschutz.de, die den Zugang zum deutschsprachigen Datenschutzwissen bietet. Daneben gibt es einen „Newsticker“, in dem im Durchschnitt jeden Tag eine Neuigkeit gemeldet wird, einen Presseverteiler, eine Suchmaschine, die die Seiten des Virtuellen Datenschutzbüros sowie der angeschlossenen Projektpartner durchsucht, sowie verschiedene Mailinglisten und weitere Foren zum Informationsaustausch.

Im Jahr 2002 wurden die Möglichkeiten zur Meldung von Beiträgen bzw. Links in das Virtuelle Datenschutzbüro wesentlich vereinfacht. Dies hatte die Folge, dass die Projektpartner intensiver Inhalte meldeten, die auf ihren oder anderen Seiten im Internet veröffentlicht sind. Mittlerweile gibt es über **1000 gemeldete Artikel**, das entspricht einer **Steigerung** innerhalb des Jahres 2002 um ca. **40 %**. Auch die Zahlen der Abrufe zeigen weiter nach oben. Wir schätzen, dass täglich zwischen 500 und 800 Nutzer die Seite ansurfen. Die Bedeutung des Portals www.datenschutz.de zeigt sich auch daran, dass bei der Suche nach dem Begriff „Datenschutz“ in der am meisten benutzten Suchmaschine „Google“ als erster Treffer das Virtuelle Datenschutzbüro erscheint.

Eine wesentliche Neuerung war der Umstieg auf ein **neues Content-Management-System**. An die Stelle des bisherigen Systems ist am 03.02.2003 eine auf der Platform Zope programmierte Software getreten. Zope hat die Vorteile, die Open-Source-Software generell bietet. Für die Seite sind auch für die Zukunft mehrere Erweiterungen geplant. So soll vor allem ein **interner Bereich** für den Austausch von Informationen unter den **Projektpartnern** geschaffen werden, in dem z. B. die Geschäftsverteilungspläne und andere interne Informationen zur Verfügung gestellt werden.

Nachdem im Jahr 2002 die Förderung ausgelaufen ist, muss sich das Projekt ohne Fördergelder „über Wasser“ halten. Die meisten Projektpartner haben zugesagt, für das Jahr 2003 einen **finanziellen Beitrag** zu leisten. Es wird sich zeigen, inwieweit es auf dieser Grundlage möglich ist, neben der bloßen Aufrechterhaltung des Betriebs zusätzlich weitere Verbesserungen vorzunehmen.

Künftig werden in verstärktem Maße auch **externe Kooperationspartner** aufgenommen. Dies können unabhängige Datenschutzexperten sein, aber auch Organisationen, Unternehmen oder Privatpersonen, die Produkte oder Dienstleistungen im Bereich Datenschutz anbieten. Mittelfristig könnte die Zusammenarbeit mit diesen Kooperationspartnern eine zusätzliche Basis zur Refinanzierung des Projekts bilden.

Nach dem Auslaufen der Förderung bietet es sich an, Bilanz zu ziehen und zu untersuchen, ob die ursprünglich angestrebten Ziele erreicht wurden. Die Schaffung eines Kontaktpunktes für die Nutzer dürfte gelungen sein. Das Virtuelle Datenschutzbüro bietet ein **One-Stop-Shopping** an, das es den Nutzern ermöglicht, an wichtige Datenschutzinformationen zu gelangen, ohne die Seiten der vielen unterschiedlichen Instanzen einzeln absurfen zu müssen. Die große Zahl von gemeldeten Artikeln und die ständige Veröffentlichung von News, die zum Teil noch nicht vorher in anderen Medien gemeldet wurden, tun ein Übriges dazu. Allerdings muss konstatiert werden, dass die ursprünglich erwartete Beteiligung auch von nicht deutschsprachigen Projektpartnern weit hinter den Erwartungen zurückgeblieben ist. Gerade mit den reduzierten Ressourcen, die nach dem Auslaufen der Förderung vorhanden sind, ist es für die wenigen Mitarbeiter im ULD nicht möglich, ohne Hilfe eine vollständige englischsprachige Datenschutzseite zu etablieren und ständig aktuell zu halten.

Die angestrebte bessere **Arbeitsteilung** und der leichtere **Informationsaustausch** werden durch das Virtuelle Datenschutzbüro realisiert. Dazu dienen u. a. die einschlägigen Mailinglisten, mit deren Hilfe sich verschiedene Arbeitskreise der Konferenz der Datenschutzbeauftragten schon gegenwärtig austauschen. Das Ziel, ein Versammlungsort für Datenschutzexperten außerhalb der Datenschutzdienststellen zu werden, wird dann weiter realisiert werden, wenn mehr Kooperationspartner gefunden worden sind, die Beiträge zum Virtuellen Datenschutzbüro liefern. Das Interesse ist groß, wie erste Anfragen zeigen.

Was ist zu tun?
Alle Beteiligten im Virtuellen Datenschutzbüro müssen ihre Anstrengungen aufrechterhalten, um dieses sinnvolle und viel genutzte Instrument auch nach dem Ende der Förderzeit am Leben zu erhalten.

9.2 AN.ON

Nachdem der Anonymisierungsdienst AN.ON vor knapp zwei Jahren den Betrieb aufgenommen hat, konnte er sich mittlerweile fest etablieren. Untersuchungen zeigen stetig steigende Nutzungszahlen.

Bereits im 23. und 24. Tätigkeitsbericht (jeweils unter Tz. 9.2) wurde über das seit Anfang 2001 bei uns in Kooperation mit der Technischen Universität (TU) Dresden sowie der Freien Universität Berlin durchgeführte und vom **Bundesministerium für Wirtschaft und Arbeit** bis Ende 2003 geförderte Projekt „AN.ON – Anonymität online“ berichtet.

Die von der Technischen Universität Dresden entwickelte Client-Software JAP kann von jedermann kostenlos aus dem Internet heruntergeladen werden. Mithilfe dieses Tools wird die anonyme Nutzung von Diensten im World Wide Web ermöglicht. Bei Verwendung des JAP wird der Kontakt zu den Webservern nicht, wie normalerweise üblich, unmittelbar aufgenommen, sondern für den Nutzer unsichtbar über eine Kette von Verschlüsselungsservern (so genannte „**Mixe**“) geleitet. Diese sorgen dafür, dass niemand Kenntnis von der IP-Adresse des Nutzers erlangen kann. Hierin besteht die Besonderheit des AN.ON-Dienstes gegenüber anderen Anonymisierungsdiensten. Der AN.ON-Dienst garantiert Anonymität und Unbeobachtbarkeit nicht nur gegenüber dem Anbieter der angesurften Webseite sowie dem eigenen Serviceprovider, sondern auch gegenüber den Betreibern des Anonymisierungsdienstes selbst.

? *JAP*

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

Der Betrieb eines Anonymisierungsdienstes wirft die Frage auf, ob er nicht zu **kriminellen Zwecken** missbraucht werden kann. Grundsätzlich lässt es sich nicht ausschließen, dass ein Anonymisierungsdienst auch missbräuchlich genutzt wird. Wir haben im Rahmen des Projektes die Aufgabe übernommen, den Betrieb des Anonymisierungsdienstes rechtlich zu betreuen. Beschwerden, in denen missbräuchliche Nutzungen des Dienstes beklagt werden, werden von uns beantwortet. Wie bereits im letzten Tätigkeitsbericht beschrieben (24. TB, Tz. 9.2), wandten sich sowohl die **Polizei** und die **Staatsanwaltschaften** als auch Privatpersonen und Firmen an uns. Die Anfragen der Strafverfolgungsbehörden betreffen in erster Linie laufende Ermittlungsverfahren bei Vorliegen eines strafrechtlichen Anfangsverdachts. Es ging hierbei z. B. um Verdachtsfälle auf Kreditkarten- und Bestellbetrug. In zwei Fällen ging es um Straftaten im Zusammenhang mit Kinderpornografie. Bei den Anfragen von Privaten bzw. Firmen handelte es sich z. B. um Beschwerden über Störungen von Diskussionsforen, beleidigende Äußerungen oder Hackerangriffe auf Internet-Angebote. Da es zum Wesen des Anonymisierungsdienstes gehört, keine Verbindungsdaten zu speichern, die eine spätere Identifizierung einzelner Nutzer zulassen, ist eine Auskunftserteilung grundsätzlich nicht möglich. Dieser Verzicht auf die Verarbeitung personenbezogener Nutzungsdaten **entspricht der aktuellen Gesetzeslage**. Die Erhebung und Speicherung derartiger Daten ist nach den Vorschriften des Teledienstedatenschutzgesetzes (TDDSG) nämlich nur dann erlaubt, wenn dies erforderlich ist, um die Inanspruchnahme des Dienstes zu ermöglichen oder abzurechnen. Diese Voraussetzungen liegen jedoch nicht vor, da die Inanspruchnahme des Dienstes anonym und kostenlos erfolgt. Die Vorgaben des TDDSG werden von uns also strikt eingehalten.

> ***Im Wortlaut:***
> ***§ 4 Abs. 6 Teledienstedatenschutzgesetz (TDDSG)***
>
> *Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.*

Im Übrigen hat der Gesetzgeber den Anbietern von Telediensten in § 4 Abs. 6 TDDSG die Verpflichtung auferlegt, dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung **anonym** oder **unter Pseudonym** zu ermöglichen. Das anonyme Surfen ist damit nicht nur zulässig, sondern rechtlich geboten. Ziel des Projektes ist es, diesem gesetzgeberischen Auftrag nachzukommen. Interessant ist, dass der Gesetzgeber auch im Rahmen der jüngsten Novellierung des TDDSG Anfang 2002 diese Vorschrift unverändert gelassen hat und die Möglichkeit zur anonymen Nutzung des Internets offenbar weiterhin als wichtiges Anliegen betrachtet. Den Bestrebungen auf europäischer Ebene, die Möglichkeit anonymer Nutzung von Internet-Diensten durch Einführung einer Pflicht der Diensteanbieter zur Vorratsdatenspeicherung einzuschränken, erteilen wir eine klare Absage (vgl. hierzu Tz. 8.5).

Nach Ablauf der Hälfte der Projektlaufzeit wurde im Sommer 2002 eine erste **Bilanz der Anzahl der Nutzungen** des Anonymisierungsdienstes gezogen. Da keine personenbezogenen Daten über die Nutzer erhoben und gespeichert werden, verfügen wir nur über statistisches Material zu den Nutzungszahlen. Die Anzahl der Downloads der Software JAP von der Webseite der Projektpartner der TU Dresden ist sicherlich nicht ohne weiteres zur Ermittlung von Nutzungszahlen geeignet, allerdings lässt sich daraus der Schluss ziehen, dass die Verbreitung des Tools JAP zunimmt. Daneben wurde das Tool mittlerweile über CD-ROM durch mehrere einschlägige Computerzeitschriften verbreitet. Die Anzahl der Nutzer innerhalb der Anonymitätsgruppe wird vom so genannten Infoservice ermittelt und den Nutzern angezeigt. Hierbei handelt es sich um Daten, die keinerlei Personenbezug ermöglichen. Seit Januar 2002 sind statistisch mindestens **600 Nutzungen pro Stunde** nachweisbar. Im Juli 2002 waren es 800, und im August 2002 ließen sich mindestens 1000 Nutzungen pro Stunde feststellen. Die Anzahl von über 2000 Nutzungen wurde erstmalig Mitte August 2002 überschritten.

Für uns war es von besonderem Interesse, diese ermittelten Nutzungszahlen ins Verhältnis zur Anzahl der Missbrauchsfälle zu setzen. Häufig wird nämlich in den Medien der Eindruck erweckt, als werde das Internet überproportional häufig für kriminelle Zwecke genutzt. Gerade bei garantierter Anonymität liegt eine derartige Annahme nahe. Wir wurden aber vom Gegenteil überrascht. Unsere im August 2002 vorgenommene Auswertung bezog sich auf den Zeitraum vom Beginn des Online-Betriebes des JAP bis Juli 2002. Nach vorsichtiger und überaus restriktiver Schätzung haben wir für diesen Zeitraum durchschnittlich ca. 5000 Nutzungen täglich zugrunde gelegt und sind von ca. **1,2 Millionen Nutzungsfällen** insgesamt ausgegangen. Dieser Zahl stehen im gleichen Zeitraum **17 Anfragen** deutscher **Strafverfolgungsbehörden** gegenüber. Außerdem wurden 15 Anfragen von Privatpersonen bzw. Firmen an uns gerichtet, in denen missbräuchliche Nutzungen des JAP beklagt wurden. Setzt man diese Zahlen ins Verhältnis zu den ermittelten Nutzungszahlen, ergibt sich ein **verschwindend geringer Promillesatz**, der auf missbräuchliche Nutzungen des Anonymisierungsdienstes hindeutet. Die er-

mittelten Zahlen über die Nutzung des JAP lassen insoweit bei aller Vorsicht den Schluss zu, dass offenbar die überwältigende Anzahl der Nutzungen gerade nicht zu kriminellen Zwecken erfolgt. Dieses Ergebnis wird von uns als sehr positives Signal gewertet und bestärkt uns in unserem Bestreben, den Anonymisierungsdienst weiter auszubauen.

AN.ON wird offenbar zunehmend auch von deutschen Firmen und Organisationen mit ausländischen Dependancen für Internet-Recherchen genutzt. Mit AN.ON ist es nämlich möglich, auch aus Ländern mit beschränktem Internet-Zugriff einen freien Informationszugang zu erlangen. Vereinzelt wurde der Zugriff auf Anonymitätsserver aus solchen Ländern, die über **keine demokratische Staatsform** verfügen, unterbunden. Darauf haben die Projektpartner ihrerseits reagiert. In einigen Fällen konnte eine Lösung gefunden werden, um die Sperrung des Zugriffs zu umgehen.

Seit August 2002 betreiben auch wir einen **eigenen Mix-Server**. Da die Kosten einer Internet-Leitung für den Betrieb eines solchen Servers sehr hoch sind, wird unser System in den Räumlichkeiten der TU Dresden unter Nutzung der dortigen Internet-Leitung betrieben. Der Rechner befindet sich physikalisch getrennt von den dort betriebenen Servern in einem speziellen PC-Tresor, der lediglich von unseren Mitarbeitern geöffnet werden kann. Zugriffe auf die Administrationsebene des Rechners sind ebenfalls ausschließlich durch uns möglich, sodass ein hoher Grad an Unabhängigkeit gewährleistet werden kann.

Die alljährlich von uns veranstaltete **Sommerakademie** stand im Jahr 2002 unter dem Motto „**Unser Recht auf Anonymität**“. Die Vorstellung des Projektes „AN.ON – Anonymität online“ nahm in diesem Zusammenhang eine zentrale Rolle ein. Das Thema wurde von Experten unterschiedlicher Disziplinen eingehend beleuchtet.

Außerdem haben wir zwei **Veröffentlichungen** zum Thema Sicherheit im Internet herausgebracht. Aus der Reihe „Safer Surfen“ ist ein neues Faltblatt erhältlich, das praktische Tipps und Hinweise zur Installation und Nutzung des JAP enthält. Außerdem haben wir eine 48-seitige Broschüre mit dem Titel „Sicherheit im Internet durch Anonymität“ herausgegeben, die Informationen zum technischen, rechtlichen sowie soziologischen Hintergrund des Projektes „AN.ON – Anonymität online“ enthält. Beide Publikationen können bei uns kostenlos bestellt werden. Im Internet stehen sie unter

www.datenschutzzentrum.de/download/anonheft.pdf
www.datenschutzzentrum.de/download/safeanon.pdf

zum Download zur Verfügung.

Weiter gehende Informationen zum Projekt befinden sich im Internet unter:

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

Das Projekt „AN.ON – Anonymität online“ wird gefördert durch das

Was ist zu tun?
Der Anonymisierungsdienst AN.ON ist weiter auszubauen. Es gehört zu unseren wichtigsten Zielen, weitere Betreiber von Mix-Servern zu gewinnen. Damit können wir die Nutzer bei der effektiven Wahrnehmung ihres gesetzlich garantierten Rechts auf Anonymität im Internet unterstützen. Bestrebungen auf EU-Ebene zur Einführung einer Vorratsdatenspeicherung ist eine klare Absage zu erteilen.

9.3 Datenschutz-Schul-CD fertig gestellt

Beim Projekt einer multimedialen Lern-CD zum Datenschutz in Aus- und Weiterbildung, das vom Bundesministerium für Bildung, Wissenschaft, Forschung und Kultur gefördert wurde, oblag uns vor allem die Erstellung des Moduls „Datenschutz in der Schule“.

Wir haben auf der CD den Tagesablauf von Schülerinnen und Schülern in Situationen dargestellt, die teilweise von hoher datenschutzrechtlicher Relevanz sind: Ein Lehrer plaudert aus der Zeugniskonferenz, Videokameras werden auf dem Pausenhof zur Schülerüberwachung installiert, im PC-Unterricht liest der Lehrer heimlich die aufgerufenen Seiten und E-Mails mit, die Polizei führt in der großen Pause eine Drogenrazzia auf dem Schulhof durch, Zeugniskladden usw. finden sich im Altpapiercontainer. Solche **realitätsnahen Lebenssachverhalte** sind uns aus Beratungsgesprächen, Eingaben und Prüfungen bekannt. Die Praxisbeispiele werden auf der CD sowohl hinsichtlich ihrer Auswirkungen auf die Betroffenen wie der rechtlichen Bewertung erläutert.

Über elf Geschichten erfolgt ein Einstieg in die **technischen und rechtlichen Fragestellungen**. Die Geschichte einer Freistunde erzählt von zwei Schülern im PC-Raum ihrer Schule, die sich per Hacking-Angriff den Entwurf einer Mathearbeit beschaffen, die ihr Lehrer auf seinem PC abgespeichert hat. Erklärt wird, was Hacking ist, welche Unterschiede zwischen Crashing und Ausspionieren von Daten aus straf- und datenschutzrechtlicher Sicht bestehen. Bei dieser Gelegenheit werden den Nutzern verschiedene Formen von Internet-Viren erläutert und Tipps gegeben, wie sie sich vor ihnen schützen können. Über kleine Rechtsfälle zum Computerstrafrecht wird z. B. erklärt, wann man strafmündig ist und wie eine Jugendstrafverhandlung abläuft.

Außerdem werden auf der CD allgemeine und aktuelle datenschutzrechtliche Fragen gestellt und Antworten gegeben. Sie führt in die **Grundbegriffe des Datenschutzes** ein und vermittelt über einen hierarchisch aufgebauten Clickstream mit Sprungmöglichkeiten und Querverweisen die Vertiefung der Kenntnisse anhand der multimedial in Text, Bild und Ton präsentierten Fälle.

Die CD wurde im Rahmen der Media-Tage Nord Schülerinnen und Schülern sowie Informatiklehrern und Interessierten vorgestellt und im Hinblick auf Ansprache, Verständlichkeit und Lerneffekte evaluiert. In den oberen Gymnasialklassen war die **Resonanz** durchweg positiv. Auch zunächst weniger an datenschutzrechtlichen Fragestellungen Interessierte konnten erkennen, welchen Nutzen der Datenschutz z. B. bei ihren vielfältigen und umfangreichen Internet-Ausflügen hat (vgl. 24. TB, Tz. 9.5).

9.4 EU-Projekte zu Datenschutzaudit und Gütesiegel

Die EU und das Wirtschaftsministerium des Landes Schleswig-Holstein fördern im Rahmen des Programms „e-Region“ die Verbreitung von Datenschutzaudits und -Gütesiegeln nach schleswig-holsteinischem Datenschutzrecht. Die Mittel der EU stammen aus den innovativen Maßnahmen des Europäischen Fonds für Regionale Entwicklung (EFRE) der Generaldirektion Regionalpolitik.

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

- **Gütesiegel**

Eine finanzielle Förderung aus dem Programm „e-Region Schleswig-Holstein“ zur Erlangung eines Gütesiegels konnte vorrangig von schleswig-holsteinischen **KMU** beantragt werden, die ein IT-Produkt herstellen oder vertreiben, das zur Nutzung in öffentlichen Stellen des Landes Schleswig-Holstein geeignet ist. Insgesamt sind bei uns 18 Anträge auf Förderung eingegangen, von denen 15 die Voraussetzungen für eine Förderung erfüllten. Unternehmen, die die Förderkriterien erfüllen, erhalten einen Zuschuss zu den Gutachterkosten. Der Eigenanteil des Unternehmens liegt bei mindestens 50 %. Darüber hinaus erbringen wir unsere an sich gebührenpflichtigen Dienstleistungen kostenfrei. Insgesamt stehen **Fördermittel** in Höhe von **50.000 Euro** zur Verfügung. Kriterium für die Entscheidung über die Förderung war das Innovationspotenzial des IT-Produkts hinsichtlich datenschutzfördernder Eigenschaften im Sinne der Datenschutzauditverordnung (DSAVO). Eine wichtige Rolle spielte auch die prospektive Wirkung auf dem IT-Markt, auf die primäre Zielgruppe des Datenschutz-Gütesiegels (öffentliche Stellen in Schleswig-Holstein) sowie allgemein

> **?** ***KMU***
>
> *Kleine und mittlere Unternehmen, die weniger als 250 Personen beschäftigen und einen Jahresumsatz von 40 Mio. Euro bzw. eine Jahresbilanzsumme von 27 Mio. Euro nicht überschreiten sowie bestimmte Unabhängigkeitskriterien erfüllen. (EU-Definition)*

der grenzübergreifende Charakter des Produkts wie z. B. die Zusammenarbeit des Herstellers mit Firmen anderer EU-Mitgliedstaaten. Die geförderten Produkte sind im Internet aufgeführt unter:

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

- **Audit**

Gegenstand des **Projekts Datenschutzaudit** ist die gebührenfreie Durchführung eines Auditverfahrens für öffentlich geförderte IT-Projekte. Neue IT-Verfahren sollen so von vornherein auf ihre dauerhafte Übereinstimmung mit den datenschutzrechtlichen Bestimmungen geprüft werden. Zu diesem Zweck werden die 12 Projektpartner des e-Region-Programms in den jeweiligen Bewilligungsbescheiden vom Wirtschaftsministerium aufgefordert, Kontakt mit uns aufzunehmen, um die Möglichkeit eines Datenschutzaudits prüfen zu lassen. Im Berichtszeitraum wurde bereits eine Vereinbarung über ein solches gefördertes Audit mit dem Kreis Segeberg geschlossen (vgl. Tz. 10.2 dieses Berichtes).

9.5 P3P – Datenschutz für Internet-Surfer

Das World Wide Web bietet viele Möglichkeiten, Nutzerdaten zu sammeln. Nutzer, die es interessiert, was die Anbieter mit ihren Daten machen, wie lange sie sie aufbewahren und welche Rechte ihnen zur Verfügung stehen, finden Antworten in den Datenschutzerklärungen der Anbieter. Doch angesichts der kurzen Verweildauer auf Websites werden diese seitenlangen, zuweilen fremdsprachigen Texte nur selten gelesen. Hier hilft P3P.

Die P3P-Technik gleicht die Datenschutzvoreinstellungen des Internet-Surfers in seinem Browser mit den Datenschutzerklärungen der Anbieter auf ihren Websites ab und gibt das Ergebnis kurz zusammengefasst in der Sprache des Browsers aus. So kann der Surfer **auf einen Blick** feststellen, ob die Erhebung, Nutzung und Aufbewahrung seiner personenbezogenen Daten für ihn akzeptabel ist, ob er seine Gestaltungsrechte ausüben oder ob er von dem Besuch der Website gänzlich absehen sollte.

P3P ist ein universeller technischer Standard, der dem Internet-Surfer in der Praxis mehr Transparenz und Kontrolle über seine Daten ermöglicht.

? P3P

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

Das **World Wide Web Consortium** (**W3C**) hat den Standardisierungsprozess für die P3P-Version 1.0, an der auch wir mitgewirkt haben (vgl. 21. TB, Tz. 7.1.4; 22. TB, Tz. 9.3; 23. TB, Tz. 8.6), im April 2002 abgeschlossen. Seitdem ist eine erste Version von P3P in ersten Browsern verfügbar, und eine zunehmende Anzahl von Webanbietern stellt – wie wir schon seit längerem (vgl. 23. TB, Tz. 8.6) – Datenschutzerklärungen für ihre Inhalte bereit.

? *W3C*

Das World Wide Web Consortium (W3C, http://www.w3.org) entwickelt interoperable Technik in Form von Spezifikationen, technischen Richtlinien und Software für das Web. Es wurde im Oktober 1994 gegründet und hat mittlerweile etwa 450 Mitgliedsorganisationen auf der ganzen Welt.

Anbieter, die Daten in Deutschland verarbeiten oder über die Verarbeitung von Daten in Deutschland entscheiden, sind an deutsches Datenschutzrecht gebunden. Dies muss sich auch in den **P3P-Datenschutzerklärungen** widerspiegeln. Für Anbieter aus dem europäischen Ausland gelten insoweit die datenschutzrechtlichen Vorschriften ihrer Länder, als Mindeststandard jedoch die Vorgaben der Europäischen Datenschutzrichtlinie.

Um zur Verbreitung von P3P und damit zu einer erhöhten Transparenz und Kontrolle für den Internet-Surfer beizutragen, erarbeiten wir im Rahmen eines vom **Wirtschaftsministerium** des Landes geförderten **Modellprojektes** rechtskonforme Datenschutzpolicies für datenintensive Webdienste (z. B. E-Commerce-Anwendungen) und stellen diese zum Download bereit.

www.datenschutzzentrum.de/p3p/

Anbieter können diese Vorlagen für ihre Websites übernehmen, sie müssen jedoch sicherstellen, dass die angegebenen Schutzstandards auch tatsächlich eingehalten werden. Eine gesetzeskonforme Datenverarbeitung liegt auch im eigenen Interesse des Anbieters, lässt sie sich doch als werblich verwertbares **Seriositätsmerkmal** dem fehlenden Vertrauen der Nutzer in Internet-Firmen entgegensetzen.

Viele Nutzer übernehmen die Voreinstellungen ihres Browsers unverändert. Damit entscheidet die **Standardeinstellung** in einem P3P-fähigen Browser wesentlich darüber, welche Schutzstandards die Internet-Surfer künftig von WWW-Anbietern verlangen werden. Für Internet-Surfer haben wir Anleitungen zur Nutzung und Konfiguration solcher P3P-Software zur Verfügung gestellt unter:

www.datenschutzzentrum.de/selbstdatenschutz/p3p/

Was ist zu tun?
Anbieter im Internet sollten sich mit datenschutzrechtskonformen Datenschutzerklärungen, die sie bei uns testen lassen können, um das Vertrauen ihrer Kunden bemühen.

9.6 Identitätsmanagement

Vom Recht auf informationelle Selbstbestimmung ist in der digitalen Welt oft kaum etwas zu sehen, denn weder haben die Nutzer eine echte Kontrolle darüber, was mit ihren Daten passiert, noch wissen sie auch nur annähernd, wer was wann über sie weiß. Identitätsmanager könnten die Situation der Nutzer entscheidend verbessern. Wir arbeiten an der Entwicklung solcher Programme mit.

Bei jeder Verwendung des Internets hinterlassen die Nutzer Spuren, wenn sie nicht spezielle Anonymisierer benutzen (vgl. Tz. 9.2). Auf der anderen Seite mangelt es an Authentizität: Es kann z. B. passieren, dass Personen unter falschem Namen im Internet agieren und dabei Unheil anrichten, das dann einem anderen zugerechnet wird. Dieser so genannte „**Identity Theft**“ ist inzwischen ein ernst zu nehmendes Phänomen geworden, über das international viele Websites informieren (z. B. http://www.idtheftcenter.org oder http://www.identitytheft.org). Schon mehrfach hatten sich betroffene Petenten an uns gewandt, doch zurzeit gibt es keine zuverlässige technische Abhilfe.

Für Anonymität und Authentizität in verschiedenen Abstufungen zu sorgen ist Aufgabe von **Identitätsmanagementsystemen** (vgl. 23. TB, Tz. 10.6; 24. TB, Tz. 8.5). Die aktuell verfügbaren Identitätsmanager sind noch nicht besonders effektiv. Sie beschränken sich meist auf kleine Funktionsbereiche wie eine Passwortverwaltung für alle möglichen Internet-Accounts (Single-Sign-On). Einige umfangreichere Systeme wie Microsoft Passport oder der Liberty-Alliance-Standardisierungsversuch wollen dem Nutzer bequeme Möglichkeiten für das Einkaufen im Web bieten, ohne dass jedes Mal die Nutzerdaten erneut eingegeben werden müssen; gleichzeitig werden die Daten für eine Weiterverarbeitung in Firmendatenbanken in einem einheitlichen Format bereitgehalten.

Die meisten Systeme erfordern, dass der Nutzer dem Anbieter die eigenen Daten anvertraut – und damit aus der Hand gibt. Datenschutzgerechte Identitätsmanagementsysteme, die Wert auf mehr Selbstbestimmung und Kontrollmöglichkeiten der Nutzer legen und auf Anonymitätstools aufsetzen, werden mittlerweile an einigen Universitäten und in Forschungslabors von Firmen entwickelt. Zusammen mit der Technischen Universität Dresden, dem IBM-Forschungslabor Zürich und der Universität Karlstad in Schweden arbeiten wir an einem **Prototyp**. Weitere europäische Partner haben ihr Interesse angemeldet.

> **?** ***Identitätsmanagement***
>
> *Identitätsmanagement bedeutet das Verwalten der eigenen Identität, d. h. die Entscheidung darüber, wem man welche seiner Daten unter welchen Bedingungen zur Verfügung stellt. Technik kann hier unterstützen, indem je nach Situation und Kontext unterschiedliche Pseudonyme statt des echten Namens verwendet werden, gegebenenfalls auch kombiniert mit der digitalen Signatur. Die Herausgabe von Daten wird mitprotokolliert, sodass der Nutzer später nachvollziehen kann, wer welche seiner Daten erhalten hat.*

In dem Berichtsjahr haben wir in Kooperation mit dem italienischen Notariat „Studio Notarile Genghini“ eine **Ausschreibung** zur Erstellung der Studie „Identity Management Systems (IMS): Identification and Comparison Study“ **gewonnen**, die von der Gemeinsamen Forschungsstelle der Generaldirektionen der Europäischen Kommission, Institut für technologische Zukunftsforschung, Sevilla initiiert wurde. In dieser Studie geht es darum, den Stand der Technik zu Identitätsmanagementsystemen darzustellen. Die einzelnen Kapitel beschäftigen sich zunächst mit den Grundlagen wie Definition, Anforderungen, Mechanismen und Design. Es folgt ein Testbericht von einer ganzen Reihe von Identitätsmanagern. Ein Fokus wird auf die europäische Sicht bei der Entwicklung und Einführung solcher Systeme gelegt. Schließlich runden die Ergebnisse einer Expertenbefragung, die wir durchführen, diese Studie ab. Fertigstellungstermin ist im Herbst 2003. Wir werden im nächsten Tätigkeitsbericht angeben, wie das europäische Institut für technologische Zukunftsforschung unsere Ideen zu Identitätsmanagement aufgenommen hat und wo man die Studie beziehen kann.

Unser Ziel ist es, den Weg für tatsächlich datenschutzfreundliche Identitätsmanagementsysteme zu bereiten. Schließlich geht es hier um ein **wichtiges Datenschutztool** der Zukunft, das uns allen den selbstbewussten, situationsadäquaten und sozial verträglichen Umgang mit unserer Identität erleichtern kann. Unsere Beiträge zu diesem Projekt können abgerufen werden unter:

www.datenschutzzentrum.de/idmanage/

Was ist zu tun?
Hersteller von Identitätsmanagern sollten Datenschutz in ihre Systeme einbauen. Wirtschaft und Verwaltung sollten prüfen, wie sie in ihren Bereichen ein datenschutzförderndes Identitätsmanagement unterstützen oder sogar selbst anbieten können. Nutzer und Anwender sollten die Vorteile von Identitätsmanagement bewusst gemacht werden.

9.7 Zuarbeit für ein Datenschutzauditgesetz des Bundes

Gemeinsam mit der Deutschen Hochschule für Verwaltungswissenschaften Speyer sind wir an einem Projekt des Bundesministeriums des Innern zur Vorbereitung eines Datenschutzauditgesetzes des Bundes beteiligt. Wir haben in diesem Rahmen einen Bericht über die Erfahrungen mit den Instrumenten Datenschutzaudit und IT-Gütesiegel in Schleswig-Holstein erstellt.

Ziel dieses Projektes ist, dem Bundesministerium des Innern für den im Jahr 2003 zu erstellenden Gesetzentwurf für ein Datenschutzauditgesetz des Bundes eine umfassende Informationsgrundlage zur Verfügung zu stellen. Während unser Beitrag in der Auswertung der in Schleswig-Holstein gewonnenen Erfahrungen besteht, führt die ebenfalls am Projekt beteiligte Hochschule für Verwaltungswissenschaften Speyer eine Gesetzesfolgenabschätzung durch. Im Rahmen dieses Projektbeitrags fand im September 2002 in Speyer ein **Workshop** statt, an dem Experten aus Wirtschaft, Wissenschaft und Verwaltung – darunter auch Vertreter des ULD – teilnahmen. Hierbei wurden unterschiedliche Modelle einer Regelung sowohl für ein Verfahrensaudit als auch für ein Produktaudit gegenübergestellt, von den Experten diskutiert und auf ihre möglichen Folgen untersucht.

Wir haben dem Bundesinnenministerium zum Jahresende unseren **Bericht übergeben**, der unsere Erfahrungen in der praktischen Anwendung der Regelungen über Audit und Gütesiegel systematisch auswertet.

Was ist zu tun?
Die Instrumente Audit und Gütesiegel können ihre Wirkung erst voll entfalten, wenn Gültigkeit und Voraussetzungen im gesamten Bundesgebiet einheitlich geregelt sind. Ein Bundesgesetz zum Datenschutzaudit sollte daher schnellstmöglich erlassen werden.

10 Gütesiegel und Audit

10.1 Pilotverfahren zum Datenschutzaudit abgeschlossen

Im Sommer 2001 begann im Rahmen einer Pilotierungsphase die konkrete Umsetzung des Datenschutz-Behördenaudits in die Praxis. Im Berichtszeitraum konnten die ersten Auditverfahren erfolgreich zum Abschluss gebracht werden.

Um **erste Erfahrungen** mit dem Datenschutz-Behördenaudit zu sammeln, haben wir nach Erlass der den Verfahrensablauf des Audits regelnden Ausführungsbestimmungen im Frühjahr 2001 eine Pilotierungsphase begonnen. Ziel war es, zunächst das nötige Know-how hinsichtlich dieses ganz neuen Instrumentes im Bereich des Datenschutzrechts zu entwickeln. In diesem Rahmen wurde einigen öffentlichen Stellen Schleswig-Holsteins die Möglichkeit eingeräumt, sich einem kostenlosen Datenschutzaudit zu unterziehen.

Bereits im letzten Tätigkeitsbericht (vgl. 24. TB, Tz. 10.6) konnte über den erfolgreichen Abschluss des Datenschutz-Behördenaudits beim **Kreis Ostholstein** im Januar 2002 berichtet werden. Das ursprünglich vom Innenminister begonnene Audit wird nicht weiterverfolgt, weil die Arbeit an dem zugrunde liegenden IT-Projekt unterbrochen wurde.

Mittlerweile wurde ein weiteres Pilotprojekt erfolgreich mit der Verleihung eines Datenschutzauditzeichens zum Abschluss gebracht. Die **Gemeinde Büchen** hat sich als erste Gemeinde in Deutschland mit ihrer gesamten Verarbeitung personenbezogener Daten einschließlich des neu eingeführten „Virtuellen Rathauses“ einem Datenschutzaudit unterzogen. Die nach den Ausführungsbestimmungen erforderliche Datenschutzerklärung enthält neben einer Bestandsaufnahme der den Gegenstand des Audits bildenden Fachverfahren sowie der im „Virtuellen Rathaus“ zum Einsatz kommenden Verfahren die Formulierung weiterer in einem präzise benannten Zeitraum noch zu erreichender Datenschutzziele. Das Datenschutzmanagementsystem enthält Vorgaben, die für eine dauerhafte Aufrechterhaltung des erreichten Datenschutzniveaus sorgen sollen. Die Datenschutzerklärung wurde von uns einer Begutachtung unterzogen. Insgesamt konnte der Gemeinde im Bereich der Verarbeitung personenbezogener Daten ein gutes datenschutzrechtliches Niveau bescheinigt werden. Mit der Einführung des „Virtuellen Rathauses“ hat die Gemeinde aus unserer Sicht außerdem ein datenschutzgerechtes E-Government-Angebot geschaffen (vgl. Tz. 8.2).

Das Auditverfahren bei der **Stadt Norderstedt** stand bei der Erstellung dieses Berichtes kurz vor dem Abschluss.

Die von uns im Rahmen der Auditverfahren erstellten Kurzgutachten können von jedermann auf der Homepage unter

www.datenschutzzentrum.de/audit/

abgerufen werden. Dort finden sich auch zahlreiche Informationen und Materialien rund um das Thema Datenschutz-Behördenaudit.

Was ist zu tun?
Der Erfolg der Pilotverfahren zum Datenschutz-Behördenaudit zeigt, dass dieses neue Instrument des Datenschutzes jetzt in der Praxis angewandt werden kann.

10.2 Verträge über weitere Datenschutzaudits

Nach Abschluss der Pilotphase hat eine Reihe weiterer Auditverfahren begonnen, die zum Teil schon abgeschlossen sind. Die ersten Zertifikate wurden an den Landtag verliehen.

Die ersten beiden Audits nach der Pilotphase sind beim **Schleswig-holsteinischen Landtag** erfolgreich abgeschlossen (vgl. Tz. 3.2). Inzwischen wurden Verträge über eine Reihe weiterer Verfahren abgeschlossen. Im Einzelnen geht es dabei um Folgendes:

- Das Auditverfahren beim Innenministerium betrifft die Betreiberfunktion des Innenministeriums für das landesweite **Schleswig-Holstein-Netz**.
- Beim Ministerium für Finanzen und Energie wird die Betreiberfunktion des Ministeriums für das landesweite **Sprachnetz** einem Audit unterzogen.
- Beim Kreis Segeberg wird im Rahmen des Programms „**e-Region Schleswig-Holstein**“ (vgl. Tz. 9.4) eine Auditierung des geförderten Projektes „ressortübergreifendes Geo-Informationssystem“ sowie des Projektes „**Verwaltung 2000**“/„Verwaltung.vol-net“ durchgeführt.
- Beim **Kreis Schleswig-Flensburg** geht es um die Anbindung des internen Netzes an das Internet.
- Das Auditverfahren bei der **Stadt Bad Schwartau** bezieht sich auf die Anbindung des internen Netzes an das Internet sowie darüber hinaus auf die Sicherheit und Ordnungsmäßigkeit der gesamten automatisierten Verarbeitung personenbezogener Daten innerhalb der Stadtverwaltung.

Was ist zu tun?
Die Nachfrage nach Audits zeigt, dass vielen Behörden, die ein vorbildliches Datenschutzkonzept anstreben, mit dem Datenschutzaudit ein attraktives neues Instrument zur Verfügung steht.

10.3 Gütesiegel

10.3.1 Akkreditierung von Gutachtern

- **Die Antragsverfahren in Zahlen**

Anträge auf Anerkennung als Sachverständiger oder sachverständige Prüfstelle konnten seit November 2001 gestellt werden. Bislang sind bei uns 23 Anträge auf Anerkennung eingegangen. Zwei Anträge wurden zwischenzeitlich zurückgenommen, drei Anträge wurden abgelehnt, und sieben Verfahren laufen noch. Ende

Dezember 2002 waren **elf Sachverständige** und sachverständige Prüfstellen aus dem gesamten Bundesgebiet von uns **anerkannt**. Wir erkennen sowohl einzelne Sachverständige als auch sachverständige Prüfstellen unter der Leitung einer fachkundigen Einzelperson an. Beide Möglichkeiten wurden mit der Anerkennung von drei Prüfstellen und acht einzelnen Sachverständigen realisiert.

Die Datenschutzauditverordnung (DSAVO) eröffnet die Möglichkeit, sich entweder für die **Gebiete Recht und Technik** oder beschränkt auf eines der beiden Gebiete anerkennen zu lassen. Von der Möglichkeit der beschränkten Anerkennung machten sieben der von uns anerkannten Gutachter und Prüfstellen Gebrauch. Dies trägt der Tatsache Rechnung, dass die hohen Anforderungen an die Fachkunde häufig eine arbeitsteilige Erstellung der Gutachten notwendig machen. In vielen Fällen kooperieren deshalb technische und rechtliche Gutachter bei der Erstellung der Gutachten, sodass bei der Begutachtung „doppelter Sachverstand" präsent ist.

- **Erkenntnisse aus den Antragsverfahren**

Die Datenschutzauditverordnung und die daraus entwickelten Anerkennungsregeln haben den **Praxistest bestanden**. Die in der DSAVO aufgezeigten Möglichkeiten sind von den Zielgruppen angenommen worden. Dazu gehören insbesondere die Anerkennung sowohl von einzelnen Gutachtern als auch von organisatorischen Einheiten und die Möglichkeit der Beschränkung auf ein Fachgebiet mit einer daraus folgenden Kooperation zwischen den Gutachtern.

Es zeigte sich, dass die geforderte einschlägige **berufliche Erfahrung im Datenschutz** (drei bzw. fünf Jahre) oftmals noch nicht oder nur schwer nachzuweisen ist. Dabei war allerdings deutlich sichtbar, dass der **Datenschutz** sich als **Geschäftsfeld** mit eigenem Markt gerade in den letzten zwei Jahren etabliert hat und – durchaus im Gegensatz zu manch anderen Bereichen im IT-Sektor – ein Wachstumsmarkt ist. Dies ist im Zusammenhang mit dem weiter erfolgreichen Sektor der IT-Security nicht überraschend. Erfreulich ist, dass die Antragsteller meist durch zunehmende Anfragen und Drängen von Kunden in den Datenschutzbereich expandiert haben. Der Datenschutz wird tatsächlich zum marktwirtschaftlichen Wettbewerbsvorteil!

- **Gebühren sparen mit dem Bausteinmodell**

Die Anträge weisen nicht selten einen gewissen Grad an Unvollständigkeit auf. Dies führte bei uns durch den umfangreichen Schriftverkehr bezüglich der Nachforderungen zu einem hohen Arbeitsaufwand. Wir haben deshalb in unsere Gebührensatzung ein **Bausteinmodell** eingeführt. Damit kann der Antragsteller jetzt durch die Vollständigkeit seines Antrags zu einem nicht geringen Teil auch über die Höhe der von ihm zu zahlenden Gebühren entscheiden. Je weniger Dienstleistungen wir für den Antragsteller im Antragsverfahren erbringen müssen, desto geringere Gebühren sind von diesem zu zahlen. Erste Erfahrungen zeigen, dass der Anreiz zur Kostenminimierung für eine sorgfältigere Antragsvorbereitung sorgt.

- **Feed-back von akkreditierten Gutachtern**

Im Anschluss an die Sommerakademie 2002 fand ein **Workshop** mit den bisher akkreditierten Gutachtern statt. Es stellte sich dabei heraus, dass die bisherigen Kriterien ein breites Maß an Freiheit für die Beibringung von Unterlagen durch die Produktanbieter erlauben. Gutachter, die entsprechend ihrer bisherigen Prüfpraxis in anderen Bereichen umfängliche und tief greifende Gutachten anbieten, werden bei Ausschreibungen durch die Hersteller von Produkten bisher aus Kostengründen eher seltener berücksichtigt. Wir werden die Prüftiefe daher zukünftig verbindlicher festlegen.

10.3.2 Erfahrungen mit den ersten Gutachten

Die ersten Gutachten haben gezeigt, dass die Bereitstellung einer **prüffähigen Musterkonfiguration** des Produkts sowie die entsprechende Dokumentation die Grundlagen einer erfolgreichen Begutachtung darstellen. Typische Schwachstellen traten in folgenden Bereichen auf:

- unzureichende Produktdokumentation, insbesondere fehlende Benutzerhandbücher, Risikoanalysen, Konfigurationshinweise;
- die freie Konfigurierbarkeit der Produkte konnte gerade zu datenschutzfeindlichen Konfigurationen führen;
- nicht dokumentierte und offene Schnittstellen, durch die unzulässige Nutzungen von Daten möglich waren (Export von datenschutzgerechten Listen in Standard-Officeanwendungen, um dort dann Verknüpfungen mit der Folge von unzulässiger Auswertung vorzunehmen);
- Mängel bei der Abgrenzung der Produkte, fehlende Einbeziehung der Basissysteme und deren Sicherheits- und Datenschutzeigenschaften;
- Vermischung von rechtlichen, technischen und wirtschaftlichen Aspekten bei den Feststellungen und Beurteilungen im Gutachten.

Wir drängen aufgrund dieser Erfahrungen verstärkt darauf, dass die Hersteller eine prüffähige Musterkonfiguration definieren und bereitstellen, die den Anwendern dann später als Orientierungshilfe für den Einsatz des Produktes dienen kann. Eine schnellere **Klärung von Rückfragen**, die sich aus einer unzureichenden oder missverständlichen Dokumentation im Gutachten ergeben, ist nach unserer Erwartung durch die Vorlage des Produktes in seiner Prüfkonfiguration gegeben.

10.3.3 Fortentwicklung der Produktkriterien

Im März 2003 haben wir eine überarbeitete Version der Produktdokumentation veröffentlicht. In dieser Version sind Hinweise von Gutachtern sowie Erfahrungen mit den ersten bei uns eingereichten Gutachten berücksichtigt worden.

> **?** ***Common Criteria***
>
> *International abgestimmte Grundlage für Prüfung und Bewertung der Sicherheitseigenschaften von Produkten und Systemen der Informationstechnik, anwendbar auch bei der Entwicklung und Beschaffung.*

Durch die allgemein gehaltenen Produktkriterien wird eine weitere Annäherung an etablierte Standards angestrebt. Hier sind insbesondere die **Common Criteria** beispielhaft zu nennen. Diese Anpassung erfolgt auch vor dem Hintergrund, dass zukünftig gegenseitige Anerkennungen von Gutachten und Prüfzertifikaten mit anderen Prüfstellen (Landesdatenschutzbeauftragte, privatrechtliche Prüfinstitute usw.) auch im Hinblick auf eine zu erwartende bundeseinheitliche Regelung erfolgen sollen.

Informationen zur Produktdokumentation unter:

www.datenschutzzentrum.de/download/proddoku.pdf

Informationen über die überarbeiteten Produktkriterien unter:

www.datenschutzzentrum.de/guetesiegel/formgs.htm

11 Aus dem IT-Labor

11.1 Parallelbetrieb Windows NT 4.0 und Windows 2000/XP

Die letzten Jahre waren bezüglich der Betriebssysteme durch eine Monokultur geprägt. Nahezu alle Daten verarbeitenden Stellen im Lande setzten das Produkt Windows NT 4.0 ein. In Zukunft werden in den Behörden verstärkt unterschiedliche Betriebssysteme zum Einsatz kommen. Dieser Entwicklung muss unser IT-Labor Rechnung tragen.

Vor zwei Jahren haben wir damit begonnen, in unserem IT-Labor zusätzlich zu dem **Referenzsystem** für das Betriebssystem Windows NT 4.0 eines für das neue Betriebssystem **Windows 2000/XP** zu installieren. Die Maßnahme, die mit nicht unerheblichen Investitionen verbunden war (vgl. 23. TB, Tz. 10.2), ist zwischenzeitlich weitgehend abgeschlossen. Unsere Mitarbeiter simulieren auf beiden Systemen einerseits die Konfigurationen, die wir bereits in der Praxis vorfinden, andererseits werden Systemkomponenten und systemnahe Software getestet, von denen wir annehmen, dass sie künftig in der öffentlichen Verwaltung im Lande eine Rolle spielen. Derartige Produkte werden uns meist von den Herstellern oder Anbietern zur Verfügung gestellt. Außerdem steht über das Internet inzwischen ein großer Markt an Free- und Shareware bereit.

Schleswig-Holstein DATENSCHUTZAKADEMIE

Kurse NT, WIN-I

Entgegen den euphorischen Prognosen einiger Marktanalysten vollzieht sich in der Verwaltung der Übergang von dem einen auf das andere Betriebssystem bei weitem nicht so schnell wie erwartet. Das bedeutet für unsere Mitarbeiter, dass wir über einen längeren Zeitraum **zweigleisig fahren** müssen. Sowohl bei Prüfungen vor Ort als auch bei Beratungen und Schulungsmaßnahmen in der DATENSCHUTZAKADEMIE Schleswig-Holstein (vgl. Tz. 17) müssen wir uns „**im fliegenden Wechsel**“ mit beiden Systemwelten befassen. Hieraus ergibt sich praktisch eine Verdopplung unserer Investitionen in die eigene Schulung und Fortbildung. Die unter Tz. 7.2 dieses Berichtes beschriebenen Anforderungen an die Daten verarbeitenden Stellen im Lande bezüglich der personellen und finanziellen Ausstattung der Systemadministration gelten also auch für unsere Dienststelle.

In den nächsten Jahren wird sich diese Problematik noch verstärken. Die Zeiten der Betriebssystemmonokulturen dürften vorüber sein. Neben der Microsoft-Systemsoftware werden sich auch **Open-Source-Produkte** anderer Anbieter auf Linux-Basis auf dem Markt etablieren. Auf der Server-Ebene ist dieser Trend im Bereich der Firewall-Systeme schon sehr ausgeprägt. Eine weitere Diversifikation unseres IT-Labors und eine Verbreiterung der Wissensbasis unserer Mitarbeiter sind daher vorprogrammiert.

11.2 Neues backUP-Magazin für Windows 2000/XP in Vorbereitung

Die beiden backUP-Magazine zu den Sicherheitsmechanismen im Betriebssystem Windows NT 4.0 waren offensichtlich für die Praktiker in den IT-Stellen der Behörden im Lande so hilfreich, dass wir gedrängt werden, entsprechende Ausarbeitungen für das Betriebssystem Windows 2000/XP zu erstellen.

Für alle auf dem Markt gängigen Betriebssysteme gibt es neben den von den Herstellern mitgelieferten Handbüchern und Online-Hilfen eine sehr breite Kommentierung durch freie Spezialisten und Praktiker. Diese in der Regel sehr umfangreichen Werke sind sicherlich für professionelle Administratoren großer IT-Systeme sehr nützlich. Ganz offensichtlich befriedigen sie aber nicht die Bedürfnisse der Mehrzahl der Systemadministratoren kleinerer Verwaltungen, wie sie im Lande vorherrschend sind. Anders ist nicht zu erklären, dass die von uns herausgegebenen **backUP-Magazine** zum Betriebssystem Windows NT 4.0 solche Renner geworden sind. Wir nutzen sie nicht nur als Grundlage für die betreffenden Kurse der DATENSCHUTZAKADEMIE Schleswig-Holstein. Es sind auch bereits einige tausend Exemplare an die Behörden inner- und außerhalb des Landes verteilt worden (vgl. 24. TB, Tz. 11.1).

Kurse NT, WIN-I

So war es nicht verwunderlich, dass wir unmittelbar nach den ersten Installationen des Betriebssystems **Windows 2000/XP** nach einer entsprechenden Handreichung gefragt wurden. Unser spezifischer Ansatz, Vorschläge für eine sichere und revisionsfähige Systemkonfiguration zu machen, die auch von einem „normalen" Administrator einer durchschnittlich großen Verwaltung verstanden und umgesetzt werden können, kann also ganz offensichtlich auch bei dem neuen Betriebssystem nicht durch die Standard-Fachliteratur abgedeckt werden.

Obwohl wir sehr frühzeitig in unserem IT-Labor mit den entsprechenden Analysen begonnen haben, müssen wir die Anfrager noch mindestens bis **Mitte 2003** vertrösten. Die Ursache hierfür liegt in der „Mächtigkeit" des neuen Betriebssystems. Es hat eine Fülle von Funktionen, die – richtig genutzt – zu einem recht hohen Sicherheitsniveau führen können. Werden bestimmte Sicherheitsstrategien aber nicht konsequent durchgehalten, können leicht gravierende Sicherheitslücken entstehen. Dies alles muss zunächst getestet werden, bevor wir die von uns favorisierten Lösungen publizieren können. Uns steht für diese Arbeit neben dem Tagesgeschäft nur wenig Zeit und entsprechend ausgebildetes Personal zur Verfügung. Man darf nicht übersehen, dass dieses Projekt nicht unserer gesetzlichen Hauptaufgabe „Kontrolle", sondern dem Nebenauftrag „Beratung" zuzuordnen ist.

Wie groß die **Bandbreite der** zu behandelnden **Themen** ist, zeigt sich an der Grobgliederung der in Arbeit befindlichen Broschüre:

Kurs WIN-I

- Migration von Windows NT 4.0 auf Windows 2000,
- Windows 2000-Grundlagen,
- Domain Name System (DNS),
- Active-Directory-Grundlagen,

- Microsoft Management Console (MMC),
- Verwaltung von Benutzer- und Gruppenkonten,
- Verwaltung von Sicherheitsrichtlinien,
- Verwaltung von Dateien und Ordnern,
- Verwendung der Überwachungsrichtlinien und Ereignisanzeigen,
- Security-Tools und Security-Informationen,
- Umgang mit Systemschwachstellen.

11.3 Mozilla – verblasst ein Stern am Browserhimmel?

Bereits im Jahr 2001 haben wir den Open-Source-Browser Mozilla ein erstes Mal unter die Lupe genommen und dabei interessante Funktionen und erfreuliche Ansätze zum Schutz der Privatsphäre gefunden. Eine neue Analyse der aktuellen Versionen lässt den einen oder anderen Fleck auf der glänzenden Oberfläche erscheinen.

Dem Nutzer bietet Mozilla (in den Versionen 1.0.0 und 1.1) die Möglichkeit, per Menü den Browser-Cache zu löschen. Diese aus Datenschutzsicht an sich zu begrüßende Option vermittelt leider nur eine trügerische Sicherheit, muss man doch feststellen, dass die **Löschfunktion nur unvollständig** durchgeführt wird (vgl. 24. TB, Tz. 11.5). Mozilla hat nämlich folgende Eigenheiten:

Über den Menüpunkt „Bearbeiten/Eigenschaften“ gelangt der Nutzer zu einem sich öffnenden Fenster, welches ihm viele interessante Möglichkeiten zur Konfiguration seines Browsers bereitstellt. Unter dem Ordner „Erweitert“ befindet sich der Unterordner „Cache“ mit dem Button „**Festplatten-Cache** löschen“. Dem Nutzer wird kurz die Funktion eines Caches mit seinem Vorteil des Geschwindigkeitsgewinns beim erneuten Aufruf von Webseiten erklärt. Falls er sich jedoch dafür entscheidet, den Festplatten-Cache per angebotenem Button zu löschen, wird dieser nicht vollständig gelöscht. Nach Einsicht in dem recht tief in der Verzeichnisstruktur liegenden Cache-Ordner erkennt man, dass vier von Mozilla erzeugte Cache-Dateien sowie eine variable Anzahl von HTML-Files erhalten bleiben.

Die größte der vier Cache-Dateien (_CACHE_001_) beinhaltet die **Historie aller besuchten Websites** im Klartext, was man mithilfe eines einfachen Texteditors feststellen kann. Es werden die URLs – einschließlich der eingegebenen Suchwörter bei einer Suchmaschine – mit Besucherdatum und -zeit sowie weitere Logdaten innerhalb eines nicht vorhersagbaren Zeitraums erfasst. Der Sinn dieser Datei ist leicht erklärt: Der Browser muss entscheiden, ob er eine Datei neu laden muss oder sie aus dem Cache abrufen kann. Nach der Anforderung einer URL vergleicht er das Datum der angeforderten Datei mit dem Datum der Datei derselben URL aus seinem Cache, falls diese dort schon vorhanden ist. Damit der Browser nicht jedes Mal eine angeforderte Datei in seinem Cache öffnen muss, um ihr Datum auszulesen, wird eine Datei (_CACHE_001_) erzeugt, in der alle wichtigen Daten von den besuchten und zwischengespeicherten Websites abgelegt

sind. Der Browser benutzt dann diese Daten in _CACHE_001_, um einen Vergleich durchzuführen. Das hat einen erheblichen Geschwindigkeitsgewinn zur Folge. Allerdings lassen sich aus diesen Daten auch sehr schnell Surfprofile von einzelnen Personen erstellen.

Zusätzlich bleiben trotz des Löschens eine unbestimmte Anzahl von HTML-Files erhalten. Einige enthalten vollständige Websites, während andere nur den Code für Frames einer Website beinhalten. Nach ersten Beobachtungen war nicht zu erkennen, nach welcher Gesetzmäßigkeit diese **HTML-Files** vom Löschen verschont bleiben. Diese Resistenz ist unabhängig von der Größe der Datei, dem Zeitpunkt ihres Aufrufs oder ihrem Inhalt. Die Files, welche vollständige Websites enthalten, lassen sich natürlich mit einem Browser aufrufen und liefern ein recht anschauliches Ergebnis über die Surfvorlieben des Nutzers.

Sicherlich bleibt dem Nutzer die Möglichkeit, den Cache-Ordner **manuell zu löschen**. Dazu muss er sich aber (unter Windows 2000) erst den folgenden langen Pfad entlanghangeln:

C:\Dokumente und Einstellungen\
Nutzername\
Anwendungsdaten\
Mozilla\
Profiles\
Profilname\
Zufallsbezeichnung.slt\
Cache\.

Dort kann er dann händisch alle Dateien löschen. Der weniger geübte Nutzer wiegt sich allerdings in Sicherheit, nachdem er den Button „Festplatten-Cache löschen“ gedrückt hat.

Dass auch von Mozilla vorgesehen war, alle Dateien im Cache zu löschen, lässt sich daran erkennen, dass die oben genannten vier Cache-Dateien bei Nichtvorhandensein von Mozilla neu erzeugt werden. Somit ist zu hoffen, dass in den **folgenden Versionen** des Open-Source-Browsers (Release 1.2 war für Ende 2002 angekündigt) dieser Mangel behoben sein wird.

11.4 Knoppix: Open Source im Westentaschenformat

Das Open-Source-Betriebssystem Linux ist immer mehr Menschen ein vertrauter Begriff, jedoch scheuen sich viele noch davor, es einmal auszuprobieren, da der Installationsaufwand zu hoch erscheint. Mit „Knoppix“ ist diese Hemmschwelle beiseite geräumt.

Bei Knoppix handelt es sich um eine **Linux-Variante**, die Office- und Internet-Anwendungen fertig installiert mitbringt, die sich von CD-ROM starten lässt und daher keine lokale Installation auf dem Rechner erfordert. Knoppix erkennt die Hardware automatisch und schreibt keine Daten auf die Festplatte, sondern nur in den Arbeitsspeicher des Rechners.

Neben dem reinen Ausprobieren von Linux ergeben sich daher noch weitere Anwendungszwecke. Denn da es sich bei der CD um ein nicht beschreibbares Medium handelt, besteht keine Gefahr, dass Nutzer absichtlich oder aus Versehen Änderungen vornehmen und den Rechner damit längere Zeit außer Gefecht setzen. Zudem lassen sich aufgrund der beschriebenen Funktionsweise auch Arbeitssitzungen realisieren, die keine Datenspuren auf dem PC hinterlassen. Knoppix wurde in unserem IT-Labor getestet und kommt nun auch als **Rettungs- und Analysesystem** zum Einsatz, wenn ein Rechner nicht mehr so will, wie unsere Techniker es gerne hätten.

Erhältlich ist Knoppix entweder als CD-Image zum **kostenlosen Download** bei http://www.knopper.net/knoppix/, als Beigabe zu PC-Zeitschriften oder per Postversand. Ende 2002 hatte auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Versand von Knoppix-CDs angeboten. Dieser Service musste zwar zwischenzeitlich wieder eingestellt werden, jedoch verweist das BSI auf seinen Webseiten immer noch auf das Download-Angebot.

11.5 TCPA & Palladium

Immer mehr Bürgerinnen und Bürger wenden sich an uns mit Fragen zum Thema TCPA und Palladium. Sie fürchten um die Hoheit über die Daten auf ihren PCs. Während diese Thematik in der Öffentlichkeit bisher nur am Rande wahrgenommen wird, gewinnt sie für die Schwerpunktthemen – Datenschutz und Informationsfreiheit – zunehmend an Bedeutung.

Bei TCPA handelt es sich um die **Trusted Computing Platform Alliance**, einen von Compaq, HP, IBM, Intel und Microsoft gegründeten Zusammenschluss, dem sich inzwischen ca. 200 weitere Firmen angeschlossen haben. Ziel dieses Zusammenschlusses ist es, eine „vertrauenswürdige“ Rechnerplattform durch Erweiterung der Hardware um eine TCPA-Komponente zu ermöglichen. **Palladium** ist eine Softwarekomponente, die Microsoft in kommende Windows-Versionen integrieren will. Sie soll auf TCPA aufsetzen und weitere Funktionen wie z. B. eine digitale Rechtekontrolle (Digital Rights Management, DRM) für Software und Inhalte bereitstellen.

Das Prinzip der schon auf den ersten Hauptplatinen zu findenden TCPA-Komponenten ist dabei recht simpel: Sobald der PC gestartet wird, überprüft die TCPA-Komponente anhand einer gespeicherten Liste, die per Internet **von einem zentralen TCPA-Server** aktualisiert werden kann, sowie anhand von digitalen Zertifikaten das System (Hardware, Software) auf dessen Vertrauenswürdigkeit. Ist diese gegeben, wird die Kontrolle an eine entsprechende Komponente des Betriebssystems (bei Microsoft Palladium) übergeben. Nach diesem Muster soll gewährleistet werden, dass ein einmal als „vertrauenswürdig“ anerkanntes System nicht von Viren oder Angreifern manipuliert wird. Nutzerinnen und Nutzer sollen sich auf ihr System verlassen können.

Nicht nur dies hört sich gut an. In der Tat führen die Befürworter von TCPA und Palladium viele Argumente an, die bereits seit Jahren von Datenschützern propagiert werden, wie z. B. die **prüfbare Authentizität** elektronischer Kommunikation durch Einsatz von starker Kryptographie.

Die **Besorgnis** der **Bürgerinnen und Bürger** bleibt dennoch nachvollziehbar, denn mit dem Einsatz von TCPA respektive Palladium wird ein großer Teil der Entscheidungsfreiheit bezüglich der auf dem eigenen Rechner stattfindenden Prozesse abgegeben. Da die Zertifikate, mittels derer sich eine Software im System authentisieren kann, einen bis zu sechsstelligen Betrag kosten sollen, dürfte eine Zertifizierung für Open-Source-Produkte indiskutabel sein. Sie werden auf TCPA-konformen Systemen (sprich: dem „Aldi-PC“ der nächsten Jahre) nicht mehr laufen. Die Verwendung von Open-Source-Software ist jedoch aus Sicht von Datenschutz und Informationsfreiheit zu bevorzugen.

Des Weiteren werden mittels TCPA-Mechanismen sämtliche **Nutzerdaten**, also auch selbst erstellte Dokumente usw., **verschlüsselt**. Das erscheint zunächst sehr erfreulich, denn so kommen Außenstehende nicht an die Dokumente, selbst wenn sie am selben Rechner sitzen. Allerdings ist es mehr als fraglich, ob die Regierungen dieser Welt und deren Sicherheitsbehörden diese standardmäßig aktivierte Verschlüsselung ebenfalls wünschen. Es ist daher davon auszugehen, dass sich entsprechende **Hintertüren** für (amerikanische) Nachrichtendienste in der Implementierung wieder finden werden. Vom Einsatz von Kryptographieprodukten, die Hintertüren für wen auch immer enthalten, ist hingegen dringend abzuraten. Der Einsatz eines derartigen Produktes in der öffentlichen Verwaltung wäre nicht verantwortlich.

So begrüßenswert es ist, bei der Arbeit mit persönlichen Daten ein System zu verwenden, das nur zertifizierte und garantiert manipulationsfreie Software zulässt, so unvereinbar ist es auch mit dem Recht auf informationelle Selbstbestimmung, wenn die Instanz, die diese relevanten Zertifikate erstellt, nicht frei gewählt werden kann. Letztlich nützt einem auch das beste Zertifikat im Zweifelsfall nichts. Ein (für viel Geld) jeweils aktuell zertifizierter **Browser** mit deutlichen **Sicherheitsmängeln** hat trotz des Zertifikats nun einmal Mängel im Bereich der Sicherheit. Die zu vermutende Entwicklung beeinträchtigt aber die Freiheit der Anwenderinnen und Anwender, bei erkannten Mängeln auf ein besseres – aber unzertifiziertes – Konkurrenzprodukt umzustellen.

Bisher gibt es so gut wie keine unabhängigen Informationen oder Erfahrungsberichte bezüglich des Einsatzes von TCPA, zudem befinden sich die Spezifikationen in einer permanenten Fortschreibung. Unsere Mitarbeiter verfolgen und analysieren daher die Entwicklung, damit wir fundiert Stellung beziehen und den Bürgerinnen und Bürgern **Informationen liefern** können.

12 Europa

Richtlinie zum Datenschutz bei der elektronischen Kommunikation verabschiedet

Nach längerer Vorarbeit wurde im Jahr 2002 die neue Richtlinie zum Datenschutz bei der elektronischen Kommunikation verabschiedet. Sie überträgt im Wesentlichen die datenschutzfreundlichen Regelungen aus dem Bereich der herkömmlichen Telekommunikation auf das Internet und bietet zudem einen besseren Schutz vor unverlangten Werbezusendungen.

Im 24. Tätigkeitsbericht (Tz. 12.2) hatten wir über die Aktivitäten der Europäischen Union berichtet, eine neue **Richtlinie zum Datenschutz bei der elektronischen Kommunikation** zu erlassen. Im Juli 2002 verabschiedete das Europäische Parlament und der Rat der Europäischen Union die fertige „Richtlinie 2002/57/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation“. Zur Problematik der unverlangten Werbezusendungen findet sich dort nun eine nutzerfreundliche Regelung. Nach Art. 13 Abs. 1 der Vorschrift darf elektronische Post nicht für Zwecke der Direktwerbung verwendet werden, wenn keine vorherige Einwilligung der Teilnehmer vorliegt. Damit hat sich grundsätzlich das Opt-In-Modell durchgesetzt. Eine Einschränkung erfährt diese Regelung lediglich in den Fällen, in denen bereits ein Kontakt zu einem Kunden beim Verkauf eines Produkts oder einer Dienstleistung besteht. In diesen Fällen gilt eine Opt-Out-Regelung, d. h., in diesen Fällen sind Werbesendungen per E-Mail zunächst gestattet. Widerspricht der Kunde jedoch einer solchen Werbung, so hat sie künftig zu unterbleiben. Die Kunden sind auf das Widerspruchsrecht hinzuweisen. Ausdrücklich verboten ist die Versendung von Werbe-E-Mails ohne Angabe des Absenders (vgl. Tz. 8.3).

? Opt-In

Die Einwilligung des Betroffenen muss ausdrücklich erklärt werden.

? Opt-Out

Solange der Betroffene nicht widerspricht, dürfen seine Daten verarbeitet werden.

Die Mitgliedstaaten müssen die Richtlinie bis Ende Oktober 2003 in **nationales Recht** umsetzen. In Deutschland sind nur wenige Rechtsänderungen nötig, da die meisten Vorgaben bereits vom geltenden deutschen Recht abgedeckt werden. Lediglich die neuen und strengeren Regelungen für unverlangte Werbe-E-Mails werden in ausdrückliche Rechtsnormen gefasst werden müssen. Neben diesen erfreulichen Änderungen enthält die neu gefasste Richtlinie allerdings auch einen Wermutstropfen. Dies ist die Öffnungsklausel, die es den Mitgliedstaaten grundsätzlich gestattet, Vorschriften zur **Vorratsspeicherung** zu erlassen (vgl. Tz. 8.5).

Was ist zu tun?
Das Land Schleswig-Holstein sollte darauf hinwirken, dass der deutsche Gesetzgeber zügig seine Pflicht zur Umsetzung der datenschutzfreundlichen Regelungen der neuen europäischen Richtlinie nachkommt.

13 Informationsfreiheit

13.1 Bilanz nach zwei Jahren Informationsfreiheitsgesetz in Schleswig-Holstein

Unsere Erhebung bei den Kommunen und Landesbehörden in Schleswig-Holstein hat ergeben, dass sich das Informationsfreiheitsgesetz inzwischen gut etabliert hat. Nennenswerte Probleme mit der Umsetzung in der täglichen Behördenpraxis gibt es offensichtlich nicht.

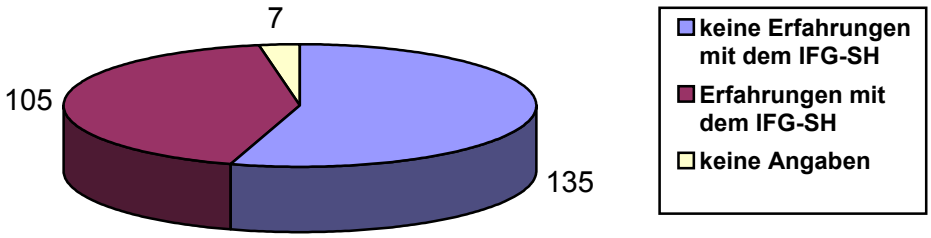
Bis zu der von uns durchgeführten Erhebung hatten wir nur sehr wenige Erkenntnisse über den Umfang der Inanspruchnahme des Informationsfreiheitsgesetzes und der dabei möglicherweise auftretenden Probleme. Wir konnten die uns bekannt gewordenen Konfliktfälle und die Beratungsersuchen nur sehr bedingt hochrechnen. Tatsächlich wurden schon in den ersten beiden Jahren nach dem In-Kraft-Treten des Gesetzes von mehr als **2000** Bürgerinnen und Bürgern **Informationsgesuche** gestellt. Vermutlich liegt die Zahl sogar noch höher, denn viele Behörden führen keine Aufzeichnungen über die Informationsgesuche und konnten deshalb keine genauen Angaben machen.

Es wurden Informationen aus **allen Verwaltungsgebieten** nachgefragt. Das größte Interesse galt dem Bau- und Planungsbereich. Hinterfragt wurden aber z. B. auch die Modalitäten der Vergabe von Kindergartenplätzen, die Arbeitsbelastung von Richtern, die landwirtschaftliche Förderpraxis, die Wirtschaftlichkeit von Kurverwaltungen, Organisationsfragen bei der Polizei und die Arbeitsweise der Tierschutzbehörden.

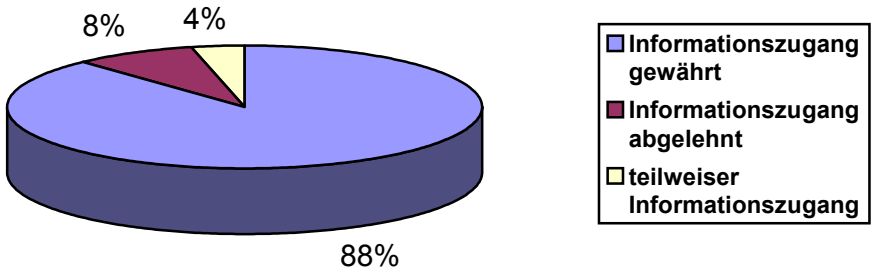
Folgende Aufstellung zeigt die Reihenfolge der Themen, wofür sich die Bürgerinnen und Bürger am häufigsten interessierten:

1. Baurecht
2. Sozial-, Jugendhilfe, Soziales, Schule
3. Kommunale Gremien (Protokolle usw. einschließlich Kosten)
4. Umwelt/Natur
5. Scientology/Sekten
6. Verkehr
7. Wasser/Abwasser/Energieverbrauch
8. Erschließung
9. Tierschutz
10. Flughafen Holtenau
11. Vergabe von Aufträgen
12. Steuern

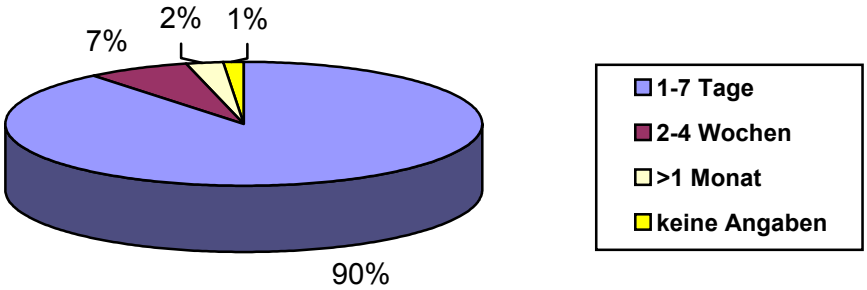
Dabei hielt sich der zur Beantwortung erforderliche **Arbeitsaufwand** in Grenzen. Die Informationsgesuche waren ziemlich gleichmäßig auf die Behörden verteilt. Die meisten Behörden, vorwiegend auf kommunaler Ebene, hatten maximal fünf Anträge zu bearbeiten. Etwa die Hälfte der Behörden hat noch keine Bekanntschaft mit dem Gesetz gemacht.



In **über 90 %** der Fälle hatten die Anträge **Erfolg**. Die begehrten Informationen wurden zugänglich gemacht.



Hervorzuheben ist, dass Schleswig-Holsteins Behörden bei Informationsgesuchen wesentlich schneller arbeiteten, als es das Gesetz verlangt. In 90 % der Fälle wurde **binnen maximal einer Woche** über die Anträge entschieden.



Damit konnte das Gesetz in der Praxis weitestgehend erfolgreich umgesetzt werden. Es zeigte sich, dass vieles, was in der Vergangenheit noch als geheimhaltungsbedürftig galt, den Bürgern mitgeteilt werden konnte. Negative Konsequenzen aus der größeren Offenheit sind uns nicht bekannt geworden.

Kulant waren die Behörden auch bei den Gebühren und Auslagen: Überwiegend wurden die **Informationen kostenlos** gegeben.

Alles in allem hat das Informationsfreiheitsgesetz in der Praxis offenbar mehr Bedeutung als bisher bekannt. Die Gesetzesanwendung funktioniert allem Anschein nach weitgehend **reibungslos und ohne Verzögerung**. Schleswig-Holsteins Bürgerinnen und Bürger nehmen ihre neuen Rechte zunehmend in Anspruch, und die Verwaltung beweist bislang beim Umgang mit der neuen Offenheit **Souveränität und Umsicht**.

13.2 Interessante Einzelfälle

- **Anwendbarkeit des IFG-SH auf Unterlagen über fiskalisches Handeln**

Einsichtsanträge in **Ausschreibungsunterlagen** haben uns bereits wiederholt beschäftigt, so auch in diesem Jahr. Ein Petent – selbst Inhaber eines Mineralölhandels – wollte Einsicht in Wärmelieferungsverträge nehmen, die ein schleswig-holsteinischer Kreis zur Versorgung seiner eigenen Gebäude mit zwei großen Energieversorgungsunternehmen abgeschlossen hatte. Der Kreis versagte die Akteneinsicht mit der Begründung, er habe hier nur zur Deckung seines Eigenbedarfes gehandelt. Der Anwendungsbereich des IFG-SH sei durch die Definition der Behörde im § 3 des Gesetzes auf öffentlich-rechtliche Handlungsformen beschränkt.

Wir haben den Kreis darauf hingewiesen, dass es für die Anwendbarkeit des Gesetzes nicht darauf ankommt, in welcher Handlungsform die Behörde konkret tätig wird. Eine Einschränkung auf klassische öffentlich-rechtliche Verwaltungstätigkeit findet im Gesetz keine Stütze (vgl. 24. TB, Tz. 13.1). Der Gesetzgeber hat nicht beabsichtigt, dass der gesamte Bereich der **staatlichen Eigenbedarfsdeckung** praktisch von der Informationsfreiheit ausgeklammert wird und damit weiterhin undurchsichtig bleibt.

Auch der Hinweis des Kreises auf den Schutz von Betriebs- und Geschäftsgeheimnissen seiner Vertragspartner zog nicht. Die uns vorgelegten Verträge und Wärmeabrechnungen enthielten zwar Mengen und Preise. Um Vertragsmodalitäten der Kategorie von Betriebs- und Geschäftsgeheimnissen zuordnen zu können, muss die Offenbarung der in den Verträgen enthaltenen Fakten jedoch einen beträchtlichen wirtschaftlichen Schaden des betroffenen Unternehmens nach sich ziehen und diese schutzwürdigen Belange das **Offenbarungsinteresse der Allgemeinheit** überwiegen. Eine dahin gehende Prognose war hier nicht zu stellen. Da es sich lediglich um Vereinbarungen über die Versorgung einzelner kreiseigener Liegenschaften handelte, also für ein regional begrenztes Gebiet, waren spezielle das Unternehmen schädigende Rückschlüsse auf dessen allgemeine Kalkulationsgrundlagen im Ganzen oder seine Stellung auf dem Markt nicht möglich. Für ein durchaus bestehendes Interesse der Allgemeinheit an der Offenbarung sprach dagegen gerade die Art und Weise der Ausschreibung: Es handelte sich nämlich um eine so genannte **freihändige Vergabe**, bei der bestimmte Konditionen zwischen den Vertragspartnern frei aushandelbar sind. Die Öffentlichkeit darf sich durchaus dafür interessieren, zu welchen Konditionen die öffentliche Hand solche Verträge abschließt. Die Abwägung der widerstreitenden Interessen musste hier also eindeutig zugunsten der Allgemeinheit getroffen werden. Da der Landrat gleichwohl den Informationszugang verweigerte, musste letztlich eine **förmliche Beanstandung** ausgesprochen werden.

- **Können sich auch Strafgefangene auf das Informationsfreiheitsgesetz berufen?**

Grundsätzlich gilt, dass sich Strafgefangene wie jede andere Bürgerin und jeder andere Bürger auf das Recht auf Informationsfreiheit berufen können. Will ein Strafgefangener also Zugang zu Informationen erlangen, die bei einer öffentlichen Stelle vorhanden sind, wozu auch die **Justizvollzugsanstalt** gehört, kann er einen entsprechenden Antrag stellen. Berechtigten Interessen der Haftanstalt – etwa wenn der Gefangene in die Baupläne der Anstalt schauen will – kann selbstverständlich ausreichend durch die im Informationsfreiheitsgesetz geregelten Ausnahme- und Beschränkungstatbestände Rechnung getragen werden.

Das Informationsfreiheitsgesetz findet hingegen **keine Anwendung** für den Fall, dass der Strafgefangene Einsicht in seine eigene Gefangenenpersonalakte nehmen will. Das **Strafvollzugsgesetz** regelt spezialgesetzlich und abschließend das Vollzugsverhältnis und somit auch die damit verbundenen Rechte des Strafgefangenen auf Informationszugang. Es trägt den Besonderheiten des Strafvollzuges dadurch Rechnung, dass ein Auskunftsinteresse dann zurückstehen muss, wenn die Sicherheitsinteressen der Anstalt dies erfordern.

- **Zugang zu Niederschriften über Verkehrsschauen**

Die Verkehrsschauen dienen dem Zweck, in regelmäßigen Abständen durch die Straßenverkehrsbehörden im Zusammenwirken mit den beteiligten öffentlichen Stellen, z. B. der Polizei, zu überprüfen, ob die Voraussetzungen für einen reibungslosen Ablauf des Straßenverkehrs vorliegen, und die erforderlichen Maßnahmen zu treffen. Es ist gut nachvollziehbar, dass die Bürgerinnen und Bürger sich über die Ergebnisse derartiger Verkehrsschauen informieren möchten, vor allem, wenn es sich dabei um die Verkehrsverhältnisse in der unmittelbaren Nachbarschaft handelt. Eine Einschränkung ist allenfalls dann zu machen, wenn **personenbezogene Daten Dritter** in der Niederschrift enthalten sind. Beispielsweise ist dies der Fall, wenn die Ausweisung eines behindertengerechten Parkplatzes ins Auge gefasst ist und dazu Daten des Betroffenen in der Niederschrift erwähnt sind. Dann muss die Niederschrift zumindest so aufbereitet werden, dass sie keinen Personenbezug enthält.

13.3 Entwicklung des Informationsfreiheitsrechts in Deutschland und in der EU

Während auf EU-Ebene die Informationsfreiheit weiter vorangetrieben wird, hat der Bundesgesetzgeber es versäumt, entsprechende Gesetze auf den Weg zu bringen. Damit ist Deutschland weiterhin Schlusslicht im internationalen Vergleich.

- **Geplante EU-Regelung über die kommerzielle Nutzung von öffentlich zugänglichen Dokumenten?**

Auf EU-Ebene besteht bereits die Verordnung über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (vgl. 24. TB, Tz. 13.3). Im Sommer dieses Jahres hat die Kommission eine **Richt-**

linie über die Verwertung und kommerzielle Nutzung von Dokumenten des öffentlichen Sektors vorgeschlagen. Ziel der Richtlinie ist die Förderung europäischer Informationsdienste und die Schaffung gleicher Grundbedingungen für alle Akteure im europäischen Binnenmarkt. Der Vorschlag bezieht sich auf allgemein zugängliche Dokumente und solche Informationen, die von öffentlichen Stellen als Ausgangsmaterial für von ihnen vertriebene Informationsprodukte oder -dienste verwendet werden. Derartige Informationen können etwa statistische oder meteorologische Daten sein, aber auch Informationen aus Tourismus oder Geographie, die von öffentlichen Informationsstellen und Presseämtern vorgehalten werden.

Zu klären ist unter anderem, was unter **kommerziell** verstanden wird. Gehören auch Informationen dazu, die ein Unternehmen einsehen möchte, um daraus einen eigenen Nutzen zu ziehen? Kann das Unternehmen diese Informationen dann später weitergeben, ohne selbst als Informationsanbieter in Betracht zu kommen? Unklar bleiben weiterhin die in dem Entwurf genannten „anderweitigen Zwecke". Hier wird der nationale Gesetzgeber, der die Richtlinie umzusetzen hat, auch im Hinblick auf die bereits bestehenden Informationsfreiheitsgesetze gefordert sein, eine Präzisierung vorzunehmen.

- **Informationsfreiheitsgesetz und Verbraucherinformationsgesetz auf Bundesebene gescheitert**

Der Bundesgesetzgeber hat es in der letzten Legislaturperiode versäumt, die Informationsfreiheitsrechte auf Bundesebene zu regeln. Damit gerät **Deutschland** immer mehr in die Rolle des **Schlusslichts** auf internationaler Ebene. Gerade angesichts der Korruptionsfälle, über die auch in diesem Jahr quer durch die Republik berichtet wurde, hätte Veranlassung bestanden, das Informationsfreiheitsgesetz auf den Weg zu bringen. Stattdessen kamen die Bedenken gegen den Gesetzentwurf gerade aus den Fachressorts, deren Unterlagen von Interesse für die Bürgerinnen und Bürger gewesen wären. Die daraufhin zusätzlich in das Gesetz eingearbeiteten Ausnahmen hätten den Grundsatz der unbeschränkten Aktenöffentlichkeit fast ins Gegenteil verkehrt. Es bleibt zu hoffen, dass in der laufenden Legislaturperiode rechtzeitig ein Versuch unternommen wird, die Informationsfreiheit auf Bundesebene zu etablieren. Ein Bundesgesetz, das den Namen Informationsfreiheitsgesetz auch wirklich verdient, hätte sicher auch Signalwirkung für diejenigen Bundesländer, in denen zurzeit noch keine Informationsfreiheit herrscht.

Ebenfalls gescheitert ist das **Verbraucherinformationsgesetz**. Blieb von dem ursprünglich von der Bundesregierung vorgelegten Entwurf nach den Beratungen im Bundestag schon nicht allzu viel übrig, so scheiterte das Gesetz endgültig im Bundesrat. Dabei wäre angesichts der vielen Skandale auf dem Gebiet des Verbraucher- und Lebensmittelrechts der letzten Jahre ein Gesetz, das die Interessen der Verbraucher tatsächlich effektiv schützen und verbessern hilft, dringend notwendig. Dass es zu den Aufgaben der Regierung gehört, durch rechtzeitige Informationen die Bewältigung von Konflikten in Staat und Gesellschaft zu erleichtern, auf Krisen schnell und sachgerecht zu reagieren sowie den Bürgern zu Orientierungen zu verhelfen, hat das Bundesverfassungsgericht am 26. Juni 2002 festgestellt. Aktuelle Krisen im Agrar- und Lebensmittelbereich, so das Gericht weiter, zeigten beispielhaft, wie wichtig öffentlich zugängliche, mit der Autorität

der Regierung versehene Informationen zur Bewältigung solcher Problemlagen sind. Es bleibt zu hoffen, dass dieser Appell nicht ungehört verhallt.

13.4 Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands (AGID)

Die Informationsbeauftragten der Bundesländer Brandenburg, Berlin, Schleswig-Holstein und Nordrhein-Westfalen haben auch in diesem Jahr den Erfahrungsaustausch über allgemeine und spezielle Fragen des Informationszuganges fortgesetzt.

Neben der Entwicklung der Informationsfreiheit auf Bundesebene (vgl. Tz. 13.3) und dem Erfahrungsaustausch über die Informationsfreiheitsgesetze in den Ländern bildete die Forderung nach mehr Transparenz im Bereich **verwaltungsinterner Vorschriften** einen Schwerpunkt. Bürgerinnen und Bürger interessieren sich häufig dafür, auf welcher Grundlage die Verwaltung Entscheidungen trifft. Durch die Veröffentlichung von internen Verwaltungsvorschriften können behördliche Entscheidungen transparenter gemacht werden und zu mehr Akzeptanz beim Bürger führen. Die Informationsbeauftragten Deutschlands haben daher in einer Entschließung die generelle Veröffentlichung aller Verwaltungsvorschriften und Richtlinien, die für Verwaltungsentscheidungen herangezogen werden, gefordert.

Was ist zu tun?
Bundes- und Landesbehörden sowie Kommunen, die im Internet präsent sind, sollten sämtliche vorhandenen verwaltungsinternen Regelungen ins Netz stellen.

14 Was es sonst noch zu berichten gibt

14.1 Neues Landesdisziplinargesetz

Mit dem Entwurf des Gesetzes zur Neuregelung des Disziplinarrechts sind gegenüber dem bisherigen Recht weit reichende Änderungen beabsichtigt. In Übereinstimmung mit dem inzwischen verabschiedeten Bundesgesetz soll auf die Institution des Untersuchungsführers verzichtet werden. Künftig ist nur noch ein einheitliches behördliches Disziplinarverfahren vorgesehen. Zur Durchführung der Aufgaben soll eine „zentrale Disziplinarbehörde“ im Innenministerium geschaffen werden, was auf eine Professionalisierung der Verfahren zielt. Diese zentrale Disziplinarbehörde soll auch beratend für den kommunalen Bereich tätig werden. Auf unseren Vorschlag wurden im Gesetzentwurf die Regelungen über die Aufbewahrung abgeschlossener Disziplinarvorgänge zugunsten der Betroffenen überarbeitet. Außerdem wurde die notwendige Befugnisgrundlage zur Übermittlung von Personalaktendaten für die Fälle in den Entwurf aufgenommen, in denen die zentrale Disziplinarbehörde Beratungsleistungen für den kommunalen Bereich erbringen soll. Nach diesen Änderungen entspricht der Entwurf den datenschutzrechtlichen Anforderungen.

14.2 Wozu braucht ein privater Hafenverwalter Angaben zur Schiffsversicherung?

Eine Kommune an der Kieler Förde hat die Verwaltung des gemeindeeigenen Sporthafens auf einen Privatunternehmer übertragen. Schiffseigner, die einen Liegeplatz haben wollen, müssen ein Antragsformular ausfüllen, auf dem neben Name, Anschrift, Telefon- und Faxnummer bestimmte Schiffsdaten (z. B. Typ, Länge, Breite, Tiefgang ...) anzugeben sind, damit ihnen geeignete Liegeplätze zugewiesen werden können. Schließlich – und genau das war für einen Liegeplatzinhaber der Stein des Anstoßes – werden noch folgende Angaben zur Schiffsversicherung abgefragt: Haftpflicht: Ja/Nein, Kasko: Ja/Nein, Name der Versicherungsgesellschaft und Versicherungsnummer.

Die Erhebung der Angaben zum Schiffseigner bzw. zum Typ sowie zur Größe des Bootes ist nicht zu beanstanden, da diese Daten für die Zuweisung und Verwaltung der Liegeplätze erforderlich sind. Auch die Bestätigung der Liegeplatzinhaber, dass überhaupt eine Schiffsversicherung vorliegt, ist durch die kommunale Hafenbenutzungsordnung gedeckt und begegnet keinen datenschutzrechtlichen Bedenken. In der Hafensatzung ist nämlich geregelt, dass alle Boote, die den Hafen benutzen, versichert sein müssen. Anders sieht es allerdings bei den Angaben „Versicherungsgesellschaft“ sowie „Versicherungsnummer“ aus, die für die Durchführung der Hafenverwaltung und der Liegeplatzzuweisung nicht unbedingt erforderlich sind. Die Verarbeitung der strittigen Angaben kann daher nur auf freiwilliger Basis erfolgen. Wir haben dem Hafenverwalter vorgeschlagen, das verwendete Formular um einen Passus zur Freiwilligkeit dieser Angaben zu ergänzen. Der Hafenverwalter ist inzwischen unserem Vorschlag gefolgt.

14.3 Auskünfte an Rundfunkgebührenbeauftragte des NDR

In letzter Zeit ist es wiederholt zu Anfragen von Rundfunkgebührenbeauftragten des NDR gekommen, die für bestimmte Wohnbereiche Listenauskünfte aus dem Bereich der Zweitwohnungssteuer wünschten. Insbesondere ging es um Daten der Zweitwohnungssteuerpflichtigen, die nicht im Meldeamt mit zweitem Wohnsitz gemeldet waren. Diese Auskunftsersuchen wurden von den jeweiligen Kommunen zu Recht abschlägig beschieden, da das in der Abgabenordnung geregelte Steuergeheimnis insoweit keine Offenbarungsbefugnisse enthält.

14.4 Der Datenhunger der GEZ

Eine Kreisverwaltung wandte sich an uns mit der Frage, ob es zulässig sei, Mitarbeitern der Gebühreneinzugszentrale (GEZ) die Daten von Kfz-Händlern zu übermitteln, die Fahrzeuge auf sich zugelassen haben (Jahreswagen, „Tageszulassungen“ usw.). Die Datenverarbeitungsbestimmungen des Straßenverkehrsgesetzes sehen eine Übermittlung dieser Daten für diese Zwecke nicht vor. Dies haben wir auch gegenüber dem Norddeutschen Rundfunk deutlich gemacht und auf die zweifelhafte Praxis der Mitarbeiter der GEZ hingewiesen. Dort war man der Auffassung, dass die Nichtanmeldung von Rundfunkgebühren eine Ordnungswidrigkeit sei, die es rechtfertige, dass Kfz-Zulassungsbehörden die Daten von Kfz-Haltern zur Verfolgung dieser Ordnungswidrigkeiten übermitteln. Dabei wurde aber übersehen, dass zur Verfolgung von Ordnungswidrigkeiten keineswegs eine Vorratsspeicherung über Kfz-Halter zulässig ist.

14.5 Bundesgerichtshof stellt klar, dass Kfz-Halterdaten nicht „offenkundig“ sind

Einige Gerichte hatten Polizeibeamte, die für Bekannte und Freunde Halterdaten über dienstliche Systeme aus dem Fahrzeugregister in Flensburg abgerufen hatten, mit der Begründung freigesprochen, dass die Daten im Fahrzeugregister „öffentlich zugängliche“ Informationen seien. Dies hatten wir ebenso wie andere Datenschutzbeauftragte kritisiert. Wir vertreten die Auffassung, dass es sich bei dem Verkehrszentralregister keinesfalls um ein öffentlich zugängliches handelt. Diese Rechtsauffassung wurde nunmehr vom Bundesgerichtshof bestätigt. Der BGH stellte fest, dass *„offenkundig im Sinne von § 203 StGB solche Tatsachen sind, von denen verständige und erfahrene Menschen ohne weiteres Kenntnis haben oder von denen sie sich jederzeit durch Benutzung allgemein zugänglicher, zuverlässiger Quellen unschwer überzeugen können. Für die vorliegende Fallgestaltung kommt es entscheidend darauf an, ob diese Fahrzeugregister als „allgemeine zugängliche Quellen“ einzustufen sind. Das ist zu verneinen. Allgemein zugänglich sind Zeitschriften, Bibliotheken, Adress- und Telefonbücher usw. Öffentliche Register gehören dann nicht zu den allgemein zugänglichen Quellen, wenn die Einsichtnahme von einem berechtigten Interesse abhängig ist.“*

14.6 Mobilfunkanlagen als Geheimsache?

Die Regulierungsbehörde für Telekommunikation und Post (RegTP) hat im Sommer 2002 eine Datenbank in Betrieb genommen, die Angaben über die Standorte ortsfester Mobilfunksendeanlagen enthält. Die Datenbank dient dem Zweck, Kommunen den Abruf von Daten zur Erfüllung ihrer Aufgaben zu ermöglichen. Die Arbeitsgemeinschaft der kommunalen Landesverbände hat uns um eine datenschutzrechtliche Stellungnahme zu der Frage gebeten, ob die Daten auch an Dritte weitergegeben werden dürfen. Das ist dann zu bejahen, wenn die Voraussetzungen für einen Informationsanspruch nach dem Umweltinformationsgesetz (UIG) oder dem Informationsfreiheitsgesetz für das Land Schleswig-Holstein (IFG-SH) vorliegen. Beide Ansprüche beziehen sich auf die bei der Behörde **vorhandenen** Informationen. Da die Informationen sich in der externen Datenbank der RegTP befinden, ist fraglich, ob dieses Merkmal erfüllt ist. Ausreichend hierfür ist allerdings allein die **rechtliche Verfügungsbefugnis**, sodass Behörden im Ergebnis verpflichtet sind, die Informationen aus der Datenbank abzurufen, wenn ein Auskunftsanspruch besteht.

Bei der Prüfung des Auskunftsanspruchs ist datenschutzrechtlich entscheidend, ob durch das Bekanntwerden der Informationen personenbezogene Daten Dritter offenbart und damit schutzwürdige Interessen der Eigentümer, auf deren Grundstücken sich die Anlagen befinden, beeinträchtigt werden. Wir vertreten die Auffassung, dass die Offenbarung der Daten über die Standorte der Mobilfunksendeanlagen zulässig ist, obwohl diese Rückschlüsse auf die Grundstückseigentümer zulassen. Mobilfunksendeanlagen sind zumeist offen sichtbar auf dem Gebäude montiert oder auf dem Grundstück angebracht, sodass die Daten für jedermann offenkundig sind. Generell stehen daher schutzwürdige Belange den Ansprüchen der Bürgerinnen und Bürger auf Auskunft nach dem UIG bzw. dem IFG-SH nicht entgegen.

Unsere vollständige Stellungnahme kann im Internet abgerufen werden unter:

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

15 Rückblick

15.1 Bestellung von Mitarbeitern des Rechnungsprüfungsamtes als Datenschutzbeauftragte

Mitarbeiter der Rechnungsprüfungsämter sind nach unserer Auffassung durchaus geeignet, die Aufgabe der oder des Datenschutzbeauftragten zu übernehmen. Beide Stellen werden als Organe der Innenrevision innerhalb kommunaler Körperschaften tätig. Die damit verbundenen möglichen Synergieeffekte liegen auf der Hand. Strittig war jedoch in der Vergangenheit, ob die in der Gemeindeordnung garantierte Unabhängigkeit der Mitarbeiter der Rechnungsprüfungsämter eine Bestellung zum oder zur Datenschutzbeauftragten ausschließt (vgl. 24. TB, Tz. 4.1.1). Diese Unsicherheiten sind im Jahr 2002 durch das Gesetz zur Stärkung der kommunalen Selbstverwaltung beseitigt worden. Die Gemeindeordnung wurde dahin gehend geändert, dass die Ausschlussregelung für die Übernahme anderer Aufgaben nicht für die Stellung einer oder eines Beauftragten für den Datenschutz gilt. Daher können ab sofort auch Mitarbeiterinnen und Mitarbeitern der Rechnungsprüfungsämter Aufgaben des behördlichen Datenschutzes übertragen werden.

15.2 EUREKA – Forderungen umgesetzt

Im 24. Tätigkeitsbericht (Tz. 5) schilderten wir das am Verwaltungsgericht für den Bereich der Geschäftsstellen und der Richterarbeitsplätze eingeführte automatisierte Verfahren EUREKA. Die von uns erhobenen Forderungen für eine datenschutzgerechte Ausgestaltung von EUREKA sind mittlerweile weitgehend umgesetzt worden. Im Bereich der Richterarbeitsplätze wird ein spezielles Programm zum Einsatz gebracht. Damit ist die Verschlüsselung der Disketteninhalte sowie der Festplattenlaufwerke sichergestellt. Auch auf den heimischen Arbeitsplätzen dürfen die personenbezogenen Daten nur verschlüsselt abgelegt werden.

15.3 Kontrollkompetenz bei Staatsanwaltschaften – Unklarheiten beseitigt

In den zurückliegenden Jahren wurden wiederholt die Kontrollrechte des ULD infrage gestellt, wenn es darum ging, dass Bürgerinnen und Bürger sich beispielsweise darüber informieren wollten, ob ihr Telefon abgehört wurde. Diese Uneinigkeit ist jetzt durch eine Vereinbarung zwischen dem ULD und dem Generalstaatsanwalt beseitigt worden.

Danach steht fest, dass auch die Staatsanwaltschaften der Kontrollbefugnis des Datenschutzbeauftragten unterliegen. Die Kontrollkompetenz erstreckt sich dabei auch auf laufende Telefonüberwachungsmaßnahmen. Zugleich ist durch eine entsprechende Formulierung sichergestellt, dass in kritischen Fällen – etwa wenn der Erfolg des Verfahrens gefährdet wäre – eine Preisgabe von Ermittlungsinhalten vermieden wird. Gleichwohl ist auch in einem derartigen Fall gewährleistet, dass den Bürgerinnen und Bürgern mit dem ULD eine unabhängige Instanz zur Seite steht, die sich ihrer Belange objektiv annimmt und eventuelle Mängel intern bei

der Staatsanwaltschaft zum Thema macht. Der Wortlaut der Vereinbarung ist zu finden unter:

www.datenschutzzentrum.de/material/themen/polizei/ermittlg.htm

15.4 Datenvermeidung bei der Zweitwohnungssteuer

Gegen die Art und Weise, wie einige Kommunen die Daten zur Festsetzung der Zweitwohnungssteuer bei den Wohnungseigentümern erhoben haben, gab es in den letzten Jahren erhebliche Proteste (vgl. 24. TB, Tz. 4.10.3). Die Erklärungsvordrucke waren in der Tat umfassend zu überarbeiten und an die rechtlichen Gegebenheiten anzupassen. Dies ist inzwischen weitgehend geschehen. Wir bekommen zwar nach wie vor noch viele Anfragen von den Steuerpflichtigen, können aber generell „Entwarnung“ geben. Die Zeiten, in denen z. B. Verzeichnisse aller Mieter mit ihren Anschriften verlangt wurden, sind vorbei. Nunmehr begnügt man sich nur mit den Namen (ohne Vornamen und Anschrift), um Plausibilitätskontrollen durchführen zu können. Im Ergebnis findet praktisch keine personenbezogene Datenerhebung mehr statt.

15.5 Neumünster macht bei der Datensicherheit Nägel mit Köpfen

Die Stadt Neumünster hatte nach einer sicherheitstechnischen Überprüfung ihrer IT-Systeme durch uns eine Mängelliste abzuarbeiten, die ca. 40 Positionen umfasste (vgl. 24. TB, Tz. 7.5.1). Dieser Aufgabe hat sie sich intensiv unterzogen. Der Zwischenbericht, der uns im Juni 2002 vorgelegt worden ist, weist aus, dass die weit überwiegende Mehrzahl der Mängel abgestellt worden ist. Hierzu bedurfte es umfassender aufbau- und ablauforganisatorischer Veränderungen. Um das erreichte Sicherheitsniveau auch für die Zukunft zu gewährleisten, sind z. B. die Aufgaben des behördlichen Datenschutzbeauftragten dem Leiter des Rechnungsprüfungsamtes übertragen worden. Dort befasst sich ein Prüfer speziell mit den datenschutzrechtlich relevanten Belangen der EDV und insbesondere der eingesetzten Software. Bei der Abarbeitung der restlichen Positionen (z. B. Umbaumaßnahmen) will die Stadt sich durch uns beraten lassen.

16 Beispiele dafür, was die Bürgerinnen und Bürger von unserer Tätigkeit haben

1. *In einer psychiatrischen Klinik wurden Patientenunterlagen über viele Jahre hinweg als „aktive" Patientendokumentationen aufbewahrt, ohne dass deren Erforderlichkeit geprüft worden wäre und ohne dass der Zugriff hierauf auf das Nötige eingeschränkt war. Dies führte dazu, dass auch Nichtberechtigte (z. B. Doktoranden) auf teilweise hochsensible Uraltunterlagen zugreifen konnten. Auf unsere Forderung wurden die laufenden von den nicht mehr aktuellen Unterlagen getrennt. Ein Teil der alten, teilweise aus der Nazizeit stammenden Unterlagen wurde in eine ordentliche Archivierung überführt; ein großer, nicht mehr benötigter Teil wurde vernichtet.*

2. *Durch ein kleines Kreuz auf einer Karte bestimmen die Patienten in der Universitätsklinik in Kiel, welches Essen am nächsten Tag an ihr Bett geliefert wird. Bisher enthielten diese Karten, die innerhalb des Krankenhauses durch unzählige Hände gehen, neben dem vollständigen Namen auch die Anschrift und das Geburtsdatum. Nachdem wir dies infrage stellten, reagierte das Universitätsklinikum prompt und verzichtet zukünftig auf die Erfassung der Anschrift und des Geburtsdatums.*

3. *In Einbürgerungsverfahren wurde den Ausländerinnen und Ausländern landesweit eine Einwilligungserklärung abverlangt, dass Auskünfte bei allen denkbaren Behörden eingeholt werden könnten. Im Fall der Weigerung wurde die Antragsablehnung in Aussicht gestellt. Dadurch wurde nicht nur der Grundsatz der Datenerhebung beim Betroffenen durchbrochen. Gravierender war, dass die Antragstellenden nicht mehr überblicken konnten, welche Informationen bei der Einbürgerung herangezogen werden. In Kooperation mit dem Innenministerium wurde ein Einwilligungsformular entwickelt, das den Betroffenen größtmögliche Transparenz und Wahlfreiheit gibt, ohne dass bürokratische Hindernisse aufgebaut würden.*

4. *Ein Kieler Kindergarten kam auf die Idee, Fotos der Drei- bis Sechsjährigen auf einer eigenen Kindergartenhomepage zu veröffentlichen, was von einigen Müttern abgelehnt wurde. Dabei erwies sich, dass sich die meisten Eltern und der Kindergarten selbst gar nicht über die Risiken einer Internet-Veröffentlichung bewusst waren. Nunmehr werden in sämtlichen Kindergärten in Kiel die Eltern ordnungsgemäß informiert und können frei entscheiden, ob sie einer Veröffentlichung der Fotos ihrer Kinder im Internet zustimmen wollen.*

5. *Im Zuge der Umsetzung des Schwerbehindertengesetzes konnte es dazu kommen, dass der Arbeitgeber vom Landesarbeitsamt über intimste Details der zur Behinderung führenden gesundheitlichen Beeinträchtigung informiert wurde. Nachdem diese Vorgehensweise auch vom Bundessozialgericht kritisiert worden war, regten wir gegenüber der zuständigen Bundesanstalt für Arbeit eine Verfahrensänderung an. Dort reagierte man umgehend: Der Arbeitgeber wird künftig nur noch in Kenntnis und mit Zustimmung des betroffenen Schwerbehinderten beteiligt.*

6. *Bei der Durchführung von Laboruntersuchungen, die nicht von den gesetzlichen Krankenkassen, sondern von den Patienten selbst bezahlt werden, wurden bisher die Labore in den Auftragsvordrucken über zur Untersuchung nicht erforderliche Patientendaten informiert. Wir setzten eine datenschutzgerechte Gestaltung dieses Vordruckes durch, sodass die Labore nur noch die tatsächlich erforderlichen Patientendaten erhalten.*

7. *Wegen Baumaßnahmen im Städtischen Krankenhaus Kiel mussten Mitarbeiterinnen und Mitarbeiter dunkle Kellerflure nutzen, um von einem Gebäude zum anderen zu kommen. Die deshalb aus Sicherheitsgründen installierte Videoüberwachungsanlage hätte auch zur Mitarbeiterkontrolle genutzt werden können. Personalrat und Verwaltungsleitung folgten unserem Rat und schlossen eine Dienstvereinbarung, die den datenschutzrechtlichen Belangen der Mitarbeiter gerecht wird.*

8. *Nur in seltenen Ausnahmefällen dürfen Sozialämter vollständige Hilfeakten mit der Gesamtgeschichte eines Hilfeempfängers und den in der Regel sehr sensiblen Informationen an andere Sozialämter weitergeben. Dies hatten wir schon im November 1998 für Schleswig-Holstein im Amtsblatt und im Internet bekannt gegeben. Unter Berufung hierauf weigerten sich Sozialämter unseres Landes, Gesamtakten auf Anforderung an Ämter anderer Länder herauszugeben. Dies führte dazu, dass nun auch andere Länder inhaltlich unsere Hinweise übernahmen, sodass länderübergreifend eine einheitliche, praxisgerechte, datensparsame und damit bürgerfreundliche Vorgehensweise gefunden wurde.*

9. *Beantragen Hilfesuchende aus gesundheitlichen Gründen Leistungen, so benötigen die Sozialämter als Entscheidungsgrundlage ein amtsärztliches Gutachten. In vielen Sozialämtern herrschte Unsicherheit, welche Fragen dem Amtsarzt zu stellen und welche Angaben zur Begutachtung zu übermitteln sind. Durch die Mitentwicklung von Vordrucken zur Beauftragung amtsärztlicher Gutachten konnten wir dazu beitragen, dass nicht erforderliche sensible Gesundheitsdaten künftig nicht mehr in den Sozialhilfeakten landen.*

10. *In einer Klinik wurde eine Patientin nach einer ambulanten Behandlung in einem Fragebogen zu ihrer häuslichen Lebenssituation befragt, angeblich, um den Datenhunger der Krankenkassen zu stillen. Unsere Bemühungen führten zu einer Überarbeitung des Fragebogens, sodass künftig die Patienten über den Grund der Datenerhebung, nämlich die bessere Information des behandelnden Arztes, korrekt informiert werden.*

11. *Zwei Unternehmen verteilten die Lohnsteuerkarten ihrer Beschäftigten offen. Damit waren unbefugte Offenbarungen von Personaldaten vorprogrammiert. In beiden Fällen sorgten wir dafür, dass die Lohnsteuerkarten künftig in geschlossenen Briefumschlägen verteilt werden.*

12. *Eine Handelsauskunftei übermittelte bereits gesperrte Daten an ihre Kunden. Durch die Weitergabe von Informationen, deren Richtigkeit die Betroffenen bestritten, wurden einige in ihren Möglichkeiten, Darlehensverträge abzuschließen, erheblich eingeschränkt. Wir bewirkten eine effektive Sperrung der Daten und die Versicherung der Auskunftei, die Daten nicht ohne vorherige Beteiligung der Betroffenen an Dritte weiterzugeben.*

13. *Ein Unternehmen übermittelte im Rahmen einer Konzerndatenbank die Leistungsbewertung eines ehemaligen Mitarbeiters als schlecht, obwohl seine Arbeitsleistungen im Zeugnis mit gut bis befriedigend angegeben wurden. Wir erreichten eine Löschung des diskriminierenden Eintrages bei allen Konzernunternehmen.*

14. *Im Entwurf des Gesetzes zur Neuregelung des Disziplinarrechts war für bestimmte Fälle, in denen eine Disziplinarmaßnahme unzulässig ist, eine weitere Aufbewahrung der betreffenden Unterlagen für die Dauer von zwei Jahren vorgesehen. Da für diese die Betroffenen belastende Datenspeicherung kein sachlicher Grund bestand, wurde die Regelung auf unseren Vorschlag dahin gehend geändert, dass die Löschung der Daten nun unmittelbar nach Rechtskraft der Entscheidung erfolgt.*

15. *Der von uns angebotene Anonymitätsdienst AN.ON, der Surfern die anonyme Webnutzung ermöglicht, hat sich mittlerweile fest etabliert. Steigende Nutzungszahlen belegen, dass die Bürgerinnen und Bürger, aber auch Wirtschaftsunternehmen, Interesse an Maßnahmen haben, die sie selbst ergreifen können, um sich vor Beobachtung ihres Surfverhaltens durch Dritte schützen zu können.*

16. *Bis zum Zeitpunkt unserer Kontrolle konnten in einem Krankenhaus eine große Zahl von Mitarbeitern externer Softwarehäuser und Fernwartungsunternehmen unkontrolliert und unkontrollierbar die medizinischen Daten von Patienten aus dem Krankenhausinformationssystem auslesen und sogar verändern. Diese Sicherheitslöcher sind aufgrund unserer Beanstandungen unverzüglich geschlossen worden.*

17. *Bei einer flächendeckenden Kontrolle aller Handels- und Wirtschaftsauskunfteien des Landes wurden Mängel bei der Handhabung von besonders sensiblen Schuldnerdaten aufgedeckt. Die daraufhin veranlassten Verbesserungen des Datenschutzes minimieren das Risiko, aufgrund ungerechtfertigter Datenverarbeitung keinen Bankkredit mehr zu bekommen.*

18. *Die Mitarbeiter der Ambulanz eines schleswig-holsteinischen Klinikums offenbarten gegenüber der Polizei, dass sich eine gesuchte Person dort aufhielt. Die Polizei nahm die Betroffene fest und führte erkennungsdienstliche Maßnahmen durch. Auf unseren Hinweis, dass auch der Umstand, dass sich eine bestimmte Person zur ambulanten Behandlung in einer Klinik aufhält, grundsätzlich von der ärztlichen Schweigepflicht umfasst ist, wies die Hausleitung die Mitarbeiter an, derartige Auskünfte künftig zu unterlassen.*

19. *Bei der Versendung von Jahresmeldungen der Versorgungsanstalt des Bundes und der Länder durch das Landesbesoldungsamt war im Anschriftenfeld auch die Versicherungsnummer der Betroffenen abgedruckt. Da die ersten sechs Stellen der Versicherungsnummer das Geburtsdatum enthalten, wurden auf diese Weise vertrauliche Daten der Mitarbeiter veröffentlicht. Auf unser Betreiben hin wurde die vom Landesbesoldungsamt vorgegebene Adressierung der Umschläge geändert.*

20. *Die jährlich 120.000 Gutachten mit medizinischen Daten des Medizinischen Dienstes der Krankenversicherungen werden aufgrund der Ergebnisse unserer Kontrolle wirksamer gegen unbefugte Kenntnisnahme abgeschottet. Dazu gehört z. B., dass die Diskettenlaufwerke der Arbeitsplatzrechner deaktiviert, die Möglichkeiten der Einsichtnahme der Systemadministratoren begrenzt und die Anonymisierungsmethoden für statistische Datensätze verbessert wurden.*

21. *Das Justiz- und Frauenministerium forderte zum Zwecke der Kontrolle der Verwendung von Fördermitteln von Frauenhäusern namentliche Listen der dort aufgenommenen geschützten Frauen und Kinder. Hiergegen wandten sich die Frauenhäuser, weil sie eine große Gefahr für die untergebrachten Frauen und Kinder befürchteten, wenn diese Listen in falsche Hände gerieten. Auf unsere Intervention hin gibt sich das Ministerium künftig mit einer pseudonymisierten Aufstellung zufrieden, die sowohl Kontrollierbarkeit als auch Vertraulichkeitsschutz gewährleistet.*

22. *Das Internet steckt voller Risiken für die Privatsphäre der Nutzerinnen und Nutzer. In unserer Reihe „Safer Surfen“ bieten wir umfangreiche Hilfestellungen zum Selbstdatenschutz rund um das Thema „Sicherheit im Internet“. Die Servicewebseiten unter www.datenschutzzentrum.de/selbstdatenschutz/ wurden im Berichtszeitraum aktualisiert und bieten neben Aspekten wie Internet-Sicherheit und Verschlüsselung auch Informationen zur Anwendung von neuen Datenschutztechnologien für den eigenen Computer.*

17 DATENSCHUTZAKADEMIE Schleswig-Holstein

17.1 Neustrukturierung der DATENSCHUTZAKADEMIE

Am 28. August 2002 wurde ein neuer Kooperationsvertrag zwischen dem **Deutschen Grenzverein** und dem Unabhängigen Landeszentrum für Datenschutz zur Fortführung der DATENSCHUTZAKADEMIE Schleswig-Holstein unterzeichnet. Er löst den Vertrag aus dem Jahre 1993 ab. Auf seiner Grundlage wurde sie neun Jahre lang erfolgreich betrieben. Insgesamt wurden in dieser Zeit 350 Kurse mit zusammengenommen ca. 7100 Teilnehmern durchgeführt. Zusätzlich wird jährlich Ende August die Sommerakademie veranstaltet, die sich mit jeweils über 300 Teilnehmern mittlerweile zu einem bundesweit beachteten Datenschutzforum entwickelt hat. Nach der Änderung des Landesdatenschutzgesetzes hat die DATENSCHUTZAKADEMIE Schleswig-Holstein eine gesteigerte Bedeutung erhalten, weil die Vermittlung von Medienkompetenz nunmehr zu den gesetzlichen Aufgaben des Unabhängigen Landeszentrums für Datenschutz gehört. Da sich der Ansatz der Akademie als dauerhaft erfolgreich herausgestellt hat, war es notwendig geworden, die vertraglichen Grundlagen zu präzisieren und auf eine längere Dauer hin auszulegen.

Das Unabhängige Landeszentrum für Datenschutz und der Deutsche Grenzverein entschlossen sich, die Zusammenarbeit auch in Zukunft fortzusetzen. Dies bot sich auch deshalb an, weil die **Nordseeakademie in Leck**, eine Einrichtung des Deutschen Grenzvereins, in den letzten Jahren ein deutliches Profil im Bereich der Vermittlung von Medienkompetenz gewonnen hat. Der neue Vertrag sieht eine Arbeitsteilung zwischen dem Deutschen Grenzverein und dem Unabhängigen Landeszentrum für Datenschutz vor. Die Geschäftsführung und die inhaltliche Konzeption des Kursangebots wird vom Unabhängigen Landeszentrum für Datenschutz getragen, während dem Deutschen Grenzverein vornehmlich die organisatorische und finanzielle Abwicklung des Kursbetriebes obliegt. Über übergreifende Fragen entscheidet ein gemeinsamer Ausschuss, der außerdem den Wirtschaftsplan beschließt und die Jahresrechnung feststellt.

17.2 Fortbildungsprogramm 2003 der DATENSCHUTZAKADEMIE

Die DATENSCHUTZAKADEMIE geht mit dem Programm 2003 in das zehnte Jahr ihres Bestehens. Wer das erste Programm aus dem Jahr 1994 mit dem Programm 2003 vergleicht, kann gut nachvollziehen, wie sehr sich in diesen Jahren Technik und Recht im Datenschutzbereich verändert haben. In all diesen Jahren hat die DATENSCHUTZAKADEMIE ihren Beitrag zur Vermittlung der zur Bewältigung dieser Umbrüche notwendigen Medienkompetenz nach den Anforderungen der Praxis geleistet. Ihr Ziel bleibt es, auch in der Zukunft den Bürgerinnen und Bürgern und den Mitarbeiterinnen und Mitarbeitern in der schleswig-holsteinischen Verwaltung und Wirtschaft ein qualitativ gutes, preisgünstiges Fortbildungsprogramm zu bieten.

Das Jahresprogramm 2003 knüpft an das bisherige Kursangebot an und hat folgende neue Kurse aufgenommen:

- Datenschutz in der Arztpraxis (auch in Form von Halbtageskursen)
- Betriebliche Datenschutzorganisation nach dem Bundesdatenschutzgesetz
- Sicherheit beim Betriebssystem Windows 2000
- Prüfung zum Systemadministrator mit Datenschutzzertifikat
- Datenschutz für Bürger
- Safer Surfen im Internet
- Datenschutz am PC-Arbeitsplatz
- Datenschutz im Krankenhaus
- E-Government
- Datenschutz für Kommunalpolitiker
- Workshop zum Datenschutz im Schulsekretariat
- Seminar für Gütesiegel-Sachverständige
- Sozialdatenschutz

Veranstaltungsübersicht 2003 für die Kurse der DATENSCHUTZAKADEMIE Schleswig-Holstein

FEBRUAR:	Landesdatenschutzrecht Schleswig-Holstein	R 13	25.02.2003
	Systemdatenschutz nach LDSG	T 13	26.02.2003
MÄRZ:	Datenschutz am PC-Arbeitsplatz	DPC 1	06.03.2003
	Behördliche Datenschutzbeauftragte Recht	DR 5	24. - 25.03.2003
	Datensicherheitsrecht, Prüfung und Bewertung von Sicherheitsmaßnahmen durch behördliche Datenschutzbeauftragte	DT 5	26. - 28.03.2003
	Seminar für Gütesiegel-Sachverständige	GS 1	31.03. - 03.04.2003
APRIL:	Windows 2000 Sicherheit I	WIN-I 1	07. - 10.04.2003
	Informationsfreiheitsgesetz Schleswig-Holstein	IFG 7	10.04.2003
	Schutz von Personaldaten	P 11	15. - 16.04.2003
MAI:	Datenschutz in der Arztpraxis Grundkurs	AR-I 1	07.05.2003
	Einstieg in das Datenschutzrecht	E 14	08.05.2003
	Datenschutz im Krankenhaus	DK 1	13.05.2003
	Grundkurs Bundesdatenschutzgesetz	BDSG-I 1	13.05.2003
	Datensicherheit im Anwendungsbereich des BDSG	SIB 4	14.05.2003
	Datenschutz in der Arztpraxis Aufbaukurs	AR-II 1	14.05.2003
	Safer Surfen	SURF 1	15.05.2003 und 22.05.2003
	Einführung Datenschutz im Schulsekretariat	ES 13	22.05.2003
JUNI:	IT-Revision	ITR 3	03.06.2003
	Bundesdatenschutzgesetz Aufbaukurs	BDSG-II 1	04.06.2003
	Datenschutz für Bürger	DB 1	05.06.2003 und 12.06.2003
	Datenschutz am PC-Arbeitsplatz	DPC 2	12.06.2003
	Sozialdatenschutz	SD 1	17.06.2003
	Windows 2000 Sicherheit I	WIN-I 2	17. - 20.06.2003

AUGUST:	Windows 2000 Sicherheit I	WIN-I 3	12. - 15.08.2003
	Workshop für betriebliche Datenschutzbeauftragte	DWBT 2	26.08.2003
	Landesdatenschutzrecht Schleswig-Holstein	R 14	28.08.2003
	Systemdatenschutz nach LDSG	T 14	29.08.2003
SEPTEMBER:	Datenschutz bei der Internet-Nutzung	NET 6	09. - 10.09.2003
	Technik und Recht von Firewalls	FW 10	11.09.2003
	Einführung Datenschutz im Schulsekretariat	ES 14	11.09.2003
	Führung von Personalakten	PA 11	15. - 16.09.2003
	Grundkurs Bundesdatenschutzgesetz	BDSG-I 2	16.09.2003
	Datensicherheit im Anwendungsbereich des BDSG	SIB 5	17.09.2003
	Datenschutz in der Arztpraxis Gesamtkurs	AR 4	18.09.2003
	Datenschutz am PC-Arbeitsplatz	DPC 3	18.09.2003
	Behördliche Datenschutzbeauftragte Recht	DR 6	22. - 23.09.2003
	Datensicherheitsrecht, Prüfung und Bewertung von Sicherheitsmaßnahmen durch behördliche Datenschutzbeauftragte	DT 6	24. - 26.09.2003
	Datenschutz für Kommunalpolitiker	EK 9	26.09.2003
OKTOBER:	Informationsfreiheitsgesetz Schleswig-Holstein	IFG 8	01.10.2003
	Windows 2000 Sicherheit I	WIN-I 4	21. - 24.10.2003
	Safer Surfen	SURF 2	21.10.2003 und 28.10.2002
	Workshop für behördliche Datenschutzbeauftragte	DW 8	28.10.2003
	E-Government	EG 1	29.10.2003
	Personaldatenverarbeitung im Rahmen des Mitbestimmungsrechts	PR 7	30.10.2003
NOVEMBER:	IT-Revision	ITR 4	04.11.2003
	Bundesdatenschutzgesetz Aufbaukurs	BDSG-II 2	05.11.2003
	Datenschutz für Bürger	DB 2	11.11.2003 und 18.11.2003
	Datenschutz in der Arztpraxis Grundkurs	AR-I 2	12.11.2003
	Workshop zum Datenschutz im Schulsekretariat	ESW 1	12.11.2003
	Datenschutz am PC-Arbeitsplatz	DPC 4	13.11.2003
	Datenschutz in der Arztpraxis Aufbaukurs	AR-II 2	19.11.2003
	Prüfung zum Systemadministrator mit Datenschutzzertifikat	SDZ 1	20.11.2003
DEZEMBER:	Einstieg in das Datenschutzrecht	E 15	04.12.2003

Das Jahresprogramm 2003 der DATENSCHUTZAKADEMIE Schleswig-Holstein mit näheren Informationen und Anmeldeformular zu den Veranstaltungen kann kostenlos angefordert werden.

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein
Holstenstr. 98, 24103 Kiel
Fax: 0431/988-1223
E-Mail: akademie@datenschutzzentrum.de

Schleswig-Holstein
DATENSCHUTZAKADEMIE

Das Programm ist auch auf unserer Homepage im Internet verfügbar:

www.datenschutzzentrum.de/akademie/

17.3 Sommerakademie 2003

Am 25. August 2003 veranstaltet die DATENSCHUTZAKADEMIE in Kiel wieder eine Sommerakademie. Sie befasst sich in diesem Jahr mit dem Themenkreis Datenschutzaudit und Datenschutz-Gütesiegel. Sie trägt den Titel „Datenschutz mit Brief und Siegel – Kontrolle ist gut, Vertrauen ist besser“.

Datenschutzaudits und -Gütesiegel sind wichtige Instrumente des neuen Datenschutzes. Während der Datenschutz bislang von Ge- und Verboten, Kontrolle und Kritik geprägt war, eröffnen Audit und Gütesiegel neue, marktwirtschaftliche Perspektiven. Sie bieten einen Anreiz für das Design datenschutzgerechter IT-Produkte und belohnen ein gutes Datenschutzmanagement in Behörden und Betrieben. In Schleswig-Holstein konnten jetzt erste Erfahrungen mit gesetzlich geregelten Audits und Gütesiegeln gemacht werden.

Auf der Sommerakademie wird hierüber berichtet und eine erste Zwischenbilanz gezogen. Außerdem werden andere Zertifizierungsverfahren in Deutschland und die Pläne für ein Bundesauditgesetz vorgestellt. Audit und Gütesiegel haben langfristig nur eine Chance, wenn sie auf internationalen Standards beruhen. Deshalb bildet der Informationsaustausch über die Grenzen hinweg einen Schwerpunkt der diesjährigen Sommerakademie, die erstmals mit englischer Simultanübersetzung durchgeführt wird.

Weitere Informationen dazu werden veröffentlicht unter:

www.datenschutzzentrum.de/somak/somak03/somak03.htm

Wer eine Einladung zu dieser Veranstaltung haben möchte und noch nicht in unserem Versandverteiler ist, kann sich gerne vormerken lassen unter:

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstr. 98, 24103 Kiel
Fax: 0431/988-1223
E-Mail: akademie@datenschutzzentrum.de

Beim **ULD SH** erhältliche Publikationen:

Neues Datenschutzrecht in Schleswig-Holstein
Text des Landesdatenschutzgesetzes, der Datenschutzverordnung, des Informationsfreiheitsgesetzes, der Regelungen zum Datenschutzaudit und Datenschutz-Gütesiegel und des Bundesdatenschutzgesetzes

Tätigkeitsbericht
des letzten Jahres als Landtagsdrucksache

Faltblätter
Datenschutz ist auch nicht mehr das, was es einmal war
(Dienstleistungsangebot des ULD)
Safer Surfen!:
Clever verschlüsselt mailen, Selbst sicher(n)!, Ich bin drin! ... Und meine Daten?, Sicherheit durch Anonymität im Internet, P3P – ich hab's gecheckt und den Rest macht mein PC
Ihre Daten sind auch bei der Polizei geschützt
Patientenfaltblatt „Datenschutz in meiner Arztpraxis"
Datenschutz im Melderecht ... und was Sie persönlich davon haben
Virtuelles Datenschutzbüro – Virtual Privacy Office
Sicherheit durch Anonymität – Security by Anonymity
Datenschutzgerechte Biometrie – Privacy-compliant Biometrics
Das Informationsfreiheitsgesetz Schleswig-Holstein
Datenschutz-Audit und Datenschutz-Gütesiegel

Broschüren
Sicherheit durch Anonymität im Internet (Hintergründe zum Projekt AN.ON)
backUP-Magazin für IT-Sicherheit (Reihe)
Datenschutz leicht gemacht – Praxistipps zum Datenschutzrecht (Reihe)
Sich wohl fühlen in der Informationsgesellschaft – Das ULD stellt sich vor

Diverse Aufkleber
Der Mensch ist mehr als Null und Eins, Virtuelles Datenschutzbüro,
Aufkleber zum Thema E-Mail-Verschlüsselung, Rote Karte für Internet-Schnüffler

---

DATENSCHUTZAKADEMIE Schleswig-Holstein
Jahresprogramm 2003

Schleswig-holsteinische Datenschutzinformationen im Internet
Alle Datenschutzinformationen aus Schleswig-Holstein finden Sie natürlich auch auf der Homepage des ULD unter: **http://www.datenschutzzentrum.de**. Auf der umfangreichen Website finden Sie neben den Publikationen des Unabhängigen Landeszentrums für Datenschutz weitere umfangreiche Informationen zum Thema Datenschutz und das Fortbildungsangebot der DATENSCHUTZAKADEMIE Schleswig-Holstein. Weiterhin ist dort der öffentliche Schlüssel des Unabhängigen Landeszentrums für Datenschutz zur Verschlüsselung von E-Mails an das ULD 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 Browser mitgeliefert. Die CD-ROM kann beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein kostenlos angefordert werden.

Index

A

B

C

D

E

F

P

R

S

T

U

V

W

Z