



Bericht

**des Landesbeauftragten für den Datenschutz
bei der Präsidentin des Schleswig-Holsteinischen Landtages**

Vierzehnter Tätigkeitsbericht

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

Becker

VIERZEHNTER TÄTIGKEITSBERICHT
des Landesbeauftragten für den Datenschutz
bei der Präsidentin
des Schleswig-Holsteinischen Landtages

nach § 23 Abs. 3 des
Schleswig-Holsteinischen Gesetzes
zum Schutz personenbezogener Informationen
vom 30. Oktober 1991

(Berichtszeitraum: März 1991 bis Februar 1992)

Inhaltsverzeichnis	Seite
1. Landesdatenschutzgesetz gut – alles gut?	5
2. Wie weit geht die Informationspflicht der Regierung gegenüber dem Parlament?	10
3. Mehr Datenschutz ins Grundgesetz	
4. Sorgen der Bürgerinnen und Bürger, Ergebnisse von Kontrollen, Beratung der Behörden	13
4.1 Allgemeine und innere Verwaltung	13
4.1.1 Personalwesen	13
4.1.1.1 Probleme bei der Führung von Personalakten	13
4.1.1.2 Wer darf in Personalakten einsehen?	15
4.1.2 Verfassungsschutz	17
4.1.2.1 Das Unvorstellbare: Bürger erhalten in Schleswig-Holstein Auskunft vom Verfassungsschutz	17
4.1.2.2 Mängel bei der Sicherheitsüberprüfung: Daten nicht sicher	17
4.1.3 Öffentliche Sicherheit	22
4.1.3.1 Neues Polizeirecht setzt Maßstäbe	22
4.1.3.2 Konsequenzen aus der Kontrolle bei der Polizei lassen auf sich warten	24
4.1.3.3 APIS: Schleswig-Holstein geht mit gutem Beispiel voran	25
4.1.3.4 „Rosa Listen“: Nichts gefunden	26
4.1.3.5 Datenschutz auch für Polizeibeamte	27

4.1.3.6	Einschränkung der Meldungen über „Wichtige Ereignisse“	29
4.1.3.7	Unzulässige erkennungsdienstliche Behandlung aller Asylbewerber in Oelixdorf	29
4.1.3.8	Automatisierung der Vorgangsverwaltung bei der Polizei	30
4.1.4	Ausländerrecht	31
4.1.5	Bau- und Wohnungswesen	32
4.2	Datenschutz im Kommunalbereich	33
4.2.1	Erfahrungen mit dem neuen Kommunal- verfassungsrecht	33
4.2.1.1	Melderegisterauskunft an Bürgerinitiativen?	33
4.2.1.2	Aktenvorlage an Fraktionen der Stadtvertretung	34
4.2.2	Weitere Probleme und ihre Lösungen	34
4.2.2.1	Übermittlung von Steuerdaten an die Kirche	34
4.2.2.2	Aufnahme von Kindern in kommunale Kindergärten	35
4.2.2.3	Einkommensermittlung für Kindergartenbeiträge	36
4.2.2.4	Weitergabe von Adressen zu Werbezwecken	36
4.2.2.5	Ein Amt reagiert nicht	37
4.2.2.6	Steuerbescheid per Telefax	37
4.3	Justiz	38
4.3.1	GAST: Noch nicht alles im Lot	38
4.3.2	Datenschutz hinter Gefängnismauern	44
4.3.3	Überweisung von Gefangenengeldern: Problem gelöst	52
4.3.4	Mitteilungen in Strafsachen: Im Schneckentempo voran	52
4.3.5	Was ein Notar bei Sammelverträgen beachten muß	53
4.3.6	„Sprechende“ Briefumschläge unzulässig	54
4.3.7	Automatisierung der Datenverarbeitung bei der Justiz: Vorschußlorbeeren	55
4.3.8	Auch Richter müssen Datenschutz beachten	56
4.4	Gelingt es der Steuerverwaltung, sich dem Landesdatenschutzgesetz zu entziehen?	56
4.5	Wirtschaft und Verkehr	58
4.5.1	Subventionsgewährung und Datenschutz	58
4.5.2	Begründen Zwangsstillegungen einen Verdacht?	59
4.6	Sozial- und Gesundheitswesen	60
4.6.1	Soziales	60
4.6.1.1	Prüfung einer Betriebskrankenkasse	60
4.6.1.2	Außendienstmitarbeiter und zentrale Verwaltung	61
4.6.1.3	Landesaufnahmegesetz	61

4.6.2	Gesundheit	62
4.6.2.1	Offenbarung von Rezeptdaten an den Untersuchungsführer für die Berufsgerichtsbarkeit der Heilberufe	62
4.6.2.2	Ärztliche Gutachten per Telefax	62
4.6.2.3	Die Diskussion über die Erfassung von Krebserkrankungen dauert an	63
4.6.2.4	Darf ein „Laie“ die ärztliche Tätigkeit eines Krankenhausarztes überprüfen?	64
4.7	Endlich ein Archivgesetz	66
5.	Datenschutz im Medienbereich und bei neuen Übermittlungstechniken	67
5.1	Staatsvertrag über den Norddeutschen Rundfunk	67
5.2	Datenschutz bei Dienstleistungen der Deutschen Bundespost	68
5.3	Positives Echo auf Telefax-Tips	69
6.	Ordnungsmäßigkeit der Datenverarbeitung	70
6.1	Rechtliche und technisch-organisatorische Kriterien	70
6.1.1	Landesregierung in der Pflicht	72
6.1.2	Regelungsvorschläge des Landesbeauftragten	72
6.2	IT-Verfahrensregelung – Verwaltungsanweisung mit Schlupfloch	77
6.3	Wer bildet EDV-Verantwortliche aus?	78
6.4	Kontrollen und Prüfungen	80
6.4.1	Das Programm, das es gar nicht gab	80
6.4.2	Für Akten weniger Datensicherung als für Datenbanken?	81
6.4.3	Datensicherungsmaßnahmen – Wer entscheidet tatsächlich?	83
6.4.4	Der dornenreiche Weg bei der Behebung von Mängeln	85

1. Landesdatenschutzgesetz gut – alles gut?

Die Frage nach dem wichtigsten Ereignis im Berichtsjahr kann der Landesbeauftragte aus seiner Sicht leicht beantworten: Es war die Verabschiedung des neuen Landesdatenschutzgesetzes, das am 01.01.1992 in Kraft getreten ist. Damit hat auch der schleswig-holsteinische Gesetzgeber die Konsequenzen aus dem Volkszählungsurteil des Jahres 1983 gezogen. Herausgekommen ist dabei ein modernes, bürgerfreundliches Datenschutzgesetz, das den Vergleich mit den Gesetzen anderer Länder nicht zu scheuen braucht. Ohne daß hier auf alle Einzelheiten eingegangen werden soll – der Landesbeauftragte wird im Laufe dieses Jahres ausführliche Hinweise zur Anwendung des neuen Gesetzes herausgeben –, ist auf einige grundlegende Neuerungen zu verweisen. Der Anwendungsbereich des Datenschutzrechts ist beträchtlich erweitert worden. Jede Form der Verarbeitung personenbezogener Daten durch Stellen der öffentlichen Verwaltung unterliegt nunmehr dem Datenschutzrecht, gleichgültig ob es sich um eine automatisierte oder manuelle Verarbeitung, um eine Verarbeitung in Dateiform oder in Akten handelt. Von seiner Bedeutung und seinen Auswirkungen her rückt damit das Datenschutzrecht in eine Reihe mit dem allgemeinen Verwaltungsverfahrensrecht.

Das Gesetz verfolgt durchgängig die Tendenz, das Verwaltungshandeln im Bereich der Datenverarbeitung für die Bürgerinnen und Bürger transparenter und kontrollierbar zu machen. Dies beginnt bei den Vorschriften über die Datenerhebung, die eine offene Erhebung mit Aufklärung des Bürgers als Regelfall vorsehen und endet mit einem erweiterten Auskunft- und Akteneinsichtsanspruch. Die erstmals in das Gesetz aufgenommene Zweckbindung soll sicherstellen, daß der Betroffene sich darauf verlassen kann, daß seine Daten nicht zweckwidrig verarbeitet werden.

Eine Reihe von Vorschriften trägt den besonderen Gefährdungen, die in der automatisierten Form der Datenverarbeitung liegen, Rechnung. Diesem Ziel dient die erstmals ins Gesetz aufgenommene Pflicht für die datenverarbeitenden Stellen, ein Verzeichnis der eingesetzten Datenverarbeitungsgeräte sowie der verwendeten Betriebssysteme und Programme zu erstellen. Werden Daten nur in automatisierten Verfahren gespeichert, so müssen Programme verfügbar sein, mit deren Hilfe die Daten jederzeit lesbar gemacht werden können. Für die Landesregierung ist der Erlaß einer Rechtsverordnung zu den Einzelheiten einer ordnungsgemäßen automatisierten Datenverarbeitung durch öffentliche Stellen verbindlich gemacht worden.

Die Pflicht, einmal übermittelte Daten im nachhinein zu berichtigen und zu ergänzen, wenn sich wesentliche Umstände geändert haben, sowie der verschuldensunabhängige Schadensersatzanspruch sind neue Elemente im Datenschutzrecht. Mit den Vorschriften über den Einsatz der Videotechnik ist ein Einstieg in die gesetzliche Bewältigung dieser neuen Form der

Informationserhebung und -verarbeitung gefunden. Die Aufzählung der Verbesserungen für den Bürger im neuen Datenschutzrecht könnte noch eine Weile fortgesetzt werden.

Auch in anderen wichtigen Gesetzgebungsvorhaben hat der Gesetzgeber im vergangenen Jahr seinen Willen dokumentiert, das Datenschutzrecht zu verbessern. Erwähnt sei hier insbesondere die Novellierung des Polizeirechts, bei der der Landesbeauftragte seine Vorstellungen zu einem großen Teil durchsetzen konnte, sowie das Landesarchivgesetz, das einen Ausgleich zwischen den Interessen der Forschung und dem Persönlichkeitsrecht der Betroffenen schafft. Insgesamt präsentiert sich Schleswig-Holstein, was die gesetzliche Regelung des Datenschutzes angeht, in guter Form. Die gesetzlichen Grundlagen zur Gewährleistung des Datenschutzes der Bürger sind damit in weiten Bereichen fürs erste einmal geschaffen.

Die Entwicklung der Informationstechnik wird freilich dazu führen, daß die Verbesserung des gesetzlichen Instrumentariums auch weiterhin stets im Auge behalten werden muß. Die immer stärkere Vernetzung der Datenverarbeitungsanlagen zwingt beispielsweise dazu, Begriffe wie „datenverarbeitende Stelle“, „Übermittlung“, „Zweckbindung“ etc. stets neu zu überdenken und in ihrer grundrechtssichernden Funktion weiterzuentwickeln. Generell zeigt sich, daß eine datenschutzrechtliche Betrachtungsweise, die sich auf die bloße Wahrung der Individualrechte beschränkt, zu kurz greift.

Die vorausschauende Beurteilung, in welcher Weise sich wichtige Neuerungen im Bereich der automatisierten Datenverarbeitung sowohl für die Grundrechte einzelner als auch beispielsweise für die informationelle Gewaltenteilung zwischen den unterschiedlichen Behörden auswirken, gewinnt immer mehr an Bedeutung. Für eine solche datenschutzspezifische Technologiefolgenabschätzung bietet das neue Datenschutzrecht erste Ansätze. Das schleswig-holsteinische Landesdatenschutzgesetz enthält nunmehr eine Reihe von Bestimmungen, die auf die elektronische Datenverarbeitung zugeschnitten sind. Dadurch wird die automatisierte Form der Datenverarbeitung als ein Regelungsgegenstand des Datenschutzrechts anerkannt.

Die der Landesregierung auferlegte Pflicht, durch eine Rechtsverordnung die Einzelheiten einer ordnungsgemäßen automatisierten Datenverarbeitung festzulegen, muß zu einem Instrumentarium führen, das geeignet ist, negativen Folgen der Automation der Datenverarbeitung entgegenzuwirken. Der Landesbeauftragte hat dem Innenminister hierzu umfangreiche erste Vorschläge gemacht (vgl. Tz. 6.1). Auch die neu in das Gesetz aufgenommene Aufgabe des Landesbeauftragten, die obersten Landesbehörden sowie die sonstigen öffentlichen Stellen in Fragen des Datenschutzes und der Sozialverträglichkeit von Datenverarbeitungstechniken zu beraten, zeigt, daß der bloß individualrechtliche Ansatz des Datenschutzrechts bereits überwunden ist:

Das Bewußtsein, daß die Nachteile neuer Datenverarbeitungstechniken für das Datenschutzrecht und die hier notwendigen Gegenmaßnahmen frühzeitig in das Kalkül einzubeziehen sind, muß allerdings noch wachsen. Gelegentlich herrscht die Meinung vor, notwendige – manchmal zugegeben nicht eben billige – Datenschutzmaßnahmen seien so etwas wie überflüssige Luxuskosten, zu deren Deckung der Datenschutzbeauftragte erst einmal Vorschläge machen müsse. Dabei wird übersehen, daß die Kosten für notwendige Datenschutzmaßnahmen von vornherein Kosten der Datenverarbeitungstechnik sind. Niemand würde auf die Idee kommen, die Kosten für die Bremsen eines Autos gesondert zu berechnen und nur dann zu verausgaben, wenn er noch Geld übrig hat.

Manch schöner, gelegentlich in rosa Farben gemalter Rationalisierungsgewinn durch die Einführung neuer automatisierter Datenverarbeitungstechnik sieht anders aus, wenn den Beteiligten bewußt wird, welche Ausgleichsmaßnahmen notwendig sind, damit nicht unverantwortliche Risiken für die betroffenen Bürger, aber auch für die Verwaltung selbst entstehen. Einige davon sind in diesem Bericht behandelt. Dabei ist insbesondere auf die Notwendigkeit einer verbesserten Dokumentation automatisierter Datenverarbeitungsverfahren zu verweisen (vgl. Tz. 6.1.2). Sie ist für eine ordnungsgemäße Datenverarbeitung und deren Revisionsfähigkeit unabdingbar. Ein anderer Gesichtspunkt ist die Fortbildung der Mitarbeiter im Leitungsbereich der Verwaltung (vgl. Tz. 6.3). Sie müssen zwar nicht so ausgebildet werden wie diejenigen, die unmittelbar mit den Datenverarbeitungsanlagen umgehen. Sollen aber die Begriffe Verantwortung, Aufsicht und Revisionsfähigkeit von Verwaltungshandeln durch die Automatisierung der Datenverarbeitung nicht leere Worthülsen werden, müssen die hierfür Verantwortlichen spezielle, auf die Ausübung dieser Funktionen zugeschnittene Kenntnisse erhalten. Die bisherigen Aus- und Fortbildungspläne zielen nur auf diejenigen ab, die die Computer bedienen, nicht auf die, die sie kontrollieren sollen. Bei realistischer Betrachtungsweise müssen solche Aufwendungen deshalb ebenso wie alle anderen Neben- und Folgekosten bei der Kalkulation neuer Datenverarbeitungssysteme frühzeitig berücksichtigt werden.

Teil der Kosten der Automatisierung der Datenverarbeitung im weitesten Sinne sind auch die Kosten für die Datenschutzkontrollinstanzen. Die Aufgaben der Datenschutzkontrolle haben sich in den vergangenen Jahren kontinuierlich und mit dem Inkrafttreten des neuen Landesdatenschutzgesetzes noch einmal schlagartig vergrößert. Einige Zahlen mögen dies verdeutlichen. Gab es vor 10 Jahren in der öffentlichen Verwaltung in Schleswig-Holstein ca. 50 größere Betriebssysteme, so sind es derzeit mehr als 500. Sie sind überdies schwerer zu kontrollieren, da sie nicht an wenigen Orten konzentriert sind. Die Zahl der Dateien, die beim Landesbeauftragten für den Datenschutz registriert sind, ist über die Jahre stets angestiegen. Derzeit sind es ca. 3.500 automatisierte Dateien. Von diesen ist bislang nur ein kleiner Prozentsatz im Wege einer Quer-

schnittskontrolle oder auch nur anlässlich einer Einzeleingabe am Rande kontrolliert worden. Die Kontrolle einer einzigen Datei wie des staatsanwaltschaftlichen Verfahrens GAST dauert mit Unterbrechungen viele Monate.

Nunmehr unterliegen mit dem Inkrafttreten des neuen Landesdatenschutzgesetzes auch die Akten und sonstige Unterlagen mit personenbezogenen Daten der Datenschutzkontrolle. Das Kontrollfeld hat sich damit auf einen Schlag mehr als verdoppelt. Wer eine effektive Kontrolle der Datenverarbeitung bei der öffentlichen Verwaltung wirklich will, muß dafür auch das notwendige Personal zur Verfügung stellen. Die Personalausstattung der Dienststelle des schleswig-holsteinischen Datenschutzbeauftragten wird derzeit den Anforderungen nicht gerecht. Gelegentlich ist der Einwand zu hören, man wolle den Datenschutzbeauftragten nicht zu einer „Überbehörde“ ausbauen. Davon kann aber bislang nicht die Rede sein. Die Dienststelle des Landesbeauftragten für den Datenschutz gehört gewiß zu den kleinsten Behörden im Lande Schleswig-Holstein.

Zudem muß die Personalausstattung auch in Relation zum Aufgabenfeld gesehen werden. Auch hier ist der Blick auf Zahlen aufschlußreich. So geben beispielsweise die Ministerien des Landes allein für die Pflege und den Unterhalt ihrer Datenverarbeitungsprogramme durch die Datenzentrale Schleswig-Holstein pro Jahr ca. 40 Millionen Deutsche Mark aus. Hinzu kommen die Aufwendungen für die in eigener Regie betriebenen Datenverarbeitungssysteme sowie die Aufwendungen der Kommunen und anderen öffentlichen Stellen. Möglicherweise kommt dann noch einmal die gleiche Summe zusammen. Dem stehen ca. 1,1 Millionen Deutsche Mark für die Dienststelle des Landesbeauftragten für den Datenschutz gegenüber. Dieses Mißverhältnis hat sich in den letzten Jahren ständig vergrößert. Denkt man bei den zugegebenermaßen knappen Haushaltsmitteln nur in linearen Kategorien, so bringt beispielsweise bereits eine 4 %ige Steigerung des Betrages, den die Landesministerien für die Datenverarbeitung durch die Datenzentrale ausgeben, eine Mehrausgabe von 1,6 Millionen, also weit mehr als der gesamte Jahresetat der Dienststelle des Landesbeauftragten für den Datenschutz. Wenn hier nicht qualitative Schwerpunkte gesetzt werden, wird sich das Verhältnis zwischen den Aufwendungen für die automatisierte Datenverarbeitung und für die Datenschutzkontrolle in den kommenden Jahren weiter verschlechtern.

Bis sich die Dinge verbessern, müssen mit den vorhandenen Mitteln Schwerpunkte gesetzt werden. Der Landesbeauftragte hat deshalb bei seiner Kontrolltätigkeit einerseits die Interessen des durchschnittlichen Bürgers im Auge gehabt (vgl. Tz. 4.2.1, 4.3.5, 4.3.8, 4.4, 6.), sich andererseits aber auf Bereiche konzentriert, in denen besonders sensible Daten verarbeitet werden, wie z.B. Personaldaten (vgl. Tz. 4.1.1), Daten im Gesundheits- und Sozialwesen (vgl. Tz. 4.6.1.1), oder Sammlungen, in denen Daten über Minderheiten, Randgruppen und

andere Personen, die ihre Rechte selbst nicht so ohne weiteres wahrnehmen können, gespeichert sind. Hierzu zählen insbesondere die Querschnittsprüfungen im Bereich der Justizvollzugsanstalten des Landes (vgl. Tz. 4.3.2) sowie im Aufnahmelager für Asylbewerber in Oelixdorf (vgl. Tz. 4.1.3.7).

Dabei sind wieder schwere datenschutzrechtliche Mängel festgestellt worden. So werden in Oelixdorf alle Asylbewerber erkennungsdienstlich behandelt, obwohl dies nach dem Gesetz nur bei Zweifeln über die Identität zulässig ist. Die Kontrolle in den Gefängnissen hat ergeben, daß dort der Datenschutz vielfach noch ein Fremdwort ist. Obwohl die Rechtsprechung schon lange klargestellt hat, daß die Grundrechte auch für Gefangene gelten, sind ihre Daten innerhalb des Gefängnisses so gut wie ungeschützt. Jeder Bedienstete kann sich ohne Begründung jederzeit umfassend aus der Gefangenenpersonalakte über jeden Gefangenen informieren, auch wenn er unmittelbar nicht mit ihm zu tun hat. Dabei geht es um hochsensible Daten: Anklageschrift, Urteil, Familiengeschichte, psychische Auffälligkeiten usw., usw. Auch Dritte sind betroffen. Nicht nur intime Daten über die Familie der Gefangenen, sondern auch über Zeugen und Opfer der Straftaten sind vermerkt. Treten vergewaltigte Frauen als Nebenklägerinnen auf, so finden sie sich mit Name und Anschrift in den Gefangenenpersonalakten des Täters wieder.

Hinter solchen zeitaufwendigen Kontrollen müssen andere Bereiche zurückstehen. Aber auch die Abarbeitung und Umsetzung der erzielten Prüfungsergebnisse ist häufig ein mühseliges und zeitraubendes Unterfangen. Da dem Landesbeauftragten keine Mittel zur Durchsetzung seiner Rechtsauffassung zur Verfügung stehen, ist er darauf angewiesen, die betreffenden Behörden von der Notwendigkeit der Verbesserungen zu überzeugen. Häufig sind hierfür mehrere Jahre notwendig. So hat beispielsweise eine umfangreiche Querschnittskontrolle der Datenverarbeitung bei den Polizeibehörden des Landes im Jahre 1988 stattgefunden. Bis heute sind die Konsequenzen aus dieser Prüfung – über deren Notwendigkeit z.T. gar kein Streit besteht – zu einem großen Teil noch nicht gezogen (vgl. Tz. 4.1.3.2). Bei GAST (vgl. Tz. 4.3.1) und bei der Datenzentrale (vgl. Tz. 6.4.4) zeichnen sich hingegen bereits konkrete Veränderungen ab. Die Gespräche und Verhandlungen hierüber haben sich aber über das ganze Jahr hingezogen. Da der Landesbeauftragte nicht gewillt ist, die Konsequenzen aus seinen Querschnittskontrollen im Sande verlaufen zu lassen, wird durch eine derartige zögerliche Haltung wie etwa der Polizeibehörden unnötige Arbeitskapazität gebunden.

Aufs Ganze gesehen ergibt sich damit trotz der erheblichen Verbesserung der Gesetzgebungssituation kein Bild der ungeübten Freude. Solange nicht die notwendige Kapazität zur Kontrolle der Einhaltung der neuen gesetzlichen Vorschriften über den Datenschutz vorhanden ist, gilt es Theorie und Praxis des Datenschutzes in Schleswig-Holstein tunlichst auseinanderzuhalten.

2. **Wie weit geht die Informationspflicht der Regierung gegenüber dem Parlament?**

Zehn voluminöse Aktenordner lagen auf dem Tisch des Landesbeauftragten, dazu die Bitte der Landesregierung, diese Vorgänge zu prüfen und dem Landtag zuzuleiten. Was war der Anlaß?

Ein Bürger hatte im Vertrauen auf die Bauleitplanung und nach verschiedentlichen Abstimmungen mit Kreis-, Gemeinde- und Landesbehörden Grundstücke erworben und umfangreiche Infrastruktur und bauliche Maßnahmen in einer Gemeinde in die Wege geleitet. Die Planungen der zuständigen Stellen änderten sich, und eine Einigung über die Zulässigkeit der Vorhaben wurde schließlich nicht erzielt. Die folgenden Auseinandersetzungen und Prozesse hatten erhebliches Aufsehen in der Öffentlichkeit erregt und dazu geführt, daß sowohl im kommunalen Bereich wie bei der Landesregierung eine Reihe von Verwaltungsvorgängen entstanden. Sie betrafen ein breites Spektrum von Fragen des Denkmalschutzes, der Umweltverträglichkeit, des Bauordnungsrechtes sowie des Kommunalrechts und der Wirtschaftsförderung.

Wegen des ihm angeblich entstandenen Schadens wandte sich der Betroffene schließlich an den Eingabenausschuß des Landtages. Dessen Vorsitzender ersuchte die Landesregierung um Zuleitung der Akten für die Beratungen des Ausschusses. Die Landesregierung war sich nicht sicher, ob und welche Unterlagen sie dem Ausschuß zugänglich machen durfte, und bat den Landesbeauftragten um Beratung.

Die Landesregierung ist nach den Bestimmungen der Landesverfassung verpflichtet, einem Verlangen des Eingabenausschusses auf Vorlage von Akten für die Erfüllung seiner Aufgaben zu entsprechen. Welche Akten zur Wahrnehmung der Ausschußaufgaben benötigt werden, entscheidet dabei zunächst der Ausschuß selbst. Hat er dazu keine Bestimmung getroffen, muß die Landesregierung prüfen, welche Unterlagen einen solchen engen Bezug zum Sachverhalt haben, daß sie als notwendige Entscheidungsgrundlage für den Eingabenausschuß in Betracht kommen.

Die Regierung kann die Vorlage von Akten jedoch ablehnen, wenn dem Bekanntwerden des Inhalts „schutzwürdige Interessen einzelner, insbesondere des Datenschutzes, entgegenstehen“. In diesen Fällen muß das Recht des Eingabenausschusses auf Zugang zu den erforderlichen Informationen im konkreten Einzelfall gegenüber dem Recht Betroffener abgewogen werden, grundsätzlich selbst über die Preisgabe und Verwendung ihrer Daten zu bestimmen. Dem Aktenvorlagerecht des parlamentarischen Ausschusses, das Verfassungsrang hat, können schutzwürdige Interessen einzelner allerdings nur entgegengehalten werden, wenn sie von vergleichbarer Bedeutung sind, und auch dann ergibt sich nicht ohne weiteres ein Vorrang eines dieser Rechte. Sie müssen vielmehr, wie das

Bundesverfassungsgericht im „Flick-Urteil“ zur Rolle eines Untersuchungsausschusses ausführt, einander im konkreten Fall so zugeordnet werden, daß beide so weit wie möglich ihre Wirkung entfalten. Bei der Abwägung ist auch zu bedenken, in welchem Maße die Interessen Dritter gefährdet sind und wieweit die Vertraulichkeit der Vorgänge geschützt ist.

Zunächst muß berücksichtigt werden, daß der Betroffene selbst das Verfahren mit seiner Petition in Gang setzt. Inwieweit damit eine Einwilligung in die Beiziehung von Unterlagen verbunden ist, sollte in zweifelhaften Fällen ausdrücklich bei ihm erfragt werden.

Hinzu kommt, daß die Vertraulichkeit im Verfahren vor dem Eingabenausschuß stärker sichergestellt ist als bei der Aktenanforderung anderer Ausschüsse oder des Landtages selbst. Denn die Sitzungen des Eingabenausschusses sind nicht öffentlich: Personenbezogene Daten sind deshalb nicht Gegenstand öffentlicher Erörterungen. Damit gewährt eine Aktenvorlage an den Eingabenausschuß weitgehend angemessene Sicherheit für personenbezogene Informationen des Petenten. Nur in ganz besonderen Fällen dürften seine Interessen angesichts der bestehenden Sicherheitsvorkehrungen überwiegen.

Eine besondere Betrachtungsweise ist bei Daten über Dritte geboten. Sorgfältige Prüfung ist beispielsweise auch bei der Beiziehung von Dokumenten mit Meinungsäußerungen und Initiativen Dritter angezeigt, bei denen zweifelhaft ist, ob es sich um eine persönliche Korrespondenz mit Entscheidungsträgern handelt oder um Initiativen, die nach dem Willen ihrer Urheber im Rahmen des Verfahrens eine breitere Erörterung auch in der Öffentlichkeit finden sollen (z.B. Äußerungen von Hochschullehrern zum Denkmalschutz, von Bürgerinitiativen zur Erhaltung des Ortscharakters, von interessierten Wirtschaftskreisen zur Erweiterung des Fremdenverkehrs). Das gleiche gilt, wenn Daten freiwillig für einen ganz bestimmten Zweck, etwa im Rahmen anderer Vertragsbeziehungen offenbart werden.

Schließlich muß auch der Schutz solcher Informationen bedacht werden, die – wie etwa kommunale Steuerdaten – einem besonderen Amts- oder Berufsgeheimnis unterliegen.

Der Landesbeauftragte hat unter diesen Umständen der Landesregierung empfohlen zu prüfen

- ob Vorgänge bzw. Teile davon tatsächlich noch zum Gegenstand der Eingabe in enger Beziehung stehen oder ob sie nur in einem weitläufigeren Zusammenhang zu dem Verfahrenskomplex gehören;
- ob Akten, die – wie etwa solche über Denkmalschutzverfahren nach Untergang des Denkmals – allenfalls mit ihrem Verfahrensabschluß bedeutsam sein können, wirklich insgesamt benötigt werden;
- in welchen der verbleibenden Unterlagen besonders schützenswerte personenbezogene Daten enthalten sind.

3. Mehr Datenschutz ins Grundgesetz

Im Zuge der Herstellung der deutschen Einheit wurde auf Beschluß des Bundesrates eine Kommission „Verfassungsreform“ gebildet. Der schleswig-holsteinische Innenminister arbeitet in dieser Kommission mit und hat den Landesbeauftragten um Stellungnahme gebeten, ob auch datenschutzrechtliche Ergänzungen des Grundgesetzes für erforderlich und zweckmäßig erachtet werden. Dies hat der Landesbeauftragte aus folgenden Gründen bejaht:

Die elektronische Datenverarbeitung hat sich im letzten Jahrzehnt in einem Maße weiterentwickelt, das dazu zwingt, auch die staatlichen Schutzvorkehrungen gegen die Überwachung der Privatsphäre der Bürger zu verbessern. Die Rechtsprechung des Bundesverfassungsgerichts allein, so sehr sie bahnbrechend gewesen ist, reicht nicht aus, den gewachsenen Gefahren für die Rechte des einzelnen Bürgers wie auch für die freiheitlich-demokratische Grundordnung auf der Ebene des Verfassungsrechts zu begegnen. Entscheidungen des Bundesverfassungsgerichts stehen stets unter dem Vorbehalt der Revidierung und Fortentwicklung bei geändertem Sachverhalt oder veränderter Senatsbesetzung. Deshalb ist es geboten, daß der Verfassungsgesetzgeber selbst die notwendigen Vorkehrungen zum Schutz des einzelnen in der herausziehenden Informationsgesellschaft trifft.

Das Grundrecht auf informationelle Selbstbestimmung sollte nicht nur aus dem allgemeinen Persönlichkeitsrecht abgeleitet, sondern ausdrücklich ins Grundgesetz aufgenommen werden. Dabei bietet es sich an, den Inhalt dieses Grundrechts in Anlehnung an das Volkszählungsurteil des Bundesverfassungsgerichts so zu bestimmen, daß jeder selbst über die Verwendung der ihn betreffenden Daten bestimmen kann. Teil dieses informationellen Selbstbestimmungsrechts muß auch ein Anspruch auf Benachrichtigung über die Speicherung von Daten bzw. auf Auskunft über die bereits gespeicherten Daten sein. Einschränkungen dieses Rechts dürfen nur durch oder aufgrund eines hinreichend bestimmten Gesetzes erfolgen. Dadurch sollte zum Ausdruck gebracht werden, daß der Normenklarheit im Bereich von Einschränkungen des Rechts auf informationelle Selbstbestimmung eine besondere, über den allgemeinen Bestimmtheitsgrundsatz hinausgehende Funktion zukommt. Der Bürger soll bereits aus dem Gesetz erkennen können, mit welchen Beschränkungen seines Rechts auf informationelle Selbstbestimmung er rechnen muß.

Neue Techniken zur optischen und akustischen Überwachung machen es möglich, Informationen aus Wohnungen zu erheben, ohne daß physisch in die Wohnung eingedrungen wird. Es sollte deshalb in Art. 13 Grundgesetz ausdrücklich zum Ausdruck gebracht werden, daß in die Unverletzlichkeit der Wohnung auch nicht mit technischen Mitteln zur heimlichen Ton- oder Bildaufnahme eingegriffen werden darf. Ausnahmen hiervon sind nur im Rahmen eng begrenzter Tatbestands-

merkmale, etwa bei Gefahr für Leib und Leben, gesetzlich zuzulassen.

Das Datenschutzrecht ist vom Ansatz her auf den Schutz des einzelnen angelegt. Das Bundesverfassungsgericht hat im Volkszählungsurteil aber schon darauf hingewiesen, daß, wenn der einzelne nicht mit hinreichender Sicherheit übersehen kann, wer welche Daten über ihn bei welcher Gelegenheit verarbeitet, auch Gefahren für die freiheitlich demokratische Grundordnung insgesamt drohen. Diesen Aspekt gilt es in der Verfassungsdiskussion fortzuentwickeln. Der stetige Ausbau der elektronischen Datenverarbeitung schafft Risiken nicht nur für den einzelnen, sondern für Staat und Gesellschaft insgesamt. Dabei geht es auch um Fragen der Überschaubarkeit und Kontrollierbarkeit der elektronischen Datenverarbeitung. Einen wichtigen Beitrag zu einer notwendigen Technologiefolgenabschätzung könnte ein ständiger Ausschuß des Deutschen Bundestages leisten, der nicht nur die ökologischen Folgen von Planungsentscheidungen, sondern auch die sozialen Auswirkungen neuer Technologien untersuchen und beurteilen sollte.

Der Innenminister hat dem Landesbeauftragten bislang noch nicht mitgeteilt, ob er diese Vorschläge unterstützt und in die Beratungen der Kommission „Verfassungsreform“ einbringen wird.

4. Sorgen der Bürgerinnen und Bürger, Ergebnisse von Kontrollen, Beratung der Behörden

4.1 Allgemeine und innere Verwaltung

4.1.1 Personalwesen

Der Landesbeauftragte hat im vergangenen Jahr über seine Prüfung im Bereich der Personalverwaltung berichtet (13. TB, S. 11). Inzwischen ist der Prüfungsbericht der Fachverwaltung zugeleitet worden, die dazu Stellung nehmen wird. Auf seine Erfahrungen aus dieser Prüfung konnte der Landesbeauftragte bei der Beurteilung weiterer Problemfälle aus der Personalverwaltung zurückgreifen.

4.1.1.1 Probleme bei der Führung von Personalakten

Datenschutzrechtliche Mängel in einem Zwangspensionierungsverfahren

Durch eine Eingabe wurde der Landesbeauftragte auf ein Zwangspensionierungsverfahren aufmerksam, bei dem dem Dienstherrn neben Verfahrensfehlern offensichtlich auch eine Reihe datenschutzrechtlicher Fehler unterlaufen waren.

Ein Beamter erledigte nach Auffassung seines Dienstvorgesetzten nur noch mit Einschränkungen seine Dienstgeschäfte.

Ursache waren zum einen häufige krankheitsbedingte Ausfallzeiten, aber auch die Tätigkeit des Betroffenen selbst gab verschiedentlich Anlaß zu Beschwerden Dritter. Da eine Versetzung auf einen anderen Arbeitsplatz nicht in Betracht kam, sah der Dienstvorgesetzte den einzigen Ausweg in einer Frühpensionierung des Mitarbeiters. Der war jedoch damit nicht einverstanden.

Eingeleitet wurde das Verfahren durch schriftliche Berichte des unmittelbaren Dienstvorgesetzten an die personalverwaltende Stelle. Sie wurden zur Personalakte des Betroffenen genommen, obwohl sie vom Inhalt und Verfahren her Mängel aufwiesen. So enthielten die Berichte

- Krankheitszeiten eines anderen Mitarbeiters;
- Fehlzeiten des Betroffenen, ohne daß deren Ursache aufgeklärt worden war;
- Beschwerden Dritter, ohne daß der Sachverhalt geklärt oder dienstrechtlich bewertet wurde;
- allgemeine dienstliche Probleme, wie Schwierigkeiten im Vertretungsfall, die unzulässig mit der Person des Betroffenen verknüpft wurden.

Wegen dieser Mängel durften die Informationen für das Pensionierungsverfahren nicht ohne weitere Aufklärung und ohne Gelegenheit zur Stellungnahme für den Betroffenen herangezogen werden und hätten deshalb auch nicht ohne diese Voraussetzungen in der Personalakte gespeichert werden dürfen. Die Voraussetzungen konnten auch nicht nachträglich erfüllt werden, da eine zeitnahe und damit sachgerechte Aufklärung oder Stellungnahme nicht mehr möglich war.

Ähnliche Mängel wies ein amtsärztliches Gesundheitszeugnis aus, in dem eine dauernde Dienstunfähigkeit des Beamten festgestellt wurde. Der Amtsarzt hatte seine abschließende Wertung auf „umfangreiche Fremdgutachten“ gestützt, ohne diese näher zu bezeichnen oder gar inhaltlich darauf einzugehen. Ohne ausreichende Begründung kann aber auch ein solches Gutachten nicht als Grundlage für ein Zwangspensionierungsverfahren herangezogen werden. Der Betroffene hat nämlich einen Anspruch darauf, daß ihm die maßgeblichen tatsächlichen und rechtlichen Gründe für die Entscheidung des Dienstherrn genannt werden. So war ihm aber nicht einmal die Prüfung möglich, ob eine Nutzung der Fremdgutachten überhaupt zulässig war.

Nach Beratung durch den Landesbeauftragten wurden die Berichte des Dienstvorgesetzten wie auch das amtsärztliche Gesundheitszeugnis wegen der genannten Verfahrensfehler aus der Personalakte entfernt. Dem laufenden Zwangspensionierungsverfahren waren damit die Grundlagen entzogen.

Schwarze Listen über Mitarbeiter eines Jugendzentrums

Zu den Aufgaben des Leiters eines kommunalen Jugendzentrums gehörte es, besondere Vorkommnisse im Jugendzentrum

(z.B. über Alkoholkonsum, Drogenkonsum, Polizeieinsätze) dem aufsichtsführenden Fachamt schriftlich zu melden. Dabei kam natürlich auch das fehlerhafte Verhalten einzelner Mitarbeiter zur Sprache. Über besonders wichtige Vorgänge mußte der Bürgermeister unterrichtet werden. Dies alles wurde schließlich in den entsprechenden Sachakten des Fachamtes dokumentiert, in die die Betroffenen zumindest nach altem Datenschutzrecht kein Einsichtsrecht hatten.

Die geprüften Sachakten wurden entsprechend ihrer Zweckbestimmung – soweit feststellbar – ausschließlich für die behördeninterne Entscheidungsfindung über die Verwaltung des Jugendzentrums, nicht aber für Personalentscheidungen genutzt. Da eine Verwendung der Daten für Personalverwaltungsaufgaben nicht vorgesehen war, ergab sich zumindest aus dem Dienstrecht kein besonderes (Personal-)Akteneinsichtsrecht für die Betroffenen. Wenn solche Unterlagen allerdings zur Begründung belastender Maßnahmen gegen Mitarbeiter herangezogen werden sollen, müssen sie in die jeweilige Personalakte übernommen werden. Dabei muß auch darauf geachtet werden, daß die Richtigkeit der Sachverhaltsdarstellung nachgewiesen ist, eine dienstrechtliche Bewertung des Vorgangs erfolgt und der Betroffene Gelegenheit zur schriftlichen Stellungnahme erhält.

Ob auf Unterlagen das Personalakteneinsichtsrecht des Mitarbeiters anzuwenden ist, richtet sich ausschließlich nach ihrem materiellen Inhalt bzw. dessen dienstrechtlicher Bewertung durch den Dienstherrn und nicht danach, in welcher Akte sie zufälligerweise abgeheftet sind. Gleichwohl hat der Dienstherr natürlich auch für eine richtige Zuordnung von Vorgängen zu Personalakten bzw. Sachakten Sorge zu tragen. Dieser Pflicht ist die geprüfte Verwaltung nicht bei allen Schriftstücken des Vorgangs ausreichend nachgekommen, ein Mangel, den der Landesbeauftragte übrigens auch bei anderen Stellen gefunden hat.

Die vorgefundenen Mängel wurden nach entsprechender Beratung durch den Landesbeauftragten noch während der Prüfung bereinigt. Den Betroffenen wurde anschließend Einsicht in ihre, nunmehr auch formal vollständigen, Personalakten gewährt.

4.1.1.2 Wer darf in Personalakten einsehen?

Einsicht in Personalakten steht nur einem eng begrenzten Personenkreis zu, nämlich den Betroffenen und den Mitarbeitern, die für die Verwaltung des einzelnen „Personalfalles“ zuständig sind. Der Landesbeauftragte konnte bei seinen Prüfungen erneut feststellen, daß gegen diesen Grundsatz verstoßen wird:

- So besteht z.B. kein Anspruch künftiger Fachvorgesetzter auf Einsicht in die Personalakte, wenn sich Mitarbeiter einer kommunalen Gebietskörperschaft in einer internen Ausschreibung um ein anderes Aufgabengebiet bewerben. Nur

die für die Bewerbung erforderlichen Daten dürfen ihnen auszugsweise von der Personalverwaltung zugänglich gemacht werden. Denn Personalakten enthalten in der Regel darüber hinaus eine Fülle sensibler Informationen, die für eine Auswahlentscheidung ohne Bedeutung sind. Etwas anderes kann nur gelten, wenn eine wirksame Einwilligung des Betroffenen vorliegt. Wenn ein Bewerber lediglich pauschal „auf die Personalakte“ verweist, so reicht dies nicht aus.

- Auch die Übersendung vollständiger Personalakten an das Landesbesoldungsamt (zur Berechnung des Besoldungsdienstalters, von Nachversicherungsbeträgen usw.) begegnet erheblichen datenschutzrechtlichen Bedenken.

Das Landesbesoldungsamt ist durch Rechtsverordnung mit einer eigenen Zuständigkeit für den Besoldungs- und Vergütungsbereich ausgestattet. Erhält es Personalunterlagen von anderen Stellen, so liegt darin eine Datenübermittlung, die einer Rechtsgrundlage bedarf.

Nach § 30 des neuen LDSG sind derartige Datenübermittlungen zwar grundsätzlich zulässig, jedoch auf das erforderliche Maß zu beschränken. Eine Übersendung vollständiger Personalakten ist damit faktisch ausgeschlossen, denn in jeder Akte sind auch Unterlagen enthalten, die für die Festsetzung und Zahlbarmachung von Vergütungen, Gehältern und Löhnen nicht erforderlich sind.

- Schließlich erhielt auch die Versorgungsausgleichskasse der Kommunalverbände von den angeschlossenen Verwaltungen immer wieder vollständige Personalakten übersandt. Auch hier ergaben sich erhebliche Bedenken.

Die Versorgungsausgleichskasse hat die Aufgabe, Versorgungsansprüche der Bediensteten bei den Kommunen und deren Hinterbliebenen auszugleichen. Zur Erfüllung dieser Aufgabe benötigt sie zwar in erheblichem Umfang personenbezogene Daten der Mitarbeiter. Eine ausreichende Ermächtigungsgrundlage für die von den Kommunen vorgenommenen Datenübermittlungen war bisher jedoch nicht vorhanden. Das Gesetz über die Versorgungsausgleichskasse aus dem Jahre 1949 enthält nur eine in dieser Hinsicht völlig unzureichende Aufgabenzuweisung.

Nunmehr hat der Innenminister einen Novellierungsentwurf vorgelegt, der den datenschutzrechtlichen Anforderungen entspricht.

Mit der Gesetzesänderung soll den Kommunen auch die Möglichkeit eingeräumt werden, die Beihilfebearbeitung und -festsetzung auf die Versorgungsausgleichskasse zu übertragen. Damit könnte endlich die Forderung des Landesbeauftragten nach einer konsequenten Trennung der Beihilfeangelegenheiten von der allgemeinen Personalverwaltung im kommunalen Bereich erfüllt werden.

4.1.2 Verfassungsschutz

4.1.2.1 Das Unvorstellbare: Bürger erhalten in Schleswig-Holstein Auskunft vom Verfassungsschutz

Im Berichtszeitraum ist das neue schleswig-holsteinische Verfassungsschutzgesetz in Kraft getreten. Die Bürgerinnen und Bürger haben jetzt einen Anspruch auf Auskunft über Daten, die der Verfassungsschutz über sie gespeichert hat und zwar ohne daß sie ihren Antrag besonders begründen müssen. Die Auskunft darf nur verweigert werden, wenn das öffentliche Interesse an der Geheimhaltung der Erkenntnisse sowie der nachrichtendienstlichen Arbeitsmethoden und -mittel gegenüber dem Interesse des antragstellenden Bürgers an der Auskunftserteilung überwiegt.

In diesem Jahr konnten erste Erfahrungen mit der Anwendung der Vorschrift gewonnen werden. Alle Bürger, die sich an den Landesbeauftragten gewandt haben, erhielten vom Verfassungsschutz Auskunft darüber, ob Daten über sie gespeichert waren oder nicht. In keinem einzigen Fall wurde die Auskunft verweigert. Auch diejenigen, die sich unmittelbar an die Verfassungsschutzbehörde wandten, erhielten bis auf wenige Ausnahmen die gewünschte Auskunft. Es handelte sich insgesamt zwar um eine relativ niedrige Zahl von Ersuchen – so daß etwaige Befürchtungen, durch eine Vielzahl von Auskunftersuchen könnte die Arbeit der Behörde lahmgelegt werden, nicht eingetreten sind –, aber sie zeigen, daß die Erteilung von Auskünften an Betroffene keineswegs unvereinbar mit der Arbeit eines Nachrichtendienstes ist.

4.1.2.2 Mängel bei der Sicherheitsüberprüfung: Daten nicht sicher

In einer breit angelegten Querschnittskontrolle hat der Landesbeauftragte die Datenverarbeitung bei den Geheimschutzbeauftragten in den Behörden Schleswig-Holsteins untersucht. In kaum einem anderen Bereich werden durch den Staat so viele Daten aus so unterschiedlichen Quellen und Lebensbereichen erhoben und über einen so langen Zeitraum aufbewahrt.

Der Ablauf der Sicherheitsüberprüfungen

Wird jemand einer Sicherheitsüberprüfung unterzogen, so werden zunächst von ihm selbst in Form des sog. Erklärungsbogens detaillierte und umfangreiche Angaben verlangt. Diese werden mit den Personaldaten abgeglichen und ggf. ergänzt. Danach werden die polizeilichen sowie die Informationssysteme des Verfassungsschutzes und der übrigen Geheimdienste abgefragt.

Bei der „erweiterten Sicherheitsüberprüfung mit Sicherheitsermittlungen“ werden darüber hinaus zusätzliche Ermittlungen

gen angestellt. Dabei werden insbesondere die vom Betroffenen selbst angegebenen Referenzpersonen sowie andere Personen befragt, die „sachdienliche Hinweise“ geben können. Da es um die Feststellung und Aufklärung von Umständen geht, die auf ein Sicherheitsrisiko hindeuten können, zielen die Fragen an die Referenz- und sonstigen Hinweispersonen häufig auf persönliche Eigenschaften und das Ehe- und Privatleben.

Die aus diesen unterschiedlichen Quellen zusammengetragenen Informationen werden in der Sicherheitsakte zusammengefaßt und so lange aufbewahrt, wie der Betreffende in sicherheitsempfindlicher Tätigkeit beschäftigt ist. Erst 5 Jahre nach dem Ausscheiden, in vielen Fällen erst nach 10 Jahren, werden die Akten vernichtet. Für viele Bedienstete folgt daraus, daß die Sicherheitsakte während ihrer gesamten beruflichen Tätigkeit und länger aufbewahrt wird. Ein etwaiger „dunkler Punkt“ oder „jugendlicher Fehltritt“, der in allen anderen in Betracht kommenden Datensammlungen längst gelöscht ist, bleibt in der Sicherheitsakte u.U. über Jahrzehnte gespeichert, da diese nicht bereinigt, sondern allenfalls nach Ablauf der geschilderten Fristen insgesamt vernichtet wird.

Die Betroffenen ahnen von der Existenz dieser belastenden Informationen gelegentlich nichts, da es – im Gegensatz zur Personalakte – in die Sicherheitsakte kein Einsichtsrecht gibt. Auch rechtliches Gehör wird nur gewährt, wenn tatsächlich ein Sicherheitsrisiko vorliegt. Gerade dann, wenn es sich um nicht so gravierende oder nicht nachweisbare negative Informationen handelt, z.B. um Gerüchte oder Übertreibungen einer Referenzperson, erfährt der Betroffene nichts von ihrer Existenz und davon daß sie u.U. über Jahrzehnte aufbewahrt werden.

Trennung zwischen Geheimschutzbeauftragten und Personalverwaltung

Um so wichtiger ist es, daß diese sensiblen Daten jedenfalls nicht zweckwidrig verwendet werden. Ein Mittel dazu ist die im neuen schleswig-holsteinischen Landesverfassungsschutzgesetz enthaltene Zweckbindungsgarantie. Auch die Sicherheitsrichtlinien des Landes enthalten Regelungen, die dem besonderen Schutz dieser Informationen dienen sollen. Sie bestimmen, daß personeller Geheimschutz und Personalverwaltung personell und organisatorisch zu trennen sind. Dadurch soll vermieden werden, daß geheimdienstliche oder sonstige belastende Informationen, gegen die sich der Betroffene mangels Kenntnis nicht wehren kann, auch nur mittelbar Personalentscheidungen beeinflussen. Der Trennung kommt deshalb aus datenschutzrechtlicher Sicht erhebliche Bedeutung zu.

Obwohl die Richtlinien eindeutig sind und keine Ausnahme von der Trennungspflicht zulassen, haben die Untersuchungen ergeben, daß sie nur in ca. 49 % der Behörden ein-

gehalten war. Einige Behörden haben noch während der Kontrolle die Konsequenzen gezogen und den personellen Geheimschutz umorganisiert. Ein Schwachpunkt bei der Einhaltung des Trennungsgrundsatzes ergibt sich sogar aus den Richtlinien selbst: Danach „können“ kleinere Behörden einen Geheimschutzbeauftragten bestellen. Tun sie es nicht, so nimmt der Dienststellenleiter die Angelegenheiten des personellen Geheimschutzes wahr. Da der Dienststellenleiter natürlich auch mit Fragen der Personalverwaltung befaßt ist, ist dem Landesbeauftragten schleierhaft, wie in diesen Fällen eine „personelle und organisatorische“ Trennung von personellem Geheimschutz und Personalverwaltung garantiert sein soll.

Der Landesbeauftragte hat dem Innenminister das Ergebnis seiner Erhebung mitgeteilt und die fehlende Trennung von personellem Geheimschutz und Personalverwaltung in mehr als der Hälfte der Fälle als einen gravierenden Verstoß gegen die Sicherheitsrichtlinien kritisiert.

Da es in kleinen Dienststellen einen erheblichen Aufwand bedeuten kann, die beiden Bereiche personell und organisatorisch strikt zu trennen, hat er als eine Möglichkeit vorgeschlagen, die Funktion des Geheimschutzbeauftragten neu zu bestimmen. Insbesondere müßte verhindert werden, daß dem Geheimschutzbeauftragten sensible oder belastende Informationen über den Personenkreis bekannt werden, der einer Sicherheitsüberprüfung unterzogen wird. Wenn dies sichergestellt wäre, dann könnte auch an eine Lockerung des strikten Trennungsprinzips gedacht werden. Der Innenminister hat sich noch nicht abschließend geäußert. Er möchte erst das Bundesgesetz zur Sicherheitsüberprüfung und ein sich daran anschließendes Landesgesetz zur Sicherheitsüberprüfung abwarten. Er könne sich aber durchaus vorstellen, daß die Funktion des örtlichen Geheimschutzbeauftragten darauf beschränkt wird, den Kreis der zu überprüfenden Mitarbeiter festzustellen sowie deren Ermächtigungen und die Belehrungen vorzunehmen. In diesem Falle würden die behördlichen Geheimschutzbeauftragten keine Kenntnis vom Inhalt der Sicherheitsakten erhalten, so daß auf eine lückenlose Einhaltung des Trennungsprinzips zwischen personellem Geheimschutz und Personalverwaltung verzichtet werden könnte.

Einsicht in Personalakten durch Geheimschutzbeauftragte

Eine andere Frage, der der Landesbeauftragte bei seiner Untersuchung nachgegangen ist, zielte darauf ab, ob und in welchem Umfang Geheimschutzbeauftragte Einsicht in Personalakten nehmen. Die Sicherheitsrichtlinien gestehen den Geheimschutzbeauftragten dieses Recht ausdrücklich zu. Allerdings fehlt es bislang an einer gesetzlichen Grundlage für diese Form der Datenübermittlung. Die Untersuchung hat ergeben, daß über 70 % der Geheimschutzbeauftragten von dem Recht auf Akteneinsicht keinen Gebrauch machen. Auch daraus ergibt sich die Frage, ob die Einräumung eines solchen Rechts

überhaupt erforderlich ist. Der Landesbeauftragte hat dem Innenminister deshalb vorgeschlagen, den Geheimschutzbeauftragten vor Ort allenfalls noch ein eingeschränktes Einsichtsrecht in die Personalakte zuzugestehen.

Soweit detaillierte Angaben aus der Personalakte für die Zwecke der Sicherheitsüberprüfung entnommen werden müssen, sollte dies durch den Sicherheitsbeauftragten des Landes geschehen. Hierzu hat der Innenminister mitgeteilt, daß dadurch eine erhebliche Arbeitsverschiebung hin zum Sicherheitsbeauftragten eintreten würde. Dies sei personal-, kosten- und zeitaufwendiger. Dieses Argument hält der Landesbeauftragte für nicht vollständig überzeugend. Wenn die behördlichen Geheimschutzbeauftragten nicht mehr in Personalakten einsehen – was sie derzeit ohnehin nur in seltenen Fällen tun –, so wird dadurch bei ihnen Arbeitskapazität frei. Daß auf der anderen Seite beim Sicherheitsbeauftragten des Landes mehr Arbeit entstehen kann, ist unbestritten. Allerdings müßte geprüft werden, inwiefern im Hinblick auf die gewandelten Aufgaben der Verfassungsschutzbehörde nicht Kapazitäten für diese Aufgabe frei werden.

Führung von Karteien bei den Geheimschutzbeauftragten

Ein weiteres Ergebnis der Untersuchung war, daß von einer Reihe von Geheimschutzbeauftragten Unterlagen, Akten, Karteien etc. über überprüfte Personen geführt werden. Die Sicherheitsrichtlinien sehen aber lediglich die Führung von Sicherheitsakten durch den Sicherheitsbeauftragten sowie die Führung von Karteien durch die Verfassungsschutzbehörde und durch den Sicherheitsbeauftragten vor. Demnach kann für die behördlichen Geheimschutzbeauftragten allenfalls eine Namenskartei, aus der sich die Namen der überprüften Personen ergeben, in Betracht kommen. Der Landesbeauftragte hat die betreffenden Geheimschutzbeauftragten darauf hingewiesen und die Bereinigung der Unterlagen verlangt.

Erweitertes rechtliches Gehör

Die Richtlinien gewähren rechtliches Gehör nur im Falle eines Sicherheitsrisikos, das der Beschäftigung in sicherheitsempfindlichen Bereichen entgegensteht. Die Verfassungsschutzbehörde kann aber auch sog. Sicherheitshinweise geben, wenn belastende Erkenntnisse zwar nicht der Ermächtigung entgegenstehen, gleichwohl aber besondere Vorsichtsmaßnahmen erfordern. Der Landesbeauftragte ist der Auffassung, daß auch in diesen Fällen dem Betroffenen rechtliches Gehör gewährt werden muß und hat dem Innenminister eine entsprechende Ergänzung der Richtlinien vorgeschlagen.

„Fürsorgemaßnahmen“

Die Sicherheitsrichtlinien sehen vor, daß Informationen, die im Rahmen der Sicherheitsüberprüfung gewonnen worden sind, für „Fürsorge- oder andere Maßnahmen“ verwendet werden dürfen. Dies stellt eine Zweckerweiterung dar, deren Notwendigkeit einer besonderen Begründung bedarf. Die Untersuchung hat ergeben, daß lediglich in 5 % der Fälle derartige Hinweise gegeben worden sind. Der Landesbeauftragte hat deshalb den Innenminister gebeten zu prüfen, ob tatsächlich ein Bedürfnis für diese Übermittlungsvorschrift besteht. Zumindest sollte vorgesehen werden, daß der Betroffene zugleich mit der Anregung an die personalverwaltende Stelle zu unterrichten ist.

Der Innenminister hat zu den beiden vorgenannten Vorschlägen mitgeteilt, er werde sie im Rahmen der Neufassung der Sicherheitsrichtlinien abschließend prüfen.

Reduzierung der Überprüfungen

Aus der Vielzahl der Geheimschutzbeauftragten, die der Landesbeauftragte im Rahmen seiner Untersuchung anzuschreiben hatte, sind ihm Zweifel erwachsen, ob tatsächlich in all diesen Stellen Geheimnisse aufbewahrt werden, die es notwendig machen, Mitarbeiter einer Sicherheitsüberprüfung mit ihren empfindlichen Rechtseingriffen zu unterziehen. Er hat deshalb in seinem Bericht an den Innenminister auch die Frage behandelt, wie sichergestellt werden kann, daß tatsächlich nur im erforderlichen Umfang Personen einer Sicherheitsüberprüfung unterzogen werden. Noch im Laufe seiner Erhebungen hat der Innenminister unabhängig davon eine weitere Reduktion der Zahl der Personen vorgenommen, die einer Sicherheitsüberprüfung zu unterziehen sind. Der Landesbeauftragte hat darüber hinaus vorgeschlagen, daß bei der Einleitung einer Sicherheitsüberprüfung vom Sicherheitsbeauftragten des Landes festgestellt wird, ob die betreffende Person tatsächlich der Überprüfung unterzogen werden muß. Hierfür müßten der Sicherheitserklärung entsprechende Informationen beigelegt werden, damit der Sicherheitsbeauftragte überhaupt in der Lage ist nachzuvollziehen, welche sicherheitsempfindliche Tätigkeit im einzelnen der zu Überprüfende wahrnehmen soll. Der Innenminister hat hierzu mitgeteilt, er halte ein besonders ausgewiesenes Mitwirkungs- und Prüfungsrecht des Sicherheitsbeauftragten für denkbar, wolle aber die klare, letztlich fachlich begründete ausschließliche Verantwortlichkeit des Dienststellenleiters nicht verwischen.

Wie geht es weiter?

Aus dem bisherigen Ergebnis der Querschnittsprüfung ergibt sich für den Landesbeauftragten Bedarf zur Änderung bzw. Ergänzung der Sicherheitsrichtlinien sowie zur Änderung des bisherigen Verfahrens. Ob damit bis zum Inkrafttreten eines

Sicherheitsüberprüfungsgesetzes gewartet werden kann, hängt davon ab, wie zügig dieses Gesetzgebungsvorhaben vorangetrieben wird. Sollte es hierbei zu Verzögerungen kommen, so wird es notwendig sein, vorab die bestehenden Mängel zu beseitigen.

4.1.3 Öffentliche Sicherheit

4.1.3.1 Neues Polizeirecht setzt Maßstäbe

Die Verabschiedung des polizeirechtlichen Teils des Landesverwaltungsgesetzes war begleitet von zum Teil heftigen öffentlichen Diskussionen. Der Landesbeauftragte konnte an diesem Gesetzgebungsverfahren in allen Stadien diskret und effektiv mitarbeiten. Im Ergebnis konnte er einen großen Teil seiner Vorstellungen durchsetzen. Sowohl aus den im 12. Tätigkeitsbericht (S. 28) veröffentlichten „Vorstellungen zur Novellierung des Landespolizeirechts“ als auch aus den im Gesetzgebungsverfahren abgegebenen Stellungnahmen konnten wesentliche Teile verwirklicht werden. Auch die Erfahrungen bei der Kontrolle der Datenverarbeitung bei der Polizei, deren Ergebnisse ebenfalls im 12. Tätigkeitsbericht (S. 18) nachzulesen sind, wurden eingebracht.

Im Endergebnis ist ein Gesetz entstanden, das eine Reihe von datenschutzrechtlichen Sicherungen enthält. Besonders hervorzuheben sind folgende Gesichtspunkte:

- Das schleswig-holsteinische Polizeirecht erlaubt weder die **Rasterfahndung** noch den Einsatz **verdeckter Ermittler**.
- Die **Datenerhebung im Vorfeld** noch nicht begangener Straftaten wurde sachlich begrenzt. Sie ist nur dann zulässig, wenn Tatsachen dafür sprechen, daß ein Verbrechen oder ein Vergehen gewerbs- oder gewohnheitsmäßig begangen werden soll. Es ist nur die Erhebung von Daten über den Verdächtigen, nicht aber – wie zunächst geplant und in anderen Bundesländern vorgesehen – über Kontakt- und Begleitpersonen zulässig. Daten über Zeugen und Hinweisgeber dürfen in abrufbarer Form nicht gespeichert werden. Die Speicherung von Daten über potentielle Opfer solcher Straftaten ist nur mit deren Kenntnis zulässig. Die im Rahmen der Vorbeugung erhobenen Daten dürfen maximal drei Jahre gespeichert werden, wobei die Erforderlichkeit der weiteren Speicherung jedes Jahr zu überprüfen ist.
- Die Voraussetzungen der **Identitätsfeststellung**, von der jedermann an bestimmten Orten betroffen sein kann, wurden enger gefaßt als im Regierungsentwurf zunächst vorgesehen. Vor allem aber wurden die Folgen für die Betroffenen abgemildert. So ist ein Festhalten zum Zwecke der Identitätsfeststellung nur noch bis maximal 12 Stunden, nicht nur wie ursprünglich vorgesehen 48 Stunden, zulässig. Die erkenntnisdienliche Behandlung unverdächtigter Personen ist nur dann zulässig, wenn sie Angaben über die Identität verweigern oder bestimmte Tatsachen den Verdacht einer

Täuschung über die Identität begründen. Der Verhältnismäßigkeitsgrundsatz wurde zusätzlich aufgenommen, damit insbesondere bei den Folgemaßnahmen einer Identitätsfeststellung immer deutlich ist, daß sie nicht außer Verhältnis zur Bedeutung des Anlasses stehen dürfen.

- Der Einsatz der **besonderen Mittel der Datenerhebung**, also insbesondere der Observation, technischer Mittel zur Anfertigung von Bildaufnahmen oder -aufzeichnungen sowie zum Abhören oder Aufzeichnen des gesprochenen Wortes auf Tonträger und der Einsatz von Personen, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist, ist nur dann zulässig, wenn Tatsachen dafür sprechen, daß ein Schaden für Leib, Leben oder Freiheit oder ein gleichgewichtiger Schaden für Sach- oder Vermögenswerte oder für die Umwelt zu erwarten ist. In diesem Falle dürfen nur Daten über Personen erhoben werden, bei denen Tatsachen dafür sprechen, daß sie als Verantwortliche in Anspruch genommen werden können. Der Einsatz der Observation, der technischen Mittel sowie die Erhebung von Daten aus Wohnungen darf nur durch den **Richter** angeordnet werden.
- Das Instrument der Kontrollmeldungen, bislang unter der Bezeichnung „**polizeiliche Beobachtung**“ bekannt, wurde präzisiert. Eine Ausschreibung von Personen zur polizeilichen Beobachtung ist nur zulässig, wenn Tatsachen dafür sprechen, daß ein Schaden für Leib, Leben oder Freiheit oder ein gleichgewichtiger Schaden für Sach- oder Vermögenswerte oder für die Umwelt zu erwarten ist. Der Zweck der Ausschreibung ist auf die Gefahrenabwehr beschränkt. Wird die ausgeschriebene Person angetroffen, so sind nur Daten über Begleitpersonen, nicht, wie vorgesehen, auch über Kontaktpersonen, zu erheben. Die Anordnung der Kontrollmeldung muß durch den Richter erfolgen. Die Speicherung der auf diesem Wege über Begleitpersonen erhobenen Daten ist nur zulässig, um ihre Bedeutung für den die Ausschreibung begründenden Sachverhalt zu überprüfen. Sie sind zu löschen, sobald feststeht, daß sie für die Verhütung des Schadens nicht in Anspruch genommen werden können und die Daten auch nicht für ein mit dem Sachverhalt zusammenhängendes Strafverfahren erforderlich sind. Die Speicherdauer ist auf maximal zwei Jahre begrenzt.
- Von weitreichender praktischer Bedeutung sind die Vorschriften über die Speicherung von **Daten aus** bereits **abgeschlossenen Ermittlungsverfahren** für Zwecke der Vorbeugung. Diese Daten machen den bei weitem größten Teil der polizeilichen Datenbestände aus. Der Landesbeauftragte hatte wiederholt kritisiert, daß in den entsprechenden Akten zumeist nur etwas über den Tatverdacht vermerkt ist, während über den Ausgang des gerichtlichen Verfahrens nichts bekannt ist. Nunmehr ist vorgeschrieben, daß sich die Polizei spätestens zwei Jahre nach Anlage der Akte aktiv bei der Justiz erkundigen muß, wie der Fall dort beurteilt

worden ist. Ist der ursprüngliche Tatverdacht entfallen, so sind die Daten zu löschen.

Schon diese kleine Auswahl der in das Gesetz eingebauten datenschutzrechtlichen Sicherungen macht deutlich, daß der Gesetzgeber erhebliche datenschutzrechtliche Anstrengungen unternommen hat. Die traditionelle polizeiliche Datenverarbeitung für Zwecke der Strafverfolgung auf der Grundlage der Strafprozeßordnung wird durch die Novelle nicht eingeschränkt. Vielmehr eröffnet das Gesetz eine zusätzliche polizeiliche Handlungsebene bereits im Vorfeld einer noch nicht begangenen Straftat. Auch wenn im Gesetz durchgängig der Terminus verwendet wird, „sprechen Tatsachen dafür, daß ...“ und auch wenn ergänzend eingefügt ist, daß allgemeine Erfahrungssätze ohne Bezug zum jeweiligen Geschehen keine Tatsachen im Sinne der Vorschriften über die Datenerhebung sind, so ist festzuhalten, daß mit diesem Gesetz der polizeiliche Handlungsspielraum beträchtlich erweitert wird. Die Polizei erhält neue Befugnisse, mehr als ihr nach Strafverfolgungs- und Gefahrenabwehrrecht bislang zustand.

Allerdings gehen die neuen Befugnisse in Schleswig-Holstein nicht so weit wie in anderen Bundesländern. Der sogenannte „Musterentwurf“ für ein einheitliches Polizeirecht, der Mitte der 80er Jahre im wesentlichen von der Polizei selbst erarbeitet worden ist und den die Gesetzgeber anderer Bundesländer weitgehend übernommen haben, wurde in beträchtlichem Umfang um datenschutzrechtliche Komponenten ergänzt. So gesehen dürfte in Schleswig-Holstein ein Polizeigesetz entstanden sein, das in Teilen seinerseits zum Muster für Gesetzgebungsvorhaben in anderen Bundesländern dienen könnte.

4.1.3.2 Konsequenzen aus der Kontrolle bei der Polizei lassen auf sich warten

Vor über drei Jahren hat der Landesbeauftragte in einer Querschnittskontrolle die Datenverarbeitung bei der Polizei unter die Lupe genommen (vgl. 13. TB. S. 28) und massive Kritik geübt. Die ersten Stellungnahmen vom Kriminalpolizeiamt und vom Innenminister ließen die Bereitschaft zu den notwendigen Verbesserungen erkennen. Die beanstandeten Einzelfälle wurden weitgehend gelöscht, die Verarbeitung von Daten über Selbsttötungsversuche eingeschränkt.

In den meisten anderen Bereichen ist es bislang aber bei Absichtserklärungen, Zwischennachrichten und Problemstellungen seitens Polizei und Innenministerium geblieben. Konkrete weitere Umsetzungsmaßnahmen sind dem Landesbeauftragten im vergangenen Jahr nicht bekannt geworden. Statt einer ausführlichen Darstellung der Konsequenzen aus der Kontrolle kann deshalb erneut nur ein Zwischenbericht über den Stand des Verfahrens gegeben werden.

Mitte des Jahres listete der Landesbeauftragte die noch nicht erledigten, d.h. die große Mehrzahl der Monita aus seinem

Prüfbericht, noch einmal auf und bat Kriminalpolizeiamt und Innenminister um ihre abschließende Stellungnahme. Diese liegt bislang noch nicht vor. Statt dessen kam es gegen Ende des Jahres zu einem Grundsatzgespräch zwischen dem Landesbeauftragten und der Leitung des Kriminalpolizeiamtes unter Beteiligung des Innenministeriums, bei dem noch einmal die offenen Fragen ausgiebig diskutiert wurden.

Das Kriminalpolizeiamt hat nunmehr eine Arbeitsgruppe eingesetzt, die die notwendigen Umsetzungsmaßnahmen vorbereiten bzw. in die Wege leiten soll. Der Landesbeauftragte hat der Arbeitsgruppe seine Unterstützung zugesagt.

Den Gliederungspunkt „Konsequenzen aus der Kontrolle bei der Polizei“ wird es zwangsläufig auch im nächsten Tätigkeitsbericht geben.

4.1.3.3 APIS: Schleswig-Holstein geht mit gutem Beispiel voran

Die Datenschutzbeauftragten des Bundes und der Länder haben in den vergangenen Jahren wiederholt Kritik an der Praxis der Datenspeicherung in der Arbeitsdatei PIOS Innere Sicherheit (APIS) geübt. Auch der Landesbeauftragte hat bei seinen Kontrollen festgestellt, daß durch schleswig-holsteinische Polizeibehörden Fälle eingespeichert worden sind, die in einer bundesweiten Verbunddatei vom Gewicht und vom Zuschnitt der APIS nichts zu suchen haben.

Die Datei APIS ist aus der Datei PIOS-Terrorismus hervorgegangen, in der zunächst nur Informationen zum Deliktsbereich Terrorismus gespeichert wurden. In APIS werden seit einigen Jahren aber auch allgemeine Staatsschutzdelikte erfaßt, wie z.B. die Sachbeschädigung durch das Beschmiern von Plakaten mit extremistischen Parolen. Während sich die APIS-Relevanz bei klassischen Staatsschutzdelikten, wie Hochverrat, verbotene Parteibetätigung, Sabotage etc., schon aus dem Delikt ergibt, werden Sachbeschädigung, Körperverletzung, Beleidigung in APIS erfaßt, wenn beim Täter eine extremistische Motivation vorhanden ist oder auch nur vermutet wird. Auswertungen haben ergeben, daß Delikte dieser Art gegenüber den „klassischen“ Staatsschutzdelikten, zu deren Zweck diese Datei eigentlich eingerichtet wurde, bei weitem in der Überzahl sind.

Das Kriminalpolizeiamt berief sich in seiner Stellungnahme zunächst auf die bundesweit geltenden Erfassungsrichtlinien der APIS. Davon könne und wolle man in Schleswig-Holstein nicht abweichen. Eine einseitige Änderung dieser Richtlinien durch ein Bundesland komme nicht in Betracht.

Nunmehr wurde eine Lösung erreicht, die diesem Gesichtspunkt Rechnung trägt. Ohne formelle Änderung der Richtlinien wurden ergänzende schleswig-holsteinische Weisungen erlassen, die auslegungsbedürftige Begriffe näher präzisieren.

Diese ergänzenden Weisungen sehen vor, daß auch bei „klassischen Staatsschutzstraftaten“ stets zu prüfen ist, ob die Speicherung in einer bundesweiten Verbunddatei verhältnismäßig ist. Insbesondere bei „Hakenkreuzschmierereien“ ist zu prüfen, ob es sich um eine unpolitische Einzeltat oder um eine Tat mit verfassungsfeindlicher Zielsetzung und Zusammenhängen zu rechtsextremistischen Organisationen handelt.

Bei der Erfassung „anderer Straftaten“ mit politischer Motivation ist stets die Schwere **und** die überörtliche Bedeutung der Tat zu berücksichtigen. Dabei ist in erster Linie darauf abzustellen, daß nur solche Straftaten erfaßt werden dürfen, die von ihrer Schwere und der Gefahr für die freiheitliche demokratische Grundordnung her mit den „klassischen“ Staatsschutzdelikten vergleichbar sind. Indiz für die Schwere der Tat ist die aktive Gewaltanwendung gegen Personen, die Androhung von Gewaltanwendung gegen Personen sowie ein Sachschaden von mehr als tausend Deutsche Mark. Generell gilt, daß, je eindeutiger die verfassungsfeindliche Motivation zu bejahen ist, desto geringere Anforderungen an die Schwere der Tat zu stellen sind und umgekehrt.

Außer diesen Gesichtspunkten ist zusätzlich die überörtliche Bedeutung des jeweiligen Falles zu prüfen. Kriterien hierfür sind:

- Die Wahrscheinlichkeit, daß der Täter außerhalb Schleswig-Holsteins erneut in Erscheinung tritt;
- die Begehung der Tat im Ausland;
- der Wohnsitz des Täters in einem anderen Bundesland.

Die Verarbeitung von Daten im Rahmen der Terrorismusbekämpfung bleibt von diesen Neuregelungen unberührt. Sie sollen zunächst befristet bis 31.12.92 gelten. Danach wollen sowohl das Kriminalpolizeiamt als auch der Datenschutzbeauftragte anhand der in diesem Zeitraum erfaßten Fälle prüfen, ob die Neuregelung für beide Seiten auf Dauer akzeptabel ist.

Der Landesbeauftragte begrüßt es, daß Schleswig-Holstein als bislang erstes Land bereit ist, die Praxis der Datenerfassung in APIS verbindlich einzuschränken. Er hält es jedoch weiterhin für geboten, daß die APIS-Errichtungsanordnung bundesweit entsprechend überarbeitet wird, da die von Schleswig-Holstein eingegebenen Speicherungen nur einen geringen Bruchteil des Gesamtdatenbestandes in APIS ausmachen.

4.1.3.4 „Rosa Listen“: Nichts gefunden

Die Homosexuellen-Initiativen befürchten seit jeher, daß die Polizei Karteien über Homosexuelle führt, sogenannte Rosa Listen.

Diese Sorge wurde durch eine groß angelegte Polizeirazzia zur Bekämpfung der Jugendprostitution in den Lübecker Wallanlagen, die als Treffpunkt kontaktsuchender Homosexueller

gelten, erneut akut, zumal alle angetroffenen Personen polizeilich kontrolliert worden waren. In der Folge erreichten den Datenschutzbeauftragten besorgte Anfragen Betroffener.

Daraufhin wurde bei der Lübecker Polizei eine datenschutzrechtliche Kontrolle durchgeführt. Dabei waren nicht Fragen der Angemessenheit des polizeilichen Großeinsatzes mit Dutzenden von Beamten, Reiter- und Hundestaffel zu beurteilen, sondern, ob etwas unter Datenschutzaspekten zu beanstanden war.

Es konnte festgestellt werden, daß die Polizei 52 Personen, die sich im Bereich der Razzia aufhielten, in der polizeilichen Erkenntnisdatei (PED) abgefragt, aber nach dem Einsatz die darüber erstellten schriftlichen Unterlagen vernichtet hatte. Die Befürchtung, es könnten im Anschluß an die Razzia „Rosa Listen“ angelegt worden sein, war unbegründet.

Einmal in Lübeck, wurde auch die sog. Lichtbildvorzeigekartei bei der Kriminalpolizeidirektion Schleswig-Holstein Süd unangemeldet kontrolliert. Unter der allerdings irreführenden Bezeichnung „Homosexualität“ waren einige wenige erkennungsdienstliche Unterlagen vorhanden. Sie betrafen ausschließlich Personen, die einer Straftat nach § 175 StGB an Minderjährigen verdächtig oder überführt waren. Insoweit ergab sich ebenfalls kein Grund zur Beanstandung.

Der Polizei wurde aber empfohlen, schon um Mißverständnisse zu vermeiden, die Bezeichnung der Sammlung zu ändern, damit nicht der falsche Schluß gezogen werden kann, Homosexualität allein sei ein Grund zur Aufnahme von Daten in diese Kartei.

„Rosa Listen“ oder wie immer bezeichnete Sammlungen, in denen Daten von Personen nur wegen homosexueller Neigungen gespeichert sind, sind rechtswidrig. Bei seinen Kontrollen hat der Landesbeauftragte bislang in Schleswig-Holstein noch keine derartige Datensammlung vorgefunden.

4.1.3.5 Datenschutz auch für Polizeibeamte

Anläßlich einer Eingabe stellte sich für den Landesbeauftragten die Frage, unter welchen Voraussetzungen bei der Einleitung eines Strafverfahrens gegen einen Polizeibeamten an wen welche Mitteilung zu machen ist. Bislang war dies in einem „WE-Erlaß“ (Wichtige Ereignisse) geregelt. Danach waren wichtige Ereignisse dem Schutzpolizeiamt, dem Kriminalpolizeiamt, dem Lagezentrum des Innenministeriums sowie nachrichtlich der vorgesetzten Behörde/Dienststelle zu melden. Zum Inhalt der WE-Meldung zählten neben dem Datum, der Uhrzeit, dem Ort des Ereignisses sowie dem Sachverhalt auch „die Personalien der Beteiligten“. Zu den meldepflichtigen Tatbeständen zählten zudem Vorkommnisse unter Beteiligung von Mitarbeitern der Polizei, insbesondere Straftaten durch Mitarbeiter von Polizeibehörden innerhalb und außerhalb (ausgenommen Privatklagedelikte) des Dienstes.

Auf der Grundlage dieses WE-Erlasses war auch im Falle des Petenten die vorgesetzte Dienststelle über die Einleitung eines strafrechtlichen Ermittlungsverfahrens unterrichtet worden. Daraufhin wurde eine bereits vorbereitete Beförderung nicht ausgesprochen. Das Ermittlungsverfahren wurde später eingestellt, die Beförderungsstelle ist inzwischen aber anderweitig besetzt worden.

Der Innenminister hat den Fall zum Anlaß genommen, eine Neuregelung der Übermittlung von Tatsachen aus Strafverfahren gegen Beschäftigte der Landespolizei zu treffen. Eine solche kommt demnach nur noch in Betracht, wenn es als wahrscheinlich erscheint, daß die Dienststellenleitung dienst- oder arbeitsrechtliche Maßnahmen wie z.B. eine Umsetzung oder ein vorläufiges Dienstverbot aufgrund des Tatverdachts veranlassen muß, weil

- dies zur Sicherung der ordnungsgemäßen Wahrnehmung der Aufgaben der Dienststelle erforderlich ist oder
- ansonsten das Ansehen der Polizei erheblich geschädigt werden würde.

Dabei sind insbesondere die Art des Delikts, die Tatumstände, die Funktion der oder des Beschäftigten und die Aufgaben der Dienststelle zu berücksichtigen.

Eine Übermittlung allein zu disziplinarrechtlichen Zwecken ist nach dem Erlaß unzulässig. Insoweit gelten ausschließlich die Vorschriften über Mitteilungen in Strafsachen (MiStra) (vgl. Textziffer 4.3.4 dieses Berichtes). Geregelt ist außerdem, daß die Mitteilung nur durch den Leiter der ermittelnden Dienststelle an den Leiter der Behörde erfolgen darf, der der Betroffene angehört. Sie ist außerdem als „vertrauliche Personalsache“ zu kennzeichnen. Eine telefonische Vorabinformation ist nur noch in besonders dringlichen Fällen zulässig.

Durch diese Neuregelung konnte zwar die im Ausgangsfall erfolgte Datenübermittlung mit all ihren Folgen für den Betroffenen nicht mehr rückgängig gemacht werden. Für die Zukunft dürfte sich daraus aber eine deutliche Einschränkung der polizeiinternen Übermittlung von Informationen über strafrechtliche Ermittlungsverfahren gegen Polizeibeamte ergeben.

Auch unter einem anderen Aspekt zeichnet sich eine datenschutzrechtliche Verbesserung für Polizeibeamte ab. Bislang werden nämlich die Daten von Polizeibeamten, gegen die strafrechtliche Ermittlungsverfahren eingeleitet werden, ebenso wie die jedes anderen Verdächtigen in der polizeilichen Erkenntnisdatei PED gespeichert. Darin liegt aber im Verhältnis zu Tatverdächtigen, die nicht der Polizei angehören, insofern eine Schlechterstellung, als alle Kollegen, die Zugriff auf die PED haben, sich Informationen über den Tatverdacht verschaffen können.

Der Landesbeauftragte hat deshalb im Rahmen seiner Kontrolle der polizeilichen Datenverarbeitung, über die im 12. TB (S. 18) berichtet wurde, angeregt, daß der Zugriff auf Daten

über Polizeibeamte in der PED beschränkt wird. Er soll in Zukunft nur noch derjenigen Dienststelle zustehen, die die Ermittlungen gegen den betreffenden Polizeibeamten führt. Das Kriminalpolizeiamt hat nunmehr zugesagt, diese Empfehlung umgehend umzusetzen.

4.1.3.6 Einschränkung der Meldungen über „Wichtige Ereignisse“

Der Landesbeauftragte hat den vorstehend geschilderten Einzelfall zum Anlaß genommen, den Innenminister generell zur Änderung des Erlasses über die Meldungen bei „Wichtigen Ereignissen“ aufzufordern. Er hat nämlich bei seinen Kontrollen in der Vergangenheit mehrfach festgestellt, daß im Wege der Meldung über „Wichtige Ereignisse“ personenbezogene Daten gestreut wurden, die zur rechtmäßigen Aufgabenerfüllung der jeweiligen Empfänger nicht erforderlich waren.

Dieser Anregung ist der Innenminister nunmehr gefolgt. Der „WE-Erlaß“ wurde dahin gehend geändert, daß personenbezogene Daten über Beteiligte an Strafverfahren nur noch in „WE-Meldungen“ aufgenommen werden dürfen, soweit dies zur Bewertung der Meldung erforderlich ist, z.B. bei Persönlichkeiten des politischen und sonstigen öffentlichen Lebens, bei namentlich in der Öffentlichkeit bereits bekannten Straftätern. Folglich ist es künftig im Regelfall nicht mehr zulässig, in einer „WE-Meldung“ der Vollständigkeit halber die Personalien der Beteiligten aufzuführen.

4.1.3.7 Unzulässige erkennungsdienstliche Behandlung aller Asylbewerber in Oelixdorf

Der Landesbeauftragte hat bei einer Prüfung im Aufnahmelager Oelixdorf festgestellt, daß sämtliche Asylbewerber, die ihren Antrag im Aufnahmelager Oelixdorf stellen, dort erkennungsdienstlich behandelt werden. Dies ist ein Verstoß gegen das Asylverfahrensgesetz, wonach die erkennungsdienstliche Behandlung eines Asylbewerbers nur zulässig ist, wenn seine Identität nicht eindeutig geklärt ist. Dies hat der Landesbeauftragte dem Innenminister mitgeteilt.

Daneben hat er auch den Umfang der erkennungsdienstlichen Behandlung kritisiert. Es wird nämlich in aller Regel ein Zehnfingerabdruck, darüber hinaus in Einzelfällen der Handabdruck genommen. Die erkennungsdienstliche Behandlung von Asylbewerbern ist aber lediglich zum Zwecke der Identitätsfeststellung zulässig. Hierfür dürfte die Abnahme des Abdrucks eines Fingers in der Regel ausreichend sein. Die Abnahme von Zehnfingerabdrücken dürfte vermutlich aus kriminalpolizeilichen Gründen erfolgen. Hierfür gibt das Asylverfahrensgesetz aber keine Rechtsgrundlage. Hinzu kommt, daß das derzeitige Verfahren der Verformelung der Fingerabdrücke in den Dateien des Bundeskriminalamtes sehr aufwendig ist. Es

stellt sich deshalb sogar die Frage, ob nicht ein Teil der zeitlichen Verzögerungen der Asylverfahren auch darauf zurückzuführen ist, daß statt des Abdruckes eines Fingers, Zehnfingerabdrücke umständlich verformelt und abgespeichert werden müssen.

Die bisherige Stellungnahme des Innenministers ist unbefriedigend. Er hat darauf verwiesen, daß Asylbewerber, die bereits einen Kontakt mit einer deutschen Behörde vor ihrer Einreise hatten, ihren Asylantrag nicht in Oelixdorf, sondern in den anderen örtlich zuständigen Ausländerbehörden stellen. Diese Antragsteller würden in der Regel nicht erkennungsdienstlich behandelt. Man könne deshalb nicht davon sprechen, daß in Schleswig-Holstein alle Asylbewerber erkennungsdienstlich behandelt würden. Dies hatte der Landesbeauftragte auch nicht behauptet. Seine Kritik bezog sich ausschließlich auf die zentrale Aufnahmestelle in Oelixdorf. Dort allerdings werden nach seinen Feststellungen alle Asylbewerber erkennungsdienstlich behandelt. Selbst wenn in Rechnung zu stellen ist, daß die Zahl der Antragsteller, bei denen Zweifel an der Identität bestehen, in Oelixdorf besonders hoch ist, so rechtfertigt dies nicht die erkennungsdienstliche Behandlung aller Antragsteller.

Auch der ergänzende Hinweis des Innenministers bei einem parteiübergreifenden Gespräch im Bundeskanzleramt sei verabredet worden, das Asylverfahrensgesetz so zu ändern, daß eine generelle erkennungsdienstliche Behandlung aller Asylbewerber vorgenommen werden darf, vermag die Praxis in Oelixdorf nicht zu rechtfertigen. Zum einen haben die Ergebnisse parteiübergreifender Gespräche im Bundeskanzleramt keine Gesetzesqualität, zum anderen unterstreicht gerade die Absicht, das Asylverfahrensgesetz zu verschärfen, daß derzeit keine ausreichende Rechtsgrundlage für die erkennungsdienstliche Behandlung aller Asylbewerber vorhanden ist.

Der Landesbeauftragte hat den Innenminister auf diese Gesichtspunkte hingewiesen und erneut verlangt, daß die routinemäßige erkennungsdienstliche Behandlung aller Asylbewerber in Oelixdorf in einer Weise eingeschränkt wird, die dem Asylverfahrensgesetz Rechnung trägt.

4.1.3.8 Automatisierung der Vorgangsverwaltung bei der Polizei

Wenn ein Bürger in Schleswig-Holstein Kontakt zur Polizei hat, hinterläßt er dort in der Regel „Spuren“ in deren diversen Buchwerken, die heute noch manuell und vor Ort geführt werden. Dabei spielt es keine Rolle, welche „Rolle“ der Bürger bei der Polizei „gespielt“ hat. Auch wer kein Verdächtiger oder Beschuldigter ist, sondern Hinweisgeber, Zeuge, Anzeigenerstatter, Helfer, Finder, Opfer, Geschädigter, Vermißter, wird in den Tagebüchern etc. der Polizei erfaßt. Auf diesem Wege wird das Verwaltungshandeln der Polizei nahezu vollständig dokumentiert. Das Verfahren soll nunmehr modernisiert, d.h. automatisiert werden. Auf der Grundlage eines Gut-

achtens, das eine Unternehmensberatung zum Thema „Möglichkeiten und Grenzen eines verstärkten Einsatzes von Informations- und Kommunikationstechniken bei der Landespolizei Schleswig-Holstein“ erstellt hat, ist eine Projektgruppe eingerichtet worden, die die Automatisierung der polizeilichen Vorgangsbearbeitung entwickeln und realisieren soll.

Zunächst soll bei Pilotdienststellen reine Textverarbeitung mit Zugriffsmöglichkeiten auf die polizeiliche Erkenntnisdatei PED sowie auf das zentrale Verkehrsinformationssystem ZEVIS, das Einwohnerinformationssystem EIS und auf das polizeiliche Bund-Länder-System INPOL eingerichtet werden. Erst später ist geplant, die Vorgangsverwaltung der schleswig-holsteinischen Landespolizei zu automatisieren. Ein Zeitpunkt hierfür ist noch nicht genannt worden.

Datenschutzrechtlich ist gegen die Modernisierung von Verarbeitungsverfahren nichts einzuwenden, sofern damit keine höheren Risiken für das informationelle Selbstbestimmungsrecht der Betroffenen verbunden sind oder diese durch geeignete Schutzvorkehrungen ausgeglichen werden. Es liegt auf der Hand, daß der Speicherung in einem automatisierten Verfahren ein anderer Stellenwert zukommt als der handschriftlichen Notiz in einem fortlaufend geführten Tagebuch. Dem muß mit einem ausgewogenen und wirksamen Schutzkonzept Rechnung getragen werden.

Bei einer ersten Kontaktaufnahme mit der Projektgruppe im August 1991 wurde der Landesbeauftragte gebeten, das Vorhaben der Polizei möglichst frühzeitig beratend zu begleiten. Sobald ihm nähere Informationen über die weiteren Planungen zugehen, wird er im Tätigkeitsbericht detaillierter auf das Vorhaben eingehen.

4.1.4 Ausländerrecht

Entwurf eines Ausländerzentralregistergesetzes

Von der geplanten Neuordnung des Ausländerzentralregisters durch ein Bundesgesetz sind nicht unwesentlich auch die Behörden der Länder und der kommunalen Gebietskörperschaften betroffen. Sie müssen nicht nur ihr Verwaltungsverfahren auf ein solches technisches Medium abstellen. Sie tragen als „Datenlieferanten“ und „-bezieher“ in weitem Umfang auch Verantwortung für die Richtigkeit und Aktualität der dort gespeicherten Daten und werden darüber hinaus von der Funktionsfähigkeit des Systems in erheblichem Maße abhängig. Das veranlaßte den Landesbeauftragten, gegenüber dem Innenminister zu dem Gesetzgebungsvorhaben kritisch Stellung zu nehmen:

- Mit der vorgesehenen Regelung würde ein kombiniertes Informationssystem über die bereits bestehende Praxis hinaus festgeschrieben, das Elemente nicht nur eines Aktennachweises, sondern auch eines Melderegisters, eines Fahndungssystems, einer zentralregisterähnlichen Dokumenta-

tion und einer Strafvollstreckungsdatei enthält. Ein solches System, das nicht nur Daten der Ausländerbehörden, sondern auch Daten anderer Behörden wie z.B. der Polizei, des Verfassungsschutzes beinhaltet und diesen zur Nutzung zur Verfügung stellt, begegnet erheblichen datenschutzrechtlichen Bedenken. Es stellt sich die Frage, ob dies nicht ein typisches Beispiel für die vom Bundesverfassungsgericht für unzulässig erklärte Kombination „tendenziell unvereinbarer Zwecke“ der Datenverarbeitung ist. Eine Vereinigung all dieser Datenspeicherungen unter der Klammer des „Ausländerrechts“ und die Anknüpfung der Datenspeicherung ausschließlich an die ausländische Staatsangehörigkeit begegnet darüber hinaus Bedenken unter dem Gesichtspunkt des Gleichheitssatzes.

- Die vorgesehenen Übermittlungsregelungen bergen die Gefahr, daß nicht aufgrund des gesamten Akteninhaltes, sondern allein aufgrund des verkürzten Registerinhaltes Sachentscheidungen gefällt werden. Dies würde zu einer unzulässigen Verkürzung der Entscheidungsgrundlage führen.
- Bedenken bestehen weiter gegen eine extensive Zulassung von Online-Verbindungen verschiedener Verwaltungsstellen mit dem Ausländerzentralregister. Die schnelle und problemlose Auswertung von Datenbeständen reizt zu einer extensiven Nutzung über das Maß des Erforderlichen hinaus. Kontrollmöglichkeiten sind bei Online-Anschlüssen in weiterem Umfang eingeschränkt als bei Datenübermittlungen auf ausdrückliches Ersuchen hin. Deshalb sollten Online-Anschlüsse nur für solche Fälle vorgesehen werden, in denen in nennenswertem Umfang Datenabfragen eilbedürftig sind. Die Bundesanstalt für Arbeit beispielsweise dürfte nicht dazu gehören. Aus ihrer Aufgabenstellung heraus ist die Notwendigkeit solcher Anschlüsse auch nicht für die Geheimdienste zu begründen.

Aus diesen grundsätzlichen Bedenken folgt eine ganze Reihe von Vorschlägen des Landesbeauftragten zu einzelnen Vorschriften. Er hofft, daß in den weiteren Beratungen das Ausländerzentralregister auf das reduziert wird, was erforderlich und verfassungsrechtlich zulässig erscheint nämlich auf eine zentrale Übersicht darüber, welche Verwaltungsvorgänge über den einzelnen Ausländer bestehen und bei welchen Behörden sie geführt werden. Der Umgang mit den einzelnen Vorgängen und die Voraussetzungen für Datenübermittlungen müssen in den jeweiligen materiellen Vorschriften der einzelnen Rechtsgebiete geregelt werden.

4.1.5 Bau- und Wohnungswesen

Abbau der Fehlbelegungen im sozialen Wohnungsbau

An ausreichendem Wohnraum besteht in der Bundesrepublik Mangel. Zu den Maßnahmen, Abhilfe zu schaffen, gehören auch Überlegungen, öffentlich geförderten Wohnraum vor-

zugsweise wirtschaftlich Schwachen zur Verfügung zu stellen. Bessern sich später die wirtschaftlichen Verhältnisse solcher Mieter, so können zwar die bestehenden Mietverhältnisse nicht aufgelöst werden, es erscheint aber angemessen, durch besondere Abgaben einen Ausgleich für die Vorteile des subventionierten Mietpreises zu bewirken. Für die Berechnung solcher Abgaben sind Feststellungen zum Einkommen sowie zu den Familien- und Wohnverhältnissen der Betroffenen erforderlich, die Personenbezug haben und von verschiedenen öffentlichen Stellen zur Kenntnis genommen werden müssen.

Ein Bundesgesetz über den Abbau der Fehlsubventionierung im Wohnungsbau regelt diese Rechtsmaterie, soweit nicht die Länder eigene Gesetze erlassen. Das ist für Schleswig-Holstein geschehen. Zu einem Gesetzentwurf der Opposition hat der Landesbeauftragte gegenüber dem Schleswig-Holsteinischen Landtag Stellung genommen. Dies hat dazu geführt, daß die Schwächen des entsprechenden Bundesgesetzes vermieden und die Eigenverantwortlichkeit des Bürgers für seine Daten gestärkt wurden:

- Betroffenen wird freigestellt, ob sie die erforderlichen Angaben machen wollen, um weiter den Vorteil einer subventionierten Miete zu genießen.
- Werden Angaben gemacht, so sind zunächst die Betroffenen dafür beweispflichtig. Die zuständigen Behörden dürfen „von Amts wegen“ nur in besonders festgelegten Ausnahmefällen eigene Ermittlungen anstellen.
- Ermächtigen die Betroffenen die zuständigen Stellen, Angaben und Auskünfte bei Dritten einzuholen, so müssen diese Stellen genau bezeichnet werden.
- Mehreren Inhabern der gleichen Wohnung, wie z.B. Mietern und Untermietern, ist die Möglichkeit eröffnet worden, die Angaben unabhängig voneinander zu machen, um unnötige Offenbarungen persönlicher Verhältnisse zu vermeiden.

4.2 Datenschutz im Kommunalbereich

4.2.1 Erfahrungen mit dem neuen Kommunalverfassungsrecht

4.2.1.1 Melderegisterauskunft an Bürgerinitiativen?

Eine Bürgerinitiative war sich nicht sicher, ob die gesammelten Unterschriften tatsächlich von wahlberechtigten Bürgern stammten und damit das Quorum der Gemeindeordnung für ein Bürgerbegehren erreichte. Sie beantragten deshalb eine Melderegisterauskunft, mit der die Wahlberechtigung der Unterzeichnenden vor Einreichung des Bürgerbegehrens festgestellt werden sollte.

Die Meldebehörde und der Innenminister befaßten den Landesbeauftragten mit dem Fall. Die datenschutzrechtliche Beurteilung der erbetenen Auskunft mußte negativ ausfallen.

Weder das Melderecht noch die Verfahrensvorschriften für Bürgerbegehren enthalten eine Rechtsgrundlage für eine solche Auskunft. Erst wenn das Bürgerbegehren einschließlich der Unterschriftenlisten bei der Gemeinde eingereicht ist, prüft die Meldebehörde Antragslisten und Einzelanträge, stellt die Wahlberechtigung und die Richtigkeit der Eintragungen fest und teilt das Ergebnis ihrer Prüfung der Kommunalaufsichtsbehörde mit. Hätte der Gesetzgeber den Bürgerinitiativen ein entsprechendes Auskunftsrecht aus dem Melderegister einräumen wollen, hätte er dies ausdrücklich im Gesetz regeln müssen.

So gelten die Vorschriften des Landesmeldegesetzes. Danach fehlt es in solchen Fällen schon an dem vom Melderecht geforderten „berechtigten Interesse“ für eine Melderegisterauskunft. Die verlangte Auskunft über die Wahlberechtigung der Unterzeichner ist für die Durchsetzung des Bürgerbegehrens nicht erforderlich.

Hinzu kommt, daß aus der erbetenen Auskunft unter bestimmten Umständen geschlossen werden könnte, wer nach dem Gemeinde- und Kreiswahlgesetz vom Wahlrecht ausgeschlossen ist, weil er unter Beistandschaft steht oder infolge Richterspruchs das Wahlrecht nicht mehr besitzt.

4.2.1.2 Aktenvorlage an Fraktionen der Stadtvertretung

An den Fraktionssitzungen einer Stadtvertretung durften nach der Geschäftsordnung auch die bürgerlichen Mitglieder der Ausschüsse teilnehmen. Der Bürgermeister hatte Bedenken, auch ihnen Akteneinsichtsrechte zu gewähren. Er befürchtete, gegen Vorschriften der Gemeindeordnung zu verstoßen, die auch dem Schutz des Persönlichkeitsrechts Betroffener dienen, und bat den Landesbeauftragten um Beratung.

Dieser mußte die Bedenken des Bürgermeisters bestätigen. Die Gemeindeordnung räumt ein Auskunfts- und Akteneinsichtsrecht nicht den Fraktionen, sondern nur den Mitgliedern der Gemeindevertretung ein und nur insoweit, als es zur Vorbereitung und Kontrolle einzelner Beschlüsse der Gemeindevertretung erforderlich ist. Die Unterlagen für die Ausschussarbeit dürfen zwar allen Mitgliedern, d.h. auch den bürgerlichen, zugänglich gemacht werden, aber daraus ist kein allgemeines Akteneinsichtsrecht herzuleiten.

4.2.2 Weitere Probleme und ihre Lösungen

4.2.2.1 Übermittlung von Steuerdaten an die Kirche

Ein evangelisch-lutherischer Kirchenkreis hatte zur Erhebung von Kirchengrundsteuern eine Amtsverwaltung ersucht, ihm folgende Daten zu übermitteln: Namen und Anschriften der evangelischen Grundsteuerpflichtigen sowie die jeweiligen Grundsteuermeßbeträge, Grundsteuerbeträge und Steuer-

nummern. Die Amtsverwaltung hatte mit Rücksicht auf das Steuergeheimnis Zweifel an der Zulässigkeit der erbetenen „Amtshilfe“.

Auch wenn Steuerdaten in Deutschland als besonders sensibel angesehen werden und dem Steuergeheimnis als einem besonderen Amtsgeheimnis unterliegen, so lassen gerade die Steuergesetze im vorliegenden Fall Ausnahmen zu. Nach der Abgabenordnung, die im kommunalen Abgabewesen entsprechend gilt, dürfen nämlich die kommunalen Steuerämter den öffentlich-rechtlichen Religionsgemeinschaften solche Besteuerungsgrundlagen mitteilen, an die im jeweiligen Zuständigkeitsbereich kirchliche Abgaben anknüpfen. Namen und Anschriften der evangelischen Grundsteuerpflichtigen sowie der auf sie entfallende Grundsteuermeßbetrag durfte daher aufgrund dieser spezialgesetzlichen Vorschriften dem Kirchenkreis mitgeteilt werden. Weitergehende Datenübermittlungen, etwa der Steuerbeträge, der Steuernummern oder Informationen über Personen, deren Zugehörigkeit zur evangelisch-lutherischen Kirche dem Amt nicht bekannt ist, sind nach der Regelung in der Abgabenordnung allerdings unzulässig.

4.2.2.2 Aufnahme von Kindern in kommunale Kindergärten

Nicht jedes Gremium einer Gemeinde ist befugt, Verwaltungsentscheidungen zu treffen und zu diesem Zweck personenbezogene Informationen aufzunehmen. Neben den kommunalverfassungsrechtlich verankerten und gewählten Ausschüssen der Gemeindevertretung, die sich nur aus Gemeindevertretern und ggf. bürgerlichen Mitgliedern zusammensetzen, werden gelegentlich unterstützende Beiräte und Gremien gebildet und ebenfalls als „Ausschüsse“ bezeichnet, an denen auch Außenstehende, Interessenvertreter und Verwaltungsmitarbeiter beteiligt werden. Solche Gremien können allenfalls beratende Funktionen haben, nicht aber Aufgaben der Gemeindevertretung nach Kommunalverfassungsrecht übertragen bekommen. Ist eine entsprechende Aufgabenübertragung aber ausgeschlossen, so benötigen diese Gremien auch keine damit zusammenhängenden personenbezogenen Daten. Erhalten sie dennoch solche Informationen von der Verwaltung, so liegt darin ein Verstoß gegen Datenschutzvorschriften.

Auf einen solchen Sachverhalt stieß der Landesbeauftragte, als er um Stellungnahme gebeten wurde, ob einem „Kindergartenausschuß“, bestehend aus drei politischen Vertretern, drei Elternvertretern und drei Vertretern der Verwaltung, Angaben persönlicher Art (einschl. Einkommensnachweis) der Eltern zugeleitet werden dürfen, wenn man ihm die Entscheidung über die Aufnahme von Kindern in den Kindergarten und über die Höhe der Kindergartenbeiträge übertragen würde.

Der Landesbeauftragte hat auf die datenschutzrechtliche Unzulässigkeit einer solchen Verfahrensweise hingewiesen. Eine Entscheidung über die Kindergartenaufnahme und die Höhe des Beitrags haben die zuständigen Verwaltungsmitarbeiter,

wenn es sich um ein Geschäft der laufenden Verwaltung handelt. Die Mitglieder der Gemeindevertretung oder eines ihrer (echten) Ausschüsse sind zuständig, wenn es als eine „für die Gemeinde wichtige Entscheidung“ im Sinne der Gemeindeordnung geht. Nur diesen Stellen dürfen personenbezogene Daten der Eltern zum Zwecke der Entscheidung übermittelt werden.

4.2.2.3 Einkommensermittlung für Kindergartenbeiträge

Um Kindergartenangelegenheiten ging es auch in einem anderen Fall. Petenten beschwerten sich darüber, daß eine Gemeinde „hinter ihrem Rücken“ Einkommensermittlungen bei ihren Arbeitgebern angestellt hatte, um über Anträge zur Ermäßigung der Kindergartenbeiträge zu entscheiden. Die Gemeinde wandte ein, daß sie aufgrund der Satzung Einkommensangaben verlangen könne. Die Betroffenen hätten dadurch, daß sie (allerdings unvollständige) Einkommensnachweise vorgelegt hätten, auch ihr generelles Einverständnis in die Ermittlung des Einkommens zum Ausdruck gebracht. Es wäre nur darum gegangen, die unvollständigen Angaben um eine Jahresverdienstbescheinigung zu ergänzen. Dies dürfe auch von Amts wegen veranlaßt werden.

Der Landesbeauftragte hat dieser Auffassung widersprochen. In den vorliegenden Fällen war eine unmittelbare Einkommensermittlung beim Arbeitgeber nicht erforderlich und verstieß damit gegen Datenschutzrecht. Die Petenten hätten auf eine eventuelle Unvollständigkeit der Einkommensnachweise aufmerksam gemacht werden können. Wären sie der Aufforderung zur Ergänzung der Unterlagen nicht nachgekommen, so hätten die Ermäßigungsanträge abgelehnt werden können.

Die Gemeinde wird künftig die Angaben durch die Betroffenen selbst nachweisen lassen und nur bei ausdrücklicher Einwilligung, d.h. auf Wunsch der Antragsteller, Auskünfte vom Arbeitgeber einholen. Damit entspricht das Verfahren auch dem neuen Datenschutzrecht, wonach Daten grundsätzlich beim Betroffenen mit seiner Kenntnis zu erheben sind.

4.2.2.4 Weitergabe von Adressen zu Werbezwecken

Aus den Grundsteuerlisten waren die Adressen von Grundeigentümern gleichermaßen jedenfalls nicht geflossen, die eine Gemeinde einem privaten Kabelfernsehunternehmen für Werbezwecke zur Verfügung gestellt hatte. Sonst wäre sogar das Steuergeheimnis verletzt gewesen. Aber man kannte seine Grundstückseigentümer ja aus Bauanträgen und Grundstückskaufverträgen und hatte über den Inhalt des Melderegisters hinaus einen „Straßen- und Hausnummernplan“ zusammengestellt. Aus diesem übermittelte man der privaten Firma die gewünschten Daten, denn gegen ein attraktives Medienangebot konnte doch eigentlich kein Grundstückseigentümer etwas

haben. Trotzdem gingen Beschwerden ein, und die Gemeinde mußte einräumen, daß sie ohne eine ausreichende Rechtsgrundlage die Informationen herausgegeben hatte.

Auch nach dem neuen Datenschutzrecht sind Datenübermittlungen an Private zu Werbezwecken unzulässig. Weder liegen die Voraussetzungen für eine Änderung des Verwendungszwecks vor noch begründen Werbezwecke ein rechtliches Interesse.

4.2.2.5 Ein Amt reagiert nicht

Der datenschutzrechtliche Fehler war eindeutig: Eine Amtskasse hatte die Pfändungs- und Überweisungsverfügung gegen einen Hauseigentümer aufgehoben und dies seinem Mieter als Drittschuldner auf einer offenen Postkarte mitgeteilt; denn die Miete stand ja nun wieder dem Vermieter zu. Eine solche Mitteilung auf offener Postkarte begegnet natürlich datenschutzrechtlichen Bedenken. Es kann nicht sichergestellt werden, daß nicht Unbefugte von den sehr sensiblen Informationen Kenntnis erhalten. Das sah auch die zuständige Amtsverwaltung ein und hat inzwischen angeordnet, daß personenbezogene Daten dieser Art nur noch in einem verschlossenen Briefumschlag versandt werden. Ähnliche Fälle hat der Landesbeauftragte in der Vergangenheit des öfteren beanstandet.

Im vorliegenden Fall mußte er allerdings auch eine Beanstandung wegen der Säumigkeit der Behörde aussprechen und die Aufsichtsbehörde unterrichten. Das Amt hatte nämlich – aus welchen Gründen auch immer – trotz dreier Erinnerungen erst auf die Beanstandung hin fast ein halbes Jahr nach der ersten Anfrage eine Stellungnahme abgegeben. Der Landesbeauftragte hält es dem Bürger gegenüber schlechthin für unzumutbar, wenn bei eindeutiger Sach- und Rechtslage sich das Verfahren ohne Not in einem solchen Maße verzögert.

4.2.2.6 Steuerbescheid per Telefax

Die gleichen Probleme wie bei einer Information auf einer Postkarte entstehen, wenn Nachrichten modern, preiswert und schnell per Telefax übermittelt werden. Ein Steuerberater hatte von der zuständigen Stadtverwaltung einen Steuerbescheid für seinen Mandanten per Telefax zugesandt bekommen. Er wandte sich an den Landesbeauftragten und wies darauf hin, daß der Absender solcher Informationen nicht ohne Rückfrage davon ausgehen könne, daß nur der Adressat des Bescheides oder ein sonstiger berechtigter oder bevollmächtigter Empfänger von dem Inhalt des Telefax Kenntnis erhalte.

Der Landesbeauftragte sieht dies genauso und hat die Stadt darauf hingewiesen, daß es für die Versendung solcher sensiblen Informationen immer einer zusätzlichen Einwilligung des Empfängers in die Übermittlung per Telefax bedarf oder auf andere Weise sichergestellt werden muß, daß Unberech-

tigte keine Möglichkeiten zur Kenntnisnahme erhalten. Auch der Städtebund Schleswig-Holstein ist dieser Auffassung beigetreten. Der Landesbeauftragte hat diesen Fall und andere (vgl. Textziffer 4.6.2.2) zum Anlaß genommen, in einer besonderen Bekanntmachung im Amtsblatt (vgl. Textziffer 5.3) auf die Gefahren aufmerksam zu machen und Hinweise gegeben, wie ihnen entgegengewirkt werden kann.

4.3 Justiz

4.3.1 GAST: Noch nicht alles im Lot

Der Landesbeauftragte hat über die umfangreiche Querschnittskontrolle des staatsanwaltschaftlichen Dateiverfahrens GAST-SH (Geschäftsstellenautomation der Staatsanwaltschaften) berichtet (13. TB., S. 42). Nunmehr liegt die abschließende Stellungnahme des Generalstaatsanwalts zu den Prüfbemerkungen vor. Die darin angekündigten Maßnahmen bringen den Datenschutz im GAST-Verfahren ein erhebliches Stück voran. Sie tragen den Kritikpunkten des Landesbeauftragten überwiegend Rechnung. Es bleiben aber noch einige grundlegende Mängel, deren Beseitigung geboten ist.

Um mit dem Positiven zu beginnen: Der Generalstaatsanwalt hat sich mit dem Prüfbericht des Landesbeauftragten intensiv und detailliert auseinandergesetzt.

Dort, wo er den Kritikpunkten nachkommt, sind die Konsequenzen entweder bereits gezogen oder ihre Realisierung ist eingeleitet. In puncto Präzision und Verbindlichkeit unterscheidet sich die Stellungnahme des Generalstaatsanwalts von der manch anderer Stellen.

Im einzelnen ergibt sich folgendes Bild: **Die Verantwortlichkeit der Staatsanwälte** für die in GAST gespeicherten Daten wird gestärkt. War es bisher eine Angelegenheit der Geschäftsstellen, die Daten in GAST zu speichern und ggf. zu korrigieren, so muß künftig spätestens im Rahmen der das Ermittlungsverfahren abschließenden Verfügung die Dezernentin/der Dezernent eine Kontrolle der Personendaten eingetragener Beschuldigter, des Tatvorwurfs und der Erledigungsart auf ihre Richtigkeit hin vornehmen und auf einem „Datenschutzkontrollblatt“ bestätigen. Dadurch soll sichergestellt werden, daß die in GAST gespeicherten Daten den Vorgang richtig wiedergeben und den Betroffenen nicht unnötig belasten.

Bei **querulatorischen und böswilligen Anzeigen** werden künftig nicht mehr die Daten des Angezeigten, sondern die des Anzeigenden gespeichert. Außerdem wird bereits im Datensatz erkennbar sein, daß das Verfahren mangels substantiierten Anzeigevorbringens eingestellt worden ist. Der Zugriff auf solche Datensätze wird auf die sachbearbeitende Staatsanwaltschaft beschränkt.

Ähnlich wird verfahren, wenn sich schon bei erster Prüfung herausstellt, daß ein Sachverhalt nicht die Voraussetzungen des Anfangsverdachts im Sinne der Strafprozeßordnung erfüllt. In diesem Falle wird als Erledigungsart eingetragen: „Keine Einleitung eines Ermittlungsverfahrens mangels Anfangsverdachts ...“. Auch insoweit wird der Zugriff auf die sachbearbeitende Staatsanwaltschaft begrenzt. Der Umfang der gespeicherten Daten wird reduziert.

Ein Hauptkritikpunkt im Prüfbericht des Landesbeauftragten war die Behandlung von **Daten über die Opfer von Sexualstraftaten**. Bislang wurden immer dann, wenn der Täter nicht ermittelt werden konnte, die Daten des Opfers in GAST mit landesweitem Zugriff gespeichert. Künftig wird wie folgt verfahren: Können keine Täterdaten ermittelt werden, so werden die Anfangsbuchstaben des Vornamens und des Nachnamens des Opfers erfaßt. Der landesweite Zugriff wird künftig nicht mehr möglich sein. Zugriff hat nur noch die Staatsanwaltschaft, bei der das Verfahren anhängig ist. Außerdem wurde der Zugriff auch innerhalb der jeweiligen Staatsanwaltschaft auf das Dezernat, das zur Verfolgung von Sexualstraftaten zuständig ist, begrenzt. Auch die bislang bereits gespeicherten Daten über Opfer von Sexualstraftaten sollen in diesem Sinne reduziert werden.

Selbsttötungsversuche werden künftig in GAST nicht mehr generell erfaßt. Lediglich dann, wenn die Kriminalpolizei Anhaltspunkte dafür hat, daß ein Fremdverschulden vorgelegen haben könnte, wird ein Datensatz wegen eines versuchten Tötungsdelikts zum Nachteil des Betroffenen angelegt. Irgendwelche Hinweise, aus denen auf eine versuchte Selbsttötung geschlossen werden könnte, sind untersagt. Etwaigen Anträgen der Betroffenen auf Löschung der Daten wird nachgekommen. Auch die Datensätze der noch gespeicherten Altverfahren werden so geändert, daß ihnen kein Hinweis mehr auf eine versuchte Selbsttötung entnommen werden kann. Bei vollendeten Selbsttötungsfällen wird künftig nur noch ein Zugriff für die sachbearbeitende Staatsanwaltschaft bestehen.

Der Landesbeauftragte hatte kritisiert, daß bei **Verkehrsunfällen** häufig auch die **Daten des Opfers** wie die eines Täters gespeichert werden. Dies wird künftig unterbleiben. Die Dezernenten haben bei neu eingegangenen Verkehrsunfallsachen zu prüfen, ob fälschlicherweise ein Beteiligter als Beschuldigter in GAST eingetragen worden ist. Hierzu wird in GAST die Möglichkeit der ersatzlosen Löschung der Personendaten eines irrtümlich eingetragenen „Beschuldigten“ programmtechnisch sichergestellt.

Positiv ist auch, daß der **Katalog der** in GAST erfaßten **Delikte** sowie insbesondere der **Katalog der Erledigungsarten** weiter verfeinert wird. Dadurch wird es künftig eher möglich sein, den Verlauf des einzelnen Verfahrens zutreffend in GAST wiederzugeben und unnötige Belastungen der Betroffenen zu vermeiden.

Im Datenfeld „**Besondere Hinweise**“ war es bislang mangels einer verbindlichen Festlegung des Inhalts möglich, wertende Hinweise zu dem Beschuldigten zu geben. Bei der Kontrolle wurden Eintragungen wie „gewalttätig“, „BTM-abhängig“, „Selbstmordgefahr“ usw. vorgefunden. Künftig dürfen in diesem Datenfeld keinerlei personenbezogene Hinweise mehr gespeichert werden. Statt dessen werden lediglich für die Akten- und Verfahrenskontrolle notwendige Sachhinweise dort erfaßt.

In dem gleichen Datenfeld waren in der Vergangenheit häufig **alte Aktenzeichen** gespeichert, obwohl die zugehörigen Akten nach den Aufbewahrungsbestimmungen längst vernichtet waren. Dadurch war es möglich, auch nach Ablauf dieser Fristen aus dem Datensatz zu ersehen, ob es sich um einen „alten Kunden“ handelte, ohne daß noch Unterlagen vorhanden gewesen wären, denen man Näheres entnehmen konnte. Dies wird künftig eingestellt. Die noch erfaßten alten Aktenzeichen werden gelöscht.

Die vereinzelt vorgefundene Praxis, bei **Wiederaufnahme eines Verfahrens** einen neuen Verfahrensdatensatz anzulegen und damit den Eindruck mehrfacher Straffälligkeit des Beschuldigten zu erwecken, wird eingestellt.

Verbessert wurde auch die Datenerfassung im Falle von **Mittäterschaft**. Bislang konnte es passieren, daß nach dem Prinzip „Mitgegangen-Mitgehangen“ die Daten aller Mittäter gleich lang gespeichert waren, obwohl die Frist für einzelne von ihnen bereits abgelaufen war. Das Verfahren ist jetzt dahingehend umgestaltet worden, daß die Speicherfristen für jeden Mittäter individuell berechnet und eingehalten werden können.

Weitere Verbesserungen wurden angekündigt hinsichtlich der **Verwendung von Ausdrucken** aus dem GAST-Verfahren sowie der **Auskunft an Betroffene**. Auf automatische Auswertungen aus GAST, die zur Verhaltens- und Leistungskontrolle verwendet werden könnten, wird künftig verzichtet.

In einer Reihe von Punkten sind die vom Generalstaatsanwalt angekündigten Maßnahmen geeignet, die datenschutzrechtlichen Bedenken überwiegend zu beseitigen. So hatte der Landesbeauftragte gerügt, daß auch die **Daten von Kindern** in GAST gespeichert sind.

Auch der Generalstaatsanwalt möchte die Zahl der Fälle, in denen Daten über strafunmündige Kinder von der Polizei an die Staatsanwaltschaft gemeldet und dort registriert werden, reduzieren. Bei schwerwiegenden Vorwürfen hält er auch für die Zukunft die Meldung solcher Daten für erforderlich, um die Vorwürfe von der Staatsanwaltschaft überprüfen zu lassen. Er will aber insoweit den Zugriff auf die sachbearbeitende Staatsanwaltschaft beschränken.

Ein wichtiger Kritikpunkt im Prüfbericht des Landesbeauftragten war, daß **gerichtliche Freisprüche** keine Konsequenzen für die weitere Speicherung der Daten in GAST hatten.

Künftig wird – von wenigen Ausnahmen abgesehen – im Falle eines Freispruchs der Zugriff auf die Daten auf die sachbearbeitende Staatsanwaltschaft begrenzt.

Verbesserungen hat der Generalstaatsanwalt auch hinsichtlich der **Datenübermittlung an Dritte** angekündigt. Insoweit handelt es sich weniger um ein GAST-spezifisches als vielmehr um ein generelles Problem. Der Landesbeauftragte hatte festgestellt, daß die Staatsanwaltschaft Ermittlungersuchen – so wie in der Justiz häufig üblich – in Form der Übersendung der Akten nachkommt. Dabei werden in der Regel auch Daten Dritter mit übermittelt. In einzelnen Fällen hatte der Landesbeauftragte festgestellt, daß sogar sensible Sozialdaten unter Verstoß gegen das Sozialgesetzbuch mit übermittelt worden waren.

Der Generalstaatsanwalt hat mitgeteilt, den datenschutzrechtlichen Verpflichtungen werde man bei Datenübermittlungen künftig nachkommen. Sofern es noch zur Versendung von Akten komme, würden besonders sensible Schriftstücke vorher entfernt und zu den Handakten genommen. Es werde künftig vermehrt Einzelauskünfte statt der Übersendung ganzer Akten geben. Die privaten Auskunftersuchen, insbesondere von Versicherungen, würden darauf hingewiesen, daß jedes Einzelauskunftersuchen einer genügenden Begründung im Sinne des neuen Landesdatenschutzgesetzes bedarf. Allerdings macht der Generalstaatsanwalt die Einschränkung, daß dies „vom Arbeitsaufwand zu vertreten“ sein müsse. Er hat darauf verwiesen, daß jährlich ca. 100.000 Datenübermittlungersuchen bei der Staatsanwaltschaft eingehen.

Darin dokumentiert sich nach Auffassung des Landesbeauftragten die ganze Tragweite dieser Problematik. Er hält es deshalb nicht für hinnehmbar, den Datenschutz gerade im Zusammenhang mit der Übermittlung so sensibler Daten wie derer aus dem Bereich der Strafverfolgung vom „Arbeitsaufwand“ abhängig zu machen. Sollte tatsächlich nicht die Möglichkeit bestehen, die einzelnen Übermittlungersuchen zu überprüfen und aus den Akten dasjenige herauszunehmen und zu übermitteln, was für die Beantwortung des Auskunftersuchens erforderlich ist, so darf dies nicht zu Lasten der Betroffenen gehen.

In einigen wichtigen Punkten ist die Stellungnahme des Generalstaatsanwalts noch nicht zufriedenstellend. Der Landesbeauftragte hatte moniert, daß die Speicherung der Daten in GAST mit **landesweitem Zugriff** erfolgt. Er hat im Rahmen seiner Kontrollen festgestellt, daß keineswegs in jedem Fall die Akten der anderen Staatsanwaltschaften beigezogen werden. Schon im Hinblick auf die Arbeitsüberlastung der Staatsanwälte wird häufig – vermutlich in der Regel – nach eigener Aktenlage entschieden. Dann ist aber ein Zugriff auf die Datensätze anderer Staatsanwaltschaften im Regelfall nicht erforderlich. Der Generalstaatsanwalt hält demgegenüber auch die bloße Auskunft aus dem GAST-System, daß z.B. der Beschuldigte bislang nicht vorbelastet ist, für eine unverzichtbare

Information, um die Einstellungsmöglichkeiten zugunsten des Bürgers auszuschöpfen.

Für das GAST-Verfahren besteht derzeit **keine ausreichende Rechtsgrundlage**. Dies haben auch die Landesregierung und der Generalstaatsanwalt eingeräumt. Daraus folgt, daß bis zur Schaffung einwandfreier Rechtsgrundlagen nur das absolut notwendige Minimum an Datenverarbeitung zulässig ist. Schleswig-Holstein ist der einzige Flächenstaat, der ein landesweites automatisiertes Aktenhinweissystem für die Staatsanwaltschaft betreibt. Bei dieser Sachlage läßt sich nach Auffassung des Landesbeauftragten schwerlich begründen, daß der landesweite Zugriff auf die in GAST gespeicherten Daten „unabdingbar“ im Sinne der Rechtsprechung des Bundesverfassungsgerichts zum sogenannten Übergangsbonus ist.

Der Generalstaatsanwalt will den landesweiten Zugriff in einigen besonders sensiblen Bereichen einschränken. Im einzelnen geht es dabei um folgende Fälle:

- Verfahren, in denen von der Einleitung eines Ermittlungsverfahrens mangels jeglichen Anfangsverdachts abgesehen worden ist,
- Verfahren, denen eine böswillige bzw. querulatorische Anzeige zugrunde lag,
- Verfahren, in denen mangels Ermittlung eines Täters die Personendaten des Geschädigten/Anzeigenden in GAST gespeichert worden sind,
- Verfahren, die eine Sexualstraftat zum Gegenstand haben und bei denen mangels Ermittlung des Täters die Personalia des Opfers in abgekürzter Form in GAST eingestellt werden,
- Verfahren, die einen unnatürlichen Tod ohne Fremdeinwirkung (z.B. vollendete Selbsttötung) betreffen,
- Verfahren, in denen Strafunmündige als Beschuldigte gespeichert sind,
- in der Regel Verfahren, in denen rechtskräftig ein Freispruch ergangen ist.

Im übrigen aber will der Generalstaatsanwalt grundsätzlich am landesweiten Zugriff auf die in GAST gespeicherten Daten auch nach Abschluß der Ermittlungen festhalten. Die besondere Erforderlichkeit – im Sinne der Rechtsprechung zum Übergangsbonus: Unabdingbarkeit – eines solchen Informationssystems für Schleswig-Holstein – im Vergleich zu anderen Flächenstaaten – begründet der Generalstaatsanwalt damit, daß Schleswig-Holstein eine besonders „fortschrittlich-rationale“ Kriminalpolitik betreibt. Gerade bei der Behandlung der Kleinkriminalität, bei der Förderung der Diversion bei jugendlichen und heranwachsenden Beschuldigten, künftig bei der Einstellung von Verfahren im Bereich des Betäubungsmittelgesetzes, wenn es um geringe Mengen von Rauschgift zum Eigengebrauch geht, sowie bei notwendigen Entscheidungen in Vollstreckungs- und Vollzugssachen sei es erforderlich, im

landesweiten Zugriff feststellen zu können, ob der Beschuldigte bereits einmal in Erscheinung getreten ist. Dies sei wichtig, um festzustellen, ob man ihm eine Chance geben könne und beispielsweise auf die Durchführung eines Strafverfahrens verzichten könne.

Der Landesbeauftragte hält es für kein sehr überzeugendes Argument, „fortschrittlich-rationale“ Kriminalpolitik und Datenschutz gegeneinander zu stellen. Er geht davon aus, daß es eher die Ausnahme sein dürfte, daß ein Täter – in Kenntnis eines ggf. reduzierten Zugriffs auf die in GAST gespeicherten Daten – beispielsweise geringwertige Sachen nacheinander in den vier Zuständigkeitsbezirken der Staatsanwaltschaft stiehlt, um mehrfach in den Genuß der Verfahrensweise im Rahmen der Kleinkriminalität zu kommen. Sollte aber tatsächlich eine Notwendigkeit zur Abdeckung dieses spezifischen Informationsbedarfs bestehen, so könnte an die Einführung eines privilegierten Abfragecodes zum Zwecke der Entscheidung über die Anwendung der Rundverfügung zur Behandlung der Kleinkriminalität, über die Diversion, über Privilegierungen nach dem Betäubungsmittelgesetz sowie über die Gewährung von Vorteilen in Vollstreckungs- und Vollzugssachen gedacht werden. Selbst wenn also die besonders „fortschrittlich-rationale“ Kriminalpolitik des Landes Schleswig-Holstein in einzelnen Fällen einen landesweiten Zugriff erforderlich machen sollte – und insoweit ein wesentlicher Unterschied zu anderen Flächenländern bestünde –, könnte zu diesem Zweck eine Lösung gefunden werden, ohne daß damit der generelle landesweite Zugriff auf alle abgeschlossenen Verfahren verbunden wäre. Der Landesbeauftragte erhält deshalb seine grundsätzlichen Bedenken aufrecht und sieht erhebliche rechtliche Risiken für das GAST-Verfahren. Dies gilt um so mehr, als nach Auffassung des Generalstaatsanwalts auch bei Verfahren, die eingestellt wurden, weil sie keinen genügenden Anlaß zur Erhebung der öffentlichen Klage ergeben haben, nach wie vor die landesweite Speicherung erfolgen soll, weil man auch aus solchen Verfahren wertvolle Hinweise für ein evtl. neues Ermittlungsverfahren gewinnen könne.

Auch in einem anderen wichtigen Punkt sind noch keine entscheidenden Fortschritte erzielt worden. Der Landesbeauftragte hatte kritisiert, daß die **Aufbewahrungsbestimmungen** für Unterlagen bei der Justiz zu lang sind und im Hinblick auf das Recht auf informationelle Selbstbestimmung der Überarbeitung bedürfen. Der Generalstaatsanwalt sieht keine Möglichkeit, von diesen bundesweit geltenden Verwaltungsvorschriften abzuweichen. Er hat darauf verwiesen, daß der Justizminister Bestrebungen eingeleitet hat, die Aufbewahrungsbestimmungen bundeseinheitlich zu verkürzen.

Auch diese Argumentation hält der Landesbeauftragte nicht für überzeugend. Die bundeseinheitlichen Aufbewahrungsbestimmungen sind Verwaltungsvorschriften, die dem im Grundgesetz verankerten Recht auf informationelle Selbstbestimmung nicht vorgehen. Hinzu kommt, daß nur das Land Schleswig-Holstein ein automatisiertes landesweites Hinweissystem

der Staatsanwaltschaft betreibt. Dies rechtfertigt es auch, in den Aufbewahrungsfristen von den übrigen Bundesländern abzuweichen. Zumindest wäre es notwendig, die Speicherungsfrist in GAST, zu der in den bundesweiten Aufbewahrungsbestimmungen nichts geregelt ist, weiter zu verkürzen.

Eng hiermit hängt ein weiterer Gesichtspunkt zusammen, in dem die Stellungnahme des Generalstaatsanwalts unbefriedigend ist. Er hat es nämlich abgelehnt, künftig die **Fristen** nach dem Ereignis und nicht wie bisher nach der letzten Verfügung „Weglegen“ zu berechnen. Der Landesbeauftragte hat anhand von Beispielsfällen dargelegt, daß sich aus dieser Berechnungsmethode Verlängerungen der Aufbewahrungsfristen um Jahrzehnte ergeben können. Auch insoweit hat sich der Generalstaatsanwalt auf die bundeseinheitlichen Verwaltungsvorschriften zur Aufbewahrung berufen. Außerdem werde auch bei der Berechnung der Speicherfristen im Bundeszentralregister das Urteil zum Ausgangspunkt genommen. Allerdings geht es bei der Speicherung von Daten im Bundeszentralregister in der Regel um Verurteilungen wegen Straftaten, während in GAST zu einem großen Teil eingeleitete und später eingestellte Ermittlungsverfahren gespeichert sind.

Insgesamt hat der Generalstaatsanwalt nach Auffassung des Landesbeauftragten wichtige Schritte zu einer datenschutzrechtlichen Verbesserung von GAST eingeleitet. Es ist aber notwendig, daß auch in den verbleibenden noch strittigen Punkten spürbare Fortschritte erreicht werden.

4.3.2 Datenschutz hinter Gefängnismauern

Die Grundrechte und damit das Recht auf informationelle Selbstbestimmung gelten auch für Gefangene. So sehr dieser Satz aufgrund der Rechtsprechung des Bundesverfassungsgerichts allgemein anerkannt ist: Seine Einhaltung in der Praxis ist zumindest in bezug auf den Datenschutz noch alles andere als selbstverständlich. Gelegentlich drängt sich sogar der Eindruck auf, als habe der Datenschutz bislang die hohen Gefängnismauern noch nicht überwunden. Eine im Berichtszeitraum durchgeführte Querschnittskontrolle in Justizvollzugsanstalten des Landes hat jedenfalls erhebliche datenschutzrechtliche Mängel offenbart.

Keine Frage, daß ein Gefangener andere und in der Summe wohl auch mehr Eingriffe in sein informationelles Selbstbestimmungsrecht hinnehmen muß als ein freier Bürger. Aber auch im Justizvollzug gilt, was die Datenverarbeitung angeht, das Erforderlichkeits- und nicht das Willkürprinzip. Nach dem Strafvollzugsgesetz ist es sogar primäres Vollzugsziel, daß der Gefangene künftig in sozialer Verantwortung ein Leben ohne Straftaten führen kann. Hieraus ergeben sich Auslegungsmaximen auch in datenschutzrechtlichen Zweifelsfragen. Alle Maßnahmen der Datenverarbeitung sind an der Erforderlichkeit für die Belange des Vollzuges und des Schutzes der Voll-

zugsbediensteten, aber auch der Resozialisierung der Gefangenen zu messen.

Der Landesbeauftragte hat bei seinen Kontrollen ein uneinheitliches Bild vorgefunden: In einzelnen Bereichen besteht ausgeprägte datenschutzrechtliche Sensibilität, während wichtige andere Fragen völlig unzureichend gelöst sind. Hierzu mag auch das Fehlen bereichsspezifischer Vorschriften beitragen. Das Strafvollzugsgesetz und seine Ergänzungsvorschriften enthalten nur einige wenige Bestimmungen zur Datenverarbeitung. Ein im vergangenen Jahr bekanntgewordener Gesetzesentwurf des Bundesministers der Justiz versucht, die Lücken zu schließen, bedarf aber noch der gründlichen Überarbeitung. Bis zu seinem Inkrafttreten ist das schleswig-holsteinische Landesdatenschutzgesetz zu beachten, das der Landesbeauftragte seinen Wertungen und Feststellungen zugrunde gelegt hat.

Die Auswertung der Prüfungsergebnisse war bei der Erstellung dieses Berichts noch nicht abgeschlossen. Schon jetzt können aber folgende Teilergebnisse berichtet werden:

Datenerhebung

Beim Neuzugang eines Gefangenen werden Daten auf verschiedenen Formularen erhoben. Basisdatensatz ist der sogenannte „A-Bogen“, der u.a. die Personengrunddaten, die Zahl der Vorstrafen bzw. früheren Maßregeln und Informationen über den Haftgrund enthält. Hinzu kommen das religiöse Bekenntnis, Familienstand und Kinderzahl, Name und Wohnung der nächsten Angehörigen, erlernter Beruf sowie Tatgenossen. Dieser Bogen dient nicht nur der Vollzugsgeschäftsstelle, sondern auch der Unterrichtung einer Vielzahl von Stellen innerhalb der Justizvollzugsanstalt. Der Einfachheit halber werden im Vervielfältigungsverfahren mehrere Durchdrucke hergestellt, die u.a. der Pforte, der Kleiderkammer, der Zahlstelle, der Arbeitsverwaltung, der Zentrale, der Eigengeldstelle, dem Werkstattleiter, dem ärztlichen Dienst, dem Oberlehrer, dem Seelsorger und anderen zur Verfügung gestellt werden.

Es bestehen erhebliche Zweifel an der Erforderlichkeit aller Daten des „A-Bogens“ für jede dieser Stellen. Beispielsweise dürften für den ärztlichen Dienst Haftgrund und Zahl der Vorstrafen, Namen von Tatgenossen, für den Oberlehrer Name und Anschrift der nächsten Angehörigen, für den Werkstattleiter Familienstand und Zahl der Kinder und für alle das religiöse Bekenntnis ohne Bedeutung sein. Ein Ergebnis der Prüfung muß es deshalb sein, innerhalb der Justizvollzugsanstalt nicht mehr Daten „kursieren“ zu lassen als für den jeweiligen Empfänger notwendig. Ein Mittel dazu ist die Änderung des A-Bogens bzw. die Beschränkung des Durchdruckverfahrens auf weniger Daten.

Ein anderes Problem im Bereich der Datenerhebung ist, inwieweit Daten über Dritte einbezogen werden dürfen. In Form eines sogenannten „F-Bogens“ werden detaillierte Daten über

die Eltern des Gefangenen erhoben, z.B., ob sie verheiratet sind, getrennt leben oder geschieden sind, wie das Verhältnis des Gefangenen zu den Eltern war und ist, ebenso Name, Alter, Beruf und Wohnort der Geschwister. Andere Fragen zielen auf Lehrherren im Rahmen der Ausbildung, Ehefrau oder Verlobte, Beziehungen zu den Kindern und mögliche Partner für Briefverkehr. Auch wenn die Prüfung keinen Hinweis erbracht hat, daß die Freiwilligkeit bei der Erstellung des „F-Bogens“ nicht gewahrt ist, so bestehen Zweifel, inwieweit die freiwillige Hergabe der Daten durch den Gefangenen eine fehlende Rechtsgrundlage im Verhältnis zu den betroffenen Dritten ersetzen kann. Es sollte deshalb geprüft werden, welche Daten auf dem „F-Bogen“ erforderlich sind, über welche davon der Gefangene verfügen kann und für welche eine Rechtsgrundlage erforderlich ist.

Daten über Dritte sind auch in der Anklageschrift, die sich häufig bei den Akten befindet, und im Urteil, das fast immer beigezogen wird, enthalten. Die Anklageschrift enthält neben den Daten der Mitangeklagten vor allem Name und Anschrift der Zeugen.

Im Urteil finden sich Informationen zu den Mitangeklagten, zur Familiengeschichte sowie zu den Opfern der Straftat. Treten diese als Nebenkläger auf, so enthält das Urteil auch ihre Anschrift. In mehreren Gefangenenpersonalakten, die stichprobenweise durchgesehen wurden, befanden sich beispielsweise Name und Anschrift von vergewaltigten Frauen. Der Landesbeauftragte ist der Auffassung, daß derartige Informationen über Dritte schon bei der Anlegung der Akte, also bei der Erhebung der Daten über den Gefangenen, unkenntlich gemacht werden müssen.

Datenspeicherung

Kernstück der Datenverarbeitung ist die Gefangenenpersonalakte, in der die Informationen über die Gefangenen zusammengefaßt und fortlaufend abgeheftet werden. Die Kontrolle hat schwere Mängel bei der Organisation und beim Zugriffsschutz offenbart. Im Grunde kann jeder Bedienstete der Justizvollzugsanstalten ohne Begründung jederzeit die vollständige Akte über jeden Gefangenen einsehen.

Die Akten hängen in einem Raum, zu dem jeder Bedienstete Zutritt hat. In der Justizvollzugsanstalt Lübeck können die Akten entnommen werden, ohne daß dies irgendwo vermerkt wird. In der Justizvollzugsanstalt Kiel gibt es zwar ein Formular, in das Aktenentnahmen einzutragen wären. Dies geschieht nach dem Prüfungsergebnis aber nur selten. In vielen Fällen konnte weder in Kiel noch in Lübeck festgestellt werden, wo sich die Akten gerade befanden, noch konnte nachvollzogen werden, wer bereits Einsicht genommen hatte.

Notwendig ist, daß die Aktenhaltung und der Aktenzugriff grundlegend reorganisiert werden. Die Akten müssen unter Verschuß gehalten werden und dürfen auch anstaltsintern nur

bei begründetem Informationsinteresse herausgegeben werden. Die Einsichtnahme in Akten sollte angesichts der besonderen Sensibilität der enthaltenen Informationen dokumentiert werden, damit nachvollziehbar bleibt, wer wann warum von ihrem Inhalt Kenntnis genommen hat.

Hinzu kommt ein weiteres: Die Akten stellen eine umfassende Datensammlung über den Gefangenen und häufig auch über Dritte dar. Nicht jeder, der eine Detailfrage zu bearbeiten hat, muß immer die gesamte Akte lesen. Der Akteninhalt muß also stärker in Teil-Informationsmengen aufgegliedert werden. Ansätze hierzu finden sich bereits in den sogenannten Heftnadeln, die die Akten in drei Teile gliedern. Es muß geprüft werden, welche weiteren Gliederungsmöglichkeiten unter datenschutzrechtlichen Gesichtspunkten bestehen und wie organisatorisch sichergestellt werden kann, daß bei Einsichtnahmen in die Akte nur jeweils der notwendige Teil zur Verfügung gestellt wird. Daß dies möglich ist, zeigt das jetzt bereits geführte sogenannte Urlaubsheft. Wer Urlaubsfragen zu bearbeiten hat, erhält und benötigt häufig nur dieses „Urlaubsheft“ und nicht die gesamte Akte.

Derzeit werden die Akten bis 30 Jahre nach dem Entlassungstermin aufbewahrt. Bei der Kontrolle waren aber Akten zu beanstanden, die fast 50 Jahre alt waren. Aber selbst 30 Jahre sind eine zu lange Frist. Kaum ein Bediensteter der kontrollierten Justizvollzugsanstalten konnte sich erinnern, je in eine Akte die älter als 10 Jahre war, gesehen zu haben. Werden die Vorstellungen zu einer stärkeren und konsequenteren Untergliederung der Akten realisiert, so könnten schon bei oder kurz nach der Entlassung große Teile der Akten vernichtet werden. Nach Ablauf von 10 Jahren sollten die restlichen Unterlagen gelöscht oder nur noch für Archivzwecke aufbewahrt werden.

Daten über Gefangene werden daneben noch in einer Vielzahl von Karteien und Buchwerken gespeichert. Hierfür gelten unterschiedliche Speicherfristen. Da bei den Buchwerken aber die Frist erst beginnt, wenn das jeweilige Buch vollgeschrieben ist, dauert die Speicherung um so länger, je dicker das Buch ist. De facto Verlängerungen der Frist um 10 Jahre und mehr sind keine Seltenheit.

Notwendig ist eine gründliche Überprüfung, ob die Buchwerke in dieser Form auch weiterhin erforderlich sind. Manche wurden vor Jahrzehnten eingeführt und beruhen auf einer Konzeption des Strafvollzugs, die heute nicht mehr gültig ist. Danach sind die Speicherfristen zu überprüfen und zumindest an die ggf. verkürzten Fristen der Aktenaufbewahrung anzugleichen. Sodann muß durch geeignete technisch-organisatorische Maßnahmen sichergestellt werden, daß nicht letztlich der Seitenumfang des benutzten Buches über die Speicherfrist entscheidet, sondern daß die Bücher jahrgangsweise geführt werden.

Offenbarung von Daten innerhalb der Justizvollzugsanstalten

Eine Reihe von hergebrachten Verhaltensweisen und Einrichtungen führt dazu, daß Daten innerhalb der Justizvollzugsanstalten ohne Notwendigkeit bekannt oder sogar Dritten offenbart werden. So befinden sich in den Zimmern der Stationsbeamten Übersichtstafeln mit Informationen über die Namen der Gefangenen der Station, ihren Arbeitseinsatz, ihre Konfession, das Geburtsdatum sowie teilweise das Entlassungsdatum. Die Tafeln sollen den Vollzugsbediensteten einen schnellen Überblick über die Belegung der Station geben und sind dementsprechend gut sichtbar in den Stationszimmern postiert.

Diese werden aber nicht nur von den Bediensteten der Abteilung, sondern auch von Gefangenen und Besuchern aufgesucht. Sie können sich auf diesem Wege bequem Informationen über die Gefangenen verschaffen, die ihnen nicht zustehen. Deshalb ist es notwendig, daß das Ziel, einen schnellen Überblick über den Gefangenenbestand einer Station zu erlangen, auf anderem Weg verfolgt wird. Denkbar sind Tafeln mit verschließbaren Klappen, die nur bei Bedarf geöffnet werden, oder Übersichten in den Schreibtischschubladen, die ebenso schnell herausgezogen werden können.

Ein altes Problem ist auch die Haftraumbeschilderung. In der JVA Kiel sind an den Zellen außen noch Schilder mit dem Namen des jeweiligen Insassen angebracht. Jeder vorübergehende Besucher kann die Namen zur Kenntnis nehmen. Wer nur eine kurze Freiheitsstrafe zu verbüßen hat und dafür heimlich seinen Urlaub verwendet, kann das Pech haben, daß gerade sein Nachbar, Kollege oder ein sonstiger Bekannter im Gefängnis zu tun hat und seine wahre „Urlaubsanschrift“ herausfindet. Schon die Tatsache, daß die JVA Lübeck auf eine derartige Haftraumbeschilderung seit einiger Zeit verzichtet, zeigt, daß sie nicht unbedingt notwendig ist. Sie sollte auch in den übrigen Vollzugsanstalten, soweit noch vorhanden, abgeschafft werden.

Kritik war auch an den baulichen Gegebenheiten des Pfortenbereichs in der JVA Kiel zu üben. Wenn dort mehrere Besucher auf einmal eintreffen, kann jeder erfahren, weswegen der andere gekommen ist. Wer seinen Namen angeben muß und vorträgt, er wolle seinen inhaftierten Sohn besuchen, muß damit den Umstehenden mehr verraten, als ihm nach den Umständen lieb sein kann.

Auch der anstaltsinterne Funkverkehr, der in der JVA Kiel bereits stark ausgebaut ist, kann eine ergiebige Datenquelle sein. Die Geräte werden zumeist eingeschaltet am Körper getragen, damit eilige Durchsagen, Alarmrufe etc. gehört werden. Werden entgegen den Vorschriften – wie mehrfach im Laufe der Kontrollbesuche – Namen über Funk durchgegeben, so erhalten die umstehenden Gefangenen oder Besucher Informationen über Gefangene, die sie nichts angehen.

Wahrung der Privatsphäre

Auch Gefangene haben ein Recht auf Wahrung ihrer Intim- und Privatsphäre. Zwar sind hier in den vergangenen Jahren bereits erhebliche Verbesserungen eingetreten, wie etwa die Möglichkeit des ungestörten Telefonierens oder die weitgehende Einschränkung der Briefkontrolle. Sie reichen aber noch nicht aus. Die Gefangenen haben sich zu Recht beklagt, daß sie kein Behältnis in der Zelle haben, in dem sie persönliche Unterlagen, Briefe, Verteidigerpost, Gerichtsakten etc. einschließen können. So können sie nie sicher sein, daß nicht Mitgefangene oder Bedienstete der Justizvollzugsanstalt in ihrer Abwesenheit unbefugt Einblick nehmen.

Es besteht keine Notwendigkeit, den Gefangenen verschließbare Behältnisse in ihren Zellen vorzuenthalten. Auch wenn zum Ausgleich dafür ein Kontrollrecht für die Anstalt auch ohne konkreten Verdacht vorgesehen werden müßte, so könnte festgelegt werden, daß dies nur im Beisein des Gefangenen ausgeübt werden darf. Zellenrevision und andere Kontrollmöglichkeiten blieben davon unberührt.

Im Rahmen der Kontrollen haben sich auch die Anstaltsleitungen der Justizvollzugsanstalten Kiel und Lübeck nicht gegen derartige abschließbare Behältnisse ausgesprochen, aber Kostenargumente geltend gemacht. Hier müßte sich aber auf absehbare Zeit eine kostengünstige Lösung realisieren lassen.

AIDS-Hinweise

Die Information, daß eine Person HIV-positiv ist, kann in den Justizvollzugsanstalten auf den verschiedensten Wegen kursieren. Der Landesbeauftragte war bereits vor seiner Querschnittskontrolle durch Einzeleingaben auf die Problematik aufmerksam geworden.

Die Kontrollen haben keinen Hinweis ergeben, daß Gefangene ohne ihre ausdrückliche Einwilligung auf eine HIV-Infektion untersucht werden. Die anschließende Verwendung der Information im Falle eines positiven Untersuchungsbefundes stößt aber auf Kritik. Es wird nämlich auf dem sog. „A-Bogen“ vorn in der Gefangenenpersonalakte der Stempel angebracht: „Vorsicht! Gesundheitsakten beachten“. Theoretisch könnte damit auch eine andere als eine HIV-Infektion gemeint sein. In der Praxis wird dies aber als der „AIDS-Hinweis“ angesehen.

Der Hinweis ist in dieser Form irreführend und unzulässig. Er erweckt nämlich den Eindruck, der Leser des Hinweises dürfe die Gesundheitsakten einsehen. Dieses Recht steht grundsätzlich nur dem Arzt zu. Die große Mehrzahl derer, die die Gefangenenpersonalakte in die Hand nehmen, hat kein Recht, in Gesundheitsakten einzusehen. In Wirklichkeit geht es nicht um ein Akteneinsichtsrecht, sondern um den für alle Eingeweihten unverblühten Hinweis auf eine HIV-Infektion.

Eine Offenbarung der AIDS-Erkrankung auf diesem Wege ist unzulässig. Die Information, daß eine Person HIV-infiziert ist,

unterliegt nämlich dem Arztgeheimnis. Der Arzt darf sie nur offenbaren, wenn er dazu vom Betroffenen ermächtigt oder durch eine Rechtsnorm befugt ist. Mangels spezieller gesetzlicher Vorschriften kommt nur ein rechtfertigender Notstand nach dem Strafgesetzbuch in Betracht. Dann müßte aber für jeden, der eine Gefangenenpersonalakte in die Hand nimmt, eine gegenwärtige, anders nicht abwendbare Gefahr für Leib oder Leben bestehen. Davon kann nicht die Rede sein, denn Gefangenenpersonalakten werden aus ganz unterschiedlichen Gründen eingesehen, z.B. um Urlaubsfragen zu klären, Kosten zu berechnen, Schriftstücke abzuheften oder um im Justizministerium über Beschwerden zu entscheiden.

In diesen Fällen der rein administrativen Befassung mit der Akte kann von einer Gesundheitsgefahr nicht gesprochen werden. In der gegenwärtigen Form ist damit der AIDS-Hinweis nicht zu rechtfertigen. Statt dessen muß ein Weg gefunden werden, der der verständlichen und berechtigten Sorge der Mitarbeiter der Justizvollzugsanstalten vor Infektionsgefahren ebenso Sorge trägt wie dem Anspruch der Gefangenen auf Beachtung des strafrechtlich geschützten Arztgeheimnisses.

Bedenklich ist auch, daß offenbar einige Gerichte verlangen, vorab telefonisch informiert zu werden, wenn ein HIV-infizierter Gefangener zum Termin vor Gericht erscheint. Für den Landesbeauftragten ist beim derzeitigen Kenntnisstand nicht nachvollziehbar, welche Übertragungsmöglichkeiten im Rahmen einer Gerichtsverhandlung bestehen sollen. Dieser Frage ist deshalb nachzugehen und darüber hinaus zu klären, wer innerhalb des Gerichts informiert wird und wo und wie lange bei Gericht diese Information aufbewahrt wird.

Automatisierte Datenverarbeitung

Die automatisierte Datenverarbeitung ist in den Justizvollzugsanstalten noch nicht sehr stark entwickelt. Es wird in erster Linie ein Verfahren namens BASIS zur Verwaltung und Abwicklung der Gefangenenengelder betrieben. Mängel des Verfahrens konnten im Laufe der Kontrollen nicht festgestellt werden.

Neben diesem, gewissermaßen formatisierten, Teil bietet BASIS den Benutzern auch die Möglichkeit – sozusagen weil die Kapazität nun einmal da ist –, weitere Dateien nach eigenen Vorstellungen einzurichten und zu betreiben. Stichproben förderten einige Dateien mit Gefangenenendaten zutage.

Was sich zunächst als Liste der Freigänger ganz harmlos ausmacht, gewinnt bei näherem Hinsehen Brisanz: Erstellt waren die Listen vom Sachbearbeiter zur Arbeitserleichterung. Wäre ein Ausdruck oder auch nur eine Kopie eines Ausdruckes in die Hände eines Außenstehenden gelangt, so hätte er ihr entnehmen können, welche Gefangenen derzeit Freigang hatten, also die Chance, auf einer Arbeitsstelle außerhalb der Justizvollzugsanstalt Tariflohn zu verdienen: Eine Information, für die jeder Gläubiger eines Gefangenen dankbar ist.

Die Kontrolle hat keinen Hinweis ergeben, daß tatsächlich unsachgemäß mit den gespeicherten Daten umgegangen wurde. Unsachgemäß war aber die Errichtung dieser Dateien: Sie hätten zumindest in der Dateienübersicht beim Datenschutzbeauftragten der Justizvollzugsanstalt verzeichnet und überdies an den Landesbeauftragten gemeldet werden müssen. Beides war nicht der Fall.

Datenübermittlung

Bei der Frage der Übermittlung von Daten an Dritte hat die Kontrolle eine relativ sensible Verfahrensweise ergeben. Das Fehlen bereichsspezifischer und präziser Übermittlungsvorschriften macht sich aber auch hier nachteilig bemerkbar. Es herrscht Unsicherheit, in welchem Umfang Übermittlungsersuchen nachzukommen ist.

Hinzu kommt, daß zwar nähere Informationen über Gefangene für den Unbefugten nicht einfach zu erlangen sein dürften, die Tatsache, ob jemand einsitzt oder nicht, aber nach wie vor relativ einfach in Erfahrung zu bringen ist. Diese Lücken müssen noch geschlossen werden. Darüber hinaus bedarf es klarer Regelungen, wer zur Auskunftserteilung nach draußen befugt ist.

Aus dem Anfang des Jahres in Kraft getretenen neuen Landesdatenschutzgesetz ergibt sich außerdem, daß jede Datenübermittlung, auch wenn sie zunächst telefonisch erfolgt ist, zu dokumentieren ist.

Abschluß

Eine Reaktion seitens des Justizministers konnte bis zur Fertigstellung dieses Berichts noch nicht vorliegen. Aus den im Rahmen der Kontrolle vor Ort geführten Gesprächen konnte der Landesbeauftragte aber Aufgeschlossenheit und guten Willen vieler Mitarbeiter der Justizvollzugsanstalten entnehmen. Die mit den gewählten Vertretern der Gefangenen geführten Gespräche brachten wertvolle praktische Hinweise und dürften deren Aufmerksamkeit für datenschutzrechtliche Fragestellungen gestärkt haben.

Noch während der Kontrolle erreichten den Landesbeauftragten Anfragen von Gefangenen, die unter Berufung auf das neue Landesdatenschutzgesetz Einsicht in ihre Gefangenenpersonalakte nehmen wollten. Ihnen wurde mitgeteilt, daß grundsätzlich auch Gefangenenpersonalakten dem Einsichtsrecht unterliegen und daß die Gewährung der Einsicht die Regel, die Verweigerung die zu begründende Ausnahme ist. Die Justizvollzugsanstalt Kiel schloß sich dem an und gewährte daraufhin einem Gefangenen Akteneinsicht, dem sie zuvor verwehrt worden war.

4.3.3 Überweisung von Gefangenengeldern: Problem gelöst

Tätigen Gefangene in Justizvollzugsanstalten Überweisungen von ihrem sog. Eigengeld, so konnte bislang der Empfänger aus dem Überweisungsbeleg erkennen, daß der Absender in der Justizvollzugsanstalt einsaß. Dies hatte der Landesbeauftragte im 13. Tätigkeitsbericht (S. 49) gerügt. Nunmehr hat die Finanzministerin mitgeteilt, daß künftig wie folgt verfahren wird:

- Die verbale Bezeichnung der Justizvollzugsanstalt als veranlassende Dienststelle wird im Zahlungsaustauschsatz nicht mehr ausgedruckt.
- Statt dessen wird in der Verwendungszweckangabe der Name des Gefangenen genannt.

Folglich wird der Zahlungsempfänger künftig den Gutschriftsdaten nicht mehr entnehmen können, daß sich der Auftraggeber als Gefangener in einer Justizvollzugsanstalt aufhält.

4.3.4 Mitteilungen in Strafsachen: Im Schnecken tempo voran

Der Landesbeauftragte hat in den vergangenen Jahren wiederholt über datenschutzrechtliche Probleme im Zusammenhang mit den Mitteilungen über Strafsachen (MiStra) berichtet (zuletzt 13. TB, S. 48). Inzwischen ist ein neuer Entwurf des Bundesjustizministers vorgelegt worden, der die Mitteilungen über Strafsachen auf eine gesetzliche Grundlage stellen soll. Er weist aus der Sicht des Landesbeauftragten nach wie vor erhebliche datenschutzrechtliche Mängel auf. Der Justizminister ist der Auffassung, daß es nicht sinnvoll sei, die Verwaltungsvorschrift über die Mitteilungen in Strafsachen (MiStra) noch zu ändern, da er mit einem Inkrafttreten des Justizmitteilungsgesetzes in „recht kurzer Zeit“ rechne.

Der Landesbeauftragte teilt diesen Optimismus nicht. Die Arbeiten am Justizmitteilungsgesetz ziehen sich bereits über Jahre hin, ohne daß ein Ende absehbar ist. Deshalb kommt es vor allem darauf an, daß bei der praktischen Anwendung der MiStra-Regelung restriktiv verfahren wird. Dies folgt daraus, daß die Regelung lediglich eine Verwaltungsvorschrift ist, die auf ihrer Grundlage vorzunehmenden Datenübermittlungen nicht legitimieren kann. Es erscheint fraglich, ob nicht die Frist, innerhalb der ohne ausreichende gesetzliche Grundlage noch Eingriffe in das Recht auf informationelle Selbstbestimmung übergangsweise vorgenommen werden dürfen, in bezug auf die MiStra-Tatbestände längst abgelaufen ist. Jedenfalls aber dürfen unter Berufung auf diesen sog. Übergangsbonus nur die absolut notwendigen Rechtseingriffe vorgenommen werden.

In dem Bemühen, die Praxis der Anwendung der MiStra-Regelung einzuschränken, gab es im vergangenen Jahr Fortschritte, vereinzelt aber auch Stagnation und Rückschritt. In einzelnen Fällen war die Anwendung der Regelung zu bemängeln. Der

Justizminister hat zugesagt, schon jetzt für mehr Zweckbindung der auf der Grundlage der MiStra übermittelten Daten beim Empfänger sowie für ein verbessertes rechtliches Gehör des Betroffenen Sorge tragen zu wollen. Eine endgültige Verfahrensregelung hierzu ist dem Landesbeauftragten bis zur Fertigstellung dieses Berichts aber noch nicht zugegangen.

Bei der Erörterung der Konsequenzen, die bei der Polizei aus dem Prüfbericht des Landesbeauftragten für die dortige Datenverarbeitung zu ziehen sind, hat sich gezeigt, daß eine Reihe wichtiger Verbesserungen nur dann erreicht werden können, wenn die Polizei über den Ausgang des gerichtlichen Verfahrens durch die Staatsanwaltschaft unterrichtet wird. Die MiStra-Regelung sieht dies auch ausdrücklich vor. Da häufig Ermittlungen zunächst unter einem schwereren Tatverdacht eingeleitet werden, während das gerichtliche Verfahren später zu einem Freispruch, einer Verfahrenseinstellung oder einer Verurteilung aus einem minderschweren Delikt führt, könnten sich derartige Mitteilungen häufig zugunsten des Betroffenen auswirken.

Der Landesbeauftragte hat wiederholt kritisiert, daß nach seinen Feststellungen diese Mitteilungsverpflichtung nicht ausreichend erfüllt wird. In vielen polizeilichen Akten ist über den Ausgang des gerichtlichen Verfahrens nichts bekannt. Wenn eine Rückmeldung über den Ausgang des Verfahrens erstattet wird, so wird häufig lediglich eine Kurzmitteilung vorgenommen, aus der die Polizei nicht die notwendigen Informationen entnehmen kann, um zu entscheiden, ob die Speicherung in ihren eigenen Dateien aufrechterhalten werden soll oder nicht.

Der Landesbeauftragte hat deshalb den Justizminister erneut darauf hingewiesen, daß es nicht nur darauf ankommt, überhaupt der Polizei Rückmeldung über den Ausgang des Verfahrens zu geben, sondern, daß aus der Mitteilung hervorgehen muß, ob nach Auffassung der Staatsanwaltschaft damit auch der Tatverdacht entfallen ist. In diesem Fall und bei Freisprüchen hat die Polizei die Zulässigkeit der weiteren Speicherung des Vorgangs in ihren Datensammlungen zu überprüfen. Bis zur Fertigstellung dieses Berichts hat der Justizminister hierzu noch keine inhaltliche Stellungnahme abgegeben.

4.3.5 Was ein Notar bei Sammelverträgen beachten muß

Ein Petent machte den Landesbeauftragten auf folgenden Vorgang aufmerksam: Seine Stadtverwaltung beabsichtigte, von ihm und weiteren fünf Anliegern Grundstücksflächen zum Ausbau eines Gehweges zu erwerben. Sie beauftragte einen Notar mit der Ausarbeitung des notariellen Kaufvertragsentwurfs. Aus Kostenersparnisgründen wurde die Form eines Sammelvertrages gewählt. Da in einem notariellen Grundstückskaufvertrag auch die Belastungen aufzuführen sind, konnten so alle betroffenen Grundstückseigentümer die Verschuldung des jeweiligen Nachbargrundstücks zur Kenntnis nehmen.

Hiergegen wandte sich der Petent zu Recht. Die Information über Grundstücksbelastungen gehört zu den besonders geschützten Daten. Einsicht in das Grundbuch darf nur nehmen, wer ein berechtigtes Interesse darlegen kann. Nur der Notar ist bei Einsichtnahme in das Grundbuch nicht gehalten, ein solches berechtigtes Interesse darzulegen. Zum Ausgleich hierfür unterliegt der Notar nach der Bundesnotarordnung einer besonderen Verschwiegenheitspflicht. Dies bedeutet, daß er Informationen, die er dienstlich erhalten hat, insbesondere auf der Grundlage ihn privilegierender Auskunftsvorschriften, nicht ohne Einwilligung des Betroffenen an Dritte weiterübermitteln darf. Im vorliegenden Falle hätte deshalb zuvor bei den Grundstückseigentümern nachgefragt werden müssen, ob sie mit der Form eines Sammelvertrages und der damit verbundenen gegenseitigen Information über etwaige Grundpfandrechte einverstanden waren oder nicht. Nach dem Sachvortrag des Petenten muß davon ausgegangen werden, daß eine solche Einverständniserklärung nicht eingeholt worden ist.

Der Landesbeauftragte hat den Notar auf die Rechtslage hingewiesen und darüber hinaus die Schleswig-Holsteinische Rechtsanwalts- und Notarkammer gebeten, in einem ihrer Publikationsorgane auf die Problematik einzugehen, damit künftig in vergleichbaren Fällen eine Verletzung der notariellen Verschwiegenheitspflicht vermieden werden kann.

4.3.6 „Sprechende“ Briefumschläge unzulässig

Ein Amtsgericht hatte bei einer Ladung – vereinfachte Zustellung – auf dem äußeren Briefumschlag neben der Geschäftsnummer den Termin vermerkt.

Eine solche Verfahrensweise hat zur Folge, daß nicht nur der zustellende Postbeamte die Informationen auf dem Umschlag lesen kann, sondern im Rahmen der Zustellung auch andere Personen als der Adressat (z.B. erwachsene Kinder, die in seinem Haushalt leben).

Die einschlägige Justizaktenordnung läßt selbst auf der Zustellungsurkunde lediglich die Geschäftsnummer und als weitere Kennzeichnung das Datum der die Zustellung veranlassenden Verfügung zu. Nur soweit zuzustellende Sendungen ausnahmsweise nicht genügend bestimmt gekennzeichnet erscheinen, kann dem Datum eine weitere zusätzliche Kennzeichnung hinzugesetzt werden, die jedoch keinerlei Rückschlüsse auf den Inhalt zulassen darf. Diese Vorschrift muß natürlich erst recht für die Beschriftung eines Briefumschlages gelten, der nicht nur vom Postbediensteten, sondern auch von Dritten gelesen werden kann.

Der Justizminister hat sich diesem Vorhalt des Landesbeauftragten angeschlossen und das Verfahren der vereinfachten Zustellung so geregelt, daß es künftig ausdrücklich untersagt ist, auf Zustellungsurkunden oder inneren Zustellungsbrief-

umschlagen das Datum eines Termins als weitere Kennzeichnung zu verwenden.

4.3.7 Automatisierung der Datenverarbeitung bei der Justiz: Vorschußlorbeeren

Im letzten Tätigkeitsbericht (13. TB, S. 52) wurde der Justizminister dafür gelobt, daß er den Landesbeauftragten zu einem sehr frühen Zeitpunkt seiner Planungen zur Automatisierung der Datenverarbeitung bei der Justiz beteiligt hat. Daraufhin hat der Landesbeauftragte vorgeschlagen, vor einer detaillierten Planung und Realisierung technischer Einzelaspekte der Automatisierung die Fragen der rechtlichen Zulässigkeit der Datenverarbeitung zu prüfen. Insbesondere sei zuerst zu fragen, ob für die in Aussicht genommene Verarbeitung personenbezogener Daten eine den Grundsätzen des Volkszählungsurteils entsprechende Rechtsgrundlage besteht.

Offenbar entsprach diese Antwort nicht den Erwartungen des Justizministers. Jedenfalls wurde kurz vor Fertigstellung dieses Berichts erneut ein Rahmenplan zur Automatisierung der Datenverarbeitung der Justiz vorgelegt. Rechtliche Fragen der Zulässigkeit der von dem Automationsvorhaben betroffenen personenbezogenen Daten sind darin praktisch nicht angesprochen. Statt dessen ist wieder detailliert von Fragen der Datenverarbeitungstechnik die Rede.

Der Landesbeauftragte befürchtet, daß bei einer derartigen Vorgehensweise zunächst die technischen Details geklärt und festgelegt sowie die entsprechenden Investitionen (übrigens mehrere Millionen) getätigt werden und danach erst untersucht wird, ob überhaupt die rechtliche Zulässigkeit der ins Auge gefaßten Datenverarbeitung geklärt ist. Erfahrungsgemäß wird in solchen Fällen dann häufig im nachhinein versucht, unter allen Umständen die Erforderlichkeit und Zulässigkeit der Datenverarbeitung zu „begründen“. Denn wenn erst einmal die aufwendigen Investitionen getätigt oder in Gang gesetzt sind, ist es meist sehr schwer möglich, noch gravierende Änderungen der Verfahren zu erreichen.

Inzwischen ist, nachdem der Rahmenplan für den Einsatz der Informationstechnik bei den Gerichten und Staatsanwaltschaften des Landes Schleswig-Holstein von der IT-Kommission des Landes „zustimmend“ zur Kenntnis genommen wurde, ein weiteres Schreiben des Justizministers eingetroffen. Darin wird betont, zunächst sollten Umsetzungserfahrungen bei einigen Gerichten und Staatsanwaltschaften gewonnen werden. Die Prüfung der vom Landesbeauftragten aufgeworfenen Rechtsfragen werde im Auge behalten. Man werde sich auch weiterhin für die berechtigten Interessen des Datenschutzes einsetzen und erbitte die Beratung durch den Datenschutzbeauftragten bei der Umsetzung des IT-Rahmenkonzeptes.

4.3.8 Auch Richter müssen Datenschutz beachten

Auch in diesem Jahr (vgl. 13. TB, S. 53) gibt es Veranlassung, unter dieser Überschrift zu berichten. Den Landesbeauftragten erreichten mehrere Eingaben, in denen sich die Petenten darüber beschwerten, daß ihre Anträge auf Prozeßkostenhilfe nebst Anlage vom Gericht der Gegenpartei zugänglich gemacht wurden. Voraussetzung für die Gewährung von Prozeßkostenhilfe ist nach der Zivilprozeßordnung u.a., daß der Antragsteller nach seinen persönlichen und wirtschaftlichen Verhältnissen die Kosten der Prozeßführung nicht, nur zum Teil oder nur in Raten aufbringen kann. Außerdem muß die beabsichtigte Rechtsverfolgung oder Rechtsverteidigung hinreichende Aussicht auf Erfolg bieten und nicht mutwillig erscheinen. Wer einen Antrag auf Prozeßkostenhilfe stellt, muß also seine persönlichen und wirtschaftlichen Verhältnisse darlegen. Im Falle eines Petenten waren z.B. ein Sozialhilfebescheid und eine Steuererklärung vorzulegen.

Auch im Verfahren der Bewilligung von Prozeßkostenhilfe hat die Gegenpartei Anspruch auf rechtliches Gehör. Der Bundesgerichtshof hat aber entschieden, daß sich dieser Anspruch nur auf den Aspekt der hinreichenden Erfolgsaussicht, nicht aber der wirtschaftlichen und persönlichen Verhältnisse des Antragstellers bezieht. Daraus folgt, daß diese Antragsunterlagen auch nicht der Gegenpartei zur Kenntnis gebracht werden dürfen. Mit dem Recht auf informationelle Selbstbestimmung des Antragstellers ist es nicht vereinbar, diese z.T. sehr persönlichen und detaillierten Daten ohne Erforderlichkeit und gesetzliche Grundlage der Gegenpartei einer streitigen gerichtlichen Auseinandersetzung zur Kenntnis zu geben.

Dies hatten die Gerichte in den Fällen, die dem Landesbeauftragten vorgetragen wurden, nicht beachtet. Im Hinblick auf die richterliche Unabhängigkeit konnte die Verfahrensweise der betreffenden Gerichte nicht formell beanstandet werden. Dies ändert aber nichts daran, daß in diesen Fällen das Recht auf informationelle Selbstbestimmung objektiv verletzt worden ist.

4.4 Gelingt es der Steuerwaltung, sich dem Landesdatenschutzgesetz zu entziehen?

Der Bundesgesetzgeber hat die Absicht, im steuerlichen Verfahrensrecht die Anwendung der Datenschutzgesetze der Länder weitestgehend auszuschließen. Hiergegen sind aus der Sicht des Landesbeauftragten erneut (vgl. 11. TB., S. 35) nachdrücklich Bedenken geltend zu machen.

Es ist dem Bund unbenommen, die in den Datenschutzgesetzen notwendigerweise abstrakt formulierten Regelungen über die Zulässigkeit der personenbezogenen Datenverarbeitung in der Abgabenordnung durch bereichsspezifische Bestimmungen über die Erhebung, Speicherung, Übermittlung und Löschung steuerlicher Daten zu konkretisieren. Dies ist unter

dem Aspekt der anzustrebenden Einheitlichkeit des Besteuerungsverfahrens aus datenschutzrechtlicher Sicht sogar zu begrüßen. Die Einheitlichkeit des Besteuerungsverfahrens kann aber nicht als Argument dafür herhalten, daß auch die Kontrollbefugnisse der Landesbeauftragten für den Datenschutz sich nach dem Bundesrecht (Bundesdatenschutzgesetz) und nicht nach dem jeweiligen Landesrecht (Landesdatenschutzgesetze) zu richten haben. Es hat mehr als zweijähriger Verhandlungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit dem Bundesfinanzminister bedurft, um den Bund von diesem Vorhaben abzubringen.

Dieser Teilerfolg darf jedoch nicht darüber hinwegtäuschen, daß nach wie vor die Absicht besteht, den Ländern die Datenschutzgesetzgebungskompetenz für einen der größten Bereiche der Landesverwaltungen vollständig zu entziehen. In der Begründung zum Gesetzentwurf werden hierfür folgende Argumente ins Feld geführt: „Soweit die Abgabenordnung keine bereichsspezifischen Datenschutzvorschriften enthält, sollen ergänzend die Vorschriften des Bundesdatenschutzgesetzes anwendbar sein. Die ergänzende Anwendung des Bundesdatenschutzgesetzes soll nicht nur wie bisher für die Bundesfinanzbehörden gelten, sondern in Verfahren nach der Abgabenordnung auch für die Landesfinanzbehörden, die bisher den Datenschutzgesetzen der Länder unterworfen sind. Der Umstand, daß die Landesbehörden bundeseinheitliches Recht anwenden, gebietet auch, in Verfahren nach der Abgabenordnung bundeseinheitliches Datenschutzrecht anzuwenden, denn dieses ist mit dem Verfahrensrecht untrennbar verbunden.“ Die zentrale These lautet: „Unterschiedliche Datenschutzgesetze der Länder können die gleichmäßige Durchführung des Besteuerungsverfahrens beeinträchtigen.“

Damit wird unterstellt, daß **alle** Regelungen der Landesdatenschutzgesetze Einfluß auf die richtige und gleichmäßige Steuerverfestsetzung haben, und es wird übersehen, daß sie auch Bestimmungen enthalten, die Ausdruck der Organisationshoheit der Länder sind. Sie sind z.B. vergleichbar mit den – auch die Steuerverwaltung bindenden – Regelungen in der Landeshaushaltsordnung, dem Gesetz über den Landesrechnungshof und dem Mitbestimmungsgesetz.

Welche Auswirkungen die Änderungen der Abgabenordnung in der Fassung des derzeitigen Entwurfes in Schleswig-Holstein hätten, mögen folgende Beispiele verdeutlichen:

- Die Landesregierung ist durch den Landesgesetzgeber dazu aufgefordert, durch eine Verordnung die Einzelheiten einer ordnungsgemäßen automatisierten Datenverarbeitung zu regeln und die technischen und organisatorischen Datensicherungsmaßnahmen fortzuschreiben. Die Oberfinanzdirektion und die Finanzämter wären an diese Verordnung nicht gebunden, da sie nicht Normadressat des der Landesverordnung zugrundeliegenden Landesdatenschutzgesetzes wären. Es wäre mithin nicht auszuschließen, daß sich in der Landessteuerverwaltung schwächere Sicherheits- und Do-

kumentationsstandards entwickeln als in der übrigen Landesverwaltung.

- Die Voraussetzungen für die Zulassung automatisierter Datenübermittlungsverfahren sind im Landesdatenschutzgesetz enger gefaßt als im Bundesdatenschutzgesetz. Vor allen Dingen wäre die Steuerverwaltung nicht verpflichtet, für alle Online-Übermittlungsverfahren Rechtsverordnungen zu erlassen.
- Die in Schleswig-Holstein obligatorische Nachberichts-pflicht für Behörden, die falsche oder zwischenzeitlich geänderte Daten an andere Stellen übermittelt haben, brauchte in der Steuerverwaltung nicht beachtet zu werden. Eine entsprechende Verpflichtung ist im Bundesdatenschutzgesetz nämlich nicht enthalten.
- Die Schadensersatzregelung im schleswig-holsteinischen Gesetz ist weitergehend als die im Bundesdatenschutzgesetz. Auch insoweit würden Rechte, die der Landesgesetzgeber gewährt hat, denjenigen vorenthalten, die Ansprüche gegen Finanzämter geltend machen wollen.
- Die Verpflichtung, Dateibeschreibungen und Geräteverzeichnisse zu führen, bestünde für die Finanzämter nicht. Sie wären auch nicht verpflichtet, dem Landesbeauftragten für den Datenschutz die entsprechenden Unterlagen zur Verfügung zu stellen. Er wäre somit nicht in der Lage, insoweit seiner Veröffentlichungspflicht nachzukommen.

Der Landesbeauftragte hat seine Bedenken der Finanzministerin und dem Innenminister dargelegt. Er hofft, daß die Landesregierung ihren Einfluß im Bundesrat dahin gehend geltend macht, daß der Bund seine Absicht, das Landesdatenschutzgesetz in dieser Weise einzugrenzen, fallen läßt.

4.5 Wirtschaft und Verkehr

4.5.1 Subventionsgewährung und Datenschutz

Bund und Land fördern durch Zuschüsse die Einrichtung photovoltaischer Solarzellen zur Stromerzeugung auf Einfamilienhäusern. Dies geschieht im Rahmen eines Breitentests über alternative Energiequellen.

Dem entsprechenden Förderungsantrag an die im Auftrag des Landes tätige Investitionsbank Schleswig-Holstein sollten umfangreiche Unterlagen, u.a. eine Kreditwürdigkeitsbescheinigung oder eine Schufa-Auskunft, beigelegt werden. Außerdem wurde unter der Überschrift „Datenschutzklausel“ die Einwilligung in eine Vielzahl von Datenübermittlungen an öffentliche und private Stellen gefordert, ohne daß der Einwilligende daraus entnehmen konnte, welche Daten zu welchem Zweck an welche Stelle gegeben werden sollten. Betroffene äußerten ihre Bedenken gegen das Verfahren.

Zweifel an einer datenschutzrechtlich einwandfreien Verfahrensgestaltung waren tatsächlich angebracht. Nach eingehender Erörterung mit der Investitionsbank Schleswig-Holstein konnte zunächst einmal erreicht werden, daß die „Datenschutzklausel“ als das ausgewiesen wird, was sie wirklich ist, nämlich als Einwilligung des Antragstellers in die Übermittlung seiner personenbezogenen Daten an verschiedene öffentliche und private Stellen. Darin wird nunmehr deutlich formuliert, welchen Stellen die Investitionsbank Daten zu welchen Zwecken zur Verfügung stellen darf. Es ist davon auszugehen, daß damit auch der Umfang der Datenübermittlung im Einzelfall erheblich reduziert und dem Betroffenen deutlich wird, welche Informationen an welche Stellen gelangen.

Datenschutzrechtliche Bedenken bestehen aber hinsichtlich des Umfangs der Datenerhebung. Wozu dient eigentlich eine Kreditwürdigkeitserklärung oder eine Schufa-Auskunft, wenn der Zuschuß erst nach Gebrauchsabnahme der Anlage und vollständiger Bezahlung der Installation ausgezahlt wird.

Im vorliegenden Fall ist datenschutzrechtlich einiges erreicht worden, es stellt sich jedoch die Frage, ob nicht vergleichbare Datenschutzprobleme auch in anderen Subventionsverfahren mit ähnlichen Richtlinien und anderen beteiligten öffentlichen und privaten Stellen bestehen.

4.5.2 Begründen Zwangsstillegungen einen Verdacht?

Der Halter eines Kraftfahrzeugs, dessen Kraftfahrzeugzulassung – aus welchen Gründen auch immer – von der Ordnungsbehörde eingezogen worden ist, wird dieses Fahrzeug voraussichtlich dennoch an seinem Wohnort weiter benutzen. Dieser Auffassung war offensichtlich das Ordnungsamt eines Kreises; denn es unterrichtete die örtlich zuständige Polizeidienststelle automatisch und stets von solchen Maßnahmen, damit sie ein wachsames Auge auf dieses Kraftfahrzeug und den Halter richte.

Dagegen wehrte sich ein Betroffener, da für eine solche generelle und ungeprüfte Datenübermittlung eine Rechtsgrundlage nicht bestehe und er überdies Gefahr laufe, in den Augen der Polizei als unzuverlässig und verantwortungslos zu erscheinen, ohne dazu Stellung nehmen zu können.

So sieht es auch der Landesbeauftragte. Auch der Innenminister hat sich der Auffassung angeschlossen, daß eine routinemäßige und ungeprüfte nur „nachrichtliche“ Mitteilung solcher ordnungsbehördlichen Maßnahmen nicht erforderlich und deshalb auch nicht zulässig ist, und dies den Polizeidienststellen im Lande mitgeteilt. Auch das betreffende Ordnungsamt wird folglich künftig von der automatischen Übermittlung solcher Ordnungsverfügungen an die Polizei absehen.

4.6 Sozial- und Gesundheitswesen

4.6.1 Soziales

4.6.1.1 Prüfung einer Betriebskrankenkasse

Obwohl im Bereich der freien Wirtschaft verankert, fallen Betriebskrankenkassen (BKK) als Sozialleistungsträger in die Kontrollzuständigkeit des Landesbeauftragten. Er hat im vergangenen Jahr die konventionelle Datenverarbeitung einer solchen Körperschaft öffentlichen Rechts und die Schnittstellen zur EDV kontrolliert.

Die Auswertung der Prüfung ist noch nicht endgültig abgeschlossen. Folgende datenschutzrechtliche Probleme wurden festgestellt:

- Bedenken begegnet die Tatsache, daß die Aufgaben des internen Datenschutzbeauftragten vom stellvertretenden Geschäftsführer der BKK wahrgenommen werden. Der betriebliche Datenschutzbeauftragte, den die Kasse nach dem Sozialgesetzbuch zu bestellen hat, soll die Einhaltung des Datenschutzes in der Kasse kontrollieren und zwar unabhängig von den für die Erledigung der Sachaufgaben verantwortlichen Stellen. Diese Unabhängigkeit ist bei einem Mitglied der Geschäftsführung nicht gegeben. Der Einwand der Krankenkasse, daß es ihr bei der geringen Mitarbeiterzahl (7) nicht möglich sei, einen anderen Mitarbeiter mit genügender Fachkunde mit dieser Aufgabe zu betrauen, kann im Ergebnis nicht überzeugen. Wenn der Mangel nicht durch geeignete Schulungsmaßnahmen zu beheben ist, muß das Problem durch die Bestellung eines „externen“ Datenschutzbeauftragten gelöst werden.
- Klärungsbedarf besteht im Zusammenhang mit der Aufbewahrungsfrist für Arbeitsunfähigkeitsbescheinigungen. Hier muß jeweils entschieden werden, ob es sich um wiederholte Einzelkrankheiten handelt, deren Unterlagen relativ bald nach Abklingen der Krankheit zu vernichten sind, oder ob es Ausbrüche einer chronischen Erkrankung sind, die eine längere Aufbewahrung der Unterlagen erforderlich machen. Weil davon die Speicherdauer für sensible Gesundheits- und Sozialdaten abhängt, muß für alle Beteiligten Klarheit herrschen. Die Prüfung hat gezeigt, daß bei den Mitarbeitern insoweit Unsicherheit besteht.
- Aus der internen Dateienübersicht ergab sich, daß nicht alle EDV-Dateien zum Register beim Landesbeauftragten gemeldet waren. Dies war zu beanstanden.
- Die Verarbeitung der Versicherungsdaten der BKK erfolgt in Zusammenarbeit mit dem Landesverband der Betriebskrankenkassen Hamburg – Schleswig-Holstein (LdB) und dem Bundesverband. Beides sind Körperschaften des öffentlichen Rechts. Der darüber abgeschlossene Vertrag zwischen LdB und BKK mit seinen Ergänzungen begegnet datenschutzrechtlichen Bedenken. Er muß z.B. deutlicher werden lassen, daß die BKK für die Aufgabenerfüllung

verantwortlich bleibt und in der Abwicklung des Vertrages als Auftraggeberin die notwendigen Weisungen erteilt und Kontrollen durchführt.

4.6.1.2 Außendienstmitarbeiter und zentrale Verwaltung

Eine Stadt hatte im Interesse einer bürgernahen Verwaltung in verschiedenen Stadtteilen Verwaltungsaußenstellen eingerichtet. Dort werden u.a. sozialpädagogische Fachkräfte zur Beratung und Betreuung der Bürger in sozialen Belangen eingesetzt. Sie nehmen gewissermaßen als Außendienstmitarbeiter Teilfunktionen für verschiedene Ämter mit sozialen Aufgaben, u.a. auch für das Sozialamt, wahr. So sollten sie beispielsweise auch bei der Stellung von Sozialhilfeanträgen behilflich sein und Angaben in Sozialhilfeanträgen für das Sozialamt überprüfen. Der Landesbeauftragte wurde um Stellungnahme gebeten, ob eine sozialpädagogische Fachkraft, die im Einzelfall Kenntnis von Veränderungen der Bedürftigkeit von Sozialhilfeempfängern erlangt hatte, ihre Erkenntnisse an das Sozialamt weitergeben darf oder ob sie damit unbefugt Sozialdaten offenbart und das Sozialgeheimnis verletzt.

Grundsätzlich ist es zulässig, die Festsetzung der Sozialhilfeleistung in einzelne Arbeitsschritte aufzuteilen und die Erhebung von Daten und die Ermittlung von Änderungen für eventuelle Korrekturen der Sozialhilfe dem einen Mitarbeiter (sozialpädagogische Fachkraft) zu übertragen, die Festsetzung der Sozialhilfe aber einem anderen Mitarbeiter (Verwaltungsfachkraft). Die Weitergabe der Entscheidungsgrundlagen von der sozialpädagogischen Fachkraft an den Verwaltungsbereich ist bei einer derartigen Organisationsform zur Aufgabenerfüllung des Sozialleistungsträgers erforderlich. Sie ist als Teil der Bearbeitung eines einheitlichen Falles zulässig.

4.6.1.3 Landesaufnahmegesetz

Frühzeitig beteiligte der Minister für Soziales, Gesundheit und Energie den Landesbeauftragten an den Entwürfen für ein „Gesetz über die Aufnahme von Aussiedlern und ausländischen Flüchtlingen sowie zur Durchführung des Bundesvertriebenengesetzes (Landesaufnahmegesetz)“. Der Entwurf sah vor, daß die amtsfreien Gemeinden, Ämter und Kreise eine Reihe personenbezogener Angaben von Aussiedlern und Flüchtlingen auch ohne deren Wissen an Betreuungseinrichtungen wie beispielsweise freie Wohlfahrtsverbände und kirchliche Einrichtungen übermitteln dürfen. Der Landesbeauftragte hat hiergegen Bedenken erhoben und auf die Gefahr einer Betreuung „wider Willen“ hingewiesen. Insbesondere sei eine Übermittlung dieser Daten dann nicht erforderlich, wenn Betroffene z.B. bei einer Familienzusammenführung oder in sonstiger Weise von Verwandten oder Freunden ausreichend betreut würden. Eine Übermittlung solle daher immer nur mit Einwilligung der Betroffenen erfolgen.

Leider ist den Bedenken des Landesbeauftragten nicht gefolgt worden. Da es sich nach der nunmehr verabschiedeten Regelung jedoch um eine „Kann-Vorschrift“ handelt, sind künftig die örtlich zuständigen Stellen gehalten, die Gegebenheiten des Einzelfalles zu prüfen und die Übermittlung nur dann vorzunehmen, wenn sie im Einzelfall erforderlich erscheint. Eine routinemäßige Übermittlung aller Daten an die Betreuungseinrichtungen ist hiernach jedenfalls ausgeschlossen.

4.6.2 Gesundheit

4.6.2.1 Offenbarung von Rezeptdaten an den Untersuchungsführer für die Berufsgerichtsbarkeit der Heilberufe

Der Landesbeauftragte hatte zu prüfen, ob eine Krankenkasse dem Untersuchungsführer für die Berufsgerichtsbarkeit der Heilberufe auf dessen Ersuchen Rezeptdaten zur Verfügung stellen und damit im Sinne des Sozialgesetzbuches offenbaren darf. Es bestand der Verdacht, daß ein Arzt seinen Patienten immer einen bestimmten Apotheker empfahl. Das wäre nach Landesrecht unzulässig und von der Berufsgerichtsbarkeit zu ahnden.

Sämtliche bei einer Krankenkasse gespeicherten Daten und somit auch die in den Rezeptunterlagen enthaltenen Daten unterliegen dem Sozialgeheimnis. Die Voraussetzungen für ihre Weitergabe bzw. Offenbarung sind im Sozialgesetzbuch abschließend geregelt. In dem konkreten Fall hatte die örtliche Krankenkasse ihrem Landesverband die Rezepte eines Quartals zur Prüfung und Weiterleitung an den Untersuchungsführer überlassen. Die Prüfung des Katalogs der Offenbarungsbefugnisse zeigt, daß eine Rechtsgrundlage dafür nicht besteht. Die Offenbarung im Rahmen der Amtshilfe war nicht zulässig, da die Vorschrift nur die Befugnis zur Offenbarung einer begrenzten Anzahl von Daten enthält. Rezeptdaten gehen über den danach erlaubten Rahmen hinaus. Auch war die Offenbarung nicht zur Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch erforderlich. Die Sozialleistungen waren bereits erbracht, und es ging auch nicht darum, Schaden von der Versicherungsgemeinschaft abzuwenden. Hier sollte lediglich ein standesrechtliches Fehlverhalten von Angehörigen der Heilberufe verfolgt werden.

Deshalb sah der Landesbeauftragte keinen Anspruch des berufsgerichtlichen Untersuchungsführers auf Herausgabe von Rezeptdaten. Die Weitergabe der Daten durch den Landesverband hat er daher als Verstoß gegen das Sozialgeheimnis beanstandet.

4.6.2.2 Ärztliche Gutachten per Telefax

Ein Gesundheitsamt hatte Ärzte und Sozialarbeiter aufgefordert, Gutachten im Rahmen des Gesetzes für psychisch Kran-

ke in Unterbringungs-fällen ggf. per Telefax an den zuständigen Kreis zu senden. Der Minister für Soziales, Gesundheit und Energie hatte den Landesbeauftragten um datenschutzrechtliche Stellungnahme dazu gebeten.

Auch bei der Versendung ärztlicher Gutachten per Telefax muß gewährleistet sein, daß die Information bei der zuständigen Stelle, hier also beim zuständigen Arzt, oder seinem ärztliche Hilfspersonal bzw. bei dem sonst zuständigen Adressaten eingeht. Das Absenden eines Telefaxschreibens an eine zentrale Registratur oder Posteingangsstelle ohne entsprechende Absicherung wäre eine unbefugte Offenbarung ärztlicher Daten. Eine Versendung als Telefax bedarf nach Auffassung des Landesbeauftragten immer dann besonderer Sicherheitsvorkehrungen, wenn auch bei konventionellem Postversand eine Zuleitung ausschließlich an bestimmte Personen (z.B. von Arzt zu Arzt) oder an bestimmte öffentliche Stellen zulässig ist und deshalb eine Zuleitung in verschlossenem Umschlag bis zum Empfänger erfolgen müßte (vgl. Tz. 5).

4.6.2.3 Die Diskussion über die Erfassung von Krebserkrankungen dauert an

Krebsregister

Der Verzicht auf ein regionales Tumorregister, über den der Landesbeauftragte vor einer Reihe von Jahren berichtet hatte (7. TB, S. 53), beendete die Erörterungen zu diesen Fragen im Lande nicht und konnte es wohl auch nicht. Überlegungen zur Nutzung des Krebsregisters der ehemaligen DDR, weiterhin erhobene Forderungen von medizinischer Seite und Aktivitäten des Bundes für ein bundeseinheitliches Krebsregister veranlaßten den Sozialminister des Landes dazu, sich in jüngster Zeit erneut für ein regionalisiertes Krebsregister in Schleswig-Holstein einzusetzen.

Fortgesetzt hat sich außerdem – auch weil einige Bundesländer über Krebsregistergesetze verfügen – die bundesweite Diskussion. Dabei stehen im Grundsatz drei Konzeptionen in der Erörterung:

- Eine obligatorische Meldung der Krebsfälle zu einem Register, durch die die ärztliche Schweigepflicht durchbrochen würde;
- eine Meldung nur mit Einwilligung der Patienten, die zur Gefahr unvollständiger Register führt und
- eine anonymisierte Meldung, die mit Hilfe von Verschlüsselungen zwar den Fall, nicht aber den Patienten identifiziert. Sie verursacht ein aufwendigeres Meldeverfahren.

Die Datenschutzbeauftragten des Bundes und der Länder haben erneut in einem Beschluß zur beabsichtigten Erarbeitung eines Bundeskrebserregistergesetzes Stellung genommen und auf die Gefahren für das Persönlichkeitsrecht der Patienten und für das Vertrauensverhältnis zwischen Arzt und Patient bei

namentlichen Meldungen hingewiesen sowie empfohlen, Daten nur mit Einwilligung des Patienten oder im Rahmen dezentraler Verschlüsselungsmodelle zu erheben.

Eine zwangsweise namentliche Registrierung der Krebsfälle in Schleswig-Holstein kommt für den Landesbeauftragten nicht in Betracht. Er hat bereits früher empfohlen, ein solches Register mit Hilfe eines Verschlüsselungsverfahrens, also mit anonymisierten Daten, zu erstellen, jedenfalls aber das Arztgeheimnis nicht ohne Einwilligung des Patienten zu durchbrechen (vgl. 6. TB, S. 47 und 7. TB, S. 53).

Leukämie im Unterelberaum

Vor diesem Hintergrund müssen die Überlegungen gesehen werden, im Unterelberaum aufgetretene Leukämiefälle auf ihren Zusammenhang mit benachbarten Kernkraftanlagen zu untersuchen. Dazu sollen

- Erkrankungs- und Todesfälle an Leukämieen und anderen Blutkrankheiten sowie von Krebserkrankungen bei der Gesamtbevölkerung erfaßt werden,
- alle relevanten Informationen der lokalen Nuklearanlagen erhoben werden und
- eine Fachkommission von Wissenschaftlern eingesetzt werden, die den Zusammenhang zwischen den aufgetretenen Leukämiefällen und den lokalen radioaktiven Immissionen untersuchen soll.

Der Landesbeauftragte hat die mit der Organisation des Forschungsvorhabens beschäftigte Arbeitsgruppe in ihrer Absicht bestärkt, Patientendaten ausschließlich mit Einwilligung der Betroffenen zu erheben und zu verarbeiten. Aus entsprechenden Datenbeständen bei öffentlichen Stellen, wie Krankenhäusern, Gesundheitsämtern, Krankenkassen u.a., dürfen ohne Einwilligung der Betroffenen Informationen nur übermittelt werden, soweit sie zuvor anonymisiert sind.

4.6.2.4 Darf ein „Laie“ die ärztliche Tätigkeit eines Krankenhausarztes überprüfen?

Im Berichtsjahr war der Landesbeauftragte zweimal mit der Frage konfrontiert, ob es zulässig ist, daß Verwaltungsbeamte die ärztliche Tätigkeit eines Krankenhausarztes überprüfen. In beiden Fällen handelte es sich um Kreiskrankenhäuser, die von der jeweiligen Kreisverwaltung überprüft werden sollten.

Fall 1

Die Petentin – eine Mitarbeiterin der Kreisverwaltung – kam als Notfallpatientin ins Kreiskrankenhaus. Obwohl eine andere Notfallpatientin schon zuvor eingeliefert war, wurde bei der

Petentin ein operativer Eingriff früher durchgeführt. Im nachhinein wurde dem behandelnden Arzt vorgeworfen, er habe die später gekommene Patientin bevorzugt. Dieser Vorwurf wurde dem Dezernenten für das Gesundheitswesen des Kreises schriftlich mitgeteilt. Um den Sachverhalt zu klären, wurden die Akten beider Patientinnen zur Prüfung des Vorwurfes dem Krankenhausverwaltungsamt vorgelegt. Hiergegen wandte sich die Petentin und schaltete den Landesbeauftragten ein.

Fall 2

In der Presse wurde darüber berichtet, daß eine andere Kreisverwaltung eine Reihe von Krankenakten aus der Abteilung Chirurgie ihres Kreiskrankenhauses zur Überprüfung angefordert hatte. Es ging um den Verdacht gravierender Behandlungsfehler durch den kommissarischen Chefarzt. Die Kreisverwaltung ließ die Krankenakten durch den Amtsarzt des Gesundheitsamtes prüfen. Dieser hat seine Ermittlungsergebnisse nach Angabe der Kreisverwaltung ohne Nennung von Patientennamen niedergelegt. Die Ermittlungsergebnisse waren dann Grundlage für die Prüfung durch den Kreisausschuß, ob hier die Staatsanwaltschaft eingeschaltet werden müsse.

Die Lösung

Im ersten Fall ist die Klärung der Frage, ob der Arzt eine Patientin bevorzugt behandelt hat, zunächst eine rein medizinische und damit eine Frage der Fachaufsicht. Der Chefarzt als Fachvorgesetzter wäre zuständig gewesen, diesen Vorwurf zu überprüfen. Erst wenn sich aus dieser Prüfung Anhaltspunkte für dienstaufsichtliche Maßnahmen ergeben hätten, wäre u.U. im Einzelfall auch die Offenbarung von Patientendaten an das Krankenhausverwaltungsamt zulässig gewesen. Das Krankenhausverwaltungsamt hätte die Beschwerde an den Chefarzt zur Überprüfung und Entscheidung zurückgeben müssen. Der Landesbeauftragte hat daher die Herausgabe der Krankengeschichten an das Krankenhausverwaltungsamt als unbefugte Offenbarung und als Verstoß gegen die ärztliche Schweigepflicht kritisiert und die Kreisverwaltung aufgefordert, durch geeignete Maßnahmen entsprechende Vorfälle in Zukunft auszuschließen.

Anders liegt der zweite Fall. Der kommissarische Chefarzt, gegen den sich die Vorwürfe richteten, hatte zum Zeitpunkt der Überprüfung keinen Fachvorgesetzten im Krankenhaus, der die Überprüfung selbst hätte vornehmen können. Da sich die Vorwürfe gegen ihn selbst richteten, hält der Landesbeauftragte die Überprüfung der Krankenakten durch den Amtsarzt grundsätzlich für zulässig. Die Verwaltungsebene hatte sich unter Gesichtspunkten der Dienstaufsicht erst mit der Stellungnahme des Amtsarztes auseinanderzusetzen, ohne von vornherein die Krankenunterlagen heranzuziehen.

4.7 Endlich ein Archivgesetz

Der Landesbeauftragte hatte es immer wieder angemahnt. Nun ist ein Landesarchivgesetz endlich verabschiedet. Es regelt die Archivierung solcher Verwaltungsunterlagen, die für die Aufgabenerfüllung der öffentlichen Hand nicht mehr benötigt werden, wenn der historische, kulturelle oder politische Sachgehalt dieser Unterlagen eine Erhaltung auf Dauer für Forschung und Bildung notwendig erscheinen läßt. Die Löschungs- bzw. Sperrungspflicht nach allgemeinem Datenschutzrecht wird für diese Fälle durch die Aufbewahrung in einem speziellen Archiv ersetzt.

Aus datenschutzrechtlicher Sicht mußte der Gesetzgeber dabei einen angemessenen Ausgleich zwischen dem Allgemeininteresse an historisch-kulturellen Informationen und dem Persönlichkeitsschutz Betroffener schaffen. Zugleich mußten die Probleme gelöst werden, die mit der Änderung des Nutzungszwecks solcher Unterlagen vom Verwaltungsvollzug zur historischen Forschung verbunden waren. Schließlich waren organisatorische und technische Maßnahmen zum Schutz der Informationen zu treffen. Der Landesbeauftragte hält die Grundkonzeption des Gesetzes für den datenschutzrechtlich richtigen Weg, einen Rechtsgüterausgleich zwischen grundsätzlicher Archivöffentlichkeit und den Persönlichkeitsrechten Betroffener zu schaffen.

Eine Reihe von Vorschlägen des Landesbeauftragten sind im Gesetz berücksichtigt worden. Insbesondere auf die Regelung, daß mit der Archivierung eine eigene, auch datenschutzrechtliche Zuständigkeit des Archivs für das Archivgut entsteht und der abgebenden Stelle keine Sonderrechte eingeräumt werden, hat der Landesbeauftragte Wert gelegt. Dadurch soll sichergestellt werden, daß ein Archiv keine erweiterte „Verwaltungsregistratur“ ist, mit deren Hilfe Vorschriften zur Löschung und Sperrung personenbezogener Daten unterlaufen werden können. Ebenso bedeutsam ist die Regelung, daß die Nutzung des Archivguts dann einzuschränken oder zur versagen ist, wenn besondere Geheimhaltungspflichten wie etwa nach dem Strafgesetzbuch betroffen sind oder Grund zur Annahme besteht, daß schutzwürdige Belange Betroffener oder Dritter entgegenstehen. Dies zeigt, daß über alle organisatorischen Regelungen und Schutzfristen hinaus im Einzelfall das informationelle Selbstbestimmungsrecht Betroffener berücksichtigt werden muß.

Der Landesbeauftragte hofft, daß mit den neuen Gesetzen die bestehende Unsicherheit im Umgang mit alten Verwaltungsunterlagen beseitigt ist. Er wird darauf hinwirken, daß in der vorgesehenen Verordnung darüber hinaus konkrete Auswahlkriterien für die Archivierung von Unterlagen festgelegt werden. Dem Betroffenen muß transparent sein, wann er mit einer dauerhaften Speicherung seiner personenbezogenen Daten im Archiv rechnen muß.

Von besonderer Bedeutung ist, daß bei der Änderung des Nutzungszwecks der Unterlagen, insbesondere bei den „son-

stigen öffentlichen Archiven“, eine strenge organisatorische Trennung von den übrigen Verwaltungsvorgängen erfolgt. Dies ist notwendig, um unzulässige Zugriffe auf solche Unterlagen zu verhindern, die zur Erfüllung der ursprünglichen Behördenaufgabe nicht mehr erforderlich sind. Hierauf wird der Landesbeauftragte bei Prüfungen achten.

5. Datenschutz im Medienbereich und bei neuen Übermittlungstechniken

5.1 Staatsvertrag über den Norddeutschen Rundfunk

Im Jahre 1991 wurde im Zusammenhang mit der deutschen Vereinigung der Staatsvertrag über den Norddeutschen Rundfunk (NDR) novelliert. Bei dieser Gelegenheit wurden Datenschutzvorschriften in den Vertrag aufgenommen. Die Staatskanzlei bezog den Landesbeauftragten frühzeitig in die Erörterungen des Vertragswerks ein und gab ihm Gelegenheit, Stellung zu nehmen.

Gegenüber den früheren Vertragsbestimmungen haben die eingehenden Beratungen Fortschritte auch für den Datenschutz gebracht. Zu kritisieren bleibt aber:

- Der Vertrag sieht für den NDR eine Aufzeichnungspflicht von Sendungen vor. Damit soll später der Nachweis über Sendungsinhalte und damit über die Verbreitung personenbezogener Informationen ermöglicht werden. Abgesehen von der sehr kurzen Aufbewahrungsfrist solcher Aufzeichnungen können Ausnahmen von der Aufzeichnungs- und Aufbewahrungspflicht zugelassen werden. Ein Grund für solche Ausnahmen, die Betroffenen Beweismöglichkeiten nehmen und sie dadurch in ihren Rechten beeinträchtigen können, war für den Landesbeauftragten nicht erkennbar.
- Die Regelung des Datenschutzes ist nicht normenklar. Grundsätzlich soll das Hamburger Datenschutzgesetz gelten, einige seiner Vorschriften sind durch den Vertrag ersetzt, weitere werden ausgeschlossen. An Stelle des Hamburgischen Datenschutzbeauftragten wird zur Kontrolle des Datenschutzes ein interner Datenschutzbeauftragter des NDR bestellt. Nach Auffassung des Landesbeauftragten wird diese Rechtslage für den Bürger nicht verständlich sein und hätte verbessert werden können.
- Ein Auskunftsrecht Betroffener über die zu ihrer Person gespeicherten Daten gehört zum heutigen Standard im allgemeinen Datenschutzrecht. Auch im NDR-Vertrag sind solche Auskunftsrechte als Grundlage des Persönlichkeitsschutzes verankert, allerdings erst, wenn der Bürger von einer Berichterstattung betroffen ist. Wirksamer wäre es gewesen, ein solches Recht schon vor einer Berichterstattung festzulegen, um Eingriffe in das Persönlichkeitsrecht Betroffener von vornherein zu vermeiden.

5.2 Datenschutz bei Dienstleistungen der Deutschen Bundespost

Mit dem „dienstintegrierenden digitalen Netzwerk“ (ISDN) der Deutschen Bundespost TELEKOM werden verschiedene Telekommunikationsdienste in einem Netz zusammengefaßt und vermittelt. Die Speicherung von Informationen wird durch Digitalisierung der Datenflüsse und Einsatz intelligenter Vermittlungsstellen erweitert und die Übermittlung beschleunigt. Neben den schon seit langem angebotenen Kommunikationsdiensten wie Fernsprechen, Telegraphie, Fernschreiben, Datenverkehr u.a.m. werden auch neue komfortablere Dienstleistungen wie Fernmessen und Fernwirken, Mail-box-Dienste und ähnliche sogenannte Mehrwertdienste angeboten. ISDN ausgestattete Endgeräte können dabei die neuen Möglichkeiten dieses Netzes voll ausnutzen. Herkömmliche, analoge Geräte bleiben mit ihrem geringeren Leistungsspektrum aber ebenfalls an das Netz angeschlossen und funktionsfähig.

Daß mit der Leistungssteigerung des Telekommunikationssystems auch Gefahren für das informationelle Selbstbestimmungsrecht der Benutzer verbunden sein könnten, wurde sehr bald durch die Hinweise der Datenschutzbeauftragten des Bundes und der Länder deutlich (13. TB., S. 77). Die datenschutzrechtlichen Probleme sollen nun durch die TELEKOM-Datenschutzverordnung (TDSV) und für privatrechtlich organisierte Telekommunikationsdiensteanbieter durch die Telekommunikationsunternehmen-Datenschutzverordnung (UDSV) gelöst werden. Trotz dieser Regelungen bleiben für die Anwender – und dazu gehören auch Behörden und sonstige öffentliche Stellen im Lande Schleswig-Holstein – offene Fragen.

Normalerweise erhält der Benutzer für seine Gebührenabrechnung wie bisher eine aufsummierte Zusammenstellung aller Gespräche. Die Gebührenrechnung enthält keine Angabe von Anschlußnummern der gerufenen Teilnehmer (Zielnummern). Im Normalfall werden die Verbindungsdaten einschließlich der Zielnummern alsbald nach Versendung der Gebührenrechnung gelöscht. Es besteht aber auch die Möglichkeit, die Verbindungsdaten mit einer um drei Stellen verkürzten Zielnummer oder auch mit der vollständigen Zielnummer längerfristig zu speichern. Für diesen Fall wird dem Teilnehmer auch die Möglichkeit geboten, einen sogenannten Einzelentgeltnachweis zu erhalten, bei dem ihm u.a. die verkürzte oder die vollständige Zielnummer der Gespräche mitgeteilt wird. In diesen Fällen bleiben die zugrundeliegenden Daten für die Abrechnung bis 80 Tage nach Rechnungsversand gespeichert.

Die Datenschutzbeauftragten haben hier vergeblich versucht, generell eine Verkürzung der Zielnummer zu erreichen und daneben die Speicherdauer der Daten zu reduzieren. So wird – wenn der Anrufende es wünscht – aus der Rechnung die Nummer des Angerufenen ersichtlich, ohne daß er darauf Einfluß hat. Auch das Kommunikationsverhalten einzelner Mitbenutzer (z.B. Familienangehöriger, Arbeitnehmer) kann kontrolliert werden. Während der langen Speicherdauer

der so entstehenden Telekommunikationsprofile können Staatsanwaltschaft, Polizei und Geheimdienst nach Maßgabe der gesetzlichen Eingriffsvorschriften auf die Daten zurückgreifen. Die vorgeschriebene Einwilligung von Mitbenutzern in dem Einzelentgeltnachweis ist kaum kontrollierbar. Die Nummern der Angerufenen werden naturgemäß ohne deren Einwilligung im Einzelgebührennachweis gespeichert.

Ein weiteres noch nicht zufriedenstellend gelöstes Problem ist die sogenannte Rufnummernanzeige. Die Möglichkeit, die Anschlußnummer des Anrufers auf dem gerufenen Apparat anzuzeigen, besteht bei ISDN-Telefonen mit Display. Im Laufe der Jahre wird voraussichtlich ein nicht unwesentlicher Teil der Benutzer diese Möglichkeit haben. Erst die Hinweise der Datenschutzbeauftragten, daß auch unbeobachtete Kommunikation möglich bleiben muß, haben hier zu einer Verbesserung des Datenschutzes geführt. Der Teilnehmer mit analogem Endgerät wird künftig nur dann mit seiner Rufnummer angezeigt, wenn er es ausdrücklich und für alle Kommunikationsfälle beantragt. Teilnehmer mit ISDN-fähigen Telefonapparaten können bei den Vereinbarungen mit der TELEKOM zwischen generellem Ausschluß der Rufnummernanzeige oder genereller Zulassung wählen und – allerdings ab 1994 – auch im Einzelfall die Anzeige ihrer Rufnummern unterdrücken, wenn ihr Gerät entsprechende Funktionen vorsieht.

Die Rufnummern bestimmter Beratungsstellen, beispielsweise von Kirchen und sozialen Diensten, werden unter Umständen im Einzelentgeltnachweis nicht ausgedruckt. Damit soll der unbeobachtete Kontakt mit diesen Stellen erleichtert werden. Allerdings bleibt das von einem Antrag dieser Stellen abhängig. Das gleiche gilt für die Unterdrückung der Rufnummernanzeige auf Endgeräten dieser Anschlüsse und die Kennzeichnung solcher anonymer Kontaktmöglichkeiten im Telefonbuch. Die Speicherung dieser Daten bei der Deutschen Bundespost bleibt jedoch und damit zugleich die Zugriffsmöglichkeit der Gerichte auf die gespeicherten Daten.

Der Landesbeauftragte hat die betroffenen Ressorts der Landesregierung und die kommunalen Landesverbände auf diese Situation hingewiesen und dringend empfohlen, in ihrem Zuständigkeitsbereich die in Betracht kommenden Stellen auf die bestehenden Risiken aufmerksam zu machen und sie zu veranlassen, die erforderlichen Anträge an die Deutsche Bundespost TELEKOM zu stellen.

5.3 Positives Echo auf Telefax-Tips

Bei dem weitverbreiteten Telefax-Dienst der Deutschen Bundespost sind zwei Faktoren von besonderer sicherheitstechnischer Bedeutung. Die Informationen werden nicht nur „offen“ übertragen, sondern erreichen den Empfänger auch in unverschlüsselter Form (vergleichbar einer Postkarte). Ist der Adressat auf den Empfang von vertraulichen bzw. geheimhaltungsbedürftigen Informationen nicht vorbereitet, kann der Absen-

der indirekt zum Verursacher einer unbefugten Kenntnisnahme dieser Daten durch Dritte im Bereich des Empfängers werden. Außerdem erfolgt die Adressierung des Empfängers über einen Code (die Telefax-Nummer) und nicht über eine Anschrift. Schreibfehler, Zahlendreher usw. fallen weniger auf, sind nicht plausibel abprüfbar und führen in der Regel gleichwohl zu einer fehlerfreien Datenübertragung (vergleichbar einer Telefonverbindung unter Benutzung einer falschen Telefonnummer).

Da diese Sicherheitsrisiken von der Bundespost nicht abgefangen werden, hat der Landesbeauftragte im Amtsblatt den Behörden folgende datenschutzrechtliche Hinweise zur Benutzung von Telefax-Geräten in der öffentlichen Verwaltung gegeben:

- Die richtige Bedienung der Geräte sollte durch eine schriftliche Dienstanweisung geregelt werden.
- Restriktive Regelungen sollten für die Übertragung von Daten getroffen werden, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen oder die aus anderen Gründen als „sensibel“ einzustufen sind (Sozial-, Steuer-, Personal- und medizinische Daten, vgl. hierzu Textziffern 4.2.2.6 und 4.6.2.2 dieses Berichtes).
- Die von dem empfangenden Gerät abgegebene Kennung sollte stets geprüft werden, damit die Verbindung bei Wählfehlern sofort abgebrochen werden kann.
- Es sollte vor der Übermittlung geprüft werden, ob der Empfänger die Übertragung der Daten auf diesem Weg erwartet (insbesondere bei unverlangten Übermittlungen).
- Die übermittelten Informationen sollten dokumentiert werden.
- Die Geräte sollten so aufgestellt werden, daß Unbefugte keine Kenntnis vom Inhalt eingehender Telefax-Schreiben erhalten können.

Die Veröffentlichung dieser Hinweise hat eine unerwartet starke Resonanz bei den Behörden im Lande gefunden. In den vielen Beratungsgesprächen, um die die Mitarbeiter des Landesbeauftragten gebeten worden sind, kam immer wieder zum Ausdruck, daß er sich häufiger auf diesem Wege zu aktuellen datenschutzrechtlichen Problemstellungen äußern möge. Er wird diese Anregung gern aufnehmen.

6. Ordnungsmäßigkeit der Datenverarbeitung

6.1 Rechtliche und technisch-organisatorische Kriterien

Seit ihren Anfängen vor nunmehr ziemlich genau 25 Jahren hat die automatisierte Verarbeitung personenbezogener Ver-

waltungsdaten nach und nach alle Bereiche der schleswig-holsteinischen Verwaltung durchdrungen. Aus wenigen zentralen und hochspezialisierten Rechenzentren sind viele hundert dezentrale Datenverarbeitungs-Organisationseinheiten entstanden, die die Aufbau- und Ablauforganisation der jeweiligen Behörden in einer geradezu revolutionären Art und Weise verändert haben.

Eine Sichtweise, wonach die Automatisierung der Datenverarbeitung lediglich die Fortsetzung gewohnter Verfahren mit anderen Mitteln ist, greift zu kurz. In aller Regel gehen mit der immensen Leistungssteigerung der automatisierten Datenverarbeitung – sonst bräuchte man nicht von Karteikarten auf den Computer umzusteigen – erhöhte Gefährdungen für das Persönlichkeitsrecht einher. Datenschutz befaßt sich also nicht nur mit der Frage, wer welche Daten verarbeiten darf, sondern vor allem auch mit der dabei verwendeten Technik. Das Bundesverfassungsgericht hat dies im Volkszählungsurteil unter dem Begriff des „Verwendungszusammenhangs“ betont. Auch das Datenschutzrecht weist mehr und mehr Vorschriften auf, die die Datenverarbeitungstechnik zum Gegenstand haben.

Um so bemerkenswerter ist es, daß Automatisierung der Datenverarbeitung in der Verwaltung nicht auf der Grundlage eines allgemeinverbindlichen Regelungswerkes geschehen ist. Jede Behörde, die zu der Auffassung gelangte, der Einsatz von Datenverarbeitungsgeräten könne zu Rationalisierungseffekten führen, war frei in der Wahl ihrer Methoden und Ziele und nutzte diese Freiheit. Undenkbar erschiene eine vergleichbare Entwicklung z.B. im Finanz- und Kassenwesen. Man stelle sich vor, die vielen Landesbezirks-, Finanz-, Stadt- und Amtskassen im Lande wären jeweils so organisiert worden, wie es aus der Sicht der betreffenden Behörde „praktisch“ gewesen wäre.

So ist es nicht verwunderlich, daß im Zusammenhang mit der automatisierten Datenverarbeitung zwar häufig der Begriff „Ordnungsmäßigkeit“ benutzt wird, daß dieser Begriff aber nirgends eindeutig definiert wurde. In der Regel wird von Ordnungsmäßigkeit nur im Zusammenhang mit der technisch-organisatorischen Abwicklung von Verwaltungsverfahren gesprochen, so auch im Landesdatenschutzgesetz („ordnungsgemäße Anwendung der Datenverarbeitungsprogramme“).

Zu wenig Beachtung hat bisher die Tatsache gefunden, daß zwischen den rechtlichen und den technisch-organisatorischen Ordnungsmäßigkeitskriterien zu differenzieren ist. Von einer ordnungsgemäßen Datenverarbeitung im Sinne der Zulässigkeit kann nach Auffassung des Landesbeauftragten nur gesprochen werden, wenn für die Verarbeitung eine einwandfreie gesetzliche Grundlage besteht. Da die automatisierte Datenverarbeitung besondere Risiken für das Recht auf informationelle Selbstbestimmung birgt, bedarf es vor der Einführung neuer Verfahren zunächst der besonders sorgfältigen Prüfung, ob die Zulässigkeit der beabsichtigten Datenverarbeitung auch tatsächlich gegeben ist. Darüber hinaus ist im Rahmen einer

Art von Technikfolgenabschätzung zu prüfen, ob und ggf. welche Gefahren mittel- und langfristig für die Rechte der Bürger und der Mitarbeiter sowie für die Funktionsfähigkeit der Verwaltung entstehen können.

Erst wenn unter diesen Gesichtspunkten die Automatisierung von Verwaltungsabläufen unbedenklich erscheint, kann damit begonnen werden, auch die sicherheitstechnischen Problemstellungen einer Lösung zuzuführen.

Die im neuen Landesdatenschutzgesetz enthaltenen „Verordnungsverpflichtungen“ für die Landesregierung und die – bei aller datenschutzrechtlichen Kritik im Detail – Bemühungen der IT-Kommission (vgl. Tz. 6.2 dieses Berichtes) zeigen, daß in Schleswig-Holstein eine Entwicklung eingesetzt hat, die diesen Überlegungen stärker als bisher Rechnung trägt.

6.1.1 Landesregierung jetzt in der Pflicht

Der Gesetzgeber hatte der Landesregierung seit Inkrafttreten des Landesdatenschutzgesetzes im Jahr 1978 die Möglichkeit gegeben, die Anforderungen an die Datensicherungsmaßnahmen entsprechend dem Stand der Technik fortzuschreiben. Diese Chance ist während der immerhin 14jährigen Gültigkeitsdauer des Gesetzes nicht genutzt worden, obwohl niemand bezweifeln kann, daß sich in der automatisierten Datenverarbeitung in der Zwischenzeit eine rasante Entwicklung vollzogen hat. Nunmehr „regelt“ die Landesregierung durch Rechtsverordnung die Datensicherungsmaßnahmen nach dem Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen. Ferner sind auf dem Verordnungswege „Anforderungen an die Verfahren sowie die Dokumentation und deren Aufbewahrungsfristen festzulegen“. Das Gesetz bezeichnet dies als „Einzelheiten einer ordnungsgemäßen automatisierten Datenverarbeitung in der öffentlichen Verwaltung“. Die Landesregierung wurde also verpflichtet, den datenverarbeitenden Stellen im Lande Weisungen zu erteilen, die unter der Bezeichnung „Grundsätze ordnungsmäßiger Datenverarbeitung“ schon seit Jahren von den Datenschutzbeauftragten (vgl. 8. TB, S. 61) gefordert werden.

6.1.2 Regelungsvorschläge des Landesbeauftragten

In Anbetracht der Tatsache, daß der Landesbeauftragte nach dem neuen LDSG bei der Entwicklung der Landesverordnung zu beteiligen ist, hat er dem Innenminister eine erste Zusammenstellung von Gesichtspunkten übermittelt, die in diesem Zusammenhang im Interesse der schutzwürdigen Belange der Bürger geregelt werden müssen. Im einzelnen geht es um folgendes:

Sicherheitsanalysen bei der Verarbeitung „sensibler Daten“

In der Vergangenheit wurden „sensible“ personenbezogene Datenbestände überwiegend in besonders gesicherten Großrechenzentren verarbeitet (in der Datenzentrale, in den Rechenzentren der Ortskrankenkassen, der Steuerverwaltung, der Landesversicherungsanstalten usw.). Bei Prüfungen wurden selbst in derart spezialisierten Organisationseinheiten technische und organisatorische Sicherheitsmängel festgestellt. In dem Maße, wie nunmehr überall kleine und kleinste „Rechenzentren“ entstehen, stellen sich die Probleme adäquater Sicherheitsvorkehrungen in immer mehr und immer kleineren Behörden. Als Beispiel ist in diesem Zusammenhang die Verarbeitung von Sozialdaten mit Hilfe von vernetzten PC in kleinen Kommunalverwaltungen zu nennen.

Es erscheint zumindest notwendig, die betreffenden Verwaltungen auf dem Ordnungswege zu verpflichten, vor dem Beginn der automatisierten Verarbeitung von Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen, von Personaldaten oder solchen, die z.B. nach der Konvention des Europarates als besonders schützenswert anzusehen sind (wie Daten über den Verdacht strafbarer Handlungen, politische oder weltanschauliche Standpunkte) spezielle Sicherheitsanalysen durchzuführen, die über die unter Textziffer 6.1 angesprochene allgemeinen Überlegungen hinausgehen. In diesen Analysen sollten die erkannten Sicherheitsrisiken und die getroffenen Abwehrmaßnahmen explizit dargestellt werden. Sie sollten zusätzlich deutlich werden lassen, welche an sich möglichen Maßnahmen ggf. aus Kostengründen nicht ergriffen worden sind.

Trennung zwischen Entscheidungs- und Sachbearbeitungsebene der EDV-Organisation

In Großrechenzentren und in größeren EDV-Organisationseinheiten ist die personelle Trennung zwischen der Entscheidungs- und der Sachbearbeitungsebene seit jeher ein wirksames Mittel der Datensicherung. Die Leiter dieser Institutionen und Dienststellen sowie die von ihnen eingesetzten Referenten, Chefprogrammierer, Rechenzentrumsleiter usw. überwachen die Arbeiten der einzelnen Sachbearbeiter (Programmierer, Operator, Techniker). Voraussetzung hierfür ist eine entsprechende Ausbildung und Berufserfahrung.

Entsprechend einer Empfehlung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder aus dem Jahr 1988 sollte in der Verordnung deshalb festgelegt werden, daß Behörden, die personenbezogene Daten in automatisierten Dateien verarbeiten, in Geschäftsverteilungs- bzw. in Organisationsplänen die Zuständigkeiten/Verantwortlichkeiten für die **Überwachung** der Handhabung der eingesetzten EDV-Systeme ausdrücklich festzulegen haben. Wegen der Bedeutung einer technikorientierten Schulung für die Mitarbeiter in die-

sen Führungspositionen wird auf Textziffer 6.3 dieses Berichtes verwiesen.

Sicherheitssoftware für PC

Es ist vom Landesbeauftragten mehrfach dargelegt worden, welche Sicherheitsrisiken mit der Benutzung von PC bei der Verarbeitung personenbezogener Daten verbunden sein können (vgl. z.B. 12. TB, S. 74).

Aus diesen Gegebenheiten sollte in der Verordnung in der Weise die Konsequenz gezogen werden, daß die Verarbeitung von personenbezogenen Daten auf Datenverarbeitungsgeräten, die konstruktionsbedingt einen unmittelbaren Zugriff auf das Betriebssystem, die Programmbibliotheken und auf die Datenbestände durch die Benutzer zulassen, nur gestattet ist, wenn unbefugte Aktivitäten durch entsprechende Sicherheitssoftware und ggf. Hardware-Modifikationen mit hinreichender Sicherheit ausgeschlossen werden.

Dokumentation der Veränderungen an Systemsteuerungsprogrammen

Die „Überwachung der ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen“ setzt nicht nur voraus, daß ausschließlich getestete und freigegebene Anwendungssoftware eingesetzt wird, es muß auch gewährleistet sein, daß die Betriebssysteme, die Datenbanksoftware, die Netzwerksteuerungsprogramme usw. nicht unbefugt verändert werden können und damit die Gefahr besteht, daß maschinelle Ergebnisse verfälscht werden. Es sollte daher den datenverarbeitenden Stellen auf dem Verordnungswege zur Pflicht gemacht werden, alle Veränderungen an dem Betriebssystem und der sogenannten systemnahen Software zu dokumentieren. Bezogen auf Großsysteme handelt es sich insoweit um eine Selbstverständlichkeit, da hier die Systemprotokollierung seit jeher (auch aus Abrechnungsgründen) sehr ausgeprägt ist.

Bei Datenverarbeitungsgeräten auf der Basis der Betriebssysteme „MS-DOS“ und „UNIX“ sind derartige Protokollfunktionen bisher nur sehr schwach ausgeprägt. Eine entsprechende Verpflichtung der Behörden würde einen „heilsamen Zwang“ auf die Anbieter und Betreiber von EDV-Systemen dieser Kategorie führen.

Verschlüsselung von Datenbeständen

In dem Maße, in dem EDV-Systeme kleiner und leichter werden, steigt auch die Diebstahlsgefährdung. Bei Großsystemen war es zwar möglich, sich große Datenbestände durch Diebstahl der Datenträger anzueignen. Die jeweiligen Datenbanken auszuwerten war jedoch nur Spezialisten möglich. Die Entwendung eines tragbaren PC oder eines „NOTEBOOK“ führt

jedoch dazu, daß dem Dieb gleichzeitig auch die Auswertungsprogramme zur Verfügung stehen.

Sofern die Speicherung personenbezogener Daten auf derartigen Geräten unvermeidlich ist (z.B. bei Außenprüfern), sollte die Verschlüsselung der Datenbestände zur Pflicht gemacht werden. Andererseits sollte ausgeschlossen werden, daß Mitarbeiter Verwaltungsdaten ohne Genehmigung verschlüsseln. Die datenverarbeitenden Stellen müssen in jedem Fall über den Entschlüsselungscode verfügen, um bei Ausfall und zur Kontrolle des Mitarbeiters selbst eine Entschlüsselung der Datenbestände vornehmen zu können.

Mindestanforderungen an die Dokumentation automatisierter Datenverarbeitungsverfahren

Seit mehreren Jahren führt der Landesbeauftragte Prüfungsmaßnahmen bei den datenverarbeitenden Stellen im Lande nach einem einheitlichen Raster durch, um einen repräsentativen Überblick über den Stand der Sicherheit und Ordnungsmäßigkeit der automatisierten Datenverarbeitung zu erhalten. Auf der Basis der bisher abgeschlossenen Prüfungen läßt sich die Dokumentationspraxis der Behörden im Lande wie folgt beschreiben:

- Die bis vor wenigen Monaten gültigen Dokumentationsvorschriften der „Gemeinsamen Geschäftsanweisung für die EDV in der Landesverwaltung“ sind von den Landesbehörden nur ansatzweise eingehalten worden. Im kommunalen Bereich und bei den sonstigen Körperschaften des öffentlichen Rechts haben sie faktisch keine Beachtung gefunden.
- Interne Dokumentationsrichtlinien bestehen nur bei sehr wenigen Behörden. In der Regel sind sie von den Datenverarbeitungsabteilungen selbst formuliert und lassen weitgehende Ausnahmen und Ermessensspielräume zu.
- Richtlinienentwürfe kann man allerdings häufiger vorfinden. Ihnen ist gemein, daß in der Regel ein sehr grundsätzlicher Ansatz gewählt wird, daß aber die Umsetzung in die Realität der betreffenden Behörde nicht mit der erforderlichen Konsequenz vollzogen ist.
- Keine der geprüften Stellen benutzte eine Dokumentationsmethode, die mit der einer anderen Behörde zumindest überwiegend identisch war.
- In den meisten größeren Rechenzentren wurde nicht einmal in einer einheitlichen Art und Weise dokumentiert.
- Besondere Schwächen waren bezüglich der Aufbereitung der Testunterlagen festzustellen. Bei fast allen überprüften Verfahren waren die Testfälle weder beschrieben noch waren die Ergebnisse aufbereitet.
- Versuche, die Ursachen für festgestellte fehlerhafte Verarbeitungen anhand der Programm- und Verfahrensdokumentationen zu analysieren, blieben in der Regel erfolglos.

Man wird sich also die Frage stellen müssen, ob nicht ein anderer Lösungsansatz als bisher gewählt werden sollte, um zu konkreten Ergebnissen zu gelangen. Weil es offenbar schwierig ist, die Form der EDV-Dokumentation verbindlich vorzuschreiben, sollte man deren Zielrichtung festlegen und von dem Ziel auf den Inhalt schließen. Als Muster können die Regelungen im Landesdatenschutzgesetz dienen. Die Gebote zur Datensicherheit strukturieren den Gesamtkomplex und geben für die Teilbereiche Zielvorgaben. Auch sie sind also ziel- und nicht formorientiert. Der Landesbeauftragte hat dem Innenminister insoweit detaillierte Vorschläge unterbreitet.

Regelungen zur formalen Darstellung von Verfahrensdokumentationen

Die rasante Entwicklung der Informationstechnik und der exponentielle Anstieg des Software-Volumens wird in den nächsten Jahren völlig neue Problemstellungen für die Dokumentation mit sich bringen.

Das Mengenproblem führt z.B. dazu, daß an die Stelle der papierernen Dokumentationen zunehmend Dokumentationen auf anderen Speichermedien treten. Die Speicherung der Daten auf elektronischen Datenträgern, die Digitalisierung von Dokumenten, das Einstellen in Datenbank-Systeme (Schlagwort: Datenbank dokumentiert Datenbank) haben unmittelbar Einfluß auf die Nutzbarkeit der Dokumentationen, denn es bedarf spezieller Programme und Kenntnisse, um die Daten sichtbar zu machen und Zugriffe auf bestimmte Dokumente zu ermöglichen.

Es erscheint daher nicht vertretbar, für die Dokumentation von IT-Maßnahmen grundsätzlich alle Darstellungsformen zuzulassen. Eine zu große „Sprachenvielfalt“ steigert den Prüfungsaufwand ins Unvertretbare. Die Entscheidung, welche Programmiersprachen, Betriebssysteme, Darstellungsformen für IT-Dokumentationen usw. zulässig sein sollen, kann nur für die gesamte öffentliche Verwaltung im Lande einheitlich getroffen werden.

In der Verordnung sollte daher ein Genehmigungsverfahren durch die jeweiligen obersten Fachaufsichtsbehörden festgeschrieben werden. Diese Behörden sollten gehalten sein, die Bandbreite der technikgestützten Dokumentationsmethoden zu begrenzen. Der Landesrechnungshof und der Landesbeauftragte für den Datenschutz sollten vor der Genehmigung einer neuen Methode gehört werden.

Festlegung von Aufbewahrungsfristen für Dokumentationsunterlagen

Die Frage nach der Aufbewahrungsdauer von Dokumentationsunterlagen läßt sich in der Theorie eindeutig beantworten: Sie sind so lange vorzuhalten, wie die mit den betreffenden Verfahren erzeugten Dateninhalte gespeichert sind; erst nach

dem Löschen der Daten besteht definitiv kein Bedarf mehr an einer Revision des Zusammenspiels zwischen den Vorgaben, den Daten, der Hard- und der Software, die diese Daten „erzeugt“ haben.

Für Verfahren, deren Datenbestände ausschließlich in automatisierten Dateien gespeichert werden, sollte diese maximale Speicherdauer daher vorgeschrieben werden. In dem Maße, wie die Datenbestände und Datenverarbeitungsprozesse anhand von visuell lesbaren Dokumenten nachvollzogen werden können, besteht die Möglichkeit, die Aufbewahrungsfristen für die Dokumentationen der automatisierten Verfahren zu verkürzen. Die Zuständigkeit hierfür sollte bei den obersten Fachaufsichtsbehörden liegen.

Ausblick

Der Landesbeauftragte geht davon aus, daß es zu eingehenden Erörterungen über die Einzelheiten der künftigen Landesverordnung auch mit den Interessenvertretern der Datenverarbeiter kommen wird. Dabei werden sich noch weitere Regelungsnecessitäten ergeben. Er hofft sehr darauf, daß Schleswig-Holstein das erste Bundesland sein wird, in dem die öffentliche Verwaltung die automatisierte Datenverarbeitung nach einheitlichen Ordnungsmäßigkeitskriterien gestaltet. Damit besteht die Chance, daß den besonderen Gefährdungen des informationellen Selbstbestimmungsrechts durch die zunehmende Automatisierung der Datenverarbeitung jedenfalls insoweit wirksam begegnet wird.

6.2 IT-Verfahrensregelung – Verwaltungsanweisung mit Schlupfloch

Es wurde wirklich Zeit, daß die aus dem Jahre 1971 stammende, mithin 20 Jahre alte „gemeinsame Geschäftsanweisung für die elektronische Datenverarbeitung in der Landesverwaltung“ (GEDV) an die heutigen Gegebenheiten der Informationsverarbeitung und den aktuellen Stand der Kommunikationstechniken angepaßt wurde. Da der Landesbeauftragte sehr frühzeitig vom Innenminister in die Beratungen über eine neue „Regelung zur Gestaltung von Maßnahmen im Bereich der Informationstechnik (IT-Verfahrensregelung)“ einbezogen wurde und zumindest ein Teil seiner Vorschläge auch ihren Niederschlag in dieser neuen Verwaltungsanweisung gefunden haben, hätte er eigentlich Grund gehabt, sie als zwar längst überfällig, im Ergebnis aber doch als gut und richtig zu bezeichnen.

Leider hat sie einen bedauernswerten „Geburtsfehler“. Sie beginnt mit einer Ausnahmeregelung, die ihr den Charakter von Mindestanforderungen nimmt und sie zu einer Art Rah-

menrichtlinie herabstuft. Den Behörden ist es nämlich gestattet, daß sie von der IT-Verfahrensregelung abweichen können, „soweit ihre Beachtung einen Aufwand verursachen würde, der außer Verhältnis zu den Kosten und der Bedeutung der IT-Maßnahme stünde“. Für eine Abweichung bedarf es nicht einmal der Genehmigung durch die oberste Fachaufsichtsbehörde oder die IT-Kommission, sie ist nur schriftlich festzuhalten und zu begründen.

Da bereits die gemeinsame Geschäftsanweisung aus dem Jahre 1971 von vielen Behörden nur partiell beachtet worden ist (vgl. Textziffer 6.1.2 dieses Berichtes), fürchtet der Landesbeauftragte, daß die IT-Verfahrensregelung unter Berufung auf diesen Ausnahmetatbestand das gleiche Schicksal erleidet.

Es stellt sich nämlich die Frage, warum die Kosten und die Bedeutung einer IT-Maßnahme ein Maßstab dafür sein können, in welcher Art und Weise diese Maßnahme geplant und realisiert wird. Zumindest für die datenschutzrechtlich relevanten Teile der IT-Verfahrensregelung kann der Kostenfaktor nicht herangezogen werden. Der Umfang der Aktivitäten der datenverarbeitenden Stellen zum Nachweis der datenschutzrechtlichen Zulässigkeit der mit der IT-Maßnahme beabsichtigten (rationelleren) Verarbeitung personenbezogener Daten, zur Festlegung und Dokumentation der Datensicherungsmaßnahmen, zur Bestimmung der Aufbewahrungs- und Löschungsfristen, für den Test und die Freigabe von Verfahren usw. sind nicht von dem damit verbundenen Aufwand abhängig, sondern richten sich nach dem Schutzbedürfnis der verarbeiteten Daten bzw. ergeben sich aus den Datenschutzrechten der Betroffenen. Könnte ein Automationsvorhaben nur dann „wirtschaftlich“ gestaltet werden, wenn auf Datenschutzmaßnahmen verzichtet wird, so müßte es als unzulässig angesehen und auf seine Einführung verzichtet werden. Es wäre deshalb zu begrüßen gewesen, wenn die Ausnahmeregelung auf rein formale Aspekte der Verfahrensentwicklung (Zusammenfassung von Analysephasen und dergleichen) begrenzt worden wäre.

Der Landesbeauftragte geht davon aus, daß diese Schwachstelle durch die von der Landesregierung zu erlassende Landesverordnung über die „Einzelheiten einer ordnungsgemäßen Datenverarbeitung durch öffentliche Stellen“ (vgl. Tz. 6.1.1 dieses Berichtes) geheilt wird.

6.3 Wer bildet EDV-Verantwortliche aus?

Noch vor wenigen Jahren konzentrierte sich die automatisierte Datenverarbeitung der öffentlichen Verwaltung im Lande auf kaum mehr als fünfzig mittlere und große Rechenzentren. Dementsprechend gering war auch der Bedarf an „EDV-Verantwortlichen“. Bei den Leitern von Programmierabteilungen, den Chef-Systemprogrammierern und den Rechenzentrumsleitern handelte es sich um speziell ausgebildete, erfahrene

Mitarbeiter, die ihren Verantwortungsbereich in der Regel hauptamtlich leiteten. Ihnen waren Programmierer, Systembetreuer, Operatoren usw. zugeordnet, die ihre Aufgaben auf Weisung unter der Kontrolle dieser Spezialisten zu erledigen hatten. Die EDV-Bereiche waren mithin in der gleichen Weise strukturiert wie die übrige Verwaltung, es gab eine operative (sachbearbeitende) Ebene und einen administrativen (anweisenden und kontrollierenden) Überbau.

Als Folge der technologischen Entwicklung ist in den vergangenen Jahren eine explosionsartige Dezentralisierung von Datenverarbeitungssystemen zu verzeichnen. Bereits im Jahr 1985 hat deshalb der Landesbeauftragte auf die Problematik der „Datenbanken in Westentaschenformat“ hingewiesen (vgl. 7. TB, S. 55). In der Zwischenzeit dürften im Lande weit mehr als 500 „Mini-Rechenzentren“ entstanden sein.

Jeder Abteilungsrechner, jedes PC-Netz und jede „Client-Server-Konfiguration“ braucht nämlich die gleichen Funktionen wie ein ausgewachsenes Rechenzentrum. Es muß jemanden geben, der sich im Betriebssystem auskennt, jemanden der die Datenträger verwaltet, der Programme (man spricht neuerdings von Reports, Relationen oder Auswertungen) erstellt, testet und implementiert, jemanden der Zugriffs- und Änderungsbefugnisse für Daten erteilt, der die Benutzer an den Terminals einweist und sie berät usw., usw. Außerdem muß es natürlich jemanden geben, der diese Aktivitäten initiiert, koordiniert und überwacht. Da all diese Arbeiten wegen des vergleichsweise geringen Umfangs der Hardware und der automatisierten Verfahren nicht einen „Full-time-job“ rechtfertigen, werden sie den betreffenden Mitarbeitern zusätzlich zu ihrer Hauptaufgabe übertragen. Dabei tritt ein überraschender Effekt ein: Der sachbearbeitenden Ebene muß man gezwungenermaßen ein umfassendes Fachwissen vermitteln, weil ohne die entsprechenden Kenntnisse die eingesetzten Hardware- und Softwarekomponenten nicht die gewünschten Ergebnisse erbringen. Dies ist für die anweisende und kontrollierende Ebene vermeintlich nicht im gleichen Maße erforderlich, solange die Verfahren zufriedenstellend laufen. Der durch andere Aufgaben ohnehin überlastete Referent, Amtsleiter usw. ist häufig gar nicht böse darüber, daß er nicht noch einmal die Schulbank drücken muß. Er selbst drängt sich nicht auf, seine Mitarbeiter drängen ihn nicht, es gibt keine Ausbildungsinstitution, die ihn mit maßgeschneiderten Angeboten veranlaßt, sich die Kenntnisse anzueignen, die erforderlich sind, um der ihm übertragenen Verantwortung wirklich gerecht werden zu können.

Ein Schlaglicht mag die Konsequenzen deutlich machen: Die Betriebssysteme MS-DOS und UNIX sind sicher hundertfach im Lande im Einsatz. Es gibt nach Kenntnis des Landesbeauftragten aber bis heute kein Programm, welches Veränderungen an dieser wichtigsten Komponente eines Computersystems zwangsdokumentiert und so aufbereitet, daß jemand, der nicht ausgebildeter Systemprogrammierer ist, die Gehehnisse nachvollziehen kann. Offensichtlich hat noch kein

DV-Verantwortlicher dies von seinem Computer-Lieferanten gefordert. Möglicherweise ist man sich mangels hinreichenden Fachwissens der Tatsache gar nicht bewußt, daß auf diese Weise in der Verwaltung immer größere revisionsfreie Bereiche entstehen.

Der Landesbeauftragte hat diese Situation in Beratungsgesprächen und, wenn er sie bei Prüfungen vorgefunden hat (vgl. Tz. 6.4.3), stets kritisiert. Aus seiner Sicht ist es dringend geboten, daß sich die IT-Kommission des Landes, die Automationskommission der kommunalen Landesverbände, die Datenzentrale und die Hersteller und Vertreiber von Computersystemen an einen Tisch setzen, um ein praktikables Konzept zu entwickeln. Er selbst ist bereit, die Vermittlung des datenschutzrechtlichen „Know-how“ in einem solchen Ausbildungsgang zu übernehmen.

6.4 Kontrollen und Prüfungen

6.4.1 Das Programm, das es gar nicht gab

Auch den Profis in großen Rechenzentren unterlaufen Unachtsamkeiten, die weitreichende datenschutzrechtliche Konsequenzen zur Folge haben können. Dies dokumentierte sich in einem Sachverhalt, auf den der Landesbeauftragte durch die Beschwerde eines Mitarbeiters einer solchen Dienststelle hingewiesen wurde.

Das Rechenzentrum setzt seit längerer Zeit ein gekauftes, sehr umfangreiches Programmpaket zur Erstellung von Vordrucken, Grafiken usw. ein. Bestandteil dieses Produktes ist auch ein sogenannter Texteditor, ein Programm, mit dem Texte erstellt, verändert und gespeichert werden können. Da standardmäßig ein anderer Editor benutzt wird, fiel das Vorhandensein eines zusätzlichen, gleichartigen Programms niemandem auf. Es war praktisch unbekannt, leider aber nicht allen Mitarbeitern. Eine Mitarbeiterin fand das „schlummernde“ Programm, als sie mit dem Gesamtpaket arbeitete, probierte es aus und setzte es ein, weil es ihr besser gefiel als der offizielle Editor. Sie dachte aber nicht daran, daß die von ihr erzeugten Texte mit Informationen über Mitarbeiter (brisante Personaldaten) in einer Datei abgelegt wurden, die – da der Systemprogrammierung nicht bekannt – nicht in die allgemeine Zugriffsüberwachung einbezogen war. So konnte ein größerer Kreis von Kollegen unbemerkt auf diese Personaldaten zugreifen. Dies geschah in der Tat, als man sich in der Systemprogrammierung über die Größe einer Datei wunderte, die es eigentlich gar nicht hätte geben dürfen. Disziplinarische und arbeitsrechtliche Auseinandersetzungen waren die Folge.

Zwischen der Rechenzentrumsleitung und dem Landesbeauftragten bestand kein Dissens darüber, daß hier ein datenschutzrechtlicher Mangel vorlag. Das Rechenzentrum war gesetzlich verpflichtet, „die ordnungsgemäße Anwendung der Datenver-

arbeitungsprogramme zu überwachen". Dies kann aber nur geschehen, wenn alle einsetzbaren Programme registriert sind. In diesem Fall wurde der Editor zwar in den Bestand übernommen, aber dann nicht weiter beachtet und die Nutzung nicht überwacht. Das Beispiel macht die praktische Relevanz der im neuen Landesdatenschutzgesetz festgeschriebenen Pflicht deutlich, für jedes Betriebssystem auch ein Programmverzeichnis zu führen.

Der Leiter des Rechenzentrums hat die Nutzung des Editors für die Verarbeitung personenbezogener Daten sofort untersagt und die „ungewollten“ Daten gelöscht. Dies führte zu neuen Problemen, denn in der arbeitsrechtlichen Auseinandersetzung spielten auch die Dateninhalte eine Rolle. Ein Mitarbeiter wollte die Informationen als Beweismittel verwertet wissen und fühlte sich durch die Löschung in seinen Rechten beeinträchtigt. Jetzt zeigte sich, welche Bedeutung die sogenannten Datensicherungsbestände erhalten können, die zur Rekonstruktion von Magnetplatten bei Hardwarefehlern angelegt werden. Da die entsprechenden Magnetbandkassetten noch nicht überschrieben waren, war es möglich, aus den Datensicherungskopien, die bereits gelöschten Daten zu rekonstruieren und den Mitarbeiter insoweit zufriedenzustellen.

6.4.2 Für Akten weniger Datensicherung als für Datenbanken?

Im Rahmen der Überprüfung von Datensicherungsmaßnahmen bei der Landesversicherungsanstalt Schleswig-Holstein ist dem Landesbeauftragten ein Zugriffsüberwachungssystem für die in Datenbanken gespeicherten Sozialversicherungsdaten präsentiert worden, dessen Konzeption weit über das hinausgeht, was bei vergleichbaren Stellen im Lande realisiert worden ist. Jeder der 120 Bildschirmarbeitsplätze ist mit einem Magnetstreifenlesegerät ausgestattet. Den Mitarbeitern, denen eine Zugriffsberechtigung auf das Rechnersystem gewährt werden soll, wird eine Magnetstreifenkarte ausgehändigt, auf der ihre Benutzerkennung codiert gespeichert ist. Die Aktivierung der Terminals ist nur mittels dieser Magnetstreifenkarte möglich. Ihr Inhalt wird gegen eine Datei der gültigen Benutzerkennungen abgeglichen. Verlorengegangene Karten oder Karten von Mitarbeitern, die längere Zeit abwesend sind, werden gesperrt.

Nachdem die Codierung vom System gelesen und akzeptiert worden ist, muß ein individuelles Passwort eingegeben werden, anhand dessen geprüft wird, ob die Karte auch von dem Mitarbeiter benutzt wird, für den sie ausgestellt worden ist. Das ist möglich, weil das Passwort nur dem rechtmäßigen Benutzer bekannt ist (verschlüsselte Speicherung) und nur von ihm geändert werden kann. Nach einem erfolgreichen Einloggen stehen dem Mitarbeiter nur die Versicherungsnummernkreise und die Systemfunktionen (Lese- bzw. Schreibberechtigung) zur Verfügung, die in einer speziellen Befugnisdatei für ihn definiert sind. Änderungen der Befugnisdatei sind nur

besonders beauftragten Mitarbeitern möglich. Die Eingabe, Überprüfung und Änderung wichtiger Versicherungsdaten wird benutzerbezogen dokumentiert.

Diesem technisch durchaus vorbildlichen Verfahren steht die Tatsache gegenüber, daß die ca. 750.000 Versicherungsakten, die neben den eigentlichen Sozialversicherungsdaten teilweise auch „hochsensible“ medizinische Daten enthalten, in der Landesversicherungsanstalt in unverschlossenen Regalen gelagert werden. Hinzu kommt, daß zum Zeitpunkt der Prüfung das Gebäude der Landesversicherungsanstalt während der Geschäftszeiten Besuchern zugänglich war.

Der Landesbeauftragte hat sich auf den Standpunkt gestellt, daß bei gleichen Dateninhalten Akten und automatisierte Dateien auch in vergleichbarer Weise zu schützen sind. Besonders Akten, deren Inhalt einem besonderen Berufs- und Amtsgeheimnis unterliegt, in diesem Fall sind es Sozial- und medizinische Daten, sind seines Erachtens so zu verwahren, daß sie Unbefugten nicht in die Hände gelangen können. Er hat die Landesversicherungsanstalt deshalb aufgefordert, für den Gesamtbestand verschließbare Behältnisse anzuschaffen und die Mitarbeiter anzuweisen, nach Dienstschluß und bei längerer Abwesenheit einen „sauberen Schreibtisch“ zu hinterlassen.

Die Landesversicherungsanstalt ist dieser Aufforderung nicht gefolgt. Sie sieht die derzeitige Lösung zwar auch nicht als „optimal“ an. Sie hat aber nur die Absicht bekundet, „im Rahmen der z.Z. laufenden Planungen für einen Neu- bzw. Ergänzungsbau für die Auskunftsstelle einen Bereich zu schaffen, der gegenüber den übrigen Diensträumen abgeschottet werden kann“. Einen Zeitpunkt für die Realisierung der verbesserten Abschottungsmaßnahmen hat sie nicht genannt. Einen „sauberen Schreibtisch“ bei allen Mitarbeitern einzuführen, würde nach ihrer Meinung einen zu großen Kosten- und Personalaufwand erfordern.

Dieser Auffassung kann sich der Landesbeauftragte beim besten Willen nicht anschließen. Er sieht in einer solchen Art der Aktenhaltung ein grundsätzliches Problem. Wenn besondere Berufs- und Amtsgeheimnisse tatsächlich Wirkung entfalten sollen, sind in der Verwaltung einheitliche Maßstäbe für ihre Sicherung anzulegen. Welchen Sinn machen technisch ausgereifte Zugangskontrollsysteme für automatisierte Dateien, wenn nebenan die Akten mit den Originaldokumenten in offenen Regalen oder auf Aktenböcken lagern? Nachdem nunmehr auch die Verarbeitung personenbezogener Daten in Akten seiner Kontrolle unterworfen ist, wird er sich mit Nachdruck dafür einsetzen, daß derart „sensible“ Datenbestände grundsätzlich unter Verschuß gehalten werden. Diese Vorsichtsmaßnahme sollte nicht nur bei Sozialleistungsträgern, sondern auch in Finanzämtern, Gesundheitsämtern, Statistikstellen usw. strikt beachtet werden.

Zwar werden die Datensicherungsmaßnahmen für Akten naturgemäß anders aussehen als bei automatisierten Dateien, das Sicherheitsniveau muß aber gleichwertig sein, damit ein ins-

gesamt stimmiges und überzeugendes Sicherheitskonzept realisiert wird.

6.4.3 Datensicherungsmaßnahmen – Wer entscheidet tatsächlich?

Mehrere Landkreise setzen automatisierte Verfahren ein, um die Festsetzung und – wie es verwaltungstechnisch heißt – die „Zahlbarmachung“ von Sozialleistungen zu beschleunigen. In diesem Zusammenhang werden in den Büros in der Regel PC installiert, die über ein behördeninternes Leitungsnetz mit einem sog. Server (eine Art Abteilungsrechner) verbunden sind. Auf diese Weise steht den Bearbeitern Rechnerkapazität unmittelbar am Arbeitsplatz zur Verfügung und gleichzeitig können auf dem Server zentrale Datenbestände geführt werden.

Da ihm die Verarbeitung von Daten, die dem Sozialgeheimnis unterliegen, in einem PC-Netz unter Sicherheitsaspekten nicht ganz unproblematisch erschien, hat der Landesbeauftragte bei einem Kreis die dort realisierten technischen und organisatorischen Maßnahmen einer Prüfung unterzogen. Dabei stellte sich heraus, daß das automatisierte Sozialhilfeverfahren selbst aufgrund einer Reihe verfahrensspezifischer Besonderheiten in der Tat keinen Anlaß zu grundsätzlichen Beanstandungen gab. Dem Verfahren liegt folgendes Konzept zugrunde: Die im Bereich der Sachbearbeitung eingesetzten PC verfügen nicht über ein funktionsfähiges Diskettenlaufwerk. Auf den Magnetplatten der PC werden keine Datenbestände geführt. Alle Datenbanken befinden sich auf dem Server. Die Betriebssysteme und Anwendungsprogramme werden durch den Systembetreuer vom Server auf die Terminals überspielt. Ein Zugriff von den Terminals auf die Betriebssystemebene des Servers ist nicht möglich. Die einzelnen zu verarbeitenden Datensätze werden vom Server auf die jeweiligen Terminals übertragen und nach den entsprechenden Änderungen/Ergänzungen dorthin zurückgespielt. Die Benutzung der Terminals ist erst nach Eingabe eines gültigen Passwortes möglich. Sollte sich ein Benutzer aufgrund spezieller Kenntnisse tatsächlich Zugang zur Betriebssystemebene seines Terminals verschaffen, könnten eventuelle Manipulationen nur Auswirkungen auf den eigenen Arbeitsplatz haben. Veränderungen an Programmen, mit denen andere Mitarbeiter arbeiten, und an Daten, für die sie verantwortlich zeichnen, sind nicht möglich. Die Prüfung hat keine Anhaltspunkte dafür ergeben, daß die Restriktionen ohne ein erhebliches Maß an krimineller Energie ausgeschaltet werden können.

Die Datenverarbeitungsorganisation des Kreises insgesamt und die Ausgestaltung anderer automatisierter Verfahren veranlaßten den Landesbeauftragten allerdings zu Beanstandungen und zu Vorschlägen zur Verbesserung des Datenschutzes. Dabei stieß er auch in dieser Behörde auf ein Problem, das für kleinere und mittlere Datenverarbeitungs-Organisationsein-

heiten typisch ist: Die Verantwortungskonzentration auf der sachbearbeitenden Ebene. Wenn einem EDV-Sachbearbeiter folgende Aufgaben übertragen werden:

- Systemanalyse,
- Hardware- und Software-Auswahl,
- Hardware-Installation,
- Generierung des Betriebssystems und der systemnahen Software,
- Entwicklung von Anwendungssoftware,
- Software-Implementierung,
- Operating und Datensicherung,
- Schulung und Beaufsichtigung der Mitarbeiter im EDV-Bereich,
- Schulung der Systembenutzer,
- Datenschutzsachbearbeitung,

wenn ihm zudem kein ständiger Vertreter zur Seite gestellt wird, wenn er diesen Gesamtkomplex darüber hinaus neben seiner eigentlichen Hauptaufgabe zu bearbeiten hat und wenn schlußendlich der ihm vorgesetzte Amtsleiter nicht über das Maß an EDV-Fachkompetenz verfügt, das für eine effektive „entlastende Kontrolle“ erforderlich ist (vgl. Tz. 6.3 dieses Berichtes), ist es nicht verwunderlich, daß wichtige systemtechnische Entscheidungen von ihm unter Zeitdruck und allein getroffen werden (müssen).

Es waren zwar in diesem konkreten Fall die meisten der konzeptionellen Entscheidungen datenschutzrechtlich nicht zu beanstanden, die grundsätzliche Problematik dieser Vorgehensweise wird jedoch an drei Beispielen deutlich:

- Seit 1988 sind von der geprüften Stelle Hardware- und Software-Investitionen in der Größenordnung von ca. 1.000.000 DM getätigt worden. Aus kleinsten Anfängen hat sich in wenigen Jahren ein PC-Netz mit ca. 80 Terminals entwickelt. Da die gesamte Planung, Realisierung und auch der Betrieb durch eine Person „gemanagt“ wurde, lagen zum Zeitpunkt der Prüfung weder ein authentischer Konfigurationsplan, noch irgendwelche Dienstsanweisungen (Soll-Regelungen) für die Handhabung des Systems vor (hätte der Sachbearbeiter sich selbst anweisen sollen?).
- Eine Reihe von vernetzten PC sind mit lauffähigen Diskettenstationen ausgerüstet. Wie in der Fachliteratur, vom Innenminister, von der Datenzentrale und vom Landesbeauftragten in vielfacher Form dargestellt, birgt eine solche Konfiguration erhebliche Sicherheitsrisiken (Zugriff auf das Betriebssystem, Virengefahr usw.), die nur durch eine entsprechende Sicherheitssoftware in den Griff zu bekommen sind. Auf die Beschaffung einer solchen Software wurde jedoch aus Kostengründen verzichtet. Die Alternative, auch diese Diskettenlaufwerke zu deaktivieren, wurde nicht näher untersucht. Aus den bei der Prüfung vorgefundenen Unterlagen ergab sich nicht, daß der Leitungsebene der Behörde dieses Sicherheitsproblem überhaupt bekannt war,

die Entscheidung ist jedenfalls auf der sachbearbeitenden Ebene gefallen.

- Wenige Tage nach Beendigung der Prüfungsmaßnahme hat der EDV-Sachbearbeiter der geprüften Stelle sich beruflich verändert. Ein eingearbeiteter Nachfolger stand zu diesem Zeitpunkt nicht zur Verfügung. Die Behörde sah sich genötigt, mit dem ausgeschiedenen Mitarbeiter einen Beratungsvertrag abzuschließen, um sein Fachwissen (zutreffender eigentlich: sein Exklusivwissen) zumindest noch für eine Übergangszeit nutzen zu können.

Der Landesbeauftragte hat diese und andere Sachverhalte beanstandet, weil die im Landesdatenschutzgesetz vorgeschriebene „Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme“ nicht in ausreichendem Maße stattgefunden hat.

6.4.4 Der dornenreiche Weg bei der Behebung von Mängeln

In seinem 13. Tätigkeitsbericht (S. 73) hat der Landesbeauftragte über eine umfassende Prüfungsmaßnahme bei der Datenzentrale Schleswig-Holstein aus dem Jahre 1990 berichtet. Er hat die beanstandeten Schwachstellen und die Tatsache dargestellt, daß mit der Datenzentrale ein weitgehendes grundsätzliches Einverständnis über die erforderlichen Maßnahmen zur Verbesserung des Datenschutzes besteht. Dieser Berichtsteil endete mit der Formulierung: „Der Landesbeauftragte erwartet eine recht kurzfristige Abstellung der Mängel und hofft, daß er in seinem nächsten Tätigkeitsbericht schildern kann, in welcher Form die von ihm vorgeschlagenen Maßnahmen ihren Niederschlag in der täglichen Praxis der Auftragsdatenverarbeitung gefunden haben“. Leider muß er am Ende dieses Berichtszeitraums feststellen, daß sich mehr als zwei Jahre nach Abschluß der Prüfung alle wesentlichen Änderungsmaßnahmen noch immer in der Planungs- bzw. in der Entscheidungsphase befinden.

In seinen regelmäßigen Gesprächen mit der Datenzentrale hat der Landesbeauftragte den Eindruck gewonnen, daß an der Umsetzung seiner Vorschläge in die Praxis durchaus mit der gebotenen personellen Kapazität gearbeitet wird, immerhin sind zwei Mitarbeiter der Datenzentrale allein für die Koordination abgestellt. Aus seiner Sicht macht der lange Zeitraum bis zu ihrer Realisierung deutlich,

- daß die auch von der Datenzentrale als richtig erachteten datenschutzrechtlichen „Verbesserungsvorschläge“ unerwartet weitreichende Auswirkungen auf die organisatorischen Strukturen und Abläufe innerhalb der Datenzentrale haben und
- daß dieser Umstellungsaufwand und die damit verbundenen nicht unerheblichen Kosten hätten vermieden werden können, wenn die entsprechenden Überlegungen sehr viel früher angestellt worden wären.

Auf diesen Aspekt weist der Landesbeauftragte auch immer wieder hin, wenn ihm Verfahrenskonzepte zur datenschutzrechtlichen Begutachtung vorgelegt werden oder wenn er von ihnen im Rahmen der Beratungen der IT-Kommission des Landes bzw. der Automations-Kommission der kommunalen Landesverbände Kenntnis erhält. Die Klärung der datenschutzrechtlichen Fragestellungen und eine verfahrensspezifische Technikfolgenabschätzung müssen bereits in einem sehr frühen Planungsstadium erfolgen. Die Festschreibung nicht hinreichend geprüfter Verarbeitungsprozesse führt oft nicht nur zu sicherheitstechnischen Risiken und zu rechtlich bedenklichen Verfahrensweisen, die dann nachträglich erforderlich werdenden Änderungen sind in der Regel auch extrem kostenintensiv (vgl. 13. TB, S. 7).