ELFTER TÄTIGKEITSBERICHT

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

nach § 19 Absatz 3 des Gesetzes zum Schutz
vor Mißbrauch personenbezogener Daten
bei der Datenverarbeitung
vom 1. Juni 1978

(Berichtszeitraum: März 1988 bis Februar 1989)

Inhaltsverzeichnis

		Seite
1.	**Die Reorganisation des Datenschutzes setzt Zeichen für einen Neuanfang**	7
2.	**Beratung des Tätigkeitsberichtes erstmals auf breiterer parlamentarischer Basis**	9
3.	**Technik und Recht driften auseinander**	10
4.	**Sorgen der Bürger, Beratung der Behörden, Feststellungen und Wertungen**	11
4.1	Allgemeine und innere Verwaltung	11
4.1.1	Meldewesen	11
4.1.1.1	Adoptionsgeheimnis - der Weg eines unbürokratischen Vorschlags	11
4.1.1.2	Verarbeitung von Meldedaten und ihre Dokumentation	12
4.1.2	Personalwesen	12
4.1.2.1	Telefondatenerfassung – Zielnummern werden endlich verschleiert	12
4.1.2.2	Eignungstests durch private Personalberater	13
4.1.2.3	Die datenschutzrechtliche Problematik einer Urteilsbekanntgabe	14
4.1.2.4	Verhaltenskontrolle – der Datenschutz setzt sehr früh an	14
4.1.3	Datenschutz im Kommunalbereich	15
4.1.3.1	Kommunale Vertretungskörperschaften und Datenschutz	15
4.1.3.2	Noch immer Probleme bei der Erhebung und Nutzung von Daten	16
4.1.3.3	Volkszählung – zum Schluß doch noch ein schwerwiegender Verstoß	17

		Seite
4.1.4	Personalausweis- und Paßwesen	18
4.1.4.1	Probleme bei der Ausgabe der neuen Personalausweise	18
4.1.4.2	Die Gesetzessprache und ihre praktische Umsetzung	19
4.1.5	Personenstandswesen	20
4.1.6	Verfassungsschutz	21
4.1.6.1	Sicherheitsrichtlinien mit Schwachstellen	21
4.1.6.2	Dateien wurden rigoros „abgespeckt“	22
4.1.6.3	Bundesinnenminister gewährleistet Zugriff auf Dokumentation	23
4.1.7	Öffentliche Sicherheit und Ordnung	24
4.1.7.1	Polizei löscht mehr Daten als vom Landesbeauftragten gefordert	24
4.1.7.2	„Automatische“ Datenweitergaben an den Verfassungsschutz	25
4.1.7.3	Wie weit wirkt die Immunität der Abgeordneten?	25
4.1.7.4	Bewerber für den Polizeidienst werden nicht mehr heimlich überprüft	26
4.1.7.5	Der Presse dürfen keine Namenskürzel mehr mitgeteilt werden	27
4.1.7.6	Hinweise auf AIDS nun doch in den Polizeidateien gelöscht	28
4.1.7.7	Die Polizei als Auge und Ohr der Ordnungsbehörden	28
4.1.8	Probleme mit dem Entwurf zum Ausländerzentralregistergesetz	29
4.1.9	Bau- und Vermessungswesen	30
4.1.9.1	Transparenz auch für die „Serviceleistungen“ der Bauaufsichtsbehörden	30
4.1.9.2	Grenzen der Auskünfte aus dem Liegenschaftskataster	31
4.1.9.3	Auch bei einer öffentlichen Planfeststellung sind persönliche Daten zu schützen	31
4.2	Justizverwaltung	32
4.2.1	Immer wieder – Mißbrauch der Grundbucheinsicht	32
4.2.2	Hilfestellung für privates Handelsregister abgelehnt	33
4.2.3	Interne Dateien doch nicht intern	33
4.2.4	Verfassungsgericht „kippt“ die Veröffentlichung von Entmündigungen – neues Gesetz in Vorbereitung	34
4.3	Steuerverwaltung	35
4.3.1	Sollen die Datenschutzbeauftragten an die Kette gelegt werden?	35
4.3.2	Kontrollmitteilungsverfahren eingestellt	36
4.3.3	Schwierigkeiten mit der Datenbank	37
4.3.4	Der Bundesfinanzhof bestätigt die Auffassung des Datenschutzbeauftragten	37

		Seite
4.4	Wirtschaft und Verkehr	38
4.4.1	Unterstützung der Gerichte durch die Industrie- und Handelskammern	38
4.4.2	Industrie- und Handelskammern sind keine Auskunfteien	38
4.5	Ernährung, Landwirtschaft, Forsten, Fischerei, Natur und Umwelt	39
4.5.1	Gutes tun und darüber reden?	39
4.5.2	Umweltschutz und Persönlichkeitsschutz	39
4.6	Sozial- und Gesundheitswesen	40
4.6.1	Soziales	40
4.6.1.1	Offenbarung von Sozialdaten an den Zahnarzt	40
4.6.1.2	Übervorsichtige Krankenhäuser	41
4.6.1.3	Sozialdatenschutzbeauftragter – Datenschutz für den Bürger vor Ort	41
4.6.1.4	Der Sozialversicherungsausweis – Totalerfassung aller Arbeitnehmer geplant	42
4.6.1.5	Strukturreform im Gesundheitswesen – der Zweck heiligt nicht alle Mittel	42
4.6.2	Gesundheit	43
4.6.2.1	Jugendzahnpflegewettbewerb – bremst der Datenschutz die Eigeninitiative?	43
4.6.2.2	Darf ein Amtsarzt Auskünfte über Prostituierte erteilen?	44
4.6.2.3	Meldungen an den „Beauftragten für die systematische Bekämpfung übertragbarer Krankheiten“	44
4.6.2.4	Unzulässig erhobene Daten müssen vernichtet werden	45
4.6.3	AIDS	46
4.6.3.1	Unzulässigkeit heimlicher AIDS-Tests	46
4.6.3.2	Einwilligung zum AIDS-Test im „Kleingedruckten“	47
4.6.3.3	AIDS-Tests bei Asylsuchenden – nur ein bißchen freiwillig?	47
4.6.4	Krankenhaus	48
4.6.4.1	Staatsanwaltschaft „bluffte“ einen Arzt	48
4.6.4.2	Vorsicht Kamera im Operationssaal	50
4.6.4.3	Wahrung des Patientengeheimnisses in privaten Stiftungen	50
4.7	Kultusbereich	51
4.7.1	Hochschulen erheben Studentendaten ohne Rechtsgrundlage	51
4.7.2	Ein neuer Schülergesundheitsbogen	51

		Seite
4.7.3	Schülerdaten auf privaten Personal-Computern der Lehrer	52
4.7.4	Datenverarbeitung und Datenschutz sollen im Schulgesetz geregelt werden	52
4.7.5	Endlich ein Archivgesetz in Aussicht?	53
5.	**Prüfungen**	54
5.1	Prüfung einer Stadtverwaltung	54
5.2	Prüfung der Kriminalaktenhaltung der Polizei – erste Ergebnisse	56
5.3	Prüfung des Statistischen Landesamtes im Rahmen der Volkszählung	58
5.4	Prüfung einer Kraftfahrzeugzulassungsstelle	59
5.5	Ist die Anonymität in den AIDS Beratungsstellen garantiert?	59
5.6	Prüfung im Klinikum der Christian-Albrechts-Universität zu Kiel	60
6.	**Telekommunikation und Poststrukturgesetz**	66
7.	**Ordnungsmäßigkeit der Datenverarbeitung**	67
7.1	Datensicherung bei Kleincomputern	67
7.2	Jetzt warnt auch der Innenminister vor Computerviren	70
8.	**Novellierung des Datenschutzrechts**	71
8.1	Datenschutzbeauftragte kritisieren den Entwurf der Bundesregierung	71
8.2	Durch ein neues Landesdatenschutzgesetz soll alles besser werden	73

1. Die Reorganisation des Datenschutzes setzt Zeichen für einen Neuanfang

Über seine Aufgaben, seine Befugnisse und seine Unabhängigkeit befragt, pflegte der „Landesbeauftragte für den Datenschutz beim Innenminister des Landes Schleswig-Holstein" häufig ungläubige Heiterkeit bei seinen Gesprächspartnern auszulösen, wenn er bestätigte, daß der Innenminister sowohl über ihn und seine Mitarbeiter die Dienstaufsicht ausübe als auch zugleich Vorgesetzter von Polizei und Verfassungsschutz sei – zwei wesentliche Bereiche datenschutzrechtlicher Kontrolle. Ähnliche Wirkung hatte regelmäßig die Antwort auf die Frage, wie viele Prüfer denn die große Zahl öffentlicher Stellen im Lande kontrollieren und über wie viele datenverarbeitungstechnisch ausgebildete Mitarbeiter der Landesbeauftragte verfüge. Es bedurfte durchweg besonderer rhetorischer Anstrengungen und Hinweise auf seine Tätigkeitsberichte, um die Zuhörer davon zu überzeugen, daß in Schleswig-Holstein trotz anscheinend unvermeidlicher Interessenkonflikte mit dem Innenminister und bei einer so geringen Personalausstattung eine effektive Datenschutzkontrolle überhaupt möglich ist. Eine Erörterung dieser Aspekte des Datenschutzes hat bei den bisherigen Beratungen der jährlichen Tätigkeitsberichte im Landtag nur ansatzweise stattgefunden. Daran ändert auch die Tatsache nichts, daß das Parlament und die Öffentlichkeit der Arbeit des Landesbeauftragten die Anerkennung nicht versagten. Den entscheidenden Anstoß für eine durchgreifende Änderung der Organisation des Datenschutzes im Lande dürfte erst der Sonderbericht des Landesbeauftragten über die datenschutzrechtlichen Aspekte der „Barschel Pfeiffer-Affäre", den er im Auftrag des Ersten Parlamentarischen Untersuchungsausschusses erstattete und der sich vornehmlich mit der Aufklärung und der Bewertung von datenschutzrechtlichen Sachverhalten im Bereich der Polizei und des Verfassungsschutzes befaßte, gegeben haben.

Mit dem Inkrafttreten des Änderungsgesetzes zum Landesdatenschutzgesetz am 1. Januar 1989, aufgrund dessen der Landesbeauftragte vom Parlament direkt gewählt wird und der Dienstaufsicht der Präsidentin des SchleswigHolsteinischen Landtages unterstellt ist, sollten die Zweifel an einer unabhängigen und von Interessenkonflikten freien Amtsführung ausgeräumt sein. Die Probleme einer ausreichenden personellen, fachlichen und bürotechnischen Ausstattung der Dienststelle harren zwar noch einer endgültigen Lösung. Die Haushaltsansätze für 1989 und die Planungen für 1990 bieten aber auch dafür positive Ansätze.

Zeichen für einen Neuanfang sieht der Landesbeauftragte insbesondere in der künftigen größeren Nähe zum Parlament. Er geht davon aus, daß man ihn mehr als in der Vergangenheit als Berater in den Gesetzgebungsverfahren in Anspruch nehmen wird, und er wird dem Parlament gern den im Verlaufe von 10 Jahren angesammelten Fundus aus praktischen Erfahrungen und das Wissen um die datenschutzrechtlichen Sorgen der Bürger zur Verfügung stellen. An Gesetzgebungsvorhaben mit datenschutzrechtlichem Bezug wird es dabei nicht mangeln. Er denkt z. B. an das Polizeigesetz, das Verfassungsschutzgesetz, das

Archivgesetz, das Personalvertretungsgesetz, das Landesstatistikgesetz und nicht zuletzt an das Landesdatenschutzgesetz. Dabei wird zu trennen sein zwischen dem Bemühen, in den parlamentarischen Beratungen der Gesetzentwürfe eine Lanze für das informationelle Selbstbestimmungsrecht der Bürger zu brechen und der klaglosen Akzeptanz des gesetzgeberischen Willens. Der Datenschutzbeauftragte ist nämlich selbstverständlich auch an solche gesetzlichen Bestimmungen gebunden, in denen seine Wünsche und Forderungen nicht in vollem Umfang berücksichtigt worden sind.

Aufgrund einer verbesserten personellen Ausstattung ergibt sich auch auf einem weiteren Gebiet die Chance für einen Neuanfang. Der Landesbeauftragte wird künftig mit besonderer Intensität die Auswirkungen der automatisierten Datenverarbeitung auf die Arbeitsweise und die Entscheidungsprozesse der öffentlichen Verwaltung im Lande beobachten. Sollte er feststellen, daß die neuen technischen Entwicklungen zu einer Beschränkung der Kontroll- und Aufsichtsmöglichkeiten des Schleswig-Holsteinischen Landtages, der kommunalen Vertretungskörperschaften, des Landesrechnungshofes oder der sonstigen mit Kontroll- und Aufsichtsaufgaben betrauten Organe der öffentlichen Stellen führen, wird er verstärkt von seinem Recht Gebrauch machen, sich direkt an das Parlament zu wenden. Deshalb hat er auch den Vorschlag gemacht, diesen Bereich im neuen Landesdatenschutzgesetz als eigenständige Aufgabe zu verankern (vgl. Tz. 8).

Voraussetzung hierfür war die Bildung eines neuen Referates in der Dienststelle des Landesbeauftragten. Es befaßt sich speziell mit Fragen der Datensicherung und der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme. Damit werden nach 10 Jahren erstmalig die Probleme des technischen und organisatorischen Datenschutzes verwaltungsübergreifend bearbeitet werden können. Diese organisatorische Maßnahme ist bei den anderen Datenschutzbeauftragten des Bundes und der Länder schon seit Jahren realisiert. Auch in Schleswig-Holstein wächst der Wunsch der Behörden nach Beratung in Fragen des technischen und organisatorischen Datenschutzes. Je kompetenter und intensiver die Beratung ist, um so eher akzeptieren die Behörden die Vorschläge und Hinweise des Datenschutzbeauftragten und „schreiben sie nicht in den Wind". Hilfreich wird für das Technikreferat die Ausstattung der Dienststelle mit einer eigenen modernen EDV-Anlage sein. Sie versetzt die Mitarbeiter in die Lage, selbst praktische Erfahrungen zu sammeln und sie für das Prüfungs- und Beratungsgeschäft zu nutzen.

Die organisatorische Einheit der Datenschutzkontrolle im Bereich der öffentlichen Verwaltung mit der – aus rechtlichen Gründen beim Innenminister verbleibenden – Datenschutzkontrolle in der Wirtschaft mußte allerdings aufgegeben werden. Der Landesbeauftragte hält es jedoch für selbstverständlich und notwendig, weiterhin eng mit der Aufsichtsbehörde für den Datenschutz in der Wirtschaft zusammenzuarbeiten. Nicht nur die Verwandtschaft der Rechtsgebiete gibt hierzu Anlaß. Es bedarf darüber hinaus ganz konkreter Abstimmungen im Einzel-

fall, etwa bei der Überprüfung von Datenflüssen zwischen dem öffentlichen in den privaten Bereich, bei der Umsetzung gleichlautender Geheimhaltungsvorschriften für beide Bereiche oder bei der Beurteilung des Inhalts und der Bedeutung von Einwilligungserklärungen in die Verarbeitung personenbezogener Daten. Dennoch wird die Umorganisation insgesamt gesehen zu einem zusätzlichen Aufwand führen. Der Datenschutzbeauftragte muß eine neue Büroorganisation und eine eigene büro-technische Infrastruktur aufbauen, die es ihm gestattet, ohne Rücksicht auf bürotechnische Abhängigkeiten seine Aufgaben ungehindert und unabhängig wahrzunehmen.

Für die Zukunft erhofft sich der Landesbeauftragte, daß die größere Nähe zum Landtag und die stärkere politische Rükkendeckung, die ihm nunmehr zuteil wird, einige Behörden und Verwaltungsbereiche veranlassen werden, sich seinen datenschutzrechtlichen Mahnungen und Forderungen eher zu öffnen, als dies in der Vergangenheit der Fall war.

2. Beratung des Tätigkeitsberichtes erstmals auf breiterer parlamentarischer Basis

Der Schleswig-Holsteinische Landtag hat den zehnten Tätigkeitsbericht des Landesbeauftragten nicht nur dem Innen- und Rechtsausschuß, sondern auch dem Ausschuß für Kultur, Jugend und Sport und dem Sozialausschuß zur Mitberatung überwiesen. Er hat damit zu erkennen gegeben, daß die Tätigkeitsberichte künftig auf einer breiteren parlamentarischen Basis beraten werden sollen als bisher.

Die ihm erstmals gebotene Chance, auch diesen Ausschüssen die Sorgen der Bürger, die Beratungsersuchen der Behörden und die Feststellungen und Wertungen aus seinen Prüfungen näherzubringen, hat der Landesbeauftragte gern genutzt. Er hat die Ausschüsse nicht nur mit den aktuellen Problemen aus dem 10. Tätigkeitsbericht vertraut gemacht, sondern auch auf die in den früheren Tätigkeitsberichten erhobenen grundsätzlichen Forderungen vor allem zur Gesetzgebung hingewiesen. Die Reaktion war erstaunlich und erfreulich.

Die Kultusministerin sagte zu, die geplante Novellierung des Schulgesetzes auch um datenschutzrechtliche Regelungen über den Umgang mit Schüler-, Lehrer- und Elterndaten sowie um Bestimmungen für den schulärztlichen Bereich zu ergänzen. Damit wurde eine sehr alte datenschutzrechtliche Forderung erfüllt. Die Verwertung archivierter Daten soll in einem Archivgesetz geregelt werden, das den Wünschen der wissenschaftlichen Forschung und dem Geheimhaltungsbedürfnis der betroffenen Bürger gleichermaßen gerecht wird. Ferner soll geprüft werden, wie das Denkmalschutzgesetz unter Einbeziehung datenschutzrechtlicher Regelungen zum Schutz der betroffenen Eigentümer normenklarer gestaltet werden kann.

Die Beratungen im Sozialausschuß über die im sozialen und medizinischen Bereich aufgetretenen und noch nicht gelösten Probleme hatten zur Folge, daß in Detailfragen Fortschritte erzielt werden konnten. Der Sozialminister wird zum Beispiel die Forderungen des Datenschutzbeauftragten gegenüber der

Ärztekammer unterstützen, die Vorschriften zur Aufbewahrung und Weitergabe von Patientendaten in der Berufsordnung noch konkreter zu fassen. In der Frage des internen und externen Austausches der Daten von Krankenhauspatienten konnte zwar bezüglich des Regelungsbedarfs ein Konsens erzielt werden, allerdings nicht über den einzuschlagenden gesetzgeberischen Weg. Der Sozialminister erhofft sich von der bevorstehenden Novellierung des Landesdatenschutzgesetzes geeignete Lösungen, während der Datenschutzbeauftragte den wirksamen Schutz der hochsensiblen Patientendaten nur durch ein bereichsspezifisches Krankenhausgesetz gewährleistet sieht. Bei der Aufarbeitung der offenen Problembereiche durfte nicht der Hinweis fehlen, daß man einfach „vergessen" hatte, den Datenschutzbeauftragten bei der Novellierung des Gesundheitsdienstgesetzes im Jahre 1986 zu beteiligen, und dadurch aus datenschutzrechtlicher Sicht wichtige Fragen des Persönlichkeitsschutzes ungeregelt blieben.

Nach allem ist die Mitberatung der Tätigkeitsberichte in den Fachausschüssen uneingeschränkt zu begrüßen. Die Fachressorts fühlen sich nach dem Eindruck des Landesbeauftragten stärker in ihre „datenschutzrechtliche Pflicht" genommen als bisher.

3. Technik und Recht driften auseinander

Die Haushaltsmittel des Landes, der Kreise und der Gemeinden sowie der anderen Einrichtungen der öffentlichen Hand weisen erstaunliche Steigerungsraten für die Planung, den Einsatz und die Pflege moderner Informations- und Kommunikationstechniken auf. Die entsprechende Infrastruktur schreitet rasch voran. Automationsreferenten stellen ihren Chefs modernste Bürokommunikationssysteme auf den Schreibtisch. Diese sehen sich erwartungsgemäß um so eher als Verfechter eines modernen Managements, je dichter in ihrer Behörde der Besatz an Bürokommunikationssystemen ist. Nicht daß dabei der Datenschutz vergessen wird, man entwickelt und realisiert Sicherheitskonzepte wie Zutrittskontrollen, Benutzeridentifikationen, Dokumentationen usw. Man ist ehrlichen Herzens sogar bereit, die Beachtung dieser Sicherheitsvorkehrungen sorgfältig zu überwachen. Der Landesbeauftragte kann all dies nur sehr begrüßen. Doch, der technische/organisatorische Datenschutz ist zwar wichtig, er ist aber nicht alles. Daß die moderne Informations- und Kommunikationstechnik auch eine andere Seite hat, verdeutlicht das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz. Danach wachsen mit dem Einsatz und dem Ausbau moderner Informations- und Kommunikationstechniken auch die Möglichkeiten, das Verhalten der Bürger zu kontrollieren, sie in ihrem Verhalten zu beeinflussen und ihre natürlichen Freiräume einzuschränken. Zum Schutz des Bürgers gegen diese Risiken ist aus der Verfassung das Recht auf informationelle Selbstbestimmung herzuleiten, das dem einzelnen Bürger die Befugnis gewährt, grundsätzlich selbst über die Freigabe und die Verwendung seiner Daten zu bestimmen, und das Einschränkungen nur im überwiegenden Allgemeininteresse zuläßt. Sie bedürfen einer gesetzlichen Grundlage, die

den Grundsätzen der Normenklarheit und der Verhältnismäßigkeit genügt.

Technik und Recht laufen derzeit gerade in den Gebieten auseinander, in denen das Persönlichkeitsrecht der Bürger als besonders schützenswert angesehen wird, am Arbeitsplatz, im Krankenhaus, im Sicherheitsbereich, im Bereich der privaten Kommunikation usw. Die Datenschutzgesetze, die weitgehend noch in der Fassung der 70er Jahre in Kraft sind, erfüllen schon lange nicht mehr die Anforderungen, die der einzelne Bürger und die breite Öffentlichkeit an sie stellen. Die schon unter einer gewissen Resignation leidenden Datenschutzbeauftragten bedürfen dringend der Unterstützung durch die Gesetzgeber. Sie müssen klar und deutlich sagen, ob die Strafverfolgungsbehörden künftig noch mehr moderne Fahndungsmittel einsetzen dürfen oder nicht, ob die Polizei ihre Datenbestände zur vorbeugenden Bekämpfung von Straftaten weiter fortführen kann oder nicht, ob der Datenaustausch zwischen den Sicherheitsbehörden einzustellen ist oder nicht, ob die Wissenschaft mit personenbezogenen Daten forschen darf oder ob sie die „Forschungsobjekte" vorher um Erlaubnis fragen muß, ob der Dienstherr oder der Arbeitgeber mit den Leistungsdaten seines Mitarbeiters auch künftig so umgehen darf, wie er es bisher als selbstverständlich ansah.

Wer den Einsatz moderner Informations- und Kommunikationstechniken forciert, muß dafür sorgen, daß die gesetzlichen Schutzmechanismen zugunsten des betroffenen Bürgers gleichziehen. Mit dem neuen Melderecht und dem Sozialgesetzbuch hat der Gesetzgeber bereits bewiesen, daß er dazu in der Lage ist. Für das Land Schleswig-Holstein ist zu hoffen, daß die angekündigten Gesetzgebungsvorhaben alsbald verwirklicht werden.

Technik und Recht müssen dringend auf Kiellinie gebracht werden!

4. Sorgen der Bürger, Beratung der Behörden, Feststellungen und Wertungen

4.1 Allgemeine und innere Verwaltung

4.1.1 Meldewesen

4.1.1.1 Adoptionsgeheimnis – der Weg eines unbürokratischen Vorschlags

Bereits seit 1986 befaßt sich der Landesbeauftragte mit der Gewährleistung des Adoptionsgeheimnisses im Meldewesen. Er will erreichen, daß nur die Stellen von einer Adoption Kenntnis erhalten, die dieses Wissen zur Erfüllung ihrer Aufgaben auch tatsächlich benötigen. Auf dieser Grundlage hat er dem Innenminister Anfang 1987 einen Vorschlag unterbreitet, der folgendes Problem aus der Welt schaffen sollte: Bisher unterrichtet ein Standesbeamter auch dann die Meldebehörde des Wohnortes der Mutter von der Geburt eines Kindes, wenn das Neugeborene sofort an einen anderen Wohnort in Adoptionspflege gegeben wird. In diesen Fällen einer von vornherein

beabsichtigten Adoption sollte nach den Vorstellungen des Landesbeauftragten die Geburt nur der Meldebehörde, in deren Zuständigkeitsbereich das Kind seinen künftigen Wohnsitz hat, mitgeteilt werden. Die aufgrund dieses Vorschlags entfalteten Aktivitäten der Verwaltung sind beeindruckend: Beteiligung des Kultusministers, Unterrichtung der Innenminister des Bundes und der Länder, Abgabe des Vorschlags an die Arbeitsgemeinschaft der obersten Landesjugendbehörden, Beschluß der Arbeitsgemeinschaft: Auftrag an die Juristenkommission, einen Vorschlag zu unterbreiten.

Das Ergebnis nach 1 1/2 Jahren: Die Juristenkommission hat sich mit der Problematik noch nicht abschließend befaßt. Es war bis zum Redaktionsschluß lediglich beschlossen worden, ein bundeseinheitliches Verfahren abzustimmen. „Die insoweit eingesetzte Arbeitsgruppe ist mit der Befassung der Angelegenheit beauftragt worden".

Der Landesbeauftragte hegt zunehmend die Befürchtung, daß auch in diesem Fall die Bürokratie über den gesunden Menschenverstand siegt.

4.1.1.2 Verarbeitung von Meldedaten und ihre Dokumentation

In verschiedenen Berichten (7. TB, S. 39; 8. TB, S. 14, 49, 63) hat der Landesbeauftragte auf die große Bedeutung der Dokumentation von Datenverarbeitungsvorgängen für den Datenschutz hingewiesen. Das Bundesverwaltungsgericht stellt in einem Beschluß (16.03.1988 – 1 B 153/87 – in NVwZ 88, 621) bezüglich der Aufbewahrungsfristen für Meldedaten gleiche Überlegungen an. Danach sollen durch die Pflicht zur Aktenführung die Behörden angehalten werden, den Geschehensablauf wahrheitsgetreu zu dokumentieren. Dies diene auch dem Schutz derjenigen Betroffenen, deren persönliche Daten in den Akten festgehalten sind. Dazu müßten die Akten solange aufbewahrt werden, daß sie ihre Nachweisfunktion im Bedarfsfall auch tatsächlich erfüllen könnten. Es könne deshalb keine Rede davon sein, daß sie, um Verletzungen des Rechts auf informationelle Selbstbestimmung zu vermeiden, schon dann vernichtet werden müßten, wenn kein Betroffener mehr aktuelle Ansprüche gegen die Behörde erheben könne. Eine Vernichtung von Akten könne erst für einen Zeitpunkt in Betracht gezogen werden, zu dem mit Sicherheit feststehe, daß diese ihre, die Gesetzmäßigkeit der Verwaltung sichernde Dokumentationsfunktion nicht mehr erfüllen.

Der Landesbeauftragte sieht sich durch diesen Beschluß in seiner Einschätzung der Bedeutung einer ausreichenden Dokumentation bestätigt.

4.1.2 Personalwesen

4.1.2.1 Telefondatenerfassung – Zielnummern werden endlich verschleiert

Noch in seinem letzten Bericht (10. TB, S. 13) hatte der Landesbeauftragte Anlaß zur Kritik. Trotz seiner Bedenken beabsichtigte nämlich der Innenminister, bei der automatisierten Gebüh-

renerfassung von privaten Telefongesprächen über dienstliche Anschlüsse die vollständige Anschlußnummer des Angerufenen (Zielnummer) aufzuzeichnen und bei der Abrechnung der Gespräche auszudrucken. Der Landesbeauftragte hatte unter Hinweis auf die Erfahrungen mit den Aufzeichnungen und Auswertungen der Zielnummern in der „Barschel-Pfeiffer-Affäre" und im Hinblick auf die Entwicklung der Rechtsprechung gefordert, hierauf zu verzichten.

Nunmehr teilt der Innenminister mit, daß künftig bei Privatgesprächen die beiden letzten Ziffern der Zielnummern nicht mehr erfaßt werden sollen. Da auf diese Weise bis zu 100 Anschlußinhaber als Gesprächspartner in Betracht kämen, sei Dritten eine eindeutige Identifizierung des Anschlusses nicht mehr möglich. Der Landesbeauftragte hält die beabsichtigte Regelung für eine wesentliche Verbesserung des derzeitigen Verfahrens. Er weist jedoch darauf hin, daß andere öffentliche Stellen offenbar vollständig auf die Aufzeichnung der Zielnummern verzichten, ohne daß es dadurch Probleme gibt.

4.1.2.2 Eignungstests durch private Personalberater

Bewerber für den allgemeinen Verwaltungsdienst des Landes haben sich grundsätzlich einem Eignungstest zu unterziehen. Der Innenminister führt dieses Auswahlverfahren in Zusammenarbeit mit einer privaten Personalberatungsorganisation durch. Sie soll ihm auf der Grundlage wissenschaftlicher Methoden Entscheidungsgrundlagen liefern. Da hierzu von den Bewerbern eine Vielzahl sehr persönlicher Merkmale erfragt werden müssen, hat der Innenminister sicherzustellen, daß die von den Bewerbern im Rahmen des Bewerbungsverfahrens freiwillig bereitgestellten Daten entsprechend den Bestimmungen des Landesdatenschutzgesetzes geschützt werden. Bedenklich erschien dem Landesbeauftragten die Tatsache, daß hierüber bisher kein schriftlicher Vertrag mit der Beratungsorganisation bestand. Das Unternehmen hätte mit den Bewerberdaten faktisch nach Belieben verfahren können.

Der Innenminister hat deshalb auf Drängen des Landesbeauftragten einen Vertrag erarbeitet, der die datenschutzrechtlichen Fragen regelt und auch für vergleichbare Fälle im kommunalen Bereich anwendbar erscheint. Der neue Vertrag sichert

- die ausschließliche Nutzung der Daten zum Zwecke der Eignungsbegutachtung,
- eine ordnungsgemäße Speicherung der Bewerberdaten bei der Beratungsorganisation,
- das Einsichtsrecht der Bewerber in ihre Testunterlagen,
- ein Verbot der Weitergabe an Dritte, es sei denn, es liegt eine schriftliche Einwilligung des Bewerbers vor,
- eine Anonymisierung der Daten spätestens 1 Jahr nach Abschluß des Einstellungsverfahrens,
- ein jederzeitiges Kontrollrecht des Auftraggebers.

4.1.2.3 Die datenschutzrechtliche Problematik einer Urteilsbekanntgabe

„Haben Sie schon gehört, Kollege X hat den Prozeß gegen unsere Dienststelle verloren, hierzu hat der Kollege Y als Gutachter entscheidend beigetragen." So hätte sich das „kollegiale Interesse" artikulieren können, weil ein für einen Mitarbeiter nachteiliges Gerichtsurteil in seiner Behörde in den Umlauf gelangt war. Es sollte eigentlich nur über die Formvorschriften bei der Beteiligung des Personalrates informieren. Anstatt sich aber auf die diese Frage tragenden Urteilsgründe zu beschränken, wurde das Urteil in seiner Gesamtheit bekanntgemacht. Wenn auch die Namen und die anderen direkten Identifikationsmerkmale der beteiligten Personen unkenntlich gemacht waren, so blieben doch so viele personenbezogene Hinweise übrig, daß zumindest im Kollegenkreis die Identifikation des Betroffenen und des Gutachters ohne Schwierigkeiten möglich war. Selbst der Inhalt eines psychologischen Gutachtens konnte dem Betroffenen zugeordnet werden.

Der Landesbeauftragte hat die Behördenleitung darauf aufmerksam gemacht, daß es insbesondere im Personalbereich nicht ausreicht, im Urteilsrubrum alle identifizierenden Hinweise unleserlich zu machen, sondern daß es auch einer sorgfältigen datenschutzrechtlichen Überprüfung der Urteilsgründe insgesamt bedarf, bevor der Inhalt einer gerichtlichen Einzelentscheidung Dritten zugänglich gemacht wird.

4.1.2.4 Verhaltenskontrolle - der Datenschutz setzt sehr früh an

Der Schutz der Mitarbeiter vor einer unzumutbaren Verhaltenskontrolle durch den Arbeitgeber ist im Bereich der privaten Wirtschaft in der Vergangenheit mehrfach Gegenstand höchstrichterlicher Entscheidungen gewesen (vgl. Beschluß des Bundesarbeitsgerichts vom 14. September 1984, BAG 46, 367). Dabei wurde festgestellt, daß Gefahren für das informationelle Selbstbestimmungsrecht nicht erst dann entstehen, wenn technische Systeme tatsächlich zum Zweck solcher Kontrollen eingesetzt werden, sondern schon dann, wenn Systeme benutzt werden, die nur objektiv geeignet sind, Verhaltens- oder Leistungsdaten von Mitarbeitern zu verarbeiten.

Das Bundesverwaltungsgericht (Beschluß vom 16. Dezember 1987 – 6 P 32.84, „Recht im Amt" 1988, 184) überträgt diesen Grundgedanken auch auf das öffentliche Dienstrecht und erweitert ihn in beachtlicher Weise. Nicht erst die Eingabe von Mitarbeiterdaten in technische Systeme konkretisiere die Gefahr, eine Gefährdung liege bereits im manuellen Ausfüllen von Tätigkeitsnachweisen, deren Inhalt erst später für eine Auswertung in die EDV-Anlage eingegeben werden sollen. Es komme nicht darauf an, ob die Daten unmittelbar durch die Einrichtung selbst erhoben werden oder ob sie dem System erst nach manueller Aufzeichnung eingegeben werden müssen. Das gelte jedenfalls dann, wenn das Ausfüllen der Tätigkeitsnachweise durch die Mitarbeiter und die anschließende Verarbeitung durch die EDV-Anlage einen Gesamtvorgang bilde, das Ausfüllen der Vordrucke also dazu bestimmt sei, technische Auswertungen der Daten zu ermöglichen.

Nach dem schleswig-holsteinischen Personalvertretungsgesetz liegt hier zwar kein Mitbestimmungstatbestand, sondern nur ein solcher der Mitwirkung des Personalrats vor. Bedeutsam ist gleichwohl, daß das Bundesverwaltungsgericht in seinem Urteil bereits eine „Vorstufe" der Datenverarbeitung, also einen Vorgang der Datenerhebung, als schutzrelevante Phase der Datenverarbeitung dem kollektiven Mitarbeiter-(daten)-schutz unterstellt.

4.1.3 Datenschutz im Kommunalbereich

4.1.3.1 Kommunale Vertretungskörperschaften und Datenschutz

Immer wieder muß der Landesbeauftragte zu Problemen im Spannungsfeld zwischen dem kommunalen Verfassungsrecht und dem Datenschutz Stellung nehmen. Die Informationswünsche kommunaler Organe konkurrieren nicht selten mit den Ansprüchen der Bürger auf vertrauliche Behandlung ihrer persönlichen Verhältnisse (8. TB, S. 3, 18).

- So war beispielsweise der Informationswunsch einer Fraktion der Gemeindevertretung zu akzeptieren, die über die zukünftige Belastung des Haushalts durch die Versorgungsbezüge eines evtl. nicht wiedergewählten Bürgermeisters unterrichtet werden wollte. Es gehört zur rechtmäßigen Aufgabe der Vertretung, die Folgen ihrer Entscheidungen abzuschätzen. Allerdings sind dabei nicht die Besonderheiten der persönlichen Verhältnisse des Betroffenen zu offenbaren, vielmehr sind nur die haushaltsmäßigen Belastungen zu erläutern. Auch sollte die konkrete Diskussion auf solche Daten beschränkt werden, die aus gesetzlichen oder satzungsmäßigen Regelungen ablesbar sind.
- Desgleichen erscheint es zur rechtmäßigen Aufgabenerfüllung eines Kreistages erforderlich, durch Einzelfallprüfungen die Auftragsvergabepraxis der Verwaltung kontrollierbar zu halten. Eine Zusammenstellung aller Auftragsvergaben in Listen und deren regelmäßige und vollständige Prüfung durch die Vertretung ist hierfür aber nicht erforderlich. Es sollte durch eine „anonymisierte" Darstellung der Einzelfälle auf die schutzwürdigen Belange der Betroffenen Rücksicht genommen werden. Daß auch dadurch wegen der örtlichen und personellen Nähe der Beteiligten zueinander eine wirkliche Vertraulichkeit in der Praxis oft nicht erreichbar ist, sieht auch der Landesbeauftragte. Er appelliert deshalb einmal mehr an den Willen der im kommunalen Bereich verantwortlich Handelnden, auch die Vertraulichkeit als eine der tragenden Säulen sozialen Miteinanders anzuerkennen und zu respektieren.
- Ein Kreisausschuß hatte im städtischen Sozialamt geprüft und einen Prüfungsbericht mit Ausführungen zu Einzelfällen zusammengestellt. Der Landesbeauftragte hielt es nicht für zulässig, dem Magistrat und der Stadtvertretung personenbezogene Einzelfälle darzulegen. Sozialleistungsträger sind die Kreise und kreisfreien Städte. Selbst wenn sie die Aufgabenerfüllung durch Satzung auf die kreisangehörigen Städte und Gemeinden übertragen haben, unterliegen diese nach wie vor

der Rechts- und Fachaufsicht der Kreise. Die Selbstverwaltungsorgane der beauftragten Kommunen sind also nicht zuständig für die fachliche Kontrolle der Aufgabendurchführung. Soweit konkrete Sozialhilfefälle Prüfungsgegenstand sind, würde die Offenbarung personenbezogener Daten in das Sozialgeheimnis eingreifen, zu dessen Wahrung die Sozialleistungsträger und die für sie tätigen Stellen verpflichtet sind.

4.1.3.2 Noch immer Probleme bei der Erhebung und Nutzung von Daten

Welche Daten dürfen Kommunalbehörden erheben und wie weit geht die Zweckbindung? Mit diesen Fragestellungen hatte sich der Landesbeauftragte auch im abgelaufenen Jahr häufiger zu befassen. Dabei ging es durchweg um Fälle, die nicht nach einer Spezialvorschrift, sondern in unmittelbarer Anwendung des Landesdatenschutzgesetzes zu entscheiden waren.

– **Überflüssige Fragen, die auch noch Geld kosten**

  Ein Antrag auf Erlaß von Grundsteuern hatte ganz offenbar von vornherein keine Aussicht auf Erfolg. Dennoch forderte die Gemeinde von dem Betroffenen zunächst weitere umfangreiche Nachweise zu seinen persönlichen und wirtschaftlichen Verhältnissen, bevor dann doch ein Ablehnungsbescheid erlassen wurde. Besonders ärgerlich war, daß dem Betroffenen durch die Beibringung der Unterlagen auch noch Kosten entstanden waren. Bei einer derart eindeutigen Sachlage waren die zusätzlichen Datenerhebungen zur Entscheidung über den Antrag nicht erforderlich und damit unzulässig.

– **Auch wenn es um Geld geht, ist nicht jedes Mittel recht(ens)**

  Kommunale Abgaben müssen richtig und gleichmäßig festgesetzt werden. Diesem Anspruch verschließt sich auch der Landesbeauftragte nicht. Anlaß zur Kritik ergab sich aber bei einigen Verfahren zur Prüfung der Zweitwohnungssteuerpflicht. Die hier verwandten Fragebögen entsprachen durchweg nicht den datenschutzrechtlichen Anforderungen. Der Landesbeauftragte hat dies gerügt und empfohlen, die einzelnen Fragen sorgfältig daraufhin zu überprüfen, ob sie tatsächlich zur Feststellung der Steuerpflicht notwendig sind. Nur dann kann nämlich eine entsprechende Antwort von dem Betroffenen verlangt werden. Bevor Angaben und Nachweise von Dritten angefordert werden, ist zunächst dem Betroffenen selbst Gelegenheit zu geben, die Unterlagen beizubringen. Auch wenn dieser versucht, sich der Steuerpflicht zu entziehen, ist nicht jedes Mittel recht(ens), um den Steueranspruch durchzusetzen.

– **Oft nicht beachtet - freiwillig bereitgestellte Daten sind streng zweckgebunden**

  Zur Feststellung der Zweitwohnungssteuerpflicht hatte das Steueramt einer Gemeinde sich einen aus seiner Sicht unbürokratischen Weg einfallen lassen. Es holte sich von der gemeindeeigenen Kurverwaltung die Namen und Adressen der

Unternehmen, die die Appartementsbesitzer mit der Vermietung ihrer Wohnung beauftragt hatten. Sie hatten diese Angaben gegenüber der Kurverwaltung gemacht, damit beide Stellen unmittelbar miteinander alle mit der Kurabgabe zusammenhängenden Fragen erledigten. Das Steueramt wandte sich nunmehr unmittelbar an die Vermietungsbüros mit der Bitte um die gewünschten Angaben zur Feststellung der Zweitwohnungssteuerpflicht, ohne daß die Wohnungsbesitzer selbst etwas von dieser „heimlichen" Verbindung wußten. Erst die Vermietungsbüros machten die Zweitwohnungsbesitzer darauf aufmerksam.

Der Landesbeauftragte mußte diesen unbürokratischen Weg kritisieren. Die Kurverwaltung hatte die Namen der Vermietungsbüros von den Wohnungsbesitzern zu einem ganz bestimmten Zweck erhalten, nämlich um sich den lästigen Schriftwechsel wegen der Kurabgabe in den einzelnen Beherbergungsfällen zu ersparen. Die Funktion der Vermietungsbüros als Clearing Stelle beruhte auf einer freien Vereinbarung zwischen Kurverwaltung und Zweitwohnungsbesitzern. Sie war deshalb verpflichtet, die im Rahmen dieser Vereinbarung mitgeteilten Adressen der Vermietungsbüros nur für den damit verfolgten Zweck zu nutzen. Die Übermittlung an das Steueramt war zweckwidrig und deshalb datenschutzrechtlich unzulässig.

Der Zweckbindungsgrundsatz tritt erst dann zurück, wenn sowohl die auskunftgebende wie auch die auskunftempfangende Stelle einen gesetzlich begründeten Anspruch hat, entsprechende Daten von den Betroffenen zu fordern. Das war bei einem Datenaustausch zwischen dem Steueramt und dem Ordnungsamt einer anderen Gemeinde der Fall. Das Ordnungsamt hatte zu prüfen, ob ein Gewerbetreibender mit seinem Beherbergungsbetrieb der Genehmigungspflicht unterlag. Die erforderlichen Angaben lagen beim Steueramt in der Liste über die Erhebung der Fremdenverkehrsabgabe bereits vor. Das Gaststättengesetz bzw. die gemeindliche Satzung reichten als Rechtsgrundlage für den Auskunftsanspruch aus. Da auch das Steuergeheimnis nicht berührt war, bestand für das Ordnungsamt in diesem Fall keine Veranlassung, die gewünschten Daten nochmals beim Bürger zu erheben.

4.1.3.3 Volkszählung – zum Schluß doch noch ein schwerwiegender Verstoß

Am 31. Juli 1988 hat das Statistische Landesamt die letzten Volkszählungsbögen zur Auswertung entgegengenommen. Damit endete die Volkszählung „vor Ort". Die Aufgabe der Erhebungsstellen war erfüllt.

Bis auf den nachfolgend geschilderten Fall blieben die festgestellten Mängel in dem Rahmen, der bereits im Tätigkeitsbericht für das Jahr 1987 (vgl. 10 TB, S. 46) aufgezeigt wurde.

Dieser eine Fall verdient allerdings besondere Aufmerksamkeit, da es nicht nur um einen offenkundigen und schwerwiegenden Verstoß gegen das Volkszählungsgesetz ging, sondern

es auch noch erheblicher Mühen bedurfte, die Behörde von der Rechtswidrigkeit ihres Tuns zu überzeugen.

Ein Auskunftspflichtiger war von dem Meldeamt seiner Stadt schriftlich aufgefordert worden, sich entsprechend seinen im Rahmen der Volkszählung gemachten Angaben auch melderechtlich registrieren zu lassen. In ihrer Stellungnahme gegenüber dem Landesbeauftragten bestätigte die Kommune wörtlich: „Von dem Erhebungsstellenmitarbeiter wurde lediglich Name undAnschrift eines Bürgers, der sich an der Volkszählung beteiligt hatte, aber nicht melderechtlich erfaßt war, an die zuständige Ordnungsabteilung hier im Hause zur ordnungsgemäßen Erfüllung ihrer Aufgaben (in diesem Falle Durchsetzung des Meldegesetzes) weitergegeben". Der klassische Fall eines Melderegisterabgleichs. Gerade das hat das Bundesverfassungsgericht in seinem Urteil aus dem Jahre 1983 als verfassungwidrig angesehen. In das Volkszählungsgesetz 1987 wurde daraufhin ein Verwendungs- und Verwertungsverbot aufgenommen. Die Weitergabe der Volkszählungsdaten an das Meldeamt stellt einen schweren Verstoß gegen dieses Verbot dar. Eine entsprechende Beanstandung sowie die Unterrichtung der zuständigen Aufsichtsbehörde war für den Landesbeauftragten deshalb selbstverständlich. Damit gab sich die Stadt jedoch nicht zufrieden. In einer weiteren umfangreichen Stellungnahme wurde der Datenaustausch nachdrücklich als rechtmäßig verteidigt. Erst eine förmliche Weisung der Kommunalaufsicht brachte die Kommune auf den richtigen Weg zurück.

4.1.4 Personalausweis- und Paßwesen

4.1.4.1 Probleme bei der Ausgabe der neuen Personalausweise

Seit fast zwei Jahren sind die neuen fälschungssicheren und maschinenlesbaren Personalausweise in Gebrauch. Anlaufschwierigkeiten ergaben sich nicht nur durch die viel zu langen Bearbeitungszeiten in der Bundesdruckerei. Aus datenschutzrechtlicher Sicht war vor allem eine zu hohe Fehlerquote bei der Vergabe der Seriennummern bedenklich. Allein in den ersten neun Monaten wurden von der Bundesdruckerei 279 Fälle einer Doppelvergabe der Seriennummer in Schleswig-Holstein registriert. Ursache hierfür waren neben Bearbeitungsfehlern der Ausweisbehörden auch Abstimmungsprobleme innerhalb der Bundesdruckerei. Durch eine maschinelle Kontrolle der Nummern vor der Ausweiserstellung konnten die Reklamationsfälle allerdings inzwischen deutlich vermindert werden.

Ein weiteres Problem bestand darin, daß durch Bearbeitungsvermerke der Ausweisbehörden auf der Rückseite der Antragsvordrucke der Bundesdruckerei in unzulässiger Weise personenbezogene Daten übermittelt wurden, die für die Herstellung der Ausweise nicht erforderlich waren. Der Landesbeauftragte hat deshalb ein Verfahren vorgeschlagen, welches sowohl datenschutzrechtlichen Gesichtspunkten als auch Zweckmäßigkeitserwägungen gerecht wird. Die Bearbeitungsvermerke werden auf besonderen Fensterumschlägen

angebracht, die während der Antragsbearbeitung bei der Bundesdruckerei als Beleg im Meldeamt verbleiben. Nach Ausgabe der Ausweise dienen die Umschläge als Registertaschen für die im Personalausweisregister aufzubewahrenden Unterlagen. Auf Anregung des Landesbeauftragten hat der Innenminister dieses Verfahren allen Paß- und Personalausweisbehörden empfohlen.

4.1.4.2 Die Gesetzessprache und ihre praktische Umsetzung

Wenn der Landesbeauftragte im Bereich der Polizei oder des Verfassungsschutzes Prüfungsmaßnahmen durch seine Mitarbeiter vornehmen läßt, muß er sie schriftlich besonders mit der Wahrnehmung dieser Aufgaben betrauen. So bestimmt es das Landesdatenschutzgesetz. Die Sicherheitsbehörden gewähren den Prüfungsbeamten konsequenterweise nur dann Einblick in ihre Unterlagen, wenn eine entsprechende Legitimation durch den Landesbeauftragten vorgelegt wird. Im Paß- und Personalausweisrecht gibt es die nahezu gleichlautende Bestimmung, daß Bediensteten anderer Behörden nur Einblick in die Paß- und Personalausweisregister gewährt werden darf, wenn das Auskunftsersuchen von Mitarbeitern gestellt wird, die vom Behördenleiter dafür besonders ermächtigt sind. Mit der Begründung, daß die Paß- und Personalausweisregister – anders als die Melderegister – grundsätzlich nicht der Erteilung von Auskünften dienen, sind darüber hinaus noch weitere Restriktionen gesetzlich festgelegt. So muß die ersuchende Behörde z. B. ohne Kenntnis der Daten nicht in der Lage sein, ihr obliegende Aufgaben zu erfüllen, und die Daten müßten beim Betroffenen nicht oder nur mit einem unverhältnismäßig hohen Aufwand erhoben werden können. Der Gesetzgeber spricht in diesem Zusammenhang von restriktiven verfahrensrechtlichen Vorschriften, die dem Datenschutz dienen.

Bei der Betrachtung der Praxis ergibt sich allerdings ein überraschendes Bild. Auf der Grundlage eines Erlasses des Innenministers sind faktisch alle Leiter von Polizeidienststellen sowie ihre Vertreter, die Revieroberbeamten, die Sachgebietsleiter und die Hauptsachbearbeiter (der Erlaß zählt 21 Gruppen auf) durch schriftliche Verfügungen ihrer Behördenleiter entsprechend zu ermächtigen. Eines persönlichen Anschreibens bzw. einer namentlichen Nennung bedarf es dabei nicht. Diese Beamten prüfen in eigener Verantwortung, ob die gesetzlich geforderten Voraussetzungen vorliegen, und entscheiden, ob und wie das Ersuchen durchgeführt wird. Nur „nach Möglichkeit" soll dies schriftlich erfolgen. Soweit es aus zeitlichen oder praktischen Gründen geboten ist, kann einem anderen Beamten eine „Unterermächtigung" erteilt werden. Eine Legitimation des Polizeibeamten der betr. Paß- oder Personalausweisbehörde gegenüber ist nicht vorgesehen. Ebenso ist nicht erläutert, in welchen Fällen (typischerweise) die gesetzlichen Voraussetzungen für eine Auswertung der Register vorliegen und wann in der Regel von einer Inanspruchnahme der Paß- und Personalausweisregister abgesehen werden sollte. Aus den Eingaben, die dem Landesbe-

auftragten vorliegen, ergibt sich, daß die Polizeibehörden offenbar überwiegend zur Feststellung der Identität der Fahrzeugführer, die wegen zu schnellen Fahrens „geblitzt" worden sind und die man Zuhause nicht angetroffen hat, Einblick in die Register nehmen.

Der Landesbeauftragte zweifelt nicht daran, daß es sich bei dem Rückgriff auf die Paß- und Personalausweisregister um eine sehr effektive Maßnahme zur polizeilichen Aufgabenerfüllung handelt und daß viele der Betroffenen auf diese Weise daran gehindert werden, sich einem Straf- oder Bußgeldverfahren zu entziehen. Es erscheint ihm jedoch bedenklich, daß so prononciert formulierten Einschränkungen im Paß- und Personalausweisrecht eine so „liberale" Praxis gegenübersteht. Für ihn stellt sich die Frage: Hat der Gesetzgeber seinen Willen zu eng formuliert, oder legt die Verwaltung den gesetzgeberischen Willen zu weit aus? Er neigt letzterem zu und wird deshalb demonstrativ auch weiterhin nicht darauf verzichten, seine Mitarbeiter im Einzelfall und sehr konkret zu ermächtigen, wenn sie Einblick in polizeiliche Dateien zu nehmen haben.

4.1.5 Personenstandswesen

Eine recht weitgehende Fürsorge für Neugeborene legte eine Reihe von Standesämtern an den Tag. Sie werden von Kliniken, Ärzten und Hebammen durch Vorlage sogenannter Geburtsbescheinigungen über die Geburt eines Kindes unterrichtet. Diese Bescheinigungen enthalten neben den Angaben zur personenstandsrechtlichen Registrierung auch Vermerke wie z. B. „Körpergewicht", „Stellung des Kindes bei der Geburt", „angewandte Kunsthilfen" und „erkennbare Fehlbildungen". Diese Informationen sind Bestandteil der gesetzlich vorgeschriebenen Statistik der Bevölkerungsbewegung und Fortschreibung des Bevölkerungsstandes.

Um im Falle von körperlichen Fehlbildungen beim Neugeborenen eine frühzeitige und wirksame Beratung und Unterstützung der Eltern zu ermöglichen, hatten die Standesämter diese Bescheinigung an die Gesundheitsämter weitergegeben. Diese wandten sich dann zum Zweck der Beratung an die Eltern. Nicht alle Eltern waren über dieses Maß an staatlicher Fürsorge erfreut und fragten den Landesbeauftragten nach dem rechtlichen Hintergrund der „Informationsautobahn" Krankenhaus – Standesamt – Gesundheitsamt. Der Landesbeauftragte hat darauf hingewiesen, daß für diese Übermittlungen sehr kritischer Daten eine Rechtsgrundlage nicht besteht. Die Weitergabe an die Gesundheitsämter ist also unzulässig. Der Innenminister hat diese Auffassung bestätigt und die Standesämter angewiesen, die Übermittlungen der Geburtsbescheinigungen an die Gesundheitsämter unverzüglich einzustellen.

4.1.6 Verfassungsschutz

4.1.6.1 Sicherheitsrichtlinien mit Schwachstellen

Seit dem Jahr 1984 bemüht sich der Landesbeauftragte in Gesprächen mit der Verfassungsschutzbehörde vergeblich darum, daß den Lebensgefährten von sicherheitsüberprüften Behördenmitarbeitern die ihnen zustehenden Datenschutzrechte gewährt werden. Durch das Inkrafttreten der „Richtlinien für die Sicherheitsüberprüfung von Personen im Rahmen des Geheimschutzes" vom 18. April 1988 wurde vom Innenminister nun endgültig ein Verfahren festgelegt, gegen das der Landesbeauftragte erhebliche Bedenken geltend machen muß. Worum geht es?

Bevor Mitarbeiter einer Behörde mit vertraulichen oder geheimen Unterlagen in Kontakt kommen, müssen sie auch detaillierte Angaben zu ihrem Ehegatten, ihrer Verlobten oder der Person, mit der sie in eheähnlicher Gemeinschaft leben, machen. Gefragt wird nicht nur nach Name, Anschrift und Geburtsdatum, sondern auch nach Beruf und Arbeitgeber sowie nach Personen, die den Lebensgefährten im Alter von 16 bis 18 Jahren kannten und mit denen möglichst noch heute Kontakt besteht. Nicht zuletzt erkundigt man sich nach den finanziellen Verhältnissen des Partners und nach dessen Kontakten und Aufenthalten zu bzw. in kommunistisch regierten Ländern. Da der Partner in keinem Rechtsverhältnis zu der betr. Behörde steht, kann er selbstverständlich nicht zur „Teilnahme" an einer solchen Überprüfung gezwungen werden. Anstatt die Person aber zunächst um ihre Einwilligung zur Einbeziehung in die Überprüfung zu bitten und sie sodann selbst zu befragen, hat der zu überprüfende Mitarbeiter mit seiner Unterschrift zu versichern, daß er seinen Partner darüber informiert hat, daß dieser in die Sicherheitsüberprüfung einbezogen wird. Der Partner selbst soll durch Unterschrift bestätigen, daß er hierüber „unterrichtet" sei. In diesem Zusammenhang wird ihm mitgeteilt, daß die über ihn erhobenen Daten „nicht gespeichert" werden.

Es fehlt demnach jeglicher Hinweis auf die Freiwilligkeit der Einbeziehung in die Überprüfung. Die Formulierung in der Bestätigung des Partners („... weil nach den Sicherheitsrichtlinien eine Sicherheitsüberprüfung anderenfalls nicht möglich ist ...") suggeriert vielmehr eine Pflicht zur Teilnahme. Als Grundlage für das Verfahren wird auf die verwaltungsinternen Sicherheitsrichtlinien und nicht auf das Verfassungsschutzgesetz verwiesen. Die Verfassungsschutzbehörde überläßt es dem zu überprüfenden Mitarbeiter, in welcher Form er seinen Partner unterrichtet. Es wird damit in Kauf genommen, daß der Partner sich der Tragweite seiner Entscheidung gar nicht bewußt wird. Der Hinweis darauf, daß die erhobenen Daten nicht gespeichert werden, ist irreführend. Sie werden sehr wohl in einem, mittels des nachrichtendienstlichen Informationssystems erschließbaren, Aktenbestand registriert. Sollten sich im Rahmen der Überprüfung des Partners verfassungsschutzrechtlich relevante Erkenntnisse ergeben (z. B. Anhaltspunkte für eine Agententätigkeit),

führt dies zu eigenständigen Datenspeicherungen. Der Partner wird nicht darauf hingewiesen, daß der zu überprüfende Mitarbeiter Angaben über ihn zu machen hat, deren Richtigkeit er zweckmäßigerweise kontrollieren und bestätigen sollte.

Insgesamt erscheint dem Landesbeauftragten das Verfahren so problematisch, daß er aufgrund seiner Beratungspflicht folgende Empfehlungen zur Verbesserung des Datenschutzes gegeben hat: Die Mitarbeiter, die einer Sicherheitsüberprüfung zu unterziehen sind, werden zunächst nur nach den Namen und den Geburtsdaten der Ehegatten, Verlobten usw. befragt. Sofern sich eine Einbeziehung dieser Personen als erforderlich erweist, werden sie von der Verfassungsschutzbehörde direkt angeschrieben, über die Sachlage aufgeklärt sowie auf die Freiwilligkeit ihrer Angaben und die Folgen einer Auskunftsverweigerung hingewiesen. Die von ihnen selbst ausgefüllten Fragebögen können der Verfassungsschutzbehörde direkt zugeleitet werden.

Der Innenminister ist den Vorschlägen des Landesbeauftragten leider nicht gefolgt. Die Sicherheitsrichtlinien seien von der Landesregierung in Kenntnis der Problematik nach Abwägung der Sicherheitsaspekte und der datenschutzrechtlichen Belange in der nunmehr vorliegenden Fassung beschlossen worden. Hieran sei er zunächst gebunden. Er hat sich lediglich bereit erklärt, den Landesbeauftragten in den Fällen zu unterrichten, in denen es zu den o. a. eigenständigen Datenspeicherungen über einen Ehepartner kommt. Dies reicht nach Auffassung des Landesbeauftragten nicht aus; er kann nur hoffen, daß der Gesetzgeber in der geplanten Novelle zum Verfassungsschutzgesetz das von ihm vorgeschlagene Verfahren verbindlich vorschreibt.

4.1.6.2 Dateien wurden rigoros „abgespeckt"

Die dateimäßig geführten personenbezogenen Datenbestände der Verfassungsschutzbehörde lassen sich in drei Gruppen gliedern:

- Daten über Personen, die im Verdacht der Spionagetätigkeit stehen,
- Daten über Personen, die einer verfassungsfeindlichen Bestrebung angehören oder eine solche Organisation unterstützen und
- Daten über Personen, die sicherheitsüberprüft wurden, weil ihnen Verschlußsachen anvertraut sind.

Wegen der großen sicherheitspolitischen und strafrechtlichen Relevanz der Datenspeicherungen über mutmaßliche Agenten und der Kenntnis der Betroffenen von der Durchführung einer Sicherheitsüberprüfung kommt diesen beiden Gruppen nicht die gleiche datenschutzrechtliche Bedeutung zu wie der Registrierung von Personen, die wegen ihrer politischen Einstellung als Verfassungsfeinde gelten.

Das Verfassungsschutzgesetz verpflichtet die Verfassungsschutzbehörde zunächst zur Sammlung und Auswertung von

Auskünften, Nachrichten und sonstigen Unterlagen über Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand und die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung von Mitgliedern verfassungsmäßiger Organe des Bundes oder eines Landes zum Ziel haben. Da derartige Bestrebungen stets von Personen getragen werden, ist eine personenbezogene Aufbereitung der gewonnenen Informationen sicherlich zur Aufgabenerfüllung der Verfassungsschutzbehörde erforderlich. Sie muß aber dem Zweck dienen, die Art und den Inhalt der verfassungsfeindlichen Aktivitäten eines „Beobachtungsobjektes", aufzuhellen. Dies führt zu der seit Jahren erhobenen Forderung des Landesbeauftragten, daß keine Daten über Personen in das nachrichtendienstliche Informationssystem eingestellt bzw. in anderer Form dateimäßig erfaßt werden dürfen, die nicht zumindest aktive Unterstützer einer verfassungsfeindlichen Bestrebung sind.

Bei seinen jüngsten Gesprächen und Prüfungsmaßnahmen in der schleswig-holsteinischen Verfassungsschutzbehörde hat der Landesbeauftragte feststellen können, daß diese Überlegungen inzwischen Eingang in die Praxis gefunden haben. Ob eine Bestrebung als verfassungfeindlich anzusehen ist und damit Beobachtungsobjekt wird oder bleibt, wird auf „allerhöchster Ebene" entschieden. Das Einspeichern und das Löschen personenbezogener Daten in das nachrichtendienstliche Informationssystem wird in jedem Einzelfall auf Referentenebene geprüft. Als Folge dieser Verfahrensweise hat sich der Bestand an Datensätzen über „Verfassungsfeinde" in den vergangenen Jahren kontinuierlich auf 10 Prozent des Ursprungsbestandes reduziert. Aus dem Verfassungsschutzbericht des Innenministers für die Jahre 1985/1986 ergibt sich, daß „lediglich" ca. 15 Organisationen/Bestrebungen als Beobachtungsobjekte angesehen werden.

Dies muß zweifellos als ein datenschutzrechtlicher Fortschritt angesehen werden. Von besonderer Bedeutung erscheint dem Landesbeauftragten dabei die Feststellung, daß diese Reduzierungen vor dem Hintergrund unveränderter Rechtsgrundlagen im Verfassungsschutzgesetz vorgenommen wurden. Nicht das Recht hat sich geändert, sondern seine Auslegung. Vor zehn Jahren vertrat man in den Diskussionen mit dem Landesbeauftragten ebenso wie heute die Auffassung, daß das jeweils gespeicherte Datenvolumen zur rechtmäßigen Aufgabenerfüllung erforderlich sei. Der Landesbeauftragte empfiehlt dem Gesetzgeber daher, bei der Novellierung des Verfassungsschutzgesetzes im Interesse der Normenklarheit Tatbestände zu schaffen, die einen derart weiten Auslegungsspielraum gar nicht erst gewähren.

4.1.6.3 Bundesinnenminister gewährleistet Zugriff auf Dokumentation

In seinem Sonderbericht für den Parlamentarischen Untersuchungsausschuß zur „Barschel-Pfeiffer-Affäre" (vgl. 10. TB, S. 63) hat der Landesbeauftragte kritisiert, daß der Bundesinnenminister faktisch in der Lage war, auf die Kontrolltätigkeit

des schleswig-holsteinischen Datenschutzbeauftragten Einfluß zu nehmen. Da die schleswig-holsteinische Verfassungsschutzbehörde keine eigene Dokumentation ihrer Zugriffe auf das Nachrichtendienstliche Informationssystem vornimmt, war er gezwungen, auf die Aufzeichnungen des Bundesamtes für Verfassungsschutz zurückzugreifen. Er bat den Bundesbeauftragten für den Datenschutz, die Unterlagen einzusehen und ihm entsprechende Merkmale mitzuteilen. Der Bundesinnenminister verweigerte die Weiterleitung der Daten an den schleswig-holsteinischen Datenschutzbeauftragten. Daraufhin forderte der Landesbeauftragte die schleswig-holsteinische Verfassungsschutzbehörde auf, künftig eigene Aufzeichnungen zu führen. Hierzu sah sich der Innenminister leider aus Kostengründen nicht in der Lage. Er hat den Landesbeauftragten lediglich davon unterrichtet, daß das Bundesamt für Verfassungsschutz bereit und in der Lage sei, dem Innenminister auf Wunsch die Dokumentation aller NADIS-Abfragen der schleswig-holsteinischen Verfassungsschutzbehörde zur weiteren Verwendung in eigener Verantwortung zur Verfügung zu stellen. Der Landesbeauftragte hofft, daß damit für die Zukunft „Komplikationen" ausgeschlossen sind.

4.1.7 Öffentliche Sicherheit und Ordnung

4.1.7.1 Polizei löscht mehr Daten als vom Landesbeauftragten gefordert

Es passiert nicht eben häufig, daß eine Behörde einen strengeren Maßstab an die Erforderlichkeit einer Datenspeicherung anlegt als der Landesbeauftragte selbst. Deshalb ist es bemerkenswert, daß das Kriminalpolizeiamt alle Datensätze, die es im Zusammenhang mit der Volkszählung in die „Arbeitsdatei PIOS Innere Sicherheit" (APIS) beim Bundeskriminalamt eingestellt hat, wieder löschen ließ. Im Rahmen einer punktuellen Überprüfung (vgl. 10. TB, S. 27) hatte der Landesbeauftragte nämlich nur die Speicherung eines Teils der Datensätze kritisiert. Daneben fand er auch Datenspeicherungen vor, bei denen seines Erachtens die rechtlichen Voraussetzungen für die Aufnahme in die APIS-Dateien gegeben waren.

Nun liegt es dem Landesbeauftragten fern, eine Behörde zu tadeln, weil sie ursprünglich für erforderlich gehaltene Daten nach nochmaliger Prüfung aus ihren „Spezialbeständen" tilgt. Es stellt sich jedoch die Frage, ob insoweit stets mit der gleichen Elle gemessen wird oder ob etwa die bundesweite Publizität der unzulässigen Speicherung der Daten von Volkszählungsgegnern in den polizeilichen Informationssystemen hier zu einer „Sonderbehandlung" geführt hat.

Bei der anstehenden datenschutzrechtlichen Prüfung im Staatsschutzdezernat des Kriminalpolizeiamtes wird der Landesbeauftragte davon ausgehen, daß die Überlegungen, die zur Löschung der Daten über die Volkszählungsgegner führten, analog auch Gültigkeit in bezug auf andere APIS-Speicherungen haben.

4.1.7.2 „Automatische" Datenweitergaben an den Verfassungsschutz

Bei seiner Überprüfung der Datenspeicherung von Volkszählungsgegnern in der INPOL-Datei-„APIS" im Januar 1988 hatte der Landesbeauftragte festgestellt, daß bis auf wenige Ausnahmen die Daten aller registrierten Personen vom Kriminalpolizeiamt an die Verfassungsschutzabteilung des Innenministeriums weitergegeben worden sind. Aufgrund seiner damaligen Beanstandungen (vgl. 10. TB, S. 29) erklärte ihm der Innenminister, daß seines Erachtens „durch eine künftig restriktivere Beurteilung der APIS-Relevanz für Straftaten die Schwelle für die Datenweitergabe an die Verfassungsschutzbehörde als angemessen anzusehen sei". Von der Regelung, daß grundsätzlich jede APIS-Eintragung zu einer entsprechenden Mitteilung an die Verfassungsschutzbehörde führt, meinte er nicht abweichen zu können.

Nicht zuletzt im Hinblick auf die öffentlichen Aussagen des Innenministers zu den Entwürfen der Sicherheitsgesetze des Bundes, in denen er sich gegen einen weitgehenden Informationsaustausch zwischen der Verfassungsschutzbehörde und anderen öffentlichen Stellen und gegen die Regelung, daß Polizeibehörden und Staatsanwaltschaften von sich aus Informationen an die Verfassungsschutzbehörde übermitteln sollen, ausgesprochen hat, hat der Landesbeauftragte erneut gefordert, das derzeitige Verfahren zu ändern. Das schleswig-holsteinische Verfassungsschutzgesetz sieht nur eine Weitergabe von Daten über Bestrebungen vor, die die Voraussetzungen für ein Tätigwerden der Verfassungsschutzbehörde erfüllen. Aus seiner Sicht müssen daher die Erkenntnisse der Polizeibehörde zumindest entweder den Verdacht einer Spionagetätigkeit begründen, oder aber es müssen konkrete Anhaltspunkte für eine Mitgliedschaft der betreffenden Person in einer Bestrebung, die Beobachtungsobjekt der Verfassungsschutzbehörde ist, vorliegen, bevor eine unaufgeforderte Datenweitergabe durch Polizeibehörden in Betracht kommt. Dies scheinen ihm Kriterien zu sein, die in der polizeilichen Praxis „handhabbar" sind. Wann der Verdacht einer Spionagetätigkeit vorliegt, ist nach strafrechtlichen Kategorien zu beurteilen, die Namen der verfassungsfeindlichen Bestrebungen im Lande sind dem Jahresbericht der Verfassungsschutzbehörde zu entnehmen.

Eine Entscheidung des Innenministers über die zukünftige Verfahrensweise steht noch aus.

4.1.7.3 Wie weit wirkt die Immunität der Abgeordneten?

Artikel 17 Abs. 2 der Landessatzung bestimmt, daß ein Abgeordneter wegen einer mit Strafe bedrohten Handlung nur mit Genehmigung des Landtages zur Verantwortung gezogen werden kann, Artikel 46 Abs. 2 Grundgesetz enthält eine gleichlautende Regelung für Bundestagsabgeordnete. Dieses klassische Privileg der Legislative, das im Sinne der Gewaltenteilung vor „Übergriffen" der Exekutive schützen soll, wird in Rechtsprechung und Literatur durchaus zugunsten der Legislative ausgelegt. Nach herrschender Meinung sind bereits oberflächlichste Ermittlungen der Polizei bzw. der Staatsanwaltschaft genehmi-

gungspflichtig. Ohne Genehmigung zulässig sind lediglich diejenigen Amtshandlungen, die als technische Voraussetzungen einer Untersuchung zu betrachten sind. Im wesentlichen dürfen die Strafverfolgungsbehörden also nur solche Aufklärungen vornehmen, die ein Ersuchen um Aufhebung der Immunität rechtfertigen. Die „Grundsätze für die Behandlung von Immunitätsangelegenheiten" des Schleswig-Holsteinischen Landtages machen deshalb die „allgemeine Genehmigung" zur Einleitung von Ermittlungsverfahren davon abhängig, daß die Parlamentspräsidentin und in der Regel auch der betroffene Abgeordnete mindestens 48 Stunden vorher hiervon in Kenntnis gesetzt worden sind.

Unter diesen Aspekten erscheint es dem Landesbeauftragten sehr problematisch, daß in dem „Spezialdatenbestand" APIS zumindest vorübergehend zwei Mitglieder des Deutschen Bundestages wegen Äußerungen, die sie in einer öffentlichen Veranstaltung getan hatten, als sogenannte „andere Personen" registriert waren. Es stellt sich die Frage, ob nicht das Recht auf Immunität berührt wird, wenn gewählte Abgeordnete befürchten müssen, in Informationssystemen der Polizeibehörden erfaßt zu sein, ohne daß sie als Verdächtige oder Beschuldigte gelten, und somit das Genehmigungsverfahren gar nicht erst in Gang gesetzt wird. Gleiches gilt für den Fall, daß ein genehmigtes Ermittlungsverfahren eingestellt worden ist oder mit einem Freispruch beendet wurde.

Der Landesbeauftragte regt an, hierüber im Rahmen der anstehenden Beratungen über eine Parlamentsreform zwischen Legislative und Exekutive eine klarstellende Vereinbarung zu treffen. Er hält es für angezeigt, daß die Parlamentspräsidentin über jede dateimäßige Registrierung eines Landtagsabgeordneten durch Strafverfolgungs- und Verfassungsschutzbehörden unterrichtet wird, um die Beeinträchtigung der Rechte des Parlaments geltend machen zu können. Gleiches müßte bezüglich der Bundestagsabgeordneten gelten.

4.1.7.4 Bewerber für den Polizeidienst werden nicht mehr heimlich überprüft

Bis vor kurzem wurden über alle Bewerber für den Polizeidienst ohne ihr Wissen Erkundigungen bei den örtlichen Polizeidienststellen eingeholt und die polizeilichen Informationssysteme ausgewertet. Derartige „Leumundszeugnisse" wurden zudem zwischen den Polizeiverwaltungen des Bundes (Bundesgrenzschutz) und den Ländern ausgetauscht. So konnte es passieren, daß Jugendliche nicht als Polizeianwärter eingestellt wurden, obwohl ihre „Dumme-Jungen-Streiche" aufgrund eines richterlichen Beschlusses nur ins Erziehungsregister eingetragen wurden, auf das die Polizei keinen Zugriff hat. Sie wertete eben ihre eigenen Datenbestände aus und umging somit die Auskunftsbeschränkungen nach dem Jugendgerichtsgesetz. In seinem 10. Tätigkeitsbericht, S. 21, hat der Landesbeauftragte hiergegen Bedenken erhoben.

Der Innenminister hat das Verfahren daraufhin geändert. Auskünfte an Polizeibehörden des Bundes und anderer Länder werden nur noch erteilt, wenn eine schriftliche Einwilligungserklä-

rung des Betroffenen vorgelegt wird. Auch die Bewerber für den Polizeidienst in Schleswig-Holstein werden nur noch überprüft, wenn sie zuvor eine Einverständniserklärung unterschrieben haben. Der Umfang der Auskünfte ist drastisch reduziert. Es dürfen keine Auskünfte mehr erteilt werden über Verfahren, die zum Freispruch geführt haben oder die mangels Tatverdachtes eingestellt worden sind,sowie über von Kindern begangene Delikte, wenn es sich erkennbar um entwicklungsbedingte Taten handelt. Jegliche Abgabe von Bewertungen ist unzulässig. Die Auskünfte haben sich auf das zu beschränken, was dienstlich zur Kenntnis gelangt ist. Auskünfte über die wirtschaftlichen Verhältnisse oder den Leumund des Betroffenen bzw. von Familienmitgliedern sind nicht zu erteilen. Besondere Erhebungen von Informationen aus Anlaß des Ersuchens sind unzulässig. Bei laufenden Verfahren oder solchen mit unbekanntem Ausgang darf lediglich Auskunft über die Tatsache polizeilicher Ermittlungen und die in Betracht kommenden Tatbestände erteilt werden. Prognosen hinsichtlich des Ausgangs des Verfahrens sind unzulässig.

Der Landesbeauftragte betrachtet das neue Verfahren mit „einem lachenden und einem weinenden Auge". Einerseits ist die rechtsverbindliche Einwilligung eines Betroffenen in die Datenverarbeitung einer Behörde eine solide datenschutzrechtliche Grundlage, die Tatsache der Überprüfung und deren Folgen werden dem Bewerber transparent, gegen eventuelle Fehlurteile kann er sich wehren. Andererseits dürfte sich die vermeintliche Freiwilligkeit in der Praxis zu einer Obliegenheit entwickeln. Welcher Bewerber hat noch die Chance, in das engere Auswahlverfahren zu kommen, wenn er nicht in die Überprüfung einwilligt? Nach wie vor werden ihm also Vorgänge, die ausschließlich im Erziehungsregister ihren Niederschlag finden sollten, bei seiner Bewerbung vorgehalten, allerdings „auf eigenen Antrag". Dabei darf man nicht übersehen, daß die Polizei Überprüfungen vornimmt, die es in dieser Weise in anderen Verwaltungen nicht gibt. Die Finanzämter prüfen nicht anhand der ihnen verfügbaren Steuerdaten, ob künftige Mitarbeiter in der Vergangenheit steuerehrlich waren, Krankenhäuser nicht, welche Krankheiten angehende Ärzte vorher hatten, und Kommunen nicht, ob der künftige Jugendpfleger in der Erziehungsberatungsstelle als ehemaliger „Schwererziehbarer" bekannt ist.

4.1.7.5 Der Presse dürfen keine Namenskürzel mehr mitgeteilt werden

Manche Dinge dauern eben ihre Zeit. Vor nunmehr acht (!) Jahren hatte der Landesbeauftragte erstmals kritisiert, daß die Polizeibehörden in ihren Mitteilungen an die Presse auch die Namenskürzel von Verdächtigen und Beteiligten offenbarten, obwohl gar nicht feststand, daß diese die Straftat auch tatsächlich begangen haben. Der Innenminister konnte sich damals nicht entschließen, dies grundsätzlich zu untersagen. So las man weiterhin in den Zeitungen, daß „nach Auskunft der Polizei gegen den ...jährigen Kaufmann X. Y. aus Z. wegen des Verdachts des ... ermittelt wurde". Dem Bekanntenkreis, den Kollegen und der Nachbarschaft des Herrn X. Y. aus Z. dürfte in

solchen Fällen klar gewesen sein, wer gemeint war. In den seltensten Fällen dürften sie aber etwas davon erfahren haben, wenn solche Ermittlungsverfahren wegen erwiesener Unschuld eingestellt wurden oder mit Freispruch endeten. Kein Zweifel also an einer vermeidbaren Beeinträchtigung der schutzwürdigen Belange der Betroffenen, denn der Makel „Straftäter" blieb haften.

Diese datenschutzrechtliche Altlast hat der Innenminister nunmehr sachgerecht entsorgt, indem er die Polizei angewiesen hat, der Presse gegenüber personenbezogene Angaben nur noch im Rahmen der Öffentlichkeitsfahndung zu machen. Die Verwendung von Namenskürzeln ist ausdrücklich untersagt.

4.1.7.6 Hinweise auf AIDS nun doch in den Polizeidateien gelöscht

Auch in einem anderen Bereich ist man den Forderungen des Landesbeauftragten inzwischen gefolgt. Im 10. Tätigkeitsbericht, S. 26, hatte der Landesbeauftragte erhebliche Bedenken gegen die Registrierung aller der Polizei bekanntgewordenen AIDS-infizierten Personen in polizeilichen Informationssystemen erhoben. Der Innenminister sah zwar auch gewisse grundsätzliche Probleme, konnte sich aber zu einer Löschung der Daten (noch) nicht entschließen. Um so erfreuter war der Landesbeauftragte, als er nunmehr die Mitteilung erhielt: „Eine Überprüfung und neue Bewertung hat ergeben, daß von einer Speicherung solcher Hinweise für Polizeibeamte kein zusätzlicher Schutz mehr zu erwarten ist. Die Speicherung des Hinweises wird daher eingestellt. Das Kriminalpolizeiamt wird angewiesen werden, Hinweise in bereits vorhandenen Datensätzen zu löschen". Daß letztlich „nur" Zweckmäßigkeitsüberlegungen und nicht Rechtsgründe für die Löschung der Daten ausschlaggebend waren, sieht der Landesbeauftragte allerdings als einen kleinen Schönheitsfehler an.

4.1.7.7 Die Polizei als Auge und Ohr der Ordnungsbehörden

Die Frage, unter welchen Voraussetzungen die Polizei anderen Behörden – insbesondere Ordnungsbehörden – welche Auskünfte erteilen darf, ist seit vielen Jahren Gegenstand datenschutzrechtlicher Diskussionen (vgl. 7. TB, S. 22; 8. TB, S. 27). Mehr und mehr stellt sich heraus, daß hier letztendlich nur der Gesetzgeber im Rahmen der Novellierung des Polizeirechts Klarheit schaffen kann. Folgender Fall mag dies verdeutlichen:

Einem Petenten war sein Führerschein wegen Fahrens unter Alkoholeinfluß entzogen worden. Aufgrund seines Antrages auf Neuerteilung fragte die Verkehrsaufsichtsbehörde bei der örtlichen Polizeibehörde an, ob Erkenntnisse vorlägen, die einer Neuerteilung der Fahrerlaubnis entgegenstünden. Dies wurde verneint. Monate später erfuhr der Polizeibeamte im Rahmen von Ermittlungen wegen einer Sachbeschädigung von einem Hausverwalter und von der getrennt lebenden Ehefrau des Petenten von deren sehr subjektiven Ansichten und Wertungen über die Trinkgewohnheiten des Petenten. Er nahm dies zum Anlaß zu einem „Nachbericht" an die Verkehrsaufsichtsbehörde, woraufhin diese die Neuerteilung der Fahrerlaubnis ablehnte.

Die Polizei rechtfertigte die Datenübermittlung mit der Regelung im Landesverwaltungsgesetz, nach der „die Polizei die zuständige Ordnungsbehörde von allen Vorgängen unverzüglich zu unterrichten hat, die deren Eingreifen erfordern oder für deren Entschließungen von Bedeutung sein können". Die amtliche Begründung zum Landesverwaltungsgesetz führt hierzu aus: „Hiernach ist die Polizei Auge und Ohr der Ordnungsbehörde auf der Straße und hat alle Gefahren für die Sicherheit oder Ordnung festzustellen".

Vor diesem rechtlichen Hintergrund hatte der Landesbeauftragte mit seinen Hinweisen auf das informationelle Selbstbestimmungsrecht und auf die schutzwürdigen Belange des Betroffenen „keine Chance". Auch der von ihm eingeschaltete Innenminister vertritt die Auffassung, daß die Polizei im Rahmen der Gefahrenabwehr die Ordnungsbehörden über mehr als nur über laufende Ermittlungsverfahren unterrichten darf. Der Auffassung des Landesbeauftragten, daß die Polizeibehörden grundsätzlich nur „harte Fakten" aus einschlägigen Ermittlungsverfahren übermitteln sollten, konnte sich der Innenminister nicht anschließen. Polizei und Ordnungsbehörden seien aufgrund ihres gemeinsamen Auftrages zur Gefahrenabwehr in ein jahrzehntelang gewachsenes Beziehungsgeflecht eingebunden. Der Informationsbedarf der Ordnungsbehörden und die Abhängigkeit von einer Informationsübermittlung durch die Polizei hätten dabei je nach der zu erfüllenden Teilaufgabe der Gefahrenabwehr (z. B. Straßenverkehr, Jugendschutz, Gewerbeaufsicht), nach der Ebene der Organisationsseinheit und je nach den spezifischen örtlichen Gegebenheiten die unterschiedlichsten Ausprägungen entwickelt. Im Hinblick auf die beabsichtigte Novellierung des Polizeirechts werde er jedoch eine Bestandsaufnahme derartiger problematischer Datenübermittlungen vornehmen, um den Regelungsbedarf zu ermitteln.

Der Landesbeauftragte hofft, daß den Polizeibeamten „vor Ort" künftig die Entscheidung leichter gemacht wird, wenn sie vor der Frage stehen, ob sie „Dinge vom Hörensagen" weitergeben müssen oder nicht. Der heutige Ermessensspielraum bürdet ihnen nach seiner Auffassung eine zu große Verantwortung auf, nicht selten auch zu Lasten ihrer Mitbürger.

4.1.8 Probleme mit dem Entwurf zum Ausländerzentralregistergesetz

Das von den Datenschutzbeauftragten seit langem (vgl. 10. TB, S. 30) geforderte Ausländerzentralregistergesetz liegt jetzt als Entwurf des Bundesinnenministers auf dem Tisch. Ein Blick in den Text offenbart leider, daß datenschutzrechtliche Belange weitgehend unbeachtet geblieben sind. Im Ausländerzentralregister werden z. Z. über alle Ausländer, die sich in der Bundesrepublik aufhalten, umfassende Daten gesammelt, ohne daß es hierfür eine gesetzliche Grundlage gibt. Das Verfahren und der Umfang der Datenspeicherungen und der Datenübermittlungen ist lediglich durch interne Regelungen der Ausländerbehörden des Bundes und der Länder festgelegt worden. Wenn nun auch der Gesetzgeber derartige Datenspeicherungen und Kontrollen nachträglich sanktionieren will, so sollte er bedenken, daß das informationelle Selbstbestimmungsrecht auch für Ausländer

gilt. Davon ist im Gesetzentwurf nämlich wenig zu spüren. Der Landesbeauftragte fordert vor allem, daß eine normenklare Regelung für die Datenübermittlungen aus dem Register geschaffen wird. Entsprechende Festlegungen sind zwar in einigen Bestimmungen enthalten. Der daneben vorgesehene Auffangtatbestand lautet aber schlicht: „Benötigt der Empfänger zur Erfüllung seiner Aufgaben zusätzliche Daten, so sind auch diese zu übermitteln." Ein weiteres Problem liegt in der häufigen Verwendung unbestimmter Rechtsbegriffe. Die Ausländerbehörden sollen z. B. darüber entscheiden, ob „Einreisebedenken" vorliegen oder ob eine Erfassung zur „Bekämpfung einer terroristischen Gefahr" erforderlich ist. Was Einreisebedenken sind oder wann eine terroristische Gefahr vorliegt, ist jedoch nicht bestimmt. Im übrigen fehlen Regelungen zu wichtigen datenschutzrechtlichen Bereichen, wie etwa der Berichtigung von Daten, der Einrichtung von Auskunftssperren, der Protokollierung von Auskünften oder der näheren Bestimmung automatischer Abrufe.

Der Landesbeauftragte geht davon aus, daß der Gesetzentwurf unter Berücksichtigung seiner Kritik noch einmal überarbeitet wird.

4.1.9 Bau- und Vermessungswesen

4.1.9.1 Transparenz auch für die „Serviceleistungen" der Bauaufsichtsbehörden

Nach der Landesbauordnung gelten mit dem Bauantrag alle Anträge auf Genehmigung, Zustimmung, Bewilligung und Erlaubnis als gestellt, die nach anderen Vorschriften unmittelbar für die Errichtung, Änderung, Nutzung oder den Abbruch von baulichen Anlagen oder Werbeanlagen erforderlich sind. Die Bauaufsichtsbehörde holt also bei anderen Behörden die notwendigen Verwaltungsentscheidungen ein und händigt diese mit der Baugenehmigung an den Antragsteller aus. Wenn auch diese staatliche „Serviceleistung" auf einem Gesetz beruht, so waren sich doch die wenigsten Antragsteller der damit verbundenen Datenübermittlungen bewußt. Der Landesbeauftragte fordert deshalb aus Gründen der Transparenz, daß die Bürger im Bauantrag über die gesetzliche „Wohltat" unterrichtet werden.

Außerdem unterrichten die Bauämter auch am Baugenehmigungsverfahren nicht beteiligte Behörden wie z. B. das Katasteramt, das Fernmeldeamt, das Energieversorgungsunternehmen usw. Insoweit reicht nach Meinung des Datenschutzbeauftragten eine bloße Information des Betroffenen nicht mehr aus. Die Bauantrags- und Genehmigungsdaten verlassen nämlich den Aufgabenbereich, für den sie der Antragsteller bestimmt hat. Nach dem Volkszählungsurteil unterliegen aber gerade freiwillig zur Verfügung gestellte Daten einer besonders strengen Zweckbindung. Da eine gesetzliche Grundlage für eine Durchbrechung in der Landesbauordnung nicht vorhanden ist, dürfen die Daten nur mit Zustimmung des Bauwilligen übermittelt werden.

Der Innenminister hat sich die Rechtsansicht des Landesbeauftragten zu eigen gemacht und zugesagt, bei einer Neufassung der Landesbauordnung die notwendigen Rechtsvorschriften zu erlassen.

4.1.9.2 Grenzen der Auskünfte aus dem Liegenschaftskataster

Wenn Investoren Liegenschaften für ihre geschäftlichen Zwecke suchen, fordern häufig Immobilienmakler bei den Katasterämtern Auskünfte über ganze Wohnviertel und Straßenzüge sowie über die Eigentumsverhältnisse einzelner Grundstücke an, um sich einen ersten Überblick über geeignete Objekte zu verschaffen. Einige Katasterämter sind derartigen umfassenden Auskunftsersuchen richtigerweise nicht nachgekommen.

Im Gegensatz zur uneingeschränkten Öffentlichkeit anderer Register, wie z. B. des Handelsregisters oder des Schuldnerverzeichnisses, unterliegen die Liegenschaftsregister nach dem Vermessungs- und Katastergesetz nur einer begrenzten Publizität. Die Einsichtnahme und Auskunftserteilung ist der des Grundbuches nachgebildet und damit von der Darlegung eines berechtigten Interesses abhängig. Makler haben kein generelles Auskunfts- und Einsichtsrecht in Katasterunterlagen. Nur beim Vorliegen eines konkreten Auftrages durch einen Kunden, Verhandlungen mit einem bestimmten Eigentümer aufzunehmen, darf von einem berechtigten Interesse ausgegangen werden. Der Schutz des einzelnen Grundstückseigentümers vor unerwünschten Kaufangeboten ist höher einzustufen als das Interesse des Maklers an einer eventuellen Geschäftsbeziehung. Auch könnte die Auskunftserteilung über alle Grundstücke in einer Region zu einer Datenvorratshaltung führen und sich zu einem zweiten Liegenschaftsregister entwickeln, ein datenschutzrechtlich sehr unerwünschter Zustand. Es dürfen auch nur die erforderlichen Daten aus dem Liegenschaftskataster bekannt gegeben werden. In der Regel sollte sich die Auskunft auf die Nennung des Grundbuches und des Grundbuchblattes beschränken. Daten über Eigentumsverhältnisse dürfen nicht übermittelt werden, weil das Liegenschaftskataster insoweit keine verbindlichen Eintragungen enthält.

4.1.9.3 Auch bei einer öffentlichen Planfeststellung sind persönliche Daten zu schützen

Die gesetzlich vorgesehene Öffentlichkeit von Verwaltungsverfahren darf nicht zu Lasten einzelner Beteiligter gehen. Darauf hat der Landesbeauftragte immer wieder hingewiesen (vgl. auch Textziffer 4.1.3.1). Er fühlt sich durch den Beschluß des Bundesverfassungsgerichts vom 14. Oktober 1987 (1 BvR 1244/87, DVBl. 87, 1263) in seiner Auffassung bestätigt.

In einem Planfeststellungsverfahren hatten die Beschwerdeführer zur Begründung ihrer Einwendungen Angaben über die Größe, die Betriebsstruktur, die Einkünfte und den Schuldenstand ihrer landwirtschaftlichen Betriebe gemacht. Diese Daten fanden sie plötzlich im öffentlich ausgelegten Planfeststellungsbeschluß wieder. Das Bundesverfassungsgericht stellte fest, daß ein Planfeststellungsbeschluß auch ohne einen Personenbezug der Betriebsdaten öffentlich bekannt gemacht werden könne.

Für die Einwender bliebe die Behandlung ihrer Einwendungen erkennbar und für den Vergleich mit anderen Einwendungen im Verfahren reichten die Angaben im Planfeststellungsbeschluß auch ohne personelle Zuordnung aus.

Die Entscheidung zeigt, daß auch in gesetzlich geregelten öffentlichen Verfahren ein möglichst umfassender Schutz Betroffener zu gewährleisten ist.

4.2 Justizverwaltung

4.2.1 Immer wieder - Mißbrauch der Grundbucheinsicht

Als sich ein Bürger beim Landesbeauftragten darüber beschwerte, daß er von einer Hausverwaltung im Rahmen eines Zivilrechtsstreits einen Auszug aus seinem Grundbuch mit allen Einzelheiten vorgelegt bekommen hatte, obwohl die Grundbuchauskunft für den Rechtsstreit selbst unerheblich war, teilte das Grundbuchamt folgendes mit: „Es ist fraglich, ob die von Ihnen erwähnten Daten aufgrund einer direkten Einsichtnahme seitens der Grundstücksverwaltung X in die hiesigen Akten bekanntgeworden sind. Ich darf darauf hinweisen, daß z. B. auch beauftragte Notare das Recht der Einsichtnahme haben. Ob hier eine direkte Einsichtnahme erfolgt ist, kann anhand der Akten nicht nachvollzogen werden, da hierüber keine Aktenvermerke gefertigt werden. Es muß aber unter den gegebenen Umständen bezweifelt werden. Ihre einzelnen Fragen vermag ich nicht zu beantworten, bei der hohen Zahl der Einsichtsfälle können sich die von mir befragten Mitarbeiter nicht an diesen Einzelfall erinnern. Schriftliche Aufzeichnungen hierüber liegen nicht vor."

Dieser Fall hat seine Vorgänger. Im Tätigkeitsbericht für das Jahr 1985 (8. TB, S. 43) hat der Landesbeauftragte Klage darüber geführt, daß Notare in Einzelfällen ihre Privilegien bei der Einsichtnahme in das Grundbuch dazu benutzten, Informationen im Rahmen ihrer Anwaltstätigkeit (z. B. in einem Zivilrechtsstreit) zu verwerten. Zwar sind Fälle dieser Art zuletzt vor vier Jahren an den Landesbeauftragten herangetragen worden. Seine Mahnungen und die Hinweise der Standesvertretungen scheinen also erfolgreich zu sein. Dennoch hat er im Hinblick auf den gesamten Komplex der Grundbucheinsicht den Grundbuchämtern vorgeschlagen, durch Kontrollen sicherzustellen, daß die beantragte Einsicht durch ein berechtigtes Interesse gedeckt ist.

Wenn in der Grundbuchordnung die Einsichtnahme und Auskunftserteilung von der Darlegung eines berechtigten Interesses abhängig gemacht wird und es bei einer verfassungskonformen Auslegung dieser Bestimmung weiterhin erforderlich ist, daß keine schutzwürdigen Belange des betroffenen Grundeigentümers beeinträchtigt werden, dann erfordert dies eine dokumentierte Einzelfallprüfung durch das Grundbuchamt, die für die Aufsichtsbehörden und den Datenschutzbeauftragten nachvollziehbar sein muß.

Der Justizminister ist anderer Ansicht und lehnt die Protokollierung der Grundbucheinsicht wegen eines unvertretbaren Perso-

nalmehraufwandes bei den Grundbuchämtern ab. Er ist lediglich bereit, die Frage mit den Justizministern des Bundes und der Länder zu erörtern, wenn die Grundbuchordnung (irgendwann einmal) novelliert werden sollte.

4.2.2 Hilfestellung für privates Handelsregister abgelehnt

Ein Wirtschaftsinformationsdienst beabsichtigte, ein privates bundesweites Handelsregister aufzubauen, und forderte die Amtsgerichte unter Berufung auf die Öffentlichkeit des amtlichen Registers auf, die notwendigen Mikroverfilmungen zu genehmigen.

Der Landesbeauftragte hat hiergegen Bedenken erhoben. Der Gesetzgeber hat sich bewußt gegen ein zentrales Handelsregister entschieden. Es wäre eine Umgehung seines Willens, wenn nunmehr ein privater Unternehmer dabei unterstützt würde, ein bundesweites zentrales Register aufzubauen. Das Vorhaben des Unternehmers würde im übrigen eine neue Dimension der Registerpublizität eröffnen. Ein zentrales, elektronisch geführtes Register würde Datenverknüpfungen ermöglichen, deren Ausmaß und deren Auswirkungen auf das einzelne Unternehmen und auf den Wettbewerb nicht ohne weiteres überblickt werden können. Schon die Möglichkeit weitreichender und sogar negativer Folgen für die Betroffenen macht es erforderlich, die Entscheidung über eine Zentralisierung des Handelsregisters dem Gesetzgeber vorzubehalten.

Der Justizminister teilt die Bedenken des Landesbeauftragten und hat die Registergerichte aufgefordert, die Genehmigung zur Herstellung von Mikroverfilmungen zu versagen. Das Unternehmen, das sich auf eine Richtlinie der Europäischen Gemeinschaft beruft, die angeblich die Mitgliedsstaaten zur Erstellung zentraler Handelsregister verpflichtet, hat den Europäischen Gerichtshof angerufen. Der Ausgang des Verfahrens bleibt abzuwarten.

4.2.3 Interne Dateien doch nicht intern

In einem von einer Staatsanwaltschaft an ein Amtsgericht übersandten Bußgeldvorgang befand sich eine sogenannte Vollauskunft aus dem staatsanwaltschaftlichen Informationssystem mit zahlreichen Daten aus früheren Verfahren gegen den Beschuldigten. Dessen Anwalt rügte die Übermittlung mit dem Vorwurf, das Amtsgericht werde durch die mit einem verkürzten Datenprofil ausgedruckte Informationsfülle über eingestellte und abgeschlossene Verfahren aus früheren Jahren beeinflußt und möglicherweise „verführt", sich bei der Urteilsfindung anstatt auf die Sachakten mehr auf den Auszug zu stützen. Bei der Zusammenstellung handelte es sich um einen Auszug der automatisierten zentralen Namenskartei der Staatsanwaltschaft. Aufgabe dieser Datei ist es, den Staatsanwälten Anhaltspunkte für weitere Ermittlungs- oder Strafverfahren gegen einen Beschuldigten, Angeklagten bzw. Täter zu liefern. Sie ist im Prinzip nur ein „Aktensuchsystem" und darf deshalb nur innerhalb der Staatsanwaltschaft genutzt werden. In jedem Bearbeitungsfall muß eine Rückkoppelung auf die eigentliche Sachakte stattfinden. Die Sachakte wird also nicht durch die EDV-Datei

ersetzt. Der Generalstaatsanwalt und die einzelnen Staatsanwaltschaften haben deshalb angeordnet, daß die Vollauskünfte in den Handakten zu verbleiben haben. Die Weitergabe der Auskünfte mit dem für das Amtsgericht bestimmten Vorgang widerspricht diesen Weisungen. Der Landesbeauftragte hat die Datenübermittlung deshalb beanstandet.

4.2.4 Verfassungsgericht „kippt" die Veröffentlichung von Entmündigungen - neues Gesetz in Vorbereitung

In seinem 9. Tätigkeitsbericht (S. 30) hatte der Landesbeauftragte die Veröffentlichung von Entmündigungsbeschlüssen durch die Vormundschaftsgerichte kritisiert und auf die damit verbundene übermäßige Beeinträchtigung der Persönlichkeitsrechte Hilfsbedürftiger hingewiesen. Das Bundesverfassungsgericht hat mittlerweile diese Veröffentlichungspflicht für verfassungswidrig erklärt (Beschluß vom 9. März 1988 – 1 BvL 49/86, RDV 88, 194).

Das Gericht kommt zu dem Ergebnis, daß in § 687 Zivilprozeßordnung die Grenzen des Zumutbaren überschritten seien. Die öffentliche Bekanntgabe einer Entmündigung entfalte keine Rechtswirkung, sondern erschöpfe sich in einer bloßen Warnung. Da das Gesetz die Bekanntmachung nur für eine geringe Zahl von Entmündigungen (Trunksucht und Verschwendung) vorsehe, bedeutet die Bekanntmachung andererseits eine tiefgreifende Beschränkung der Befugnis des einzelnen, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Die Bekanntmachung betreffe nicht nur die im Rechtsverkehr erhebliche Eigenschaft der Geschäftsfähigkeit, sondern die Persönlichkeit als Ganzes. Sie berge die Gefahr einer sozialen Abstempelung in sich und könne die soziale Wiedereingliederung erschweren. Überdies erreiche sie eine nicht überschaubare Zahl von Adressaten. Die Verwendung dieser Information ließe sich nicht eingrenzen. Die Zivilprozeßordnung verstoße deswegen insoweit gegen das Grundgesetz.

Das Gericht nutzte zudem die Gelegenheit, noch einmal zum informationellen Selbstbestimmungsrecht Stellung zu nehmen. Es stellt fest, daß die Möglichkeiten und Gefahren der automatisierten Datenverarbeitung zwar die Notwendigkeit des Schutzes persönlicher Daten deutlicher hervortreten ließen, nicht aber Grund und Ursache ihrer Schutzbedürftigkeit seien. Das Recht auf informationelle Selbstbestimmung schütze vielmehr wegen seiner persönlichkeitsrechtlichen Grundlage generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten und sei nicht auf den jeweiligen Anwendungsbereich der Datenschutzgesetze oder datenschutzrelevanter gesetzlicher Sonderregelungen beschränkt. Sodann nimmt es seine aus dem Volkszählungsurteil bekannte Position wieder auf und weist darauf hin, daß der einzelne Einschränkungen seines Persönlichkeitsrechts nur im überwiegenden Allgemeininteresse hinnehmen müsse, solche Beschränkungen bedürften einer gesetzlichen Grundlage.

Der Entscheidung kommt nicht nur im Hinblick auf die Rechtsposition des betroffenen Bürgers eine erhebliche Bedeutung zu, sie zeigt darüber hinaus, daß das Bundesverfassungsgericht

nach wie vor an der klaren Aussage über die grundrechtliche Verankerung des informationellen Selbstbestimmungsrechts festhält und bereit ist, auch „altehrwürdige" Gesetze, wie die Zivilprozeßordnung, an diesem Maßstab zu messen.

Der aufgrund dieses Beschlusses erarbeitete Entwurf eines Betreuungsgesetzes läßt nicht nur die öffentliche Bekanntmachung einer Entmündigung entfallen, sondern sieht weitere grundlegende Änderungen im Recht hilfsbedürftiger Volljähriger vor. Er macht vor allem den Versuch, den Gedanken der persönlichen Betreuung zu stärken und die Stigmatisierung der Betreuten als gesellschaftliche Außenseiter zu vermeiden. Beides kann unter datenschutzrechtlichen Gesichtspunkten nur begrüßt werden. Um diese Ziele wirklich zu erreichen, muß der Entwurf allerdings noch überarbeitet werden. Insbesondere der geplante Informationsaustausch zwischen den an der Betreuung beteiligten Personen und den Behörden muß auf seine Notwendigkeit hin überprüft werden. Der Umfang, die beteiligten Stellen und die Zweckbestimmung der übermittelten Daten müssen konkretisiert und in normenklarer Weise geregelt werden. Unbestimmte Rechtsbegriffe – wie z. B. das „Wohl des Betroffenen"– sollten konkreter gefaßt werden. Insbesondere sollte auch eine umfassende Information des zu Betreuenden vorgesehen werden.

Der Landesbeauftragte hat seine Überlegungen dem Justizminister dargestellt und hofft, daß dieser sie in die Beratungen des Bundesgesetzes einbringen wird.

4.3 Steuerverwaltung

4.3.1 Sollen die Datenschutzbeauftragten an die Kette gelegt werden?

Solange es das Datenschutzrecht gibt, streiten sich die Steuerverwaltungen des Bundes und der Länder und die Datenschützer darüber, welche Kontrollbefugnisse dem Bundes- und den Landesbeauftragten zustehen. Unter Hinweis auf das Steuergeheimnis verweigert man ihnen Einblick in die Steuerdateien, sofern nicht konkrete Beschwerden der Steuerpflichtigen vorliegen. Deshalb sind die Finanzämter die einzigen Behörden, in denen keine systematischen Querschnittsprüfungen möglich sind. Hiergegen protestieren die Datenschutzbeauftragten seit Jahren und haben den Bundesgesetzgeber aufgefordert, durch eine Änderung der Abgabenordnung Rechtsklarheit zu schaffen (vgl. 7. TB, S. 34).

Was zu einem Mehr an Datenschutz führen sollte, droht zu einem Waterloo für die Datenschutzbeauftragten zu werden. Sollte der als Referentenentwurf des Bundesfinanzministers vorliegende und bereits mit den obersten Finanzbehörden der Länder abgestimmte „Gesetzentwurf bereichsspezifischer Datenschutzvorschriften im Anwendungsbereich der Abgabenordnung" vom November 1988 realisiert werden, dürften sie endgültig „an die Kette gelegt werden".

- Die Kontrollbefugnisse des Bundesbeauftragten für den Datenschutz sind dann nicht mehr im Bundesdatenschutzgesetz,

sondern in der Abgabenordnung selbst festgelegt. Was und wie er kontrollieren darf, soll also in einem Steuergesetz geregelt werden.

- Seine Kontrolle soll im übrigen auf die dateimäßige Datenverarbeitung beschränkt sein.
- Die Datenerhebung der Finanzämter soll generell nicht der Kontrolle des Datenschutzbeauftragten unterliegen.
- Einblick in personenbezogene Unterlagen erhält der Bundesbeauftragte für den Datenschutz erst, nachdem das Einverständnis der Betroffenen eingeholt worden ist.
- Es ist nicht eindeutig geregelt, daß er die Betroffenen über das Ergebnis der Prüfungen unterrichten darf.

Diese verfassungsrechtlich sicher höchst problematischen Neuregelungen „verblassen" aber vor der Absicht, auch die Landesdatenschutzgesetze auszuhebeln. Auch die Rechte der Landesbeauftragten für den Datenschutz sollen sich nämlich nach den o. a. restriktiven Regelungen der Abgabenordnung richten. Bisher gründen sich die Befugnisse eines Landesbeauftragten auf „sein" Landesdatenschutzgesetz. Er hat entsprechend den Vorgaben des Landesgesetzgebers zu überwachen, ob die Finanzminister als Landesbehörden die bundesgesetzlichen Regelungen des Steuerrechts im datenschutzrechtlichen Sinne richtig anwenden. Diese Gesetzgebungskompetenz will der Bund den Ländern offenbar streitig machen. Als Begründung wird angeführt, daß die unterschiedlichen Datenschutzgesetze der Länder wegen ihres Einflusses auf die Durchführung des Besteuerungsverfahrens die verfassungsrechtlich gebotene gleichmäßige Besteuerung der Bürger beeinträchtige. Außerdem entstünden bei unterschiedlichem Datenschutzrecht vielfältige, schwer lösbare Fragen des interlokalen Datenschutzrechts im Verhältnis der Länder und des Bundes zueinander. Würde man dieser Argumentation folgen, müßte die Arbeit der Landesrechnungshöfe in gleicher Weise in Frage gestellt werden.

Für den Landesbeauftragten stellt sich die Frage, was die Steuerverwaltung zu verbergen hat, daß sie sich so sehr darum bemüht, nicht der gleichen Kontrolle durch die Datenschutzbeauftragten zu unterliegen wie alle anderen Verwaltungen. Nach Abschluß der Beratungen mit seinen Kollegen beim Bund und den Ländern wird er dem Finanzminister seine „Änderungswünsche" zu dem Gesetzentwurf vorlegen.

4.3.2 Kontrollmitteilungsverfahren eingestellt

Unter der Überschrift „Neue Probleme mit Kontrollmitteilungen" hat der Landesbeauftragte in seinem 10. Tätigkeitsbericht (S. 37) ein Verfahren kritisiert, durch das Empfänger staatlicher Zuschüsse verpflichtet wurden, ihre Kunden und die mit ihnen getätigten Geschäfte zu offenbaren. Er sah die Landeshaushaltsordnung nicht als ausreichende Rechtsgrundlage für derart weitreichende Mitteilungspflichten an. Dieser Auffassung sind die Finanzminister des Bundes und der Länder in der Zwischenzeit gefolgt. Das Verfahren ist eingestellt worden.

4.3.3 Schwierigkeiten mit der Datenbank

Eine besondere „Stärke" automatisierter Datenbanken besteht darin, daß Informationen, die ein Benutzer eingibt, allen anderen (befugten) Benutzern sofort zur Verfügung stehen. Deshalb werden die Personendaten in vielen Bereichen (Meldewesen, polizeiliche Erkenntnisdatei, Geschäftsstellenautomation der Staatsanwaltschaften usw.) mit Hilfe derartiger Datenbanken verwaltet. Auch die Steuerverwaltung setzt seit Jahren ein solches System ein. Den gewünschten Rationalisierungseffekt erzielt man aber nur dann, wenn die Datenverarbeitungsprogramme alle denkbaren Fallgestaltungen berücksichtigen und fehlerhafte Eingaben erkennen. Jede Nachlässigkeit auf diesem Gebiet kann fatale Folgen haben. In der Steuerverwaltung war folgendes passiert: Ein Finanzamt änderte einen Datensatz und beging dabei eine im Grunde kleine Unachtsamkeit. Das Änderungsprogramm war hierauf „nicht gefaßt". Als ein anderes Finanzamt auf den Bestand zugriff, interpretierte das Auswertungsprogramm die vorgefundenen Daten so falsch, daß bei einer Steuerpflichtigen die fälligen Kraftfahrzeugsteuern der geschiedenen Frau ihres Mannes angemahnt wurden. Wo die Finanzämter so sehr auf das Steuergeheimnis bedacht sind, war dies natürlich eine peinliche Angelegenheit, die durch entsprechende Korrekturen im automatisierten Verfahren und in den Programmen sofort bereinigt wurde.

Der Landesbeauftragte stellt diesen Vorfall nicht nur deshalb in seinem Tätigkeitsbericht dar, weil hier strenggenommen gegen das Steuergeheimnis verstoßen worden ist, sondern um unter Bezugnahme auf seine früheren Ausführungen (vgl. 8. TB, S. 64) nochmals auf die Bedeutung umfassender Programmtests und sorgfältiger Freigabeverfahren hinzuweisen.

4.3.4 Der Bundesfinanzhof bestätigt die Auffassung des Datenschutzbeauftragten

Im Jahr 1983 (6. TB, S. 41) hat der Landesbeauftragte die Steuerverwaltung kritisiert, weil sie sich bei umfassenden Übermittlungen von Steuerdaten an Gewerbebehörden zum Zweck der Gewerbeuntersagung auf eine Rechtsgrundlage berufen hat, die vom Bundesverwaltungsgericht als nicht gegeben angesehen worden war. Trotz dieser höchstrichterlichen Entscheidung beharrten die Finanzminister der Länder damals auf ihrem Rechtsstandpunkt, mit der Folge, daß sie sich nunmehr dem Spruch „ihres eigenen" obersten Gerichts beugen müssen: Der Bundesfinanzhof hat nämlich in einem Urteil vom 10. Februar 1987 (VII R 77/84) festgestellt, daß die Erteilung von Auskünften in gewerberechtlichen Untersagungsverfahren zwar im zwingenden öffentlichen Interesse liegen könne, sich aber auf die Steuerdaten zu beschränken habe, die mit der Ausübung des Gewerbes, das untersagt werden soll, im Zusammenhang stehen. Dabei sei der Grundsatz der Verhältnismäßigkeit zu beachten.

Zwischen den Entscheidungen des Bundesverwaltungsgerichtes und des Bundesfinanzhofes scheint es qualitative Unterschiede zu geben, denn erst jetzt haben die Länderfinanzminister ihre Verwaltungsanweisungen entsprechend geändert.

4.4 Wirtschaft und Verkehr

4.4.1 Unterstützung der Gerichte durch die Industrie- und Handelskammern

Auf die Tatsache, daß allgemeine Aufgabenzuweisungen den Behörden nicht zugleich Zwangsbefugnisse gegenüber dem Bürger verleihen, mußte der Landesbeauftragte eine Industrie- und Handelskammer aufmerksam machen. Kammern sind zwar nach dem Gesetz über die Angelegenheiten der freiwilligen Gerichtsbarkeit zur Unterstützung der Gerichte verpflichtet, wenn es z. B. für die Eintragung in das Handelsregister um die Prüfung der Eigenschaft als Vollkaufmann geht. Damit ist ihnen aber nicht die Befugnis gegeben, die entsprechenden Daten zwangsweise beim Gewerbetreibenden zu erheben. Anlaß für diese Feststellung, war die Beschwerde eines Kaufmanns, der sich zu Recht weigerte, von der Kammer gestellte Fragen zu beantworten, die Aufschlüsse über Jahresumsätze, Eigenkapital, Fremdkapital und Kreditaufnahmen zuließen.

Mit dieser datenschutzrechtlichen Bewertung will der Landesbeauftragte nicht die Aufgaben der Kammern in Frage stellen, Vorgänge von rechtlicher Bedeutung an die Registergerichte zu melden und auf deren Ersuchen Gutachten zu erstellen, Auskünfte zu erteilen oder Stellungnahmen zu Eintragungsanträgen abzugeben. Eine zwangsweise Erhebung von Daten ist jedoch allein dem Gericht als dem Herren des Verfahrens vorbehalten. Der Gewerbetreibende darf darüber nicht im unklaren gelassen werden. Er muß erkennen können, ob er zur Auskunft gesetzlich verpflichtet ist oder ob seine Angaben freiwillig sind. Diesem von Verfassungs wegen zu beachtenden Transparenzgedanken muß ggf. durch einen ausdrücklichen Hinweis auf die Freiwilligkeit Rechnung getragen werden.

4.4.2 Industrie- und Handelskammern sind keine Auskunfteien

Die Industrie- und Handelskammern verwalten umfangreiche Datenbestände über ihre Mitglieder und deren Betriebe und verwenden sie zur Erfüllung ihrer durch Gesetz und Satzung vorgeschriebenen Aufgaben der Beratung, Überwachung und Förderung. Solche Datenbestände sind für Behörden und private Institutionen attraktiv und üben deshalb eine große Anziehungskraft aus. So bat z. B. eine kommunale Katastrophenschutzbehörde um Übersendung von Namen und Anschriften bestimmter Gewerbebetriebe, um einen Katastrophenabwehrkalender zu erstellen. In einem anderen Fall wünschte das Umweltamt eines Kreises die Übermittlung von Namen und Anschriften derjenigen Gewerbebetriebe, die mit umweltgefährdenden Stoffen umgehen.

Ohne Zweifel benötigen die beiden Behörden derartige Daten zur Erfüllung der ihnen durch Gesetz übertragenen Aufgaben. Mit dieser Aufgabenzuweisung ist aber nicht die Befugnis der Industrie- und Handelskammern verbunden, Daten für die gänzlich anders gearteten Zwecke der empfangenden Behörden zu übermitteln. Die Zweckbindung ist ganz besonders bei den Daten zu beachten, die ihnen von den Kammermitgliedern freiwillig bereitgestellt worden sind. Auch die Vorschriften über die Amtshilfe können nicht als gesetzliche Übermittlungsgrund-

lage herangezogen werden. Sie sind nicht anwendbar, weil Amtshilfe nur im Einzelfall auf besondere Anforderung zu leisten ist.

Der Landesbeauftragte hat den Kammern deshalb den Rat gegeben, von den betroffenen Kammermitgliedern vor der Übermittlung entweder die Einwilligung einzuholen oder ihnen ein Widerspruchsrecht innerhalb einer angemessenen Frist einzuräumen. Selbstverständlich müssen die Betroffenen zuvor ausführlich über den Vorgang unterrichtet werden.

4.5 Ernährung, Landwirtschaft, Forsten, Fischerei, Natur und Umwelt

4.5.1 Gutes tun und darüber reden?

Der Europäische Fonds für die regionale Entwicklung gewährt Fördermittel zur Strukturverbesserung. Damit die Erfüllung dieser ohne Zweifel wichtigen Aufgabe in das rechte Licht gerückt wird, werden die Förderfälle in einer Dokumentation in personenbezogener Form veröffentlicht. Gern nehmen die Landesbehörden die Veröffentlichung zum Anlaß, um auch ihrerseits entsprechende Informationen an die Presse zu geben. So fanden Fischer, Inhaber von Krabbenschälbetrieben und Betreiber von Siloanlagen zu ihrer Überraschung nicht nur ihre Namen und Adressen, sondern auch den Betrag der Gesamtinvestition und den Anteil aus dem Strukturförderungsfonds der EG in der Presse wieder. In einigen Fällen wurden sogar weitere Details gebracht, so z. B. die Zahl der einzustellenden Mitarbeiter und die weiteren Ziele der Geschäftspolitik. In ihren Beschwerden machten die Zuschußempfänger geltend, daß z. B. Konkurrenten durch die Veröffentlichung des genauen Zahlenwerks Rückschlüsse auf das Geschäftsgebaren und die Finanzsituation des Unternehmens ziehen konnten.

Der Landesbeauftragte begrüßt es deshalb, daß aufgrund seiner Empfehlung der Minister für Ernährung, Landwirtschaft, Forsten und Fischerei vor künftigen Veröffentlichungen die Einwilligung der betroffenen Unternehmer einholen will. Zwar hat auch die EG-Kommission ihre Veröffentlichungspraxis im Jahr 1988 dahin gehend modifiziert, daß auf die Ausweisung des Namens bzw. der Firma des Förderungsempfängers verzichtet wird. Das bedeutet allerdings nur eine unvollkommene Anonymisierung, da mit gewissen Branchenkenntnissen nach wie vor Rückschlüsse auf den einzelnen Förderungsempfänger möglich sind. Nach Kenntnis des Landesbeauftragten werden auch kartellrechtliche Enscheidungen der Kommission und Urteile des Europäischen Gerichtshofs ohne eindeutige Rechtsgrundlage und ohne sachlich zwingende Gründe personenbezogen veröffentlicht. Die EG beruft sich darauf, daß sie als überstaatliche Einrichtung nicht unter das deutsche Datenschutzrecht fällt.

4.5.2 Umweltschutz und Persönlichkeitsschutz

Die Information des einzelnen und der Öffentlichkeit sind bewährte Prinzipien des Datenschutzes, um die von einer geheimnisvollen „Aura“ umgebene elektronische Datenverarbeitung nachvollziehbar und kontrollierbar zu machen. Es mehren sich

die Stimmen, die gleichen Prinzipien auch für die Bekämpfung der zunehmend sichtbar werdenden Beeinträchtigungen unserer Umwelt zugrunde zu legen. Die Forderungen, die Namen der Personen und Institutionen zu veröffentlichen, die im Verdacht stehen, die Umwelt durch hohe Immissionen zu schädigen, werden lauter und drängender. Es sollen „Roß und Reiter" genannt werden.

- So wurde der Landesbeauftragte mit der Frage befaßt, ob und unter welchen Voraussetzungen eine Gemeinde Immissionsdaten einschl. des Namens des Verursachers in den Selbstverwaltungsgremien bekanntgeben und veröffentlichen darf. Er mußte darauf hinweisen, daß das Bundesimmissionsschutzgesetz verbietet, Einzelangaben der Immissionserklärung zu veröffentlichen, wenn aus diesen Rückschlüsse auf Betriebs- oder Geschäftsgeheimnisse gezogen werden können.
- Der gesamte Bereich der Überwachung von Abwassereinleitungen in oberirdische Gewässer, in das Grundwasser oder in die Küstengewässer ist eine den Landräten und Bürgermeistern der kreisfreien Städte zur Erfüllung nach Weisung übertragene Aufgabe, zu deren Erleichterung natürlich auch eine kartei- oder EDV-mäßige Erfassung von personenbezogenen Daten zulässig ist. Für eine Datenweitergabe an die Selbstverwaltungsgremien oder für eine Veröffentlichung gibt das Landeswassergesetz jedoch keine Befugnis.
- Gleiches gilt für die Veröffentlichung von personenbezogenen Einzelangaben über die Einleitungen in die kommunalen Abwässeranlagen. Einer öffentlichen Bekanntmachung der Schmutzwassermenge einzelner Bürger bzw. Unternehmen stehen die Geheimhaltungs- und Verschwiegenheitspflichten der Verwaltung und letztlich auch das Landesdatenschutzgesetz entgegen.

So verständlich das Interesse der kommunalen Gremien sein mag, Transparenz auch im Bereich des Umweltschutzes zu schaffen, das sog. Volkszählungsurteil des Bundesverfassungsgerichts schiebt hier einen Riegel vor. Solange keine klaren Befugnisnormen in den Immissionsschutz- und Wassergesetzen unter angemessener Berücksichtigung der schützenswerten Interessen der Betroffenen geschaffen werden, steht das informationelle Selbstbestimmungsrecht dem „Öffentlichkeitsprinzip" entgegen.

4.6 Sozial- und Gesundheitswesen

4.6.1 Soziales

4.6.1.1 Offenbarung von Sozialdaten an den Zahnarzt

Daß verwaltungspraktische Überlegungen erheblichen Einfluß auf die Wahrung der Rechte der Bürger haben, zeigt der Fall eines Petenten, in dem das Sozialamt die vom Patienten zu tragenden Restkosten einer zahnärztlichen Behandlung übernahm. Das Sozialamt setzte nicht nur ihn, sondern auch den behandelnden Zahnarzt von der Restkostenübernahme in

Kenntnis. Der Zahnarzt rechnete nur einen Teil der Kosten mit der Krankenkasse und den anderen Teil mit dem Sozialamt ab. „Ganz nebenbei" erfuhr er so, daß sein Patient Sozialhilfeempfänger war.

Nach Auffassung des Landesbeauftragten stellt die Restkostenübernahme keine Sachleistung, sondern einen Zuschuß zu den Behandlungskosten dar. Das zuständige Kreissozialamt ist dieser Auffassung beigetreten. Das Verfahren wurde umgestellt. Die überflüssige Information wird in Zukunft entfallen.

4.6.1.2 Übervorsichtige Krankenhäuser

Viele Krankenhäuser stellen bei den Trägern der Sozialhilfe vorsorglich Anträge auf Erstattung der Krankenhauskosten, sobald leiseste Zweifel daran bestehen, daß eine Kostenübernahme durch eine Krankenkasse erfolgt oder der Patient die Kosten selbst tragen kann. Findet sich später ein anderer Kostenträger, wird das Sozialamt eben nicht in Anspruch genommen. Deshalb heißt die Devise: „Lieber einmal mehr als zu wenig". Mit den Anträgen, die unmittelbar nach der Einweisung abgeschickt werden, erfahren die Sozialämter neben einer Vielzahl persönlicher Daten des Patienten auch die Einweisungsdiagnose.

Obwohl der Landesbeauftragte sich davon überzeugen lassen mußte, daß die Einweisungsdiagnose mitgeteilt werden muß und daß von der Rechtsprechung ein recht frühzeitiger Antrag auf Kostenerstattung gefordert wird, hat er darauf hingewiesen, daß vorsorgliche Kostenübernahmeanträge vom Gesetz nicht als Regelfall, sondern als Ausnahme vorgesehen sind. Auch die Offenbarung von Patientendaten auf diesem Wege bedarf einer Begründung im Einzelfall.

4.6.1.3 Sozialdatenschutzbeauftragter - Datenschutz für den Bürger vor Ort

Nach den Bestimmungen des Sozialgesetzbuches sind von den Sozialleistungsträgern „Sozialdatenschutzbeauftragte" zu bestellen, wenn bei einer automatisierten Verarbeitung personenbezogener Daten mindestens fünf, sonst mindestens 20 Mitarbeiter ständig im Sozialamt beschäftigt sind. Der Landesbeauftragte wurde nun von einigen Gemeinden um Stellungnahme zu der Frage gebeten, wer im Falle der Übertragung der Aufgaben vom eigentlich zuständigen Kreis auf die kreisangehörigen Städte und Gemeinden einen solchen Beauftragten zu bestellen hat. Der Schleswig-Holsteinische Landkreistag hält nämlich die Bestellung der Beauftragten zentral bei den Kreisen für ausreichend. Dies stelle eine einheitliche Handhabung des Rechts bei den örtlichen Sozialämtern sicher.

Der Landesbeauftragte ist anderer Auffassung. Die Sozialdatenschutzbeauftragten sollen nach der Konzeption des Sozialgesetzbuches ihre Aufgaben dort erfüllen, wo Sozialdaten verarbeitet werden. Die Fälle einer Aufgabendelegation sind im Sozialgesetzbuch zwar nicht ausdrücklich geregelt. Diesem in der Praxis häufig vorkommenden Sachverhalt kann in Auslegung des gesetzgeberischen Willens aber nur durch die Bestellung eines Datenschutzbeauftragten vor Ort Rechnung getragen werden.

4.6.1.4 Der Sozialversicherungsausweis - Totalerfassung aller Arbeitnehmer geplant

Die Bundesregierung beabsichtigt, zur wirksameren Bekämpfung der Schwarzarbeit einen Sozialversicherungsausweis einzuführen. Er soll bei jedem Beschäftigungsbeginn dem Arbeitgeber vorgelegt werden. In bestimmten Bereichen der Wirtschaft (Baugewerbe) soll der Ausweis sogar während der Arbeit stets mitgeführt werden. Das mit dem Gesetzentwurf verfolgte Ziel, die Schwarzarbeit zu bekämpfen und die soziale Sicherung der Arbeitnehmer zu gewährleisten, ist verständlich. Den Sozialversicherungsausweis sollen aber auch geringfügig beschäftigte Personen, die keiner Sozialversicherungspflicht unterliegen, erhalten. Hierzu gehören in erster Linie Schüler, Werkstudenten und Hausfrauen mit einer Nebenbeschäftigung. Sie alle sollen künftig umfangreichen Meldepflichten unterliegen und in eine zentrale Datei beim Verband Deutscher Rentenversicherungsträger aufgenommen werden.

Eine derartige zentrale „Verdatung" nicht versicherungspflichtiger Bürger erscheint dem Landesbeauftragten nicht erforderlich und unverhältnismäßig. Als Einzugsstellen für die Rentenversicherung erreichen die Krankenkassen diesen Personenkreis bereits heute durch ihre Kontrollen. Daß sie dabei nur ihren eigenen Zuständigkeitsbereich überprüfen können und sich einige Arbeitnehmer gelegentlich der Kontrolle entziehen, rechtfertigt kaum eine totale und zentrale Erfassung aller Arbeitnehmer. Die vielfältigen Nutzungsmöglichkeiten des Sozialversicherungsausweises bergen erhebliche Gefahren für seine zweckfremde Verwendung in sich. Deshalb sind strenge Beschränkungen für seine Benutzung zu fordern.

Man wird auch die Frage prüfen müssen, ob es überhaupt verfassungsrechtlich zulässig ist, die Rentenversicherungsnummer zur Bekämpfung der Schwarzarbeit zu verwenden. Soweit andere Stellen als die Rentenversicherungsträger die Rentenversicherungsnummer nutzen dürfen, ist dies auf konkrete Aufgaben im Zusammenhang mit Leistungen nach dem Sozialgesetzbuch beschränkt.

Der Landesbeauftragte hat den Minister für Soziales, Gesundheit und Energie von seinen Bedenken in Kenntnis gesetzt.

4.6.1.5 Strukturreform im Gesundheitswesen - der Zweck heiligt nicht alle Mittel

In den Beratungen des inzwischen in Kraft getretenen Gesundheitsreformgesetzes sind durch die Bemühungen der Datenschutzbeauftragten des Bundes und der Länder die Informationswünsche der Krankenkassen und der kassenärztlichen Vereinigungen entscheidend zurückgeschraubt worden. Stand am Anfang des Gesetzgebungsverfahrens das Ziel im Vordergrund, Einsparungen im Gesundheitswesen durch Erhebung und Verarbeitung der Gesundheitsdaten von Millionen von Bundesbürgern zu erreichen und die Verfahren möglichst verwaltungsfreundlich zu gestalten, so sind im geltenden Gesetz an die Stelle der Totalkontrolle aller in Form eines „Leistungskontos" für jeden Versicherten einzelne Stichproben und Wirtschaftlich-

keitsuntersuchungen getreten. Dies ist als ein datenschutzrechtlicher Erfolg zu werten.

Der Landesbeauftragte fragt sich allerdings: Warum mußten erst die Datenschutzbeauftragten darauf aufmerksam machen, daß eine lückenlose Übersicht über die Leistungen der Ärzte, der Apotheken und der Kliniken sowie die Verknüpfung und Auswertung dieser Informationen die Versicherten, die Ärzte und die Apotheker total durchleuchten und damit tief in das Grundrecht auf informationelle Selbstbestimmung eingreifen würden? Warum bedurfte es wiederum der Warnungen der Datenschutzbeauftragten, bevor entschieden wurde, daß die Rentenversicherungsnummer nicht im Krankenversicherungsbereich verwendet werden darf? Die Gefahr lag doch auf der Hand, daß sie bereichsübergreifend im gesamten Sozialwesen eingesetzt – mit einem einheitlichen Ordnungsmerkmal über fünfzig Millionen Bundesbürger identifizierbar machen und damit in die Nähe eines allgemeinen Personenkennzeichens gerückt würde.

Die Ursache mag darin liegen, daß der Datenschutz von den Gesetzes„machern" oft nur als „abstrakte Beschreibung abstrakter Gefahren" abgetan wird. Man glaubt einfach nicht, daß er einen gesetzlichen Handlungsbedarf für konkrete Schutzvorkehrungen auslösen kann. So bleibt den Datenschutzbeauftragten wohl auch weiterhin die undankbare Aufgabe, sich bei Gesetzgebungsvorhaben seherisch als „Kassandra" zu den Risiken für das Persönlichkeitsrecht der betroffenen Bürger zu Wort zu melden. Auch wenn das Bundesverfassungsgericht in dem Volkszählungsurteil die Feststellung trifft, daß der rechtzeitigen Beteiligung unabhängiger Datenschutzbeauftragter eine erhebliche Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung zukommt, sollten Regierung und Verwaltung sich nicht gehindert sehen, auch ihrerseits über die Gewährleistung des Rechts auf informationelle Selbstbestimmung vorausschauend und eingehend nachzudenken.

4.6.2 Gesundheit

4.6.2.1 Jugendzahnpflegewettbewerb - bremst der Datenschutz die Eigeninitiative?

Mitunter wird dem Datenschutz vorgeworfen, er lege der Entfaltung sozialer Eigeninitiative unnötige bürokratische Hindernisse in den Weg. Dieser Eindruck könnte auch im Zusammenhang mit dem Jugendzahnpflegewettbewerb entstanden sein. Auf der Grundlage des Gesetzes über die öffentliche Jugendzahnpflege werden Kinder in Kindergärten und Schulen zahnärztlich untersucht. Von der Behandlungsbedürftigkeit werden die Erziehungsberechtigten durch Vordruck unterrichtet und gebeten, die Behandlung durchführen zu lassen. Ein Erlaß des Sozialministers regelt nun, daß eine Behandlungsbescheinigung an die Schulen zurückgegeben und von den Lehrern kontrolliert werden sollte. Die Ortskrankenkassen hatten nämlich Prämien für diejenigen Schulklassen ausgelobt, in denen alle Schüler auf diese Weise gesunde Zähne oder eine regelmäßige Zahnbehandlung nachwiesen.

Eine gesetzliche Grundlage, die die Eltern zwingt, über zahnärztliche Behandlungen ihrer Kinder in der Schule Rechenschaft abzulegen, besteht nicht. Der Landesbeauftragte hat daher den Sozialminister aufgefordert, seine Verwaltungsanweisung neu zu fassen und in dem Benachrichtigungsvordruck die Eltern darauf hinzuweisen, daß die Rückmeldung über die zahnärztlichen Behandlungen der Kinder freiwillig ist. Er ist der Empfehlung des Landesbeauftragten gefolgt. Der Jugendzahnpflegewettbewerb wird durch diese Anderung natürlich nicht in Frage gestellt. Den Erziehungsberechtigten wird vielmehr nur deutlich gemacht, daß die Beteiligung am Wettbewerb freiwillig erfolgt und daß nicht befürchtet werden muß, daß Angaben gegen den Willen der Eltern gesammelt und möglicherweise zum Nachteil der Kinder verwendet werden.

4.6.2.2 Darf ein Amtsarzt Auskünfte über Prostituierte erteilen?

Auch Amtsärzte unterliegen der ärztlichen Schweigepflicht. Das konnte der Landesbeauftragte einem Arzt bestätigen, der Zweifel hatte, ob er dem Ordnungsamt Auskunft über die Zuverlässigkeit einer Prostituierten geben durfte, die sich freiwillig vom Gesundheitsamt betreuen ließ und nun einen Antrag auf eine Konzession für einen Getränkekiosk gestellt hatte. Die Betroffene machte von einem Beratungsangebot des Gesundheitsamtes Gebrauch. Sie hätte jederzeit wieder davon Abstand nehmen können. Der Freiwilligkeit dieser Kontaktaufnahme kommt eine besondere datenschutzrechtliche Bedeutung zu. Der Amtsarzt durfte die ihm von der Betroffenen offenbarten Informationen nur verwenden, um sie ihrem Wunsch gemäß vorsorglich zu untersuchen und zu beraten. Die Weitergabe von Daten und insbesondere von Werturteilen an das Ordnungsamt hätte daher ihrer Einwilligung bedurft.

Der Landesbeauftragte weist seit Jahren darauf hin, daß Informationen aus freiwilligen Kontakten der Bürger mit öffentlichen Stellen nicht für Zwangsmaßnahmen der Eingriffsverwaltung genutzt werden dürfen (vgl. 9. TB, S. 8).

4.6.2.3 Meldungen an den „Beauftragten für die systematische Bekämpfung übertragbarer Krankheiten"

Über bestimmte Krankheiten gehen von den Gesundheitsämtern regelmäßig personenbezogene Meldungen an den „Beauftragten für die systematische Bekämpfung übertragbarer Krankheiten". Grundlage für diese Meldungen ist ein Runderlaß des Sozialministers, mit dem der Leiter des Medizinaluntersuchungsamtes der Abteilung „Medizinische Mikrobiologie" der Christian-Albrechts-Universität zu Kiel zum Beauftragten bestellt wurde. Der Erlaß regelt ausdrücklich, daß die Kreisgesundheitsbehörden bereits Verdachtsfälle zu melden haben. Auf die Frage des Landesbeauftragten nach einer gesetzlichen Grundlage für diese Meldungen, die den Forderungen des Verfassungsgerichts zum informationellen Selbstbestimmungsrecht entspräche, wies der Minister für Soziales, Gesundheit und Energie auf verschiedene Gesichtspunkte hin:

Die Aufgabe des Beauftragten für die systematische Bekämpfung ansteckender Krankheiten sei mit der allgemeinen Aufga-

benübertragung auf die Gesundheitsbehörden nach dem Bundesseuchengesetz, das ggf. sogar Verordnungen der Landesregierungen ermögliche, zu rechtfertigen. Zur Erfüllung dieser Aufgaben könne sich der Sozialminister nach dem Gesundheitsdienstgesetz eines Sachverständigen bedienen. Die genannten Vorschriften gestatten nach Meinung des Landesbeauftragten aber nur konkrete Maßnahmen im Rahmen einer Gefahrenabwehr, nicht jedoch die Einführung einer erweiterten Meldepflicht über den Bereich des örtlichen Gesundheitsamtes hinaus.

Außerdem rechtfertigte der Minister den Auftrag damit, daß er Fachaufsichtsbehörde über die Gesundheitsämter sei, infolgedessen er die Vorlage jeder einzelnen Akte fordern könne und mit deren Auswertung er den Beauftragten betrauen dürfe. Dem jedoch widerspricht es, daß die Meldungen eben nicht zur Aufsicht über die Gesundheitsämter, sondern zur „systematischen Bekämpfung" ansteckender Krankheiten dienen sollen.

Der Versuch, die datenschutzrechtliche Problematik durch Anonymisieren der Meldungen zu umgehen und keine personenbezogene Daten mehr weiterzugeben, scheiterte, weil der Beauftragte den konkreten, einzelnen Krankheitsfall im Auge behalten und mit anderen Einzelfällen eine vergleichende Übersicht erreichen sollte.

Schließlich wurde versucht, die Rechtsgrundlage durch einen Vertrag aller Gesundheitsämter des Landes mit dem Beauftragten zu schaffen. Auch das mußte scheitern, denn die Kreise können zwar einen Sachverständigen beauftragen, die kreiseigenen Daten zu verarbeiten, nicht jedoch, diese Informationen über den Zuständigkeitsbereich des einzelnen Kreises hinauszutragen. Gerade diese Erlaubnis müßten die Kreise aber erteilen, wenn eine kreisübergreifende Auswertung stattfinden soll.

Der Erlaß bildet deshalb nicht nur keine ausreichende Rechtsgrundlage für die Meldungen an den Beauftragten, mit ihm umgeht man darüber hinaus auch konkrete gesetzliche Bestimmungen. Es handelt sich hier nämlich um eine Erweiterung der Meldepflicht nach dem Bundesseuchengesetz. Hierzu wäre aber eine Verordnung des Bundesministers für Jugend, Familie, Frauen und Gesundheit bzw. der Landesregierung erforderlich. Da entsprechende Verordnungen nicht bestehen, vermochte der Landesbeauftragte eine Rechtsgrundlage für die Datenübermittlung nicht festzustellen. Der Minister für Soziales, Gesundheit und Energie bleibt aufgefordert, die entsprechenden Datenübermittlungen zu unterbinden oder eine ausreichende Rechtsgrundlage zu schaffen, falls er die zentrale Sammlung und Auswertung aus fachlichen Gründen für unverzichtbar hält.

4.6.2.4 Unzulässig erhobene Daten müssen vernichtet werden

Diese Auffassung des Landesbeauftragten hat das Verwaltungsgericht Frankfurt am Main in einem Urteil vom 27. Januar 1988 (RDV 88, 209) auch für die Führung von Akten bestätigt.

Ein Ehemann hatte mit der Angabe, seine Frau benehme sich seltsam und bedrohe ihn und sich selbst in Tötungsabsicht, bei dem sozialpsychiatrischen Dienst eines Gesundheitsamtes ein nervenfachärztliches Gutachten erwirkt, aufgrund dessen die

Ehefrau für kurze Zeit in ein psychiatrisches Krankenhaus eingewiesen wurde. Die Angaben des Mannes erwiesen sich als falsch. Die Maßnahme wurde aufgehoben. Die Ehefrau forderte die Vernichtung der entsprechenden Akten im Gesundheitsamt. Das Verwaltungsgericht bejahte einen Vernichtungsanspruch, weil die weitere Aufbewahrung der Unterlagen das informationelle Selbstbestimmungsrecht der Frau beeinträchtige. Nicht die sachliche Unrichtigkeit der Akten ist Anlaß für die Auffassung des Gerichts. Es weist vielmehr nach Prüfung des in Hessen geltenden Rechts darauf hin, daß das Gesundheitsamt gar nicht befugt gewesen sei, auf Anregung einer Privatperson ein nervenfachärztliches Gutachten für eine Zwangseinweisung zu erstellen. Aus der Unzuständigkeit des Gesundheitsamtes für die Erhebung der entsprechenden Patentienteninformationen folge die Unzulässigkeit einer - auch aktenmäßigen – Speicherung und damit auch der Aufbewahrung der entsprechenden Akte im Gesundheitsamt. Darüber hinaus berge der Akteninhalt die erhebliche Gefahr, daß die Betroffene durch den Akteninhalt einer sozialen Etikettierung, Abstempelung oder Stigmatisierung ausgesetzt sein könne, was zu einer erneuten Beeinträchtigung ihres Persönlichkeitsrechts führe.

4.6.3 AIDS

4.6.3.1 Unzulässigkeit heimlicher AIDS-Tests

Zur Frage der Zulässigkeit von AIDS-Tests erging vom Amtsgericht Mölln (Urteil vom 6. Oktober 1988 – C 405/88) ein Urteil, das nach Auffassung des Landesbeauftragten Zeichen setzt. Das Gericht hatte sich mit der Frage zu befassen, ob die Durchführung eines HIV-Tests ohne besondere Einwilligung des Betroffenen einen so erheblichen Eingriff in dessen allgemeines Persönlichkeitsrecht darstellt, daß die Zahlung eines Schmerzensgeldes gerechtfertigt ist.

In einer Kurklinik wurde den Patienten mit ihrem Einverständnis im Rahmen der Eingangsuntersuchungen Blut entnommen und, wie allgemein üblich, auf verschiedene Erkrankungen untersucht. Ohne daß dies den Betroffenen mitgeteilt worden wäre, wurde das Blut dabei auch auf HIV-Antikörper überprüft. Das Testergebnis wurde ihnen allerdings nicht mitgeteilt. Das Gericht sieht zwar die Blutentnahme selbst aufgrund der Einwilligung des Patienten als gerechtfertigt an. In das allgemeine Persönlichkeitsrecht des Betroffenen greife der behandelnde Arzt aber dann ein, wenn er sich zusätzliche Informationen über den Gesundheitszustand des Patienten ohne dessen Wissen verschafft. Das habe er dadurch getan, daß er ohne Aufklärung des Betroffenen und ohne seine Einwilligung das Blut auf HIV-Antikörper habe untersuchen lassen. Selbst ein verständiger Patient müsse angesichts der weitreichenden Folgen eines positiven Untersuchungsergebnisses nicht ohne weiteres mit der Durchführung dieses Tests einverstanden sein. Er müsse deshalb den Umfang des den behandelnden Ärzten erteilten Heilauftrages selbst bestimmen können. Auch die Verpflichtung der Klinik, Personal und Patienten so umfassend wie möglich vor einer HIV-Infektion zu schützen, rechtfertige den heimlichen Test

nicht. Hierfür stünden andere, weniger einschneidende Möglichkeiten zur Verfügung.

Das Urteil bildet für den Landesbeauftragten den Maßstab für die datenschutzrechtliche Beurteilung der nachfolgend geschilderten Sachverhalte.

4.6.3.2 Einwilligung zum AIDS-Test im „Kleingedruckten"

Die Kieler Universität beabsichtigte, in die Krankenhausaufnahmeverträge des Klinikums folgenden informatorischen Hinweis aufzunehmen: „Mir ist bekannt, daß im Klinikum alle medizinisch notwendigen Untersuchungen einschl. eines HIV-Antikörper-Tests durchgeführt werden." Dies sollte als ausdrückliche Einwilligung verstanden werden.

Der Landesbeauftragte hat hiergegen erhebliche Bedenken erhoben. Die Durchführung eines AIDS-Tests und die Dokumentation des Testergebnisses kann weitreichende Folgen für die Rechtsstellung des Patienten haben. Ein positives Testergebnis kann seine gesellschaftliche Situation beeinträchtigen, seine familiären Beziehungen belasten und schließlich die Persönlichkeit des Patienten entscheidend verändern. Vor einem solchen Test ist er deshalb über den Zweck, den Umfang der Datenspeicherung und die Konsequenzen hinreichend aufzuklären. Eine allgemein gehaltene Information reicht nicht aus. Vielmehr erscheint eine ausdrückliche Einwilligung in den AIDS-Test unmittelbar vor dem Eingriff unerläßlich. Sie bedarf der Schriftform und sollte in der gleichen Weise dokumentiert werden, wie es auch bei sonstigen Eingriffen geschieht.

Der Minister für Soziales, Gesundheit und Energie und die Ministerin für Bildung, Wissenschaft, Jugend und Kultur haben die Auffassung des Landesbeauftragten unterstützt. Die Universität wird entsprechend verfahren.

4.6.3.3 AIDS-Tests bei Asylsuchenden - nur ein bißchen freiwillig?

Bereits Ende der 70er Jahre, lange vor dem ersten erkannten AIDS-Fall in der Bundesrepublik, hatten die Gesundheitsminister abgesprochen, Asylsuchende grundsätzlich medizinisch zu untersuchen. Derzeit werden nach Auskunft des Ministers für Soziales, Gesundheit und Energie in Schleswig-Holstein auch Asylbewerber aus Ländern mit einem hohen AIDS-Durchseuchungsgrad von den Gesundheitsämtern „freiwillig routinemäßig" (was immer das bedeuten mag) auf AIDS getestet.

Diese Praxis ist ein klassisches Beispiel dafür, wie nicht verfahren werden darf. Gesundheitspolizeilich – also von der Eingriffsverwaltung – für sinnvoll angesehene Untersuchungen sollen dadurch „reibungsloser" erfolgen, daß die Asylsuchenden aufgefordert werden, freiwillig von angebotenen Untersuchungsmöglichkeiten Gebrauch zu machen. Es besteht also weder für die betroffenen Ausländer noch für die beteiligten Stellen der deutschen Verwaltung eine ausreichende Klarheit über die Rechtsgrundlage, die Rechtsnatur und den Umfang der zulässigen Erhebung, Speicherung und Weitergabe der Untersuchungsergebnisse.

Der Landesbeauftragte hat nicht zu untersuchen, ob aus fachlicher Sicht zwangsweise durchgeführte AIDS-Tests bei Asylsuchenden gesundheitspolizeilich erforderlich sind. Er schließt nicht aus, daß sie im konkreten Einzelfall aufgrund gesetzlicher Regelungen (Bekämpfung ansteckender Krankheiten nach dem Bundesseuchengesetz) zulässig sein können. Sie müssen dann aber im Rahmen des Aufnahmeverfahrens nach dem Asylverfahrensgesetz als Auflagen angeordnet werden, stellen Verwaltungsakte dar und könnten verwaltungsgerichtlich nachgeprüft werden. Ob und wieweit dabei Datenspeicherungen und Datenweitergaben zulässig sind, wäre nach den genannten gesetzlichen Vorschriften am Maßstab der Erforderlichkeit zu prüfen.

Wird Asylsuchenden allerdings nur empfohlen, angebotene HIV-Tests freiwillig zu nutzen, so muß der Betroffene auf die Freiwilligkeit der Untersuchung sowie darauf hingewiesen werden, daß ihm aus einer Weigerung an der Teilnahme keine Nachteile erwachsen. Er muß über Art und Umfang der Datenverarbeitung unterrichtet, über beabsichtigte Datenweitergaben und Datenübermittlungen aufgeklärt werden und schließlich in Kenntnis aller wesentlichen Verfahrensumstände schriftlich in den Test sowie die Datenspeicherung und -weitergabe einwilligen. Die Einwilligung beschreibt und begrenzt dann zugleich den Umfang zulässiger Datenverarbeitung.

Daß die Verwaltung diese Verfahrensformen nicht immer klar unterscheidet, macht folgendes Beispiel deutlich. Eine Kreisverwaltung hatte eine freiwillige Untersuchung veranlaßt, die Information „HIV-positiv" aber gleichwohl zur „Risikobegrenzung" an eine Vielzahl von Stellen (Sozialamt, Sozialministerium, Leiter der Sammelunterkunft) gestreut. Als die betroffene Person dies erfuhr, entzog sie sich dem Verfahren, indem sie „untertauchte". Pikanterweise stellte sich später heraus, daß das Untersuchungsergebnis unrichtig war. Davon hat die Betroffene möglicherweise bis heute noch nichts erfahren. Die Verwendung der Ergebnisse freiwilliger Untersuchungen zu Zwangsmaßnahmen im Asylverfahren mit der Begründung, man hätte ja auch eine zwangsweise Untersuchung anordnen können, ist unzulässig. Der Landesbeauftragte fordert daher klare Anweisungen in der Frage von HIV-Tests bei Asylsuchenden.

4.6.4. Krankenhaus

4.6.4.1 Staatsanwaltschaft „bluffte" einen Arzt

Von einem leitenden Arzt des Klinikums der Universität wurde der Landesbeauftragte auf einen Sachverhalt hingewiesen, bei dem man wohl ohne Übertreibung von einem „Bluff" sprechen kann. Anlaß war das an den betreffenden Arzt gerichtete Ersuchen einer Staatsanwaltschaft, für Zwecke des Todesermittlungsverfahrens bezüglich des verstorbenen Ministerpräsidenten Dr. Barschel dessen medizinische Daten herauszugeben. (Un)mißverständlich hieß es in dem Schreiben: „Um eine Durchsuchung und eine Beschlagnahme zu vermeiden, wird um freiwillige Herausgabe gebeten". Der Arzt, hin- und hergerissen zwischen der ärztlichen Schweigepflicht einerseits und seinen Loyalitätspflichten als Mitarbeiter der Universität ande-

rerseits, gab die Unterlagen heraus, wobei auch die Überlegung eine Rolle spielte, eine Weigerung habe doch keinen Zweck, da ihr die Beschlagnahme auf dem Fuße folgen würde.

Der Landesbeauftragte hat ernste Zweifel an der Rechtmäßigkeit des Vorgehens der Staatsanwaltschaft und des Arztes.

Das Auskunftsersuchen hätte zunächst einmal an die Universität als Eigentümerin der Krankenunterlagen gerichtet werden müssen. Weder das Klinikum noch dessen einzelne medizinischen Abteilungen besitzen eine eigene Rechtspersönlichkeit. Sodann ist auch ein Chefarzt gehalten, nur zusammen mit der Universität über das Herausgabeverlangen einer Staatsanwaltschaft zu entscheiden. Nur die Einhaltung dieses Weges gewährleistet die gebotene Prüfung unter strafprozessualen und standesrechtlichen/medizinischen Aspekten. Bei der komplizierten Rechtslage in einem Todesermittlungsverfahren wäre es gerade auf die strafprozessuale Prüfung angekommen. Unter Hinweis auf die allgemeinen Persönlichkeitsrechte des verstorbenen Patienten und seiner Angehörigen und die Gesichtspunkte der Verhältnismäßigkeit und der Erforderlichkeit hätte die Universität die Herausgabe u. U. von einer richterlichen Beschlagnahme abhängig machen müssen. Mit ihr hätten sie und der Arzt eine einwandfreie und sichere Befugnis zur Offenbarung der Patientendaten in den Händen gehabt.

In dem Schreiben der Staatsanwaltschaft an den „rechtsunsicheren" Arzt wurde der Eindruck erweckt, daß der Gerichtsbeschluß als zwangsläufige Konsequenz bei einer Weigerung nur ein Formalakt sei. Dies hieße die richterliche Unabhängigkeit zu unterschätzen. Ein Richter hätte bei Würdigung der rechtlichen Gegebenheiten durchaus zu einer Ablehnung des Antrages der Staatsanwaltschaft kommen können. Besonders bedenklich ist es, daß der Jurist den Mediziner nicht in fairer Weise über die Rechtslage unterrichtete. Vielmehr suggerierte er ihm den Eindruck, wie immer er auch entscheide, die Staatsanwaltschaft erhalte die Informationen in jedem Fall.Die unterschwellige Drohung „freiwillig oder mit Gewalt" erscheint fehl am Platze.

Der Landesbeauftragte hat die Universität aufgefordert, verbindliche Regelungen für den Fall zu schaffen, daß eine Staatsanwaltschaft wieder einmal um die Herausgabe von Patientendaten „bittet". Von dem Justizminister und dem Generalstaatsanwalt hat der Landesbeauftragte gefordert, daß die Staatsanwaltschaften angewiesen werden, künftig Ersuchen um Auskünfte oder Herausgabe von Beweismitteln nur an den Eigentümer zu richten und die Rechtsgrundlagen eindeutig zu bezeichnen. Nach seiner Auffassung handelt es sich hier um einen Fall von grundsätzlicher datenschutzrechtlicher Bedeutung. Dem Vertrauen der Patienten bzw. ihrer Angehörigen darauf, daß in einem Krankenhaus ihre medizinischen Daten in bester Obhut sind und daß sie an Dritte nur auf der Basis einer sicheren Rechtsgrundlage und nach sorgfältiger Prüfung ihrer schutzwürdigen Belange herausgegeben werden, muß Rechnung getragen werden. Die Frage, ob eine andere Person oder Stelle überhaupt einen Rechtsanspruch auf eine Auskunft, eine Einsichtnahme oder eine Herausgabe von Unterlagen hat, kann nicht der Mediziner, sondern muß der Jurist entscheiden.

Erst wenn die Rechtsfragen abschließend geklärt sind, kann der Arzt unter Beachtung seines Standesrechts entscheiden, welche Patientendaten für den jeweiligen Zweck offenbart werden müssen.

4.6.4.2 Vorsicht Kamera im Operationssaal

Keineswegs als Spaß verstanden wurde ein Vorgang, den eine zerbrochene Glaskachel in einem Krankenhaus zutage brachte. In vier Operationssälen waren verdeckte Videokameras installiert worden. Zwischen 1978 und 1980 hatte ein Unbekannter im mehreren Fällen die Narkosegeräte manipuliert und damit Patienten gefährdet. Ein Jahr lang liefen die versteckten Kameras in den Operationssälen, danach wurden die Aufzeichnungsgeräte wieder entfernt, denn die Aktion blieb erfolglos. Dieser Fall ist nach Meinung des Landesbeauftragten ein Beispiel dafür, wie moderne Techniken, eingesetzt zu einem gutgemeinten Zweck, in die Persönlichkeitsrechte unbeteiligter Personen eingreifen können. Die Kameras wurden von der Krankenhausleitung (nicht von der Polizei) nämlich heimlich installiert, denn man hielt die verdeckte Dauerüberwachung der Narkosegeräte für die einzige Möglichkeit, den Täter zu überführen. Sicher, die Gefahr für die Patienten war da, eine Abhilfe notwendig. Doch allein die Überwachung der Geräte per Video brachte diese Abhilfe nicht. So oder so mußten die Geräte jedesmal auf ihre Funktionstüchtigkeit überprüft werden. Die Videoaufzeichnungen sollten vielmehr strafbare Handlungen aufklären. Dann stellt sich aber die Frage nach der Verwertbarkeit der Videoaufnahmen. Die Strafprozeßordnung läßt z. B. Tonbandaufzeichnungen von Telefongesprächen nur bei bestimmten Straftaten und unter bestimmten Voraussetzungen zu. In der Rechtsprechung ist die Verwertbarkeit unrechtmäßig erlangter Beweismittel im Strafverfahren umstritten. Für den Landesbeauftragten stehen demgegenüber die Verletzung der Persönlichkeitsrechte aller an einer Operation Beteiligten, ein möglicherweise unzulässiger Eingriff in die Schweigepflicht des Arztes und nicht zuletzt ein Eingriff in die Intimsphäre des Patienten. Der Träger des Krankenhauses hat dieser Auffassung widersprochen. Nach seiner Meinung waren die Maßnahmen im Rahmen der Güterabwägung gerechtfertigt und überdies hätten die Patienten und das Operationspersonal nicht identifiziert werden können.

Der Vorgang bestärkt den Landesbeauftragten gleichwohl in seiner Forderung, den Einsatz technischer Hilfsmittel bei der Strafverfolgung und bei der Gefahrenabwehr gesetzlich datenschutzgerecht zu regeln. Solche Art von Beweiserhebungen gehören seines Erachtens ausschließlich in die Hände der Strafverfolgungsbehörden und sind in jedem Einzelfall von Richtern zu kontrollieren.

4.6.4.3 Wahrung des Patientengeheimnisses in privaten Stiftungen

Presseberichte ließen den Landesbeauftragten aufhorchen: Das Land beabsichtigte, ein Institut für angewandte Krebsforschung in der Rechtsform einer Stiftung des bürgerlichen Rechts zu gründen. Auf diese Weise sollte die Arbeit eines Sonderfor-

schungsbereiches an der Universität weitergeführt werden. Das Institut sollte das Datenmaterial des Lymphknotenregisters übernehmen. Ein Kooperationsvertrag sollte die Zusammenarbeit zwischen dem Institut und der Universität regeln und u. a. auch die Voraussetzungen für Promotionen und Habilitationen am Institut schaffen.

Der Landesbeauftragte hat die Universität auf die weitreichenden Rechtsfolgen einer unbefugten Offenbarung von Patientendaten im Sinne des § 203 Strafgesetzbuch hingewiesen. Weder für die Übermittlung der Registerdaten vom Klinikum an das private Institut noch für den Zugriff darauf durch Doktoranden und Habilitierende hätte eine hinreichende rechtliche Befugnis bestanden. Die Registerdaten wären vom öffentlichen in den privaten Bereich gewandert. Das in private Trägerschaft überführte Register wäre den im öffentlichen Bereich geltenden strengeren Datenschutzvorschriften der Kontrolle durch den Landesbeauftragten entzogen worden.

Inzwischen hat die medizinische Fakultät beschlossen, die Aufgaben weiterhin in einem Institut der Universität wahrnehmen zu lassen. Diese Entwicklung kann der Landesbeauftragte nur begrüßen. Die Befürworter von Maßnahmen der „Entstaatlichung" mögen auf die Vorteile der größeren Flexibilität und des Abbaus von Bürokratismus hinweisen (vgl. 10. TB, S. 42). Die ärztliche Schweigepflicht hat aber auch demgegenüber absoluten Vorrang.

4.7 Kultusbereich

4.7.1 Hochschulen erheben Studentendaten ohne Rechtsgrundlage

Die Hochschulen benötigen für die Verwaltung und für die Organisation der Studiengänge umfangreiche persönliche Angaben über die Studierenden. Für die Erhebung und Verarbeitung dieser Daten besteht bisher keine ausdrückliche gesetzliche Grundlage. Man hält es für vertretbar, die nach dem Hochschulstatistikgesetz allein für statistische Zwecke erhobenen Daten gleichzeitig auch für Verwaltungszwecke zu nutzen. Einer solchen Zweckentfremdung hat jedoch das Bundesverfassungsgericht in seinem Volkszählungsurteil einen Riegel vorgeschoben, indem es die Verwendung von Statistikdaten für Aufgaben des Verwaltungsvollzugs ausdrücklich für unzulässig erklärt.

Der Landesbeauftragte hat deshalb gefordert, eine entsprechende Rechtsgrundlage im Hochschulgesetz zu schaffen oder aber die Daten nur auf freiwilliger Basis zu erheben. Die Ministerin für Wissenschaft, Bildung, Jugend und Kultur hat inzwischen mit den Arbeiten an einem entsprechenden Gesetzentwurf begonnen.

4.7.2 Ein neuer Schülergesundheitsbogen

Anfang 1989 wurde ein neuer landeseinheitlicher Schülergesundheitsbogen eingeführt, nachdem der Landesbeauftragte wiederholt (vgl. 9. TB, S. 40) datenschutzrechtliche Bedenken gegen das zu umfangreiche Datenprofil des bisherigen Untersu-

chungsbogens geltend gemacht hatte. Auch der neue Schülergesundheitsbogen folgt nicht in allen Punkten den Anregungen des Landesbeauftragten, der Umfang der von den Eltern abgefragten Daten ist jedoch spürbar reduziert worden. Leider wurde auf problematische Angaben wie z. B. „Besonderheiten der Familienanamnese" und „Besonderheiten im Schwangerschafts- und Geburtsverlauf" nicht verzichtet. Der Landesbeauftragte hat deshalb gefordert, daß die Schulärzte hier künftig nur in begründeten Einzelfällen Eintragungen vornehmen.

4.7.3 Schülerdaten auf privaten Personal-Computern der Lehrer

Verschiedentlich wurde der Landesbeauftragte gefragt, ob auch die Dateien zum Datenschutzregister zu melden seien, in denen Lehrer personenbezogene Daten von Schülern und Eltern auf privaten Personal-Computern zuhause speicherten. Es handelte sich um teilweise umfangreiche und sensible Datensammlungen über Verhaltensauffälligkeiten der Schüler und den Inhalt von Elterngesprächen. Neben der Antwort, daß auch derartige Dateien grundsätzlich zu melden seien, hat der Landesbeauftragte den Hinweis gegeben, daß in dieser Art der Datenverarbeitung erhebliche Sicherheitsrisiken und rechtliche Probleme liegen. Schülerdaten erhält der Lehrer nur aus seiner dienstlichen Aufgabenstellung heraus und darf sie nur zu dienstlichen Zwecken verwenden. Sie bleiben Daten der Schule. Wer personenbezogene Daten verarbeitet, hier also die jeweilige Schule, hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um den Datenschutz und die Datensicherheit zu gewährleisten. Die Schule hat also dafür zu sorgen und zu überwachen, daß die Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden, in rechtlich zulässiger Weise richtig und sicher arbeiten. Die Schulleiter sind jedoch nicht in der Lage, dies zu kontrollieren, wenn von den Lehrern Daten auf privaten Personal-Computern im häuslichen Bereich verarbeitet werden. Sie können weder tatsächlich noch in jedem Fall rechtlich

- nachprüfen, ob und welche dienstlichen Daten in welchen Dateien gespeichert werden,
- dafür sorgen, daß nicht mehr benötigte Daten wieder gelöscht werden,
- durch technische und organisatorische Maßnahmen kontrollieren, wer Zugang zu den Daten hat,
- verhindern, daß die Daten aus dem Verfügungsbereich der Lehrer hinausgelangen,
- die Kontrolle über die Datenverarbeitung auf den privaten Personal-Computern erzwingen.

Datenschutz und Datensicherung beschränken sich vielmehr auf das Vertrauen, daß die Lehrer sorgsam und nur im Rahmen ihrer dienstlichen Aufgaben mit den personenbezogenen Daten umgehen. Der Landesbeauftragte hat daher der Kultusministerin mitgeteilt, daß nach seiner Rechtsauffassung private Personal-Computer für die dienstliche Verarbeitung von Schülerdaten weder in der Schule noch im häuslichen Bereich eingesetzt werden dürfen. Die Kultusministerin hat sich dem angeschlos-

sen und durch Runderlaß diese Art der Datenverarbeitung untersagt. Der Landesbeauftragte regt an, im Rahmen der Novellierung des Schulgesetzes auch diese Frage unmittelbar im Gesetz zu regeln.

4.7.4 Datenverarbeitung und Datenschutz sollen im Schulgesetz geregelt werden

Das Schulgesetz soll nach Ankündigung der Kultusministerin nun doch durch Vorschriften zur Datenverarbeitung und zum Datenschutz ergänzt werden. Damit ist die seit 1980 (vgl. 7. TB, S. 51) andauernde Diskussion zur Frage 1 „Brauchen wir überhaupt eine gesetzliche Regelung?" beendet. Jetzt richtet der Landesbeauftragte seinen Blick auf den Inhalt des Gesetzes. Gerade die Vielfalt der Informationsbeziehungen im Schulalltag, die sehr unterschiedliche Sensibilität der schulischen Daten und die differierenden schutzwürdigen Belange von Schülern, Eltern und Lehrern erfordern klare und detaillierte Regelungen. Bereits ein Blick in die früheren Tätigkeitsberichte des Landesbeauftragten (2. TB, S. 22; 3. TB, S. 34; 7. TB, S. 51) zeigt zahlreiche Beispiele für Regelungslücken auf. Dabei geht es z. B. um Fragen im schulärztlichen Bereich, um schulische Gutachten über jugendliche Zeugen und Beschuldigte, um Zeugnisinhalte, um die Verwendung des Grundschulgutachtens, um die Rechte und Pflichten der Elternbeiräte, um das Spannungsverhältnis zwischen Lehrinhalt und Persönlichkeitsschutz, um die Datenflüsse bei Schulwechsel und Versetzung, um die Forschung mit Schüler-, Eltern- und Lehrerdaten und um Fragen des Datenprofils, der Aufbewahrung, Sicherung und Vernichtung von personenbezogenen Daten. Auf die Textziffern 4.7.2 und 4.7.3 dieses Berichtes wird verwiesen.

Der Landesbeauftragte wird im Gesetzgebungsverfahren hierzu konkrete Regelungsvorschläge machen.

4.7.5 Endlich ein Archivgesetz in Aussicht?

Die „kompromißlose" Position des Landesbeauftragten in der Frage der Verwertung archivierter personenbezogener Daten für die Aufarbeitung historischer Ereignisse der jüngeren Vergangenheit (vgl. 8. TB, S. 35) wird von Wissenschaft und Verwaltung seit Jahren als ausgesprochenes „Ärgernis" empfunden. Dabei verweist der Landesbeauftragte allein auf die Rechtslage, die dem Geheimhaltungsbedürfnis der betroffenen Bürger den Vorrang vor den Wünschen der wissenschaftlichen Forschung einräumt. Diese Maxime unseres freiheitlichen Rechtsstaates dokumentiert sich nicht nur im Datenschutzrecht, wonach nicht mehr erforderliche Daten zu sperren sind und damit sehr strengen Nutzungsbeschränkungen unterliegen, sondern auch in den vielfältigen Verschwiegenheits- und Geheimhaltungsvorschriften, deren Beachtung nicht von Fristen oder anderen einschränkenden Kriterien abhängig ist. In diesem Zusammenhang muß man sich auch das Volkszählungsurteil des Bundesverfassungsgerichts in Erinnerung rufen, wonach grundsätzlich jeder selbst über die Preisgabe und die Verwendung seiner Daten zu bestimmen hat, und die Einschränkungen dieses Rechts nur im überwiegenden Allgemeininteresse und aufgrund

einer normenklaren und datenschutzgerechten gesetzlichen Grundlage zulässig sind. Ein solches Archivgesetz mit einer Forschungsklausel gibt es im Lande eben nicht. Im gegenwärtigen Zeitpunkt sind daher die einzigen legalen Wege, um historische Forschung mit personenbezogenen Daten betreiben zu dürfen, die Einwilligung der Betroffenen oder die Anonymisierung der Daten. Nach dem Eindruck des Landesbeauftragten wurde die Diskussion bisher sehr einseitig aus der Interessenlage der historischen Forschung geführt. Während die Forscher eigentlich immer sehr konkret wissen, welchen Personenkreis sie in ihre Arbeit einbeziehen wollen, bleiben die betroffenen Bürger im allgemeinen im unklaren darüber, welcher Kreis von Forschern und Hilfskräften sich gerade mit ihren häufig sehr sensiblen persönlichen Daten befaßt. Die Wahrung der Rechte der durch die Datenverarbeitung betroffenen, aber unwissenden Bürger ist die klassische Aufgabe des Datenschutzbeauftragten.

Inzwischen hat sich im Lande aber offenbar ein Wandel vollzogen. Die Vertreter der Archive, der Forschungseinrichtungen und der Verwaltung sehen ein, daß die Probleme nur mit Hilfe eines Archivgesetzes gelöst werden können. Die Kultusministerin hat dem Landesbeauftragten mitgeteilt, daß im Arbeitsprogramm der Landesregierung der Entwurf eines Landesarchivgesetzes noch für diese Legislaturperiode vorgesehen ist. Der Landesbeauftragte begrüßt dieses Vorhaben. Er wird allerdings bei der Beratung der einzelnen Regelungen im Gesetzgebungsverfahren immer wieder auf die Tatsache hinweisen, daß die Archivierung von personenbezogenen Daten für den betroffenen Bürger einen belastenden Eingriff in seine Rechte darstellt. Wer hat es schon gern, daß sein „Verwaltungssündenregister" der Nachwelt erhalten bleibt, während das seines Nachbarn im Reißwolf landet. Aus verfassungsrechtlichen Gründen sind an ein Archivgesetz daher sehr hohe Anforderungen zu stellen.

5. Prüfungen

5.1 Prüfung einer Stadtverwaltung

Mit der Prüfung der Verwaltung einer kleineren Stadt hat der Landesbeauftragte begonnen, sich wieder intensiver mit der datenschutzrechtlichen Praxis in den Kommunalverwaltungen zu befassen. Die letzte Prüfung dieser Art liegt immerhin acht Jahre zurück (vgl. 4. TB, S. 37). Die Schwerpunkte dieser Untersuchungen liegen bei den technischen und organisatorischen Datensicherungsmaßnahmen sowie bei Einzelfragen zur Rechtmäßigkeit der Datenverarbeitung.

– Datensicherung

Ohne technische und organisatorische Datensicherungsmaßnahmen ist eine ordnungsgemäße Verarbeitung personenbezogener Daten nicht zu gewährleisten. Zu den organisatorischen Maßnahmen gehören vor allem schriftliche Dienst- und Geschäftsanweisungen, eine Aktenordnung sowie eine Hausordnung. Geregelt werden müssen insbesondere die Befugnisse zum Umgang mit Dateien, die Zugangsberechtigungen zu Räumen, in denen sich Dateien befinden, die Aus-

kunftserteilung und die Art der technischen Sicherung von Dateien. Wichtige technische Maßnahmen sind die Sicherung der Dienstgebäude und der einzelnen Diensträume, die Aufbewahrung personenbezogener Daten entsprechend ihrer Schutzbedürftigkeit in ausreichend gesicherten Behältnissen und eine Trennung von Bearbeitungs- und Publikumsbereichen, um eine unbefugte Einsichtnahme in dienstliche Vorgänge auszuschließen. Bis auf eine Dienstanweisung über die automatisierte Datenverarbeitung bestanden bei der geprüften Stadt keine schriftlichen Regelungen zur organisatorischen Gewährleistung des Datenschutzes. Auch fehlte es an einer durchgängigen Sicherheitsanalyse und den daraus resultierenden Anweisungen.

– **Rechtmäßigkeit der Datenverarbeitung**

Eine Reihe von Einzelfragen zur Rechtmäßigkeit der Datenverarbeitung im kommunalen Bereich haben bereits unter Textziffer 4.1 Eingang in diesen Bericht gefunden. Daneben ist auf weitere Sachverhalte von grundsätzlicher Bedeutung hinzuweisen.

Telefondatenerfassung

Im Rahmen der Prüfung hat sich gezeigt, daß sich auch bei einer manuellen Telefondatenerfassung erhebliche Probleme ergeben können. Daten über Privatgespräche dürfen grundsätzlich nur zu Abrechnungszwecken erfaßt werden. Hierfür ist die Erfassung des Namens und des Wohnortes des Angerufenen sowie die Zielnummer nicht erforderlich, wenn die Identität des Anrufenden im Rahmen der Handvermittlung durch die Telefonistin festgestellt werden kann. Für eine Aufbewahrung der Unterlagen über einen Zeitraum von fast sieben Jahren bestand keine Rechtfertigung. Die Löschung der Daten hätte vielmehr unverzüglich nach Abrechnung der Privatgespräche erfolgen müssen. Aus diesem Grunde wurde auch eine Trennung von Dienst- und Privatgesprächen bei der Erfassung empfohlen.

Verpflichtung auf das Datengeheimnis

Bei der Datenverarbeitung beschäftigte Personen sind bei der Aufnahme ihrer Tätigkeit schriftlich auf das Datengeheimnis zu verpflichten. Zur Datenverarbeitung gehört jede Speicherung, Veränderung, Löschung oder Übermittlung von personenbezogenen Daten, unabhängig von der Art des angewandten Verfahrens. Eine Beschränkung auf die automatisierte Datenverarbeitung besteht nicht. Von der geprüften Stelle waren nicht alle entsprechenden Mitarbeiter verpflichtet worden.

Personalaktenführung

Personalrechtliche Maßnahmen, wie Einstellungen oder Beförderungen, werden von den entsprechenden Gremien der Stadtvertretung beschlossen. Waren in einer Sitzung mehrere personalrechtliche Entscheidungen zu treffen, wurden diese in einem Beschlußvorschlag zusammengefaßt. Entsprechende Auszüge wurden ungekürzt zu den jeweiligen Perso-

nalakten genommen, und so enthielten die einzelnen Akten auch wichtige personenbezogene Daten anderer Mitarbeiter. Hierin lag nicht nur eine Verletzung des Datenschutzes, sondern auch ein Bruch der Amtsverschwiegenheit.

Dokumentationspflichten im Melderecht

Im Rahmen der Prüfung war auch eine Durchsicht von erweiterten Melderegisterauskünften beabsichtigt. Die entsprechenden Entscheidungen des Meldeamts waren jedoch nicht dokumentiert worden. Nach der Rechtsprechung des Bundesverwaltungsgerichts (vgl. Textziffer 4.1.1.2) besteht die Pflicht zur Führung wahrheitsgetreuer und vollständiger Akten. Die Unterlagen über erweiterte Melderegisterauskünfte hätten also aufbewahrt werden müssen. Die Prüfung hat daneben noch eine ganze Reihe von kleineren Mängeln aufgezeigt. Deshalb ist die ausdrückliche Bereitschaft der Stadt zu begrüßen, unverzüglich für Abhilfe zu sorgen. Die vom Landesbeauftragten vorgetragenen Anregungen und Bedenken wurden konstruktiv aufgegriffen und soweit wie möglich sofort in die Praxis umgesetzt.

5.2 Prüfung der Kriminalaktenhaltung der Polizei - erste Ergebnisse

Mit der seit längerem geplanten umfassenden datenschutzrechtlichen Überprüfung der Kriminalaktenhaltung bei Polizeibehörden hat der Landesbeauftragte im Berichtszeitraum begonnen. Da sie leider noch nicht zum Abschluß gebracht werden konnte (allein die Bestandsaufnahme der einschlägigen polizeilichen Dienstvorschriften, Erlasse und Vereinbarungen mit dem Bundeskriminalamt erstreckte sich über mehrere Monate), sind in diesem Tätigkeitsbericht nur erste Teilergebnisse darstellbar:

- **Kriminalaktensammlungen sind als Dateien anzusehen**

  Wie wichtig eine genaue Funktionsanalyse der einzelnen Datenbestände der Verwaltung ist, zeigte sich bei der datenschutzrechtlichen Beurteilung der Kriminalaktensammlungen. Die Kriminalakten haben nämlich nicht, wie die Aktensammlungen anderer Behörden, die Funktion der vollständigen und chronologischen Dokumentation des Verwaltungshandelns. Sie enthalten vielmehr nur einen Extrakt (in der Regel in Form von Merkblättern) aus den eigentlichen Ermittlungsvorgängen. Sie werden auch nicht angelegt, um in einem eventuellen Beschwerdeverfahren die Rechtmäßigkeit des polizeilichen Handelns nachweisen zu können. Sie sollen vielmehr im Rahmen der vorbeugenden Bekämpfung von Straftaten frühere strafrechtlich relevante Erkenntnisse schnell verfügbar machen. Dies ist eine ganz typische Dateifunktion. Die vor einigen Jahren geführte Diskussion um die Kontrollbefugnisse des Datenschutzbeauftragten haben sich somit als gegenstandlos erwiesen. Die Aufbewahrung einer Kriminalakte ist also nur dann zu rechtfertigen, wenn aufgrund einer hinreichend begründeten kriminalpolizeilichen Prognose der Verdacht besteht, daß die betreffende Person eine Straftat erstmalig oder zum wiederholten Male begehen wird. Es darf also nicht jeder Ermittlungsvorgang automa-

tisch zum Anlegen einer Kriminalakte führen. Kriminalakten müssen vernichtet werden, sobald die ursprünglichen Verdachtsmomente sich nicht bestätigt haben. Insbesondere die Registrierung von Personen, die nicht rechtskräftig verurteilt worden sind (Freispruch, Einstellung des Verfahrens), ist ein gravierender Eingriff in deren informationelles Selbstbestimmungsrecht. Ihre Kriminalakten sind sofort bzw. spätestens dann zu vernichten, wenn die vermeintliche Straftat verjährt ist.

– **Sachgerechte Aussonderung reduziert die Datenbestände**

Noch vor einem Jahr glaubte der Landesbeauftragte bezüglich der Aufbewahrungsfristen von Kriminalakten mit dem Innenminister „nicht auf einen Nenner zu kommen". Nunmehr dürfte doch ein Durchbruch erreicht worden sein. Nachdem die Prüfung ergeben hatte, daß einige Polizeibehörden von sich aus die regelmäßige Aussonderungsüberprüfung nicht mehr erst nach zehn Jahren, sondern bereits fünf Jahre nach Anlegen der Kriminalakte vornehmen, hat der Innenminister dies durch einen Erlaß für alle Dienststellen verbindlich vorgeschrieben. Nach den Erkenntnissen des Landesbeauftragten ist zu erwarten, daß etwa zwei Drittel der Kriminalakten fünf Jahre früher als bisher gelöscht werden. Diese Neuregelung, verbunden mit den generellen „Aktenbereinigungsaktionen" der Polizeibehörden, schlägt sich deutlich in Zahlen nieder. Noch vor 19 Jahren verfügte die Polizei über einen konstanten Bestand von über 600 000 Kriminalakten (bei ca. 2,5 Millionen Einwohnern in Schleswig-Holstein). Dieser hat sich bis Anfang 1988 schrittweise auf 270 000 Akten reduziert. Der Landesbeauftragte glaubt und hofft, daß bei einer sachgerechten Handhabung der neuen Kriterien und Fristen letztlich ein Bestand von nicht mehr als 150 000 Kriminalakten als erforderlich angesehen wird. Wie sehr sich die heutige Speicherungspraxis der Polizeibehörden von der früheren unterscheidet, wurde ihm im Aktenraum einer Polizeidirektion deutlich: Der ursprünglich für 100 000 Akten ausgelegte Raum enthielt nur noch 30 000 Akten. Hieran war sicher nicht nur der Datenschutzbeauftragte „schuld", sondern in erster Linie die „neue" Flexibilität im Denken der Polizei. Dieses hebt der Landesbeauftragte im Namen der mehreren hunderttausend Bürger, die auf diese Weise nicht mehr polizeilich registriert sind, ausdrücklich hervor.

– **Auskünfte werden eingeschränkt und dokumentiert**

Dem Landesbeauftragten ist in den vergangenen Jahren immer wieder dargelegt worden, daß die Sammlungen der Kriminalakten und die polizeiliche Erkenntnisdatei lediglich polizeiinterne Datenbestände seien. Dieser Aussage standen leider die Beschwerden von Betroffenen über eine recht großzügige Auskunftspraxis der Polizei gegenüber. Die laufende Prüfung hat in diesem Zusammenhang deutlich werden lassen, daß die Polizeibehörden dabei sind, ihr Auskunftsgebaren, zumindest soweit es Auskünfte aus Kriminalakten betrifft, grundlegend zu ändern. Außerdem werden die Auskünfte inzwischen grundsätzlich dokumentiert. Auch wenn noch nicht alle Zweifelsfragen und Problemfälle im Sinne

des Datenschutzrechts gelöst sind (vgl. z. B. Textziffer 4.1.7.2), wertet der Landesbeauftragte die erkennbare Tendenz sehr positiv. Zu Recht weigern sich die Polizeibehörden immer konsequenter, von anderen Behörden als Auskunftei „mißbraucht" zu werden. Ein Informationsaustausch findet im Grunde nur noch untereinander bzw. zwischen ihnen und den speziellen Ordnungsbehörden (Führerscheinstellen, Genehmigungsbehörden usw.) statt. Sind Vorgänge bereits an die Staatsanwaltschaft abgegeben, wird in der Regel nur noch das dortige Aktenzeichen mitgeteilt. Jede Kriminalakte enthält ein Vorblatt, in dem die erteilten Auskünfte registriert werden. Fazit: Wenn sich alle Polizeibehörden an die vom Innenminister erteilten Weisungen halten, dürften Beschwerden über eine polizeiliche „Geschwätzigkeit" der Vergangenheit angehören.

Bezüglich einer Reihe wichtiger Fragestellungen sind die Prüfungsmaßnahmen und die Erörterungen mit dem Innenminister noch nicht beendet. Deshalb wird den vorstehenden durchweg positiven Bemerkungen im nächsten Jahr sicher die Darstellung einiger kritisierter oder kontrovers diskutierter Problembereiche folgen.

5.3 Prüfung des Statistischen Landesamtes im Rahmen der Volkszählung

In seinem letzten Tätigkeitsbericht (10. TB, S. 15) hat sich der Landesbeauftragte eingehend mit der datenschutzgerechten Erhebung der Volkszählungsdaten „vor Ort" befaßt. Im Jahr 1988 stand die ordnungsgemäße Aufbereitung der Erhebungsdaten beim Statistischen Landesamt im Vordergrund der Prüfungen. Etwa vier Millionen Erhebungsbögen mit einem Gesamtgewicht von 150 Tonnen waren zu bearbeiten. Das Projekt „Volkszählung" konnte deshalb zu Recht als ein Massengeschäft bezeichnet werden. Wichtige Voraussetzung für dessen ordnungsgemäße Abwicklung war eine sorgfältige Planung und Organisation aller anfallenden Arbeiten. Die vom Statistischen Landesamt getroffenen Regelungen entsprachen diesen Anforderungen. Es wurden im Rahmen der Prüfung weder Fehler noch Probleme sichtbar, die auf eine mangelhafte Organisation zurückzuführen waren. Dennoch hat es Mängel gegeben, die aus der Sicht des Landesbeauftragten vermeidbar gewesen wären. Hierfür einige Beispiele:

- Trotz vorbildlicher Regelungen zum Betreten und Verlassen des Dienstgebäudes konnte während der Prüfung beobachtet werden, daß Lieferanten freien Zugang zum Gebäude erhielten.
- Bei ungültigen Erhebungsunterlagen wurde versäumt, die nach dem Volkszählungsgesetz vorgeschriebene Trennung der Erhebungsmerkmale von den Hilfsmerkmalen vorzunehmen.
- Erhebungsunterlagen, die von Bürgern direkt an das Statistische Landesamt gesandt worden waren, wurden auch dann unmittelbar an die örtlichen Erhebungsstellen weitergeleitet, wenn den Unterlagen eindeutig entnommen werden konnte,

daß der Betroffene mit dieser Weiterleitung nicht einverstanden war.

Mit der Vernichtung der Erhebungsvordrucke hätte Anfang Dezember 1988 begonnen werden können, da zu diesem Termin die Prüfarbeiten abgeschlossen waren. Tatsächlich hat die Vernichtung erst zwei Monate später stattgefunden. Die Ursachen für die Verschiebung des Vernichtungstermins konnte der Landesbeauftragte nicht klären. Er hat sich aber von der Ordnungsmäßigkeit der Vernichtungsaktion überzeugt.

5.4 Prüfung einer Kraftfahrzeugzulassungsstelle

23 Millionen Bürger sind im zentralen Verkehrsinformationssystem (ZEVIS) des Kraftfahrt-Bundesamtes gespeichert und über das Kraftfahrzeugkennzeichen und über den Namen des Kraftfahrzeughalters auffindbar. Ein komfortables „Bundesadreßregister", hervorragend geeignet für umfassende Personenkontrollen, könnte sich für die Polizeibehörden eröffnen, weil die Daten innerhalb von Sekunden verfügbar sind. Der Gesetzgeber hat die entsprechenden Konsequenzen gezogen und im Straßenverkehrsgesetz die rechtlichen Grundlagen für die automatisierte Datenübermittlung an die Polizeibehörden detailliert geregelt. Zur Überprüfung der Rechtmäßigkeit und der Erforderlichkeit hat das Kraftfahrt-Bundesamt die Abrufe entsprechend einer vorgegebenen Stichprobenquote zu dokumentieren. In seinem 9. Tätigkeitsbericht(S. 36) hat der Landesbeauftragte davor gewarnt, bei „problematischen" Anfragen diese Protokollierungspflicht dadurch zu umgehen, daß die Polizei statt beim Zentralregister bei der örtlichen Zulassungsstelle anfragt.

Tatsächlich wurden in der geprüften Behörde keine Aufzeichnungen über telefonische oder mündliche Auskünfte aus dem Fahrzeugregister geführt. Der Landesbeauftragte hat deshalb den Minister für Wirtschaft, Technik und Verkehr aufgefordert, den Kraftfahrzeugzulassungsstellen auch für mündliche und telefonische Auskünfte aus dem Fahrzeugregister die Pflicht zur Dokumentation verbindlich vorzuschreiben.

Die Prüfung erstreckte sich auch auf Fragen der Erhebung und Speicherung von Halter- und Fahrzeugdaten. Kritisiert werden mußte, daß nach wie vor bei Ausländern die Paßnummern und die Heimatadressen erhoben und gespeichert wurden, obwohl diese Daten in dem neuen Datenkatalog des Straßenverkehrsgesetzes nicht mehr enthalten sind. Der Landesbeauftragte hält es für bedenklich, daß derartige Rechtsänderungen nicht unverzüglich in den landesweit eingesetzten automatisierten Verfahren Berücksichtigung finden. Auf sein Drängen hat der Minister für Wirtschaft, Technik und Verkehr die Zulassungsstellen angewiesen, diese Daten nicht mehr zu erheben und die unzulässig gespeicherten Daten zu löschen.

5.5 Ist die Anonymität in den AIDS-Beratungsstellen garantiert?

Die Gesundheitsämter der Kreise und kreisfreien Städte bieten anonyme AIDS-Beratungen an. Wegen der hohen Sensibilität der dabei anfallenden Daten und der Ängste der Ratsuchenden,

ob die garantierte Anonymität auch wirklich das hält, was sie verspricht, hat der Landesbeauftragte eine Beratungsstelle überprüft. Die Prüfung hat ergeben, daß die Ängste der Ratsuchenden in diesem Fall unbegründet waren. Es wurde folgendes Verfahren praktiziert. Der ratsuchende Bürger vereinbart mit den Mitarbeitern in der Beratungsstelle unter einem frei gewählten Stichwort einen Gesprächstermin. Während des Gespräches werden keine Notizen gemacht. Die Berater füllen lediglich ein Formular aus, das die Tatsache der Beratung ohne jeglichen Personenbezug dokumentiert, und halten bestimmte Merkmale als Grundlage für die Folgeberatungen fest (z. B. die Art der Risikogruppe). Zum Wiederauffinden dieses Vorgangs dient nur das vereinbarte Stichwort und eine vom Berater vergebene Kennnummer. Unter dieser Nummer werden die Betroffenen an einen Arzt weitergeleitet, der die Blutentnahme durchführt und die Probe dem Medizinaluntersuchungsamt übersendet. Auf dem gleichen Wege gelangt das Untersuchungsergebnis an den Berater zurück. Der informiert den Betroffenen im Rahmen eines zuvor vereinbarten Gesprächs. Nach Abschluß der Beratung werden nur die statistischen Daten sowie das Testergebnis und beim Arzt die anonymisierte Eintragung im „Blutbuch" aufbewahrt.

Allerdings kommt es vor, daß ratsuchende Bürger ihre Identität preisgeben, vor allem, wenn sie mit einem positiven Untersuchungsergebnis konfrontiert werden. In diesen Fällen beschränken die AIDS-Berater der geprüften Stelle die personenbezogenen Notizen auf ein Minimum. Die Unterlagen wurden allerdings mit nach Hause genommen, weil die Berater keine Möglichkeit sahen, sie in Schreibtischen oder Schränken sicher zu verschließen. Der Landesbeauftragte hat dies kritisiert. Die Daten können nicht wie das private Eigentum der Berater behandelt werden. Sie bleiben behördliche Daten und unterliegen somit den strengen Geheimhaltungs- und Verschwiegenheitspflichten und der Pflicht zur schnellstmöglichen Löschung. Inzwischen hat das geprüfte Gesundheitsamt sichergestellt, daß die AIDS-Berater ihre Unterlagen in den Behördenräumen ausreichend sicher verwahren können.

Insgesamt hat der Landesbeauftragte bei der Prüfung dieser Beratungsstelle ein positives Bild vom Stand des Datenschutzes in diesem hochsensiblen Bereich gewonnen. Er wird sich davon überzeugen, daß dieser Standard auch in anderen Gesundheitsämtern erreicht ist.

5.6 Prüfung im Klinikum der Christian-Albrechts-Universität zu Kiel

Der Landesbeauftragte hat nach seiner Prüfung im Verwaltungsbereich des Klinikums der Christian-Albrechts-Universität zu Kiel nunmehr auch den Umgang mit personenbezogenen medizinischen Behandlungsdaten in einigen Abteilungen des Klinikums geprüft. Auf erste Feststellungen konnte er bereits im 10. Tätigkeitsbericht (S. 49 ff.) hinweisen. Neben anderen haben sich die dort erwähnten Sachverhalte auch bei den weiteren Untersuchungen als datenschutzrechtliche Problembereiche gezeigt. Dabei war Grundlage der Überlegungen, daß die Verarbei-

tung derjenigen personenbezogenen Patientendaten, die für die Behandlung, also für die Heilung oder Linderung einer Krankheit, notwendig ist, wie die dafür erforderliche ärztliche Leistung selbst, ihre Rechtsgrundlage und Rechtfertigung in den Vertragsbeziehungen zwischen Patient und Klinikum bzw. behandelndem Arzt findet. Davon ausgehend ergab sich eine Reihe von kritischen Feststellungen, bezogen auf zwei Abteilungen.

–Zuständigkeit für Datenschutzfragen

In den Klinikabteilungen gab es zum Prüfungszeitpunkt keinen Mitarbeiter, dem ausdrücklich die Zuständigkeit für den „Datenschutz" zugewiesen worden war. Erst auf Anregung des Landesbeauftragten sind inzwischen in den einzelnen Klinikabteilungen Mitarbeiter für Fragen des Datenschutzes eingesetzt worden. Weiter wurde eine Datenschutzbeauftragte für das gesamte Klinikum bestellt.

–Fehlende organisatorische Regelungen

Schriftliche Regelungen über die Verwaltung und die Verwahrung von Patientenunterlagen liegen nicht vor. Auch gibt es keine Anweisungen über die Sperrung, Löschung und Übermittlung von Patientendaten. Krankengeschichten werden deshalb unbegrenzt aufbewahrt, auch wenn sie für konkrete Behandlungen schon lange nicht mehr benötigt werden. Ferner fehlen schriftliche Organisationsregelungen, die sicherstellen, daß Krankengeschichten nur von den zuständigen Ärzten und ihrem Hilfspersonal eingesehen und verwaltet werden dürfen. Die geprüften Stellen betrachten mündliche Anweisungen als ausreichend. Der Landesbeauftragte hält in einem so sensiblen Bereich wie dem Klinikum schriftliche Regelungen über den Zugriff auf und die Verwaltung und Verwahrung von Patientenunterlagen für unerläßlich. Er erwartet, daß solche Regelungen geschaffen werden.

– **Datenübersicht nicht geführt**

Nach den Bestimmungen des Landesdatenschutzgesetzes ist eine interne Übersicht über alle konventionellen und automatisierten Dateien zu führen. Erst im Verlaufe der Prüfung hat die Klinikumsverwaltung eine (allerdings unvollständige) Übersicht nachgereicht. Der Landesbeauftragte hat empfohlen, künftig besonderes Gewicht auf diese Übersicht zu legen. Sie verschafft der Klinikleitung die erforderliche Kontrollmöglichkeit und ist die Grundlage für die Einführung der notwendigen technischen und organisatorischen Datensicherungsmaßnahmen.

– **Keine Meldungen zum Dateienregister**

Automatisiert betriebene Dateien sind zum Landesdatenschutzregister zu melden. Für den Prüfungskomplex war lediglich eine einzige Datei gemeldet, die bezeichnenderweise nicht einmal mehr bestand. Im Verlaufe der Prüfung wurde zwar die Mehrzahl der bestehenden EDV-Dateien nachgemeldet, aber noch immer sind nicht alle Datenbestände erfaßt. Der Landesbeauftragte hat dies als Verstoß gegen das Landesdatenschutzgesetz förmlich beanstandet.

– **Mitteilungen an die Hausärzte**

Mitteilungen über Diagnosen und Therapien an die Hausärzte bzw. an die weiterbehandelnden Ärzte sind nicht grundsätzlich erforderlich. Die Patienten können auch hierüber frei entscheiden. Der Landesbeauftragte hat deshalb gefordert, sie künftig bei der Aufnahme nicht nur nach dem Namen des Hausarztes, sondern auch danach zu fragen, ob dessen Unterrichtung gewünscht wird.

– **Keine Vorlage von Schweigepflichtentbindungsklauseln**

Private Versicherungen und öffentliche Institutionen weisen in ihren Auskunftsersuchen in der Regel nur darauf hin, daß eine Einwilligung des Patienten vorliege. Das genügt nicht. Der Landesbeauftragte hat die Vorlage der Schweigepflichtentbindungserklärungen im Original gefordert. Nur auf diese Weise kann geprüft werden, auf welche Daten sich die Einwilligung erstreckt.

– **Auskünfte aus dem Archiv**

Die Mitarbeiterinnen des Archivs erteilten routinemäßig ohne Beteiligung der behandelnden Ärzte Auskünfte an Sozialleistungsträger. Der Landesbeauftragte geht davon aus, daß in diesen Fällen durch den verantwortlichen Arzt keine Prüfung stattgefunden hat, ob eine Befugnis zur Übermittlung vorlag. Er hat dieses Verfahren beanstandet. Die Überprüfung der Verfahrensweise hat weiter gezeigt, daß der Zugriff von Unbefugten auf Krankengeschichten möglich ist, daß Vollständigkeitskontrollen nicht durchführbar sind und daß Krankengeschichten unauffindbar sind, da gelegentlich Entleihvermerke fehlen oder Krankengeschichten verloren oder falsch eingeordnet sind. Dies hat der Landesbeauftragte als erheblichen Verstoß gegen die Grundsätze des Datenschutzes, insbesondere gegen die Verpflichtung zur Gewährleistung der Datensicherheit, beanstandet.

– **Operationsberichte in Bewerbungsunterlagen**

Dem Landesbeauftragten wurde während der Prüfung von mehreren Ärzten erklärt, daß Kopien von Operationsberichten mit voller Namensangabe des Patienten den Bewerbungsunterlagen der Ärzte beigefügt werden, wenn diese beabsichtigen, an ein anderes Krankenhaus zu wechseln. Damit werden den Mitgliedern von Berufungsgremien Daten zugänglich gemacht, die der ärztlichen Schweigepflicht unterliegen. Der Landesbeauftragte hat dies als unzulässige Offenbarung gewertet und gefordert, künftig nur in anonymisierter Form über durchgeführte Operationen zu berichten (vgl. 10. TB, S. 51). Das Klinikum hat den Sachverhalt zwischenzeitlich bestritten. Der Landesbeauftragte hat dies zur Kenntnis genommen. Er glaubt allerdings nicht, daß die betreffenden Ärzte ihm eine unrichtige Darstellung gegeben haben.

– **Labordokumentationssystem**

Das Hauptlabor der Chirurgie plant den Aufbau eines umfangreichen EDV-Dokumentationssystems für die Analysen.

Der Landesbeauftragte hat empfohlen, dabei auf die Speicherung der Namen der Patienten zu verzichten und andere Identifizierungsmerkmale wie Patientennummern oder Codewörter zu benutzen. Das Klinikum will dieser Anregung folgen.

– **Krankenblätter nicht immer unter Verschluß**

Die Aufbewahrung von Patientendaten in den Arzt- und Stationszimmern ist verbesserungsbedürftig. Patientenunterlagen, wie Krankengeschichten, Fieberkurven, pflegerische Dokumentationen usw., werden durchweg unverschlossen aufbewahrt. Auch die Zimmer sind unverschlossen und häufig nicht besetzt. Hier sind zusätzliche Datensicherungsmaßnahmen erforderlich.

– **Verarbeitung von Statistikdaten**

Innerhalb des Klinikums nimmt die Abteilung für medizinische Statistik und Dokumentation (AMSD) die Aufgabe eines internen Service-Rechenzentrums wahr. Sie erfaßt in Zusammenarbeit mit den Klinikabteilungen Patientendaten für die verschiedensten Funktionen. Den Umfang der Datenverarbeitung für Forschungszwecke und die Berechtigung, Daten für Forschungszwecke zu speichern, hat der Landesbeauftragte im gegenwärtigen Zeitpunkt zwar noch nicht geprüft, es ist ihm aber bekannt, daß dies die wesentliche Aufgabenstellung der AMSD ist. So liefert sie z. B. Computerlisten über ausgewählte Behandlungsfälle. Der Landesbeauftragte hat hierzu angemerkt, daß bei personenbezogenen Auswertungen die Anweisung des Abteilungsleiters oder leitenden Oberarztes der behandelnden Abteilung die Einwilligung der betroffenen Patienten nicht ersetzen kann, da auch diese Klinikabteilung die Daten nur zum Zwecke der Behandlung vorhält und die Computerlisten eindeutig für Forschungszwecke genutzt werden.

– **Weitergabe von Daten an Doktoranden**

Wie in allen Universitätskliniken haben auch im geprüften Bereich Doktoranden Zugriff auf archivierte Krankengeschichten. Sie sind in dieser Funktion jedoch nicht an der Behandlung eines Patienten, die häufig schon Jahre zurückliegt, beteiligt. Der Behandlungsvertrag kann somit nicht Grundlage für die Offenbarung der Patientendaten sein. Im Regelfall liegt auch keine ausdrückliche Einwilligung der betroffenen Patienten zur Offenbarung der Daten an den Doktoranden vor. Auch aus der Tatsache, daß in vielen Fällen der den Doktoranden betreuende Hochschullehrer gleichzeitig der behandelnde Arzt ist, kann keine Befugnis abgeleitet werden. Die Anfertigung einer Dissertation ist keine Hilfsfunktion bei der Behandlung, sondern dem Bereich wissenschaftlicher Tätigkeit zuzuordnen. Die ärztliche Berufsordnung bestimmt hierzu, daß für wissenschaftliche Forschung der Schweigepflicht unterliegende Tatsachen und Befunde nur anonym mitgeteilt werden dürfen, soweit der Patient nicht ausdrücklich zugestimmt hat. Offenbarungen gegenüber Doktoranden sind damit in der Regel unbefugt im Sinne

von § 203 Abs. 1 Strafgesetzbuch. Der Landesbeauftragte hat gefordert, entweder nur anonymisierte Patientendaten zur Verfügung zu stellen oder aber eine ausdrückliche Einwilligung der Patienten einzuholen.

– **Nachuntersuchungen zur Forschungszwecken**

Gelegentlich werden Patienten zu sog. Nachuntersuchungen eingeladen, ohne sie darüber aufzuklären, daß nicht eine Behandlung, sondern eine Datenerhebung für wissenschaftliche Zwecke beabsichtigt ist. Problematisch erscheint, daß den Patienten suggeriert wird, es gehe hier um einen Bestandteil der Behandlung, weil sie sonst möglicherweise nicht so bereitwillig an den Nachuntersuchungen teilnehmen würden. Datenerhebungen für wissenschaftliche Forschung sind nur zulässig, wenn die Betroffenen ausdrücklich zugestimmt haben. Das setzt aber voraus, daß sie im vollen Umfang über die Zusammenhänge aufgeklärt wurden. Der Landesbeauftragte hat eine ausreichende vorherige Information gefordert.

– **Keine Übersicht über die EDV-Hardware**

Besonders schwierig gestaltete sich die Prüfung des EDV-Einsatzes in den geprüften Abteilungen. Der Landesbeauftragte mußte erheblichen Spürsinn an den Tag legen. Hieß es zunächst: „EDV haben wir nicht, es gibt lediglich Schreibautomaten, die jedoch keine personenbezogenen Daten speichern", tauchte dann im Verlaufe der Prüfung ein Computer nach dem anderen auf. Die Prüfung des Landesbeauftragten richtete sich im wesentlichen auf die Frage, ob die erforderlichen organisatorischen Maßnahmen für die Datensicherheit und die Ordnungsmäßigkeit der Datenverarbeitung getroffen wurden. Das war nicht der Fall. Mangels eines Gesamtverzeichnisses der eingesetzten Hardware einschl. der Personal-Computer fehlte eine wirkliche Übersicht über das EDV-Geschehen. Das ist aber Grundlage jeder wirksamen Kontrolle. Der Landesbeauftragte hat nachdrücklich eine solche Übersicht und entsprechende Sicherungsmaßnahmen gefordert.

– **Keine Freigabe und Dokumentation der EDV-Programme**

Bei fast allen in den Klinikabteilungen eingesetzten EDV-Anwendungen stellte sich weiter heraus, daß eigentlich keiner der zuständigen Ärzte detaillierte Angaben über die Anwendungssoftware machen konnte. Die Klinikabteilungen haben von den Herstellern mehr oder weniger fertig entwikkelte Programme erworben und vertrauen darauf, daß diese Software den Anforderungen des Krankenhausbetriebes entspricht. Das genügt nicht. Der Landesbeauftragte hat gefordert, daß die Anwender zu einer Entscheidung über die Funktionsfähigkeit und Ordnungsmäßigkeit der Datenverarbeitung in der Lage sein müssen. Dazu gehört es, daß jede EDV-Anwendung vor der Inbetriebnahme getestet, förmlich freigegeben und dokumentiert wird.

– **Unkontrollierter Einsatz von Personal-Computern**

Den unkontrollierten Einsatz von Personal-Computern in einem Krankenhaus wertet der Landesbeauftragte als höchst problematisch. Eine interne Überwachung und Prüfung der automatisierten Datenverarbeitung auf derartigen Geräten ist im Regelfall kaum möglich. So auch in den geprüften Stellen. Informiert über den Gegenstand der jeweiligen Datenverarbeitung waren nur die Ärzte, die in den einzelnen Funktionsbereichen mit „ihrem" System zu tun hatten. Auch wenn im Einzelfall keine Verletzung schutzwürdiger Belange der Patienten festgestellt werden konnte, muß auf die Dauer eine größere Kontrolle der Anwendungen auf Personal-Computern sichergestellt werden.

– **Patientendaten auf privaten Personal-Computern**

Neben dienstlichen wurden auch private Personal-Computer zur Verarbeitung von Patientendaten eingesetzt. Nähere Angaben über deren Einsatzbereiche konnten die Gesprächspartner dem Landesbeauftragten nicht machen. Die Sicherungsmaßnahmen bestehen offenbar nur aus dem Vertrauen in die Zuverlässigkeit der betreffenden Mitarbeiter. Dies verstößt gegen die Bestimmungen des Landesdatenschutzgesetzes und wurde vom Landesbeauftragten beanstandet.

– **Zusammenarbeit mit einem privaten Transplantationszentrum**

Im Gebäude der Chirurgie ist ein privatrechtlich organisiertes Transplantationszentrum untergebracht. Es unterliegt nicht der Kontrolle des Landesbeauftragten. Allerdings wurde im Rahmen der Prüfung untersucht, welche Patientendaten vom Klinikum an diese Zentrale fließen und worauf sich die Befugnis für die Datenübermittlung stützt. Dabei stellte sich heraus, daß zwar von den Patienten bzw. künftigen Patienten Einwilligungserklärungen abgegeben werden, diese jedoch nicht den datenschutzrechtlichen Anforderungen genügen und nicht alle praktizierten Informationsflüsse umfaßten. Datenschutzrechtlich unzulässig war z. B. der Zugriff der Mitarbeiter des Transplantationszentrums auf vollständige Krankengeschichten des Klinikums.

Insgesamt hat die Prüfung im Klinikum der Christian-Albrechts-Universität eines gezeigt: Obwohl Verantwortliche und Mitarbeiter die Bedeutung der ärztlichen Schweigepflicht und des Patientendatenschutzes durchweg erkennen, wird im konkreten Umgang mit personenbezogenen Behandlungsdaten dagegen immer wieder verstoßen. Zentrale Aufgabe einer Klinik ist es zwar, Patienten medizinisch zu betreuen. Es darf aber nicht dazu führen, daß das Bedürfnis, Behandlungsabläufe von Formalismen möglichst zu entlasten, zu einem ungesicherten und mitunter unbedachten Umgang mit personenbezogenen Daten führt. Sorglosigkeit kann gerade bei den hier in Frage stehenden äußerst sensiblen Informationen fatale Folgen für den Patienten und seine Persönlichkeitsrechte haben. Deshalb mußte der Landesbeauftragte auf bedenkliche Praktiken im Umgang mit Behandlungsdaten hinweisen und die Verletzung daten-

schutzrechtlicher Vorschriften beanstanden. Er betrachtet das nicht als Kritik um der Kritik willen, sondern als notwendigen Hinweis auf Verfahrensschwächen.

6. Telekommunikation und Poststrukturgesetz

Die Diskussionen um die technische und organisatorische Entwicklung der Deutschen Bundespost haben auch im Berichtsjahr angehalten. Der Landesbeauftragte hat die Erörterungen aufmerksam verfolgt und kritisch beobachtet. Denn es gehört zu seiner Zuständigkeit, zu prüfen, ob für Landes- und kommunale Stellen in Schleswig-Holstein die Nutzung der Postdienste hinreichenden Datenschutz und ausreichende Datensicherheit gewährleistet. Zwei Entwicklungen haben im Jahre 1988 den Überlegungen (vgl. 9. TB, S. 60) neue Aktualität und zum Teil eine neue Richtung gegeben. Am 1. Januar 1988 ist die neue Telekommunikationsordnung in Kraft getreten. Sie markiert einen Einstieg der Deutschen Bundespost, weg von bisher getrennten Fernmeldenetzen und -diensten, in ein einziges, dienstintegriertes Telekommunikationsnetz für die Übermittlung aller Nachrichtenarten. Zum anderen bringt der vorgelegte Entwurf eines Poststrukturgesetzes insbesondere im Bereich der Telekommunikation neue organisatorische Strukturen. Er bedeutet vor allem eine Öffnung der Postdienste auch für private Anbieter.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich in mehreren Entschließungen zu der neuen Situation geäußert. Unter Hinweis auf frühere und nur teilweise berücksichtigte Forderungen haben sie auf folgendes hingewiesen:

- Durch die Zusammenführung der verschiedenen Telekommunikationsdienste werden auch diejenigen personenbezogenen Daten zusammengeführt, die zur Abwicklung der entsprechenden Dienstleistungen erforderlich sind. Dadurch fallen an zentralen Stellen künftig erheblich mehr und leichter auswertbare personenbezogene Daten an als bisher, die Rückschlüsse auf das Kommunikationsverhalten der Teilnehmer erlauben. Die uneingeschränkte Verwendung solcher Daten für alle Telekommunikationsdienste begegnet erheblichen Bedenken.
- Die Möglichkeiten der neuen Dienste der Deutschen Bundespost müssen auch im allgemeinen Datenschutzrecht berücksichtigt werden. Alle personenbezogenen Daten aus Bild-, Sprach-, Text- und Datenübertragung müssen geschützt werden. Die Zulässigkeit, personenbezogene Daten zu verarbeiten und den Vorgang zu kontrollieren, sowie die dafür erforderlichen technisch-organisatorischen Maßnahmen sind an die neuen technischen Gegebenheiten anzupassen.
- Die im Bereich der Europäischen Gemeinschaft mittlerweile erhobenen Forderungen zur Entwicklung eines gemeinsamen Marktes für Telekommunikationsdienstleistungen und -geräte dürfen nicht dazu führen, daß die nationalen Datenschutz- und Datensicherheitsstandards in der Bundesrepublik unterschritten werden.

– Die Länder sind im Rahmen ihrer Zuständigkeit aufgerufen, die Nutzung der Telekommunikation zu regeln und dabei auch die notwendigen Datenschutzvorschriften zu erlassen. Der Bildschirmtext-Staatsvertrag könnte hierzu als Vorbild dienen. In einem entsprechenden Vertrag müßten auch die materiellen Voraussetzungen zum Betrieb privater Telekommunikationsdienste geregelt werden.

– Die Öffnung des Telekommunikationsbereichs für private Anbieter darf nicht zu unterschiedlichem – insbesondere geringerem – Datenschutz führen. Der Schutz des informationellen Selbstbestimmungsrechts bei der Telekommunikation darf nicht davon abhängig sein, welcher Anbieter „zufällig" und unbeeinflußbar vom Nutzer den entsprechenden Dienst betreibt. Das erfordert eine umfassendere gesetzliche Regelung, als es heute vorgesehen ist. Eine Verordnungsermächtigung reicht hierzu nicht aus, insbesondere wenn sie, wie derzeit vorgesehen, die Bundesregierung nur unzureichend zum Handeln verpflichtet. In einem Gesetz muß der Umfang der zulässigen Datenverarbeitung beschrieben, ihr Zweck bestimmt und das Verfahren dem Nutzer transparent gemacht werden. Die entsprechenden Vorschriften dürfen nicht durch privatrechtliche Vereinbarungen, z. B. allgemeine Geschäftsbedingungen im Rahmen privater Telekommunikationsdienste, unterlaufen werden. Schließlich müssen die Betreiber, Bundespost wie Private, die erforderlichen organisatorischen und technischen Maßnahmen zur Sicherung der personenbezogenen Daten treffen. Die privaten Betreiber müssen einer angemessenen Datenschutzkontrolle unterworfen werden, die der Kontrolle der Bundespost anzugleichen ist.

Der Landesbeauftragte wird bei seinen Prüfungen beobachten, ob die Nutzung der Postdienste durch Behörden des Landes und der kommunalen Körperschaften in Schleswig-Holstein den Datenschutz ausreichend gewährleistet.

7. Ordnungsmäßigkeit der Datenverarbeitung

7.1 Datensicherung bei Kleincomputern

Bereits seit mehreren Jahren befaßt sich der Landesbeauftragte im Rahmen seiner Kontrollmaßnahmen, seiner Beratungs- und Informationsgespräche und seiner jährlichen Tätigkeitsberichte (7. TB, S. 55; 9. TB, S. 59) mit Fragen der Sicherheit und der Ordnungsmäßigkeit beim Einsatz kleinerer Datenverarbeitungsanlagen und insbesondere bei der individuellen Nutzung der Personal-Computer. Da es sich dabei um eine bundesweite Problematik handelt, haben seine Kollegen beim Bund und in den anderen Bundesländern gleiches getan. Betrachtet man die jüngste Entwicklung der automatisierten Datenverarbeitung in der öffentlichen Verwaltung, so muß man trotzdem feststellen, daß es den Datenschutzbeauftragten offenbar nicht gelungen ist, den Behörden die spezifischen technisch-organisatorischen Problemstellungen und Sicherheitsaspekte hinreichend transparent zu machen.

Um ihren Forderungen mehr Nachdruck zu verleihen, hat sich die Konferenz der Datenschutzbeauftragten des Bundes und

der Länder veranlaßt gesehen, mit einer gemeinsamen Entschließung an die Öffentlichkeit zu treten. Die Datenschutzbeauftragten haben sich dabei von folgenden Überlegungen leiten lassen:

Die Zuverlässigkeit der automatisierten Datenverarbeitung ist eine als selbstverständlich unterstellte Voraussetzung des rechtmäßigen Verwaltungshandelns. Insbesondere dann, wenn die Verarbeitungslogik der Programme verbindlich vorgeschrieben ist – das gilt z. B. für alle Verfahren, die in den Erlaß eines Verwaltungsaktes einmünden –, sind die Behörden darauf angewiesen, einen den gesetzlichen Vorschriften und den Verwaltungsanweisungen entsprechenden Verfahrensablauf sicherstellen zu können. Ein Abweichen von der Verarbeitungslogik durch individuelle Einflußnahme auf die Datenverarbeitung, z. B. durch Manipulationen an Geräten und Programmen, kann nicht hingenommen werden.

In den vergangenen Jahrzehnten wurden Organisationsformen und Verfahren entwickelt, die es den großen Rechenzentren ermöglichen, die Datenverarbeitung hinreichend sicher abzuwickeln. Der Datensicherheit dienen dabei vor allem

- eine starke Strukturierung der internen Organisation der Rechenzentren,
- die Festlegung von Funktionstrennungen zwischen Anwendungsprogrammierung, Operating und Systemgenerierung,
- automatisierte Aufzeichnungen über alle Systemaktivitäten,
- Sicherung der Datenverarbeitungsanlagen,
- detaillierte Regelung der Arbeitsabläufe durch Dienstanweisungen und
- institutionalisierte Kontrollen der Arbeitsdurchführung.

Wenn in größeren Rechenzentren ein sicherer Betrieb ohne derartige Maßnahmen unbestritten nicht möglich ist, erscheint es bedenklich, daß heute in zunehmender Zahl kleinere Datenverarbeitungsanlagen installiert werden, bei denen z. B. wegen der geringen Mitarbeiterzahl hierauf verzichtet wird. Es erhebt sich in diesen Fällen die Frage, ob die Behörden überhaupt noch in der Lage sind, eine den Vorschriften und Weisungen entsprechende Verarbeitung der Daten sicherzustellen.

Folgende Schwachstellen werden erkennbar:

- Zwar gibt es häufig noch eine Funktion, die man organisatorisch als Rechenzentrum bezeichnen könnte. Diese wird aber nur von wenigen oder einem einzigen Mitarbeiter wahrgenommen. Möglicherweise ist dieser einzige Mitarbeiter sogar nur während eines Teils seiner Arbeitszeit für die Maschinenbedienung und im übrigen innerhalb des Anwenderbereiches tätig. Nicht selten sind ihm gleichzeitig Programmieraufgaben zur selbständigen Erledigung übertragen. Zur Vertretung des Maschinenbedieners werden häufig Mitarbeiter aus dem Anwenderbereich vorgesehen.
- Eine interne Überwachung und Prüfung der Arbeitsdurchführung ist in vielen Fällen nicht institutionalisiert, weil kein Mitarbeiter mit der dafür erforderlichen Fachkunde verfügbar

ist. Häufig ist der Vorgesetzte zu einer Beurteilung der Arbeit seines Mitarbeiters nicht in der Lage.

- Beim Einsatz von Personal-Computern, die den Benutzern für individuelle Anwendungen zur Verfügung stehen, kann sogar nicht mehr von einer organisatorisch abgrenzbaren Rechenzentrumsfunktion gesprochen werden. Die Benutzer sind Anwender, Maschinenbediener und Programmierer in einer Person.

Unter diesen Gegebenheiten wird die Datensicherheit soweit eingeschränkt, daß dies bei einem großen Rechenzentrum - jedenfalls für die Verarbeitung personenbezogener Daten nach verbindlich vorgeschriebener Verarbeitungslogik - als nicht hinnehmbar angesehen werden würde. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder folgende Empfehlungen gegeben:

- Vor jeder Entscheidung, ob für die Arbeiten eines Aufgabengebietes ein Personal-Computer oder eine sonstige kleinere Datenverarbeitungsanlage eingesetzt werden kann, muß geprüft werden, ob die dabei erzielbare Datensicherheit ausreichend ist. Die Verarbeitung personenbezogener Daten in einem automatisierten Verfahren, das keine angemessene Datensicherheit bietet, verstößt gegen die Datenschutzgesetze.
- Um die Datensicherheit zu gewährleisten, haben die Behörden die dem neuesten Stand der Technik entsprechenden Maßnahmen zu treffen. Weisungen an die Mitarbeiter sollten schriftlich erteilt und in Dienstanweisungen zusammengefaßt werden. Durch wirkungsvolle Kontrollen ist sicherzustellen, daß alle Vorschriften und Weisungen befolgt werden.
- Die Hersteller von Hard- und Software werden aufgefordert, Verfahren zu entwickeln, die einen Betrieb dieser Geräte mit einem Maß an Datensicherheit ermöglichen, das demjenigen großer Rechenzentren entspricht. Vor allem müssen Hilfsmittel verfügbar gemacht werden, die es den datenverarbeitenden Stellen ermöglichen, sicherzustellen, daß eine verbindlich vorgeschriebene Verarbeitungslogik auch tatsächlich eingehalten werden kann. Dazu bedarf es dringend solcher Betriebssysteme, die gewährleisten, daß Programme ausschließlich in der freigegebenen Fassung zum Ablauf kommen können. Wesentliche, der Datensicherheit dienende Komponenten sollten in die Betriebssysteme integriert werden, um Manipulationen und Umgehungsmöglichkeiten zu erschweren.

Der Landesbeauftragte würde es begrüßen, wenn die Überlegungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Ausgangspunkt einer konstruktiven Erörterung und Lösung der immer deutlicher zutage tretenden Probleme zwischen den Herstellern, den Anbietern, den Dienstleistungseinrichtungen, den Anwendern und den Datenschutzbeauftragten würden. Er warnt davor, die Lösung der Probleme solange vor sich herzuschieben, bis erste schwere Beeinträchtigungen der schutzwürdigen Belange der Bürger zu verzeichnen sind.

7.2 Jetzt warnt auch der Innenminister vor Computerviren

Als der Landesbeauftragte im Jahre 1985 erstmals vor der Gefahr der Computerviren gewarnt hat (8. TB, S. 62), rief dies bei den Behörden bestenfalls ungläubiges Kopfschütteln hervor. Von einigen Seiten wurden ihm sogar Panikmache und eine fahrlässig oberflächliche Beurteilung der technischen Gegebenheiten vorgeworfen. Hiervon ist heute keine Rede mehr. „Computerviren" sind ebenso Realität wie „trojanische Pferde", „logische Bomben" und „Würmer". Über 20 unterschiedliche Versionen sind allein in der Bundesrepublik bekannt. Wie viele dieser Programme bereits in den USA und damit wahrscheinlich bald auch hier mehr oder weniger erfolgreich „ihre Arbeit verrichten", kann man nur ahnen. Nahezu jeden Monat werden neue Virensuch- und -abwehrprogramme auf dem Softwaremarkt annonciert. Seit kurzem bietet ein Institut der Hamburger Universität seine Dienste bei der „Entseuchung" infizierter Computersysteme an.

Eigentlich könnte der Landesbeauftragte die „Szene" mit einer gewissen Gelassenheit betrachten, denn im Augenblick müssen ja nur die Datenverarbeiter um ihre Millioneninvestitionen in Computer-Software fürchten und nutzlos vertaner Maschinenzeit für Reparatur- und Wiederherstellungsmaßnahmen nachtrauern. Eine solche Sicht würde allerdings einen ganz entscheidenden Aspekt unberücksichtigt lassen: Viren, trojanische Pferde, Würmer usw. können nur deshalb erfolgreich sein, weil eine Reihe weitverbreiteter Computer und Betriebssysteme so gravierende konzeptionelle Schwächen aufweist, daß sie zu Manipulationen an Programmen und Daten geradezu einladen. Mit denselben Methoden, mit denen man heute von Deutschland aus Weihnachtsgrüße auf Datensichtgeräten in den USA erscheinen und Großcomputer sich so sehr mit sich selbst beschäftigen läßt, daß internationale Datennetze zusammenbrechen, wird man morgen Datenbanken mit personenbezogenen Informationen ausspähen und ihren Inhalt zum Nachteil der Betroffenen manipulieren können. Kurz gesagt: Es fehlt mit Sicherheit nicht am Know-how, sondern offenbar (bis jetzt noch) nur am Motiv.

Nach Auffassung des Landesbeauftragten ist der Zeitpunkt gekommen, wo die Behörden handeln müssen, und zwar insbesondere diejenigen, die die besonders „anfälligen" Personal-Computer einsetzen. Er weiß sich darin mit dem Innenminister einig, der für seinen Zuständigkeitsbereich erfreulicherweise ein Merk- und Informationsblatt zum Thema Computerviren herausgegeben hat. Darin erläutert er, daß das ungewollte Einschleusen von Computerviren in Arbeitsplatzrechner und Personal-Computer in der Regel über Disketten oder bei vernetzten Systemen mittels Datenübertragung erfolgt. „Virusverdächtig" seien vor allem Demonstrationsdisketten von Software-Firmen (insbesondere unverlangt zugesandte Demonstrations-Disketten), Disketten mit sog. Public-Domain-Software (Billigangebote in Computerläden, die keinem Urheberrechtsschutz unterliegen) und Disketten mit Computer-Spielen. Eventuelle Sicherheitsmaßnahmen gegen unerwünschte Virenprogramme müssen seines Erachtens aufgrund deren spezifischen Eigenschaften

bereits sehr früh ansetzen, damit die Implementierung eines Virus verhindert oder zumindest erschwert wird. Folgende Maßnahmen sollten sofort für dienstlich genutzte Personal-Computer getroffen werden:

- Ausschließliche Nutzung der Software-Produkte, die für die „offiziellen" Anwendungen beschafft und freigegeben worden sind. Keine Nutzung von Spiel-Disketten, sog. Public-Domain-Software und Privatdisketten.
- Kein ungeschütztes Einspielen von Demonstrationsdisketten.
- Für alle Programme ist eine irreversible Checksumme zu ermitteln, die deren Länge widerspiegelt. Die Checksumme soll auf einer besonderen Diskette gespeichert werden. Diese Diskette ist unter Verschluß zu halten, so daß Manipulationen an der Prüfsumme unmöglich sind.
- Regelmäßig sollen diese Checksummen mit dem aktuellen Summenstand der zu schützenden Programme verglichen werden.
- Bei Abweichung der Prüfsummen sind unverzüglich weitere Nachforschungen nach einer etwaigen Vireninfektion anzustellen.
- Die Prüfungsintervalle sind so zu bemessen, daß auf noch intakte - nicht verseuchte - Programme zurückgegriffen werden kann.

Der Landesbeauftragte betrachtet die vom Innenminister angeordneten Sicherheitsmaßnahmen als „Stand der Technik". Er wird künftig in allen ihm bekanntwerdenden Fällen, in denen entgegen seiner Empfehlung (vgl. Textziffer 7.1) personenbezogene Daten mit Hilfe von Personal-Computern verarbeitet werden, ohne daß vorstehende Sicherungen realisiert worden sind, Beanstandungen aussprechen.

8. Novellierung des Datenschutzrechts

8.1 Datenschutzbeauftragte kritisieren den Entwurf der Bundesregierung

Zu den zahlreichen Versuchen der Bundesregierung und der Fraktionen des Bundestages, das Bundesdatenschutzgesetz durch eine Novellierung an die heutigen rechtlichen und tatsächlichen Gegebenheiten anzupassen, hat sich der Landesbeauftragte in seinen früheren Tätigkeitsberichten (vgl. zuletzt 10. TB, S. 60) überwiegend kritisch geäußert. Er wiederholt seine Auffassung, daß die bisher vorgelegten Entwürfe nicht für sich in Anspruch nehmen können, eine ausgereifte und umfassende Antwort auf die Rechtsprechung des Bundesverfassungsgerichts, die Erkenntnisse der Praxis und die Herausforderungen der technischen Entwicklungen zu sein.

Diese Einschätzung wird von seinen Kollegen geteilt. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung zu dem Gesetzentwurf des Bundesinnenministers vom November 1987 festgestellt, daß die beabsichtigte Neufassung des Bundesdatenschutzgesetzes die gleichen Mängel aufweist wie der entsprechende Entwurf, der in

der 10. Legislaturperiode des Bundestages eingebracht worden ist. Die Datenschutzbeauftragten halten es insbesondere für verfehlt, das allgemeine Datenschutzrecht aufzusplittern in ein streng auf die Datenverarbeitung in Dateien bezogenes Bundesdatenschutzgesetz und ein den Datenschutz in Akten regelndes Verwaltungsverfahrensgesetz, das wichtige Verwaltungsbereiche, wie z. B. die Finanzverwaltung, die Strafverfolgung und die Sozialverwaltung, nicht erfaßt.

Sie bedauern ferner, daß bei der Vorbereitung des Entwurfs ihre Empfehlungen sowie die zwischenzeitlich von einigen Bundesländern erlassenen, in wesentlichen Punkten vorbildlichen Neuregelungen des Datenschutzes nahezu unberücksichtigt geblieben sind. Es ist zwar nicht zu verkennen, daß auch der jetzige Entwurf einige Verbesserungen gegenüber dem geltenden Recht aufweist. Insgesamt jedoch werden die in der Begründung des Entwurfs genannten Ziele der beabsichtigten Weiterentwicklung des Bundesdatenschutzgesetzes nicht erreicht. Die Anpassung an die Grundsätze des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz ist in mehrfacher Hinsicht nicht gelungen.

So enthält der Entwurf keine ausdrückliche Regelung der Datenerhebung, obwohl gerade diese den Bürger unmittelbar belastet. Die geplanten Vorschriften im Verwaltungsverfahrensgesetz reichen nicht aus. Auch erfährt der Grundsatz der Zweckbindung zu weitgehende Ausnahmen. Die Transparenz der Datenverarbeitung, insbesondere das Recht des Betroffenen auf Auskunft, bleibt hinter verfassungsrechtlichen Anforderungen zurück. Dem Fortschritt auf dem Gebiet der Informations- und Kommunikationstechnik (z. B. Arbeitsplatzcomputer, neue optische Speichermedien, Videoaufzeichnungen, Telekommunikation und Vernetzung) wird der Entwurf nicht gerecht. Der verwandte Dateibegriff und die Beibehaltung des bisherigen Katalogs technischer und organisatorischer Datensicherungsmaßnahmen entsprechen nicht der technischen Entwicklung. Die Kontrollbefugnis des Bundesbeauftragten für den Datenschutz wird insgesamt eingeschränkt, insbesondere durch den Ausschluß systematischer Kontrollen bei der Erhebung und der Verwendung personenbezogener Informationen außerhalb von Dateien. Keinesfalls kann eine Einschränkung der Kompetenz der Landesbeauftragten durch den Bundesgesetzgeber hingenommen werden. Die Datenschutzvorschriften für den nichtöffentlichen Bereich orientieren sich nicht an dem Grundsatz der Zweckbindung und räumen unvertretbare Verarbeitungsprivilegien ein.

Der Entwurf entspricht daher nicht den Erwartungen an ein zeitgemäßes Datenschutzrecht als Ausprägung des verfassungsrechtlich garantierten Rechts des Bürgers auf informationelle Selbstbestimmung. Dieses Recht ist erst jüngst durch das Bundesverfassungsgericht in seiner Entscheidung vom 9. März 1988 bestätigt worden. Dort heißt es:

„In dieses Recht wird nicht nur dann eingegriffen, wenn der Staat vom einzelnen die Bekanntgabe persönlicher Daten verlangt oder diese der automatisierten Datenverarbeitung zuführt ... Das Recht auf informationelle Selbstbestimmung schützt

vielmehr wegen seiner persönlichkeitsrechtlichen Grundlage generell vor staatlichen Erhebungen und Verarbeitungen personenbezogener Daten und ist nicht auf den jeweiligen Anwendungsbereich der Datenschutzgesetze des Bundes und der Länder oder datenschutzrelevanter Sonderregelungen beschränkt."

Die Konsequenz daraus muß eine möglichst lückenlose und präzise Regelung des Datenschutzes sein, um Rechtssicherheit für Bürger und Verwaltung herzustellen. Im Hinblick auf diese signifikanten Schwachstellen hat der Landesbeauftragte den Innenminister gebeten, in den weiteren Beratungen im Bundesrat auf eine grundlegende Überarbeitung des Gesetzentwurfs zu drängen. Den Verlautbarungen des Innenministers der Presse gegenüber hat der Landesbeauftragte entnommen, daß dies geschehen wird.

8.2 Durch ein neues Landesdatenschutzgesetz soll alles besser werden

Mit seiner Kritik an den vom Bundeskabinett inzwischen verabschiedeten Entwürfen zu den neuen „Datenschutz- und Sicherheitsgesetzen" hat der Innenminister des Landes Schleswig-Holstein die Ankündigung verbunden, für den Landesbereich eigene Gesetze zur Verbesserung des Datenschutzes im allgemeinen sowie speziell bei der Polizei und beim Verfassungsschutz zu erarbeiten. Dies wird vom Landesbeauftragten ausdrücklich begrüßt. Dabei ist für ihn von besonderer Bedeutung, daß er offenbar von Anfang an am Gesetzgebungsverfahren beteiligt werden soll. Es erscheint ihm jedenfalls bemerkenswert, daß der Innenminister ihn gebeten hat, einen „Wunschzettel", bezogen auf das neue schleswig-holsteinische Datenschutzrecht, zu erstellen, bevor mit den Arbeiten an einem Referentenentwurf im Innenministerium begonnen worden ist. Der Landesbeauftragte hat diese Gelegenheit „ganz unbefangen" genutzt und in einem ca. 50 Positionen umfassenden Katalog seine Wünsche und Anregungen zusammengestellt.

Bei der Fortentwicklung des Datenschutzrechts im Sinne der neueren Verfassungsgerichtsrechtsprechung ist seines Erachtens zunächst von folgenden „Eckwerten" auszugehen:

- Das geltende Datenschutzrecht hat sich, obwohl mit ihm gesetzgeberisches Neuland beschritten wurde, in der täglichen Praxis in einem Maße bewährt, daß alle Erwartungen übertroffen wurden. Das Landesdatenschutzgesetz enthält keine Bestimmung, von der man im nachhinein sagen muß, der Gesetzgeber sei damit „über das Ziel hinausgeschossen". Es gibt also keinen Grund, datenschutzrechtliche Regelungen zurückzunehmen oder abzuschwächen, weil sich herausgestellt hat, daß den Rechten des einzelnen in unverhältnismäßiger Weise Vorrang vor den Rechten der Allgemeinheit eingeräumt worden ist.
- Demgegenüber zwingt die Rechtsprechung des Bundesverfassungsgerichts dazu, jede gesetzliche Neuerung daraufhin zu überprüfen, ob durch sie das Recht auf informationelle Selbstbestimmung konkret gestärkt oder etwa geschwächt wird. Bereichsspezifische Gesetze mögen die Persönlich-

keitsrechte der Bürger unter Beachtung der verfassungsrechtlichen Rahmenbedingungen einschränken; das Landesdatenschutzgesetz hat als Schutzgesetz die vorrangige Aufgabe, sie zu stärken.

– Die datenschutzrechtlichen Neuregelungen sollten so ausgestaltet sein, daß die Öffentlichkeit in ihnen eine überzeugende Antwort auf die in den vergangenen zehn Jahren erkennbar gewordenen Probleme sieht. Wenig überzeugend wäre es zum Beispiel, die bisherigen Bestimmungen zur Datensicherheit und zur ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme unverändert zu lassen, obwohl in Fachkreisen und in der öffentlichen Diskussion unbestritten ist, daß die heutige und die künftige automatisierte Datenverarbeitung ganz andere und wesentlich komplexere Sicherheitsrisiken in sich birgt als diejenige von vor zehn bis fünfzehn Jahren.

– Die notwendigerweise abstrakten Rahmenbedingungen des Datenschutzrechts müssen mit dem bereichsspezifischen Verfahrensrecht korrespondieren. Es erscheint z. B. nicht sinnvoll, das Datenschutzrecht mit einer Vielzahl von Grundsatz- und Ausnahmeregelungen über die Zweckbindung erhobener Daten zu befrachten, ohne gleichzeitig im Landesverwaltungsgesetz die Voraussetzungen und Grenzen der Amts- und Informationshilfe neu zu definieren.

– Das vom Bundesverfassungsgericht hervorgehobene Gebot der Normenklarheit gesetzlicher Regelungen gilt im besonderen Maße auch für Datenschutzgesetze. Um dies zu erreichen, genügt es nicht, auf unverständliche Formulierungen und komplizierte Verweisungstechniken zu verzichten. Ebenso wichtig ist es, daß die Öffentlichkeit nicht im unklaren über die tatsächlichen Folgen der Neuregelungen gelassen wird.

Unter diesen Gesichtspunkten hat der Landesbeauftragte angeregt, in einer Neuregelung u. a. folgende Überlegungen zu berücksichtigen:

– Der Anwendungsbereich des Datenschutzrechts sollte nicht auf die dateimäßige Datenverarbeitung begrenzt bleiben. Auf die als „Vorsichtsmaßnahme" gedachte Beschränkung des Landesdatenschutzgesetzes auf solche Datenbestände, die ein besonderes Gefährdungspotential darstellen, kann nach nunmehr zehnjähriger Erfahrung mit dem Datenschutzrecht verzichtet werden. In der Praxis wenden bereits heute die Verwaltung und die Datenschutzbeauftragten die materiellen datenschutzrechtlichen Bestimmungen entsprechend auch auf solche Datenbestände an, die nicht die Dateiqualifikation erfüllen. Die Bürger geben sich schon lange nicht mehr mit der Auskunft zufrieden, die Daten seien nicht in Dateien gespeichert, mithin stünden ihnen keine Datenschutzrechte zu. Die novellierten Datenschutzgesetze anderer Bundesländer gelten bereits für alle Datenbestände der öffentlichen Verwaltung, ohne daß es Anwendungsschwierigkeiten bezüglich der in Akten gespeicherten Daten gegeben hat.

– Der Gesamtkomplex der Auftragsdatenverarbeitung bedarf dringend einer grundsätzlichen Neuregelung. In erster Linie

sollten dabei konkrete Voraussetzungen definiert werden, unter denen es einer Behörde gestattet ist, Dritte mit der Verarbeitung personenbezogener Daten zu beauftragen. Die Regelungen sollten restriktiv sein, da die Auftragsdatenverarbeitung als Ausnahme und nicht als Regelfall anzusehen ist. Der Auftraggeber sollte den Nachweis erbringen müssen, daß er in der Lage ist, als „Herr der Daten" die uneingeschränkte Verantwortung für die Rechtmäßigkeit und die Sicherheit der Datenverarbeitung beim Auftragnehmer zu tragen. Deshalb sollten schriftliche Verträge und Weisungen sowie Kontrollbefugnisse obligatorisch sein. Dabei darf es keine Rolle spielen, ob die Daten beim Auftragnehmer in oder außerhalb von Dateien verarbeitet werden. Besondere Restriktionen sind erforderlich für Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen und bezüglich der Einschaltung nichtöffentlicher Stellen als Auftragnehmer.

– Ein weiterer Komplex von sehr weitreichender und grundsätzlicher Bedeutung ist die datenschutzrechtliche Behandlung der personenbezogenen Daten, die die Behörden aufgrund privatrechtlicher Verträge mit den Bürgern verarbeiten. Hierzu zählen z. B. Kaufverträge, Dienst- und Arbeitsverträge, Behandlungsverträge mit Krankenhäusern, Energielieferungsverträge und letztlich jede Form der freiwilligen Bereitstellung von Daten.

  Nach dem geltenden Datenschutzrecht bestimmt sich die Zulässigkeit der Verarbeitung der Daten durch eine Behörde zunächst danach, was zu ihrer „rechtmäßigen Aufgabenerfüllung erforderlich ist". Die vertraglichen Verpflichtungen der Behörden kommen erst dann zum Tragen, wenn man sie als eine Begrenzung bzw. Ausgestaltung der rechtmäßigen Aufgabenerfüllung betrachtet. Insoweit ergeben sich in der Praxis immer wieder komplizierte Zweifelsfragen (hindert z. B. eine vertraglich vereinbarte Pflicht zur Verschwiegenheit eine Behörde daran, die Daten im Rahmen der Amtshilfe weiterzugeben?).

  Es erscheint erforderlich und konsequent, das gesamte fiskalische Handeln der öffentlichen Stellen den gleichen datenschutzrechtlichen Regeln zu unterwerfen, die gelten, wenn die Bürger miteinander in vertragliche Beziehungen treten. Auch der Staat müßte dann im Zeitpunkt des Vertragsabschlusses offenlegen – und damit zum Gegenstand des Vertrages machen -, was er im Verlaufe der Vertragsabwicklung und danach mit den personenbezogenen Vertragsdaten zu tun gedenkt. Darüber hinausgehende Nutzungen sollten der einschränkenden Bedingung unterliegen, daß schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden.

– Es dürfte unumgänglich sein, die Erhebung personenbezogener Daten als eine Phase der Datenverarbeitung im Datenschutzrecht zu verankern. Bisher wurde von Behörden immer wieder der Versuch unternommen, zwischen der vermeintlich datenschutzrechtlich nicht relevanten Datenerhebungsphase und der eigentlichen Speicherung der Daten zu differenzieren. In der Regel sollte durch das Ausklammern der Datenerhebung eine datenschutzrechtliche Überprüfung der Daten-

quelle und der Art der Informationsgewinnung vermieden werden. Künftig sollte im Landesdatenschutzgesetz ausdrücklich klargestellt werden, daß öffentliche Stellen nur solche Daten speichern dürfen, die sie auf rechtmäßige Art und Weise gewonnen haben.

– Angesichts der rasanten Entwicklung der elektronischen Datenverarbeitung kommt der technischen und organisatorischen Absicherung der automatisierten Verfahren eine immer größere Bedeutung zu. Der Gesetzgeber war sich bereits vor zehn Jahren der Dynamik des technischen Fortschritts durchaus bewußt und hat die Verwaltung durch eine entsprechende Verordnungsermächtigung in den Bundes- und Landesdatenschutzgesetzen zur Anpassung der Regelungen über die Datensicherung an den Stand der Technik „aufgefordert". Das ist weder beim Bund noch in einem der Bundesländer geschehen. Der Landesbeauftragte zählt es nicht zu seinen „Verdiensten", daß er in den vergangenen Jahren nicht stärker auf eine Fortschreibung der Datensicherungsvorschriften gedrängt hat. Deshalb erscheint ihm eine Novellierung des schleswig-holsteinischen Datenschutzgesetzes ohne eine Anpassung der Regelungen über die Datensicherheit nicht denkbar. Durch eine detaillierte Ausgestaltung der einschlägigen Bestimmungen sollten die Grundlagen für allgemein anerkannte „Grundsätze ordnungsmäßiger Datenverarbeitung in der öffentlichen Verwaltung" geschaffen werden.

– In der Diskussion um die Novellierung der Datenschutzgesetze ist grundsätzlich unbestritten, daß ein verschuldensunabhängiger Schadensersatzanspruch, der nicht nur auf Vermögensschäden begrenzt ist, gesetzlich zu verankern ist. Die bisherigen Regelungen bzw. Entwürfe sind jedoch dadurch gekennzeichnet, daß durch Unschärfen und Einschränkungen die Durchsetzung der Ansprüche nicht gerade erleichtert wird. Es ist davor zu warnen, einen Anspruch zuzugestehen, der in der Praxis nicht realisierbar ist.

– Die bisher in den Datenschutzgesetzen festgeschriebenen Ausnahmeregelungen zur Zweckbindung von Daten erscheinen dem Landesbeauftragten wenig überzeugend.

  Daten, die ein Bürger freiwillig für einen ganz bestimmten Zweck zur Verfügung gestellt hat, dürfen grundsätzlich nicht zweckentfremdet werden.

  Über die geplante „anderweitige" Nutzung von Daten, die er freiwillig zur Erlangung eines begünstigenden Verwaltungsaktes offenbart hat, ist er spätestens bei der Erteilung des Verwaltungsaktes aufzuklären, in der Regel sollte die Aufklärung bereits bei der Antragstellung erfolgen.

  Nur Daten, die dem Staat aufgrund gesetzlicher Verpflichtungen zu „liefern" sind, kann dieser im Rahmen der einschlägigen verfahrensrechtlichen Vorschriften grundsätzlich auch zu anderem rechtmäßigen Verwaltungshandeln nutzen (z. B. im Rahmen der Amtshilfe).

  Darüber hinaus kann die Zweckbindung nur durch die Einwilligung des Betroffenen aufgehoben werden oder wenn eine Einzelfallprüfung ergibt, daß sie im Interesse des Betroffenen liegt.

- Der Bedeutung einer vollständigen Dokumentation der Datenübermittlungen dürfte in der Vergangenheit zu wenig Beachtung geschenkt worden sein. Sie ist in der Praxis jedoch die entscheidende Voraussetzung zur Verfolgung von Datenströmen und die Grundlage für datenschutzrechtliche Überprüfungen. Es ist daher zu fordern, daß vollständig erfaßt wird, welcher Stelle wann welche Daten übermittelt worden sind. Auch die Übermittlungsersuchen gehören zu dieser Dokumentation. Bei programmgesteuerten Datenübermittlungen aus automatisierten Dateien sind die Bedingungen, unter denen regelmäßig Daten übermittelt werden, der Datenumfang und die Datenempfänger zu dokumentieren. Online-Abfragen sind zumindest temporär zu dokumentieren und ihre Erforderlichkeit stichprobenweise bei der abrufenden Stelle zu überprüfen. In diesem Zusammenhang erscheint ein generelles Verbot von Datenübermittlungen an nichtöffentliche Stellen im Wege von OnlineAbrufen angebracht. Eine Ausnahme kann nur gelten für Zugriffe auf öffentliche Datenbestände, die an keinerlei rechtliche Bedingungen geknüpft sind.
- Die Zulässigkeitsvoraussetzungen für Datenübermittlungen an nichtöffentliche Stellen sollten keinesfalls erweitert werden. Von dem Grundsatz der Amtsverschwiegenheit, wie er sich z. B. in § 88 a Landesverwaltungsgesetz dokumentiert, sollte das Datenschutzgesetz nur wenige, exakt beschriebene Ausnahmen zulassen.
- Die allseits begrüßte Gebührenfreiheit für Auskünfte und für die Akteneinsicht dürfte nur praktikabel sein, wenn in das Gesetz auch eine Mißbrauchsklausel eingefügt wird.
- Wird eine Auskunft abgelehnt, sollte die Behörde verpflichtet sein, den Betroffenen auf die Möglichkeit der Überprüfung dieser Entscheidung durch den Landesbeauftragten für den Datenschutz oder durch Gerichte hinzuweisen. Wird dem Betroffenen die Tatsache der Datenspeicherung vorenthalten, sollte die Behörde verpflichtet sein, den Landesbeauftragten für den Datenschutz über den Vorgang zu unterrichten.
- Es sollte im Landesdatenschutzgesetz klargestellt werden, daß die Berichtigung von Daten auch deren Vervollständigung umfaßt. Darüber hinaus sollte generell die Pflicht bestehen, im Falle der Berichtigung von Daten alle, also nicht nur die regelmäßigen Empfänger der unrichtigen Informationen, entsprechend zu benachrichtigen. Ausnahmen von dieser Regel sollten nur zugelassen werden, wenn die Berichtigung schutzwürdige Belange des Betroffenen beeinträchtigen würde oder wenn die richtigen Daten beim Empfänger offensichtlich nicht mehr erforderlich sind.
- Bezüglich der Sperrung von Daten sollte ein novelliertes Datenschutzgesetz zu mehr Flexibilität führen. Grundsätzlich sollten personenbezogene Daten zum frühestmöglichen Zeitpunkt gesperrt werden. Dazu bedarf es jedoch der gesetzlichen Klarstellung, wann Daten nicht mehr zur rechtmäßigen Aufgabenerfüllung einer Behörde erforderlich sind. Die Ausnahmen vom Nutzungsverbot sollten auf die Einwilligung

des Betroffenen und die Beweisnot der speichernden Stelle begrenzt werden.

- Die Regelungen über die Erstellung von Datenübersichten und Meldungen zum Dateienregister sollten neu gestaltet werden. Beide Dokumentationen sollten miteinander vereinigt und als Datenregister bezeichnet werden. Es sollten darin nur Daten erfaßt werden, die dateimäßig gespeichert sind, weil sich Akteninhalte kaum strukturieren lassen. Die Darstellung sollte allerdings nicht datei-, sondern verfahrensbezogen erfolgen. Die modernen Verfahren der automatisierten Datenverwaltung (z. B. relationale Datenbanken) kennen den Begriff der Datei ohnehin nicht mehr. Das Datenregister sollte Auskunft geben über die Bezeichnung und den Inhalt des Datums, die Rechtsgrundlage der Speicherung, die Datenquelle, die möglichen Datenempfänger, den Zeitpunkt der Sperrung, die Bezeichnung der Verfahren, in denen das Datum genutzt wird bzw. des Verwendungszweckes und die Bezeichnung des Datenbestandes, in dem das Datum gespeichert ist. Neben dem Datenregister sollten Behörden, die personenbezogene Daten für sich oder andere Behörden automatisiert verarbeiten, auch ein authentisches Verzeichnis der installierten Hardware und der eingesetzten DV-Programme führen. Die Nutzung von Hard- und Software, die nicht in dieser Weise registriert und dokumentiert ist, sollte als unzulässig gelten.
- Die Öffentlichkeit sollte vom Landesbeauftragten für den Datenschutz alle fünf Jahre in einem besonderen Bericht über „Art und Umfang der automatisierten Datenverarbeitung der öffentlichen Stellen im Lande" informiert werden. Grundlage dieser Information wären die Dateienregister der Behörden, die dem Landesbeauftragten ebenfalls alle fünf Jahre in einer fortgeschriebenen Fassung vorzulegen wären. Dieses Verfahren würde an die Stelle der jetzigen Veröffentlichung des Dateienregisters treten, das sich nicht bewährt hat.
- Die Aufgaben des Landesbeauftragten für den Datenschutz sollten dahingehend erweitert werden, daß er die Auswirkungen der automatisierten Datenverarbeitung auf die Arbeitsweise und die Entscheidungsprozesse der Behörden und sonstigen öffentlichen Stellen zu beobachten hat. Stellt er fest, daß sie zu einer Beschränkung der Kontroll- und Aufsichtsmöglichkeiten des Schleswig-Holsteinischen Landtages, der kommunalen Vertretungskörperschaften, des Landesrechnungshofes oder der sonstigen mit Kontroll- und Aufsichtsaufgaben betrauten Organe öffentlicher Stellen führen, hat er Maßnahmen vorzuschlagen, die dem entgegenwirken.
- Im Hinblick auf die enge Anbindung des Landesbeauftragten an das Parlament sollten auch die einzelnen Fraktionen des Landtages ein gesetzlich verankertes Recht zur Inanspruchnahme seiner Beratungs- und Gutachterfunktion erhalten. Bisher steht dies lediglich dem Parlament insgesamt, der Landesregierung und den Behörden zu.
- Um die in der Vergangenheit immer wieder aufgetretenen Zweifel auszuräumen, sollte im Landesdatenschutzgesetz

ausdrücklich klargestellt werden, daß dem Landesbeauftragten für den Datenschutz auch ohne Einwilligung des Betroffenen, jedoch nicht gegen dessen Willen, ein uneingeschränktes Kontroll- und Einsichtsrecht bezüglich solcher Datenbestände zusteht, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen, die gesperrt sind oder bei denen dem Betroffenen oder einem Dritten Vertraulichkeit zugesichert worden ist.

- Auf eine Wissenschaftsklausel sollte im Landesdatenschutzgesetz verzichtet werden. Die Frage, unter welchen Voraussetzungen personenbezogene Verwaltungsdaten durch öffentliche oder durch nichtöffentliche Stellen ohne Einwilligung des Betroffenen entgegen der ursprünglichen Zweckbestimmung zu wissenschaftlichen Zwecken genutzt werden dürfen, kann nach Auffassung des Landesbeauftragten nur in bereichsspezifischen Gesetzen hinreichend normenklar geregelt werden. In wichtigen Teilbereichen, wie z. B. für Sozial- und Patientendaten, ist dies bereits geschehen. Der Versuch, allgemeingültige, mithin abstrakte Regelungen zu formulieren, dürfte daran scheitern, daß weder die Zweckbindung freiwillig bereitgestellter Daten durch Ausnahmetatbestände außer Kraft gesetzt werden kann, noch der Begriff „wissenschaftliche Forschung", insbesondere bei privaten Stellen, abschließend zu definieren ist.
- Derzeit ist nicht hinreichend geklärt, unter welchen Voraussetzungen öffentliche Stellen ohne Einwilligung des Betroffenen Videoaufzeichnungen anfertigen und für längere Zeit speichern dürfen. Der Einsatz automatisierter Identifizierungs- und Abgleichverfahren sollte eng begrenzt, wenn nicht gar untersagt sein.
- Die Verwendung personenbezogener Daten zu Archivierungs-, Planungs- und statistischen Zwecken stößt immer mehr auf Probleme. Entsprechende Regelungen im Landesdatenschutzgesetz könnten umfassende Archiv-, Planungs- und Statistikgesetze allerdings nur in Teilbereichen ersetzen.
- Die Grenzen des Einsatzes von Fernmeß- und Fernwirksystemen sollten festgelegt werden.
- Die relative Selbstständigkeit des Landesfunkhauses Schleswig-Holstein und des Landesstudios des ZDF sollten zu landesspezifischen datenschutzrechtlichen Regelungen für Rundfunkanstalten in öffentlich-rechtlicher Trägerschaft führen. Die Aktivitäten der Rundfunkanstalten, die nicht unter das Presseprivileg fallen (Verwaltung, Personal), sollten der Kontrolle des Landesbeauftragten für den Datenschutz unterliegen.

Auch wenn der Landesbeauftragte davon ausgehen muß, daß nicht all seine Vorschläge Berücksichtigung finden werden, so hofft er doch, daß es ihm als „Bürgeranwalt" gelingt, im weiteren Verlauf des Gesetzgebungsverfahrens die Interessen der von der Datenverarbeitung betroffenen Bürger erfolgreich zu vertreten.

Sachregister
zu den Tätigkeitsberichten
des Landesbeauftragten für den Datenschutz

(die römischen Ziffern verweisen auf den betr. Tätigkeitsbericht, die arabischen Ziffern entsprechen den Seitenzahlen der jeweiligen Landtagsdrucksache)

1. Tätigkeitsbericht = Landtagsdrucksache 8/1872 v. 08.01.1979
2. Tätigkeitsbericht = Landtagsdrucksache 9/364 v. 14.01.1980
3. Tätigkeitsbericht = Landtagsdrucksache 9/862 v. 22.01.1981
4. Tätigkeitsbericht = Landtagsdrucksache 9/1326 v. 25.01.1982
5. Tätigkeitsbericht = Landtagsdrucksache 9/1738 v. 20.01.1983
6. Tätigkeitsbericht = Landtagsdrucksache 10/355 v. 07.02.1984
7. Tätigkeitsbericht = Landtagsdrucksache 10/961 v. 13.05.1985
8. Tätigkeitsbericht = Landtagsdrucksache 10/1466 v. 08.04.1986
9. Tätigkeitsbericht = Landtagsdrucksache 10/1990 v. 31.03.1987
10. Tätigkeitsbericht = Landtagsdrucksache 12/10 v. 03.06.1988
11. Tätigkeitsbericht = Landtagsdrucksache 12/330 v. 12.05.1989

A

Abgabenordnung s. Steuerverwaltung
Adoptionsdaten VII/13; VIII/65; XI/11
Adreßbücher
– Berufsgruppen VI/50
– Einwohnermeldedaten s. Meldedaten
– Straßenverzeichnisse IV/11; V/14; VI/10; VII/7
AIDS – s. Medizinische Daten
Amtshilfe II/9; III/9; V/38; VI/43, 57; VII/8
Anschriftenfelder s. Datensicherungsmaßnahmen
Archivwesen
– gesetzliche Regelung IV/14; V/29; VI/32; VIII/35; XI/53
– Nutzung Archivdaten II/24; III/12; IV/13, 35; V/15, 29, 30; VIII/14, 53
Aufsichtsbehörde für den Datenschutz
– Gleichartigkeit datenschutzrechtlicher Problemstellungen bei der – III/43; V/44, 50
– Kontrollanspruch bei privatrechtlichen kirchlichen Einrichtungen IV/36
Auftragsdatenverarbeitung
– Datensicherungsmaßnahmen II/28; IV/38, 41
– Dokumentation von Aufträgen s. Dokumentation
– Einbindung automatisierter Verfahren in die Organisation des Auftraggebers IV/38, 41
– Fachamt als behördeninterner Auftraggeber IV/38
– Verantwortung der Auftraggeber s. Verantwortung
Aushänge am „Schwarzen Brett" s. Schüler-, Eltern- und Studentendaten
Auskunftsersuchen mit Begründung VI/19, 57; VII/35
Ausländerzentralregister VI/25; VII/18; X/30; XI/29
Ausschüsse s. kommunale Vertretungskörperschaften
Automationskommissionen
– Freigabe von Verfahren IV/39; VIII/66
– Zusammenarbeit mit dem Landesbeauftragten I/9; II/7

B

Bauerlaubnis XI/30
Bausparkassen
– Einsatz von „Werbern" IV/44
Barschel-Pfeiffer-Affäre X/63; XI/48
Beihilfe s. Personaldaten
Beobachtende Fahndung der Polizeibehörden s. polizeiliche Tätigkeit
Bereichsspezifischer Datenschutz
– Anforderungen an gesetzliche Regelungen VII/10, 14, 18, 21, 51; IX/7, 50
– vorrangige Geltung V/5
Berufsständische Vereinigungen s. Kammern
Besoldung s. Personaldaten
Besondere Vertragsbedingungen s. Vertragsgestaltung
Bewerberdaten XI/13
Bewerberkarteien s. Grundstücksinteressenten
Bildschirmtext s. Medien
Bundeskriminalamt s. polizeiliche Informationssysteme
Bundeszentralregister
– Auskunft VIII/47
– Löschung von Daten II/12
– Mitteilungen der Staatsanwaltschaften s. Staatsanwaltschaften

C

Computerviren VIII/62; XI/70

D

Daktyloskopische Daten s. polizeiliche Informationssysteme
Dateibegriff s. Novellierung des Datenschutzrechts
Dateienregister I/18; II/26; III/5, 26, 38, 41; IV/32, 50, 58; V/8; IX/29; X/33, 55; XI/61
Datenschutzbeauftragte in Behörden
– allgemein V/8; VII/55; XI/160
– Sozialbereich III/29; IV/31; V/10, 37; VII/55
Datensicherungsmaßnahmen s. a. Ordnungsmäßigkeit der Datenverarbeitung
– Aufbewahrung und Vernichtung von Unterlagen II/16; IV/40, 43; V/45; VIII/45; IX/18, 46
– Auftragsdatenverarbeitung s. Auftragsdatenverarbeitung
– Begrenzung des Datenprofils bei Datenübermittlung III/40; IV/22; VII/14, 46
– Dokumentation automatisierter Anfragen s. Dokumentationspflichten
– Fortschreibung durch Technologiewandel I/4; III/45; VII/55; VIII/67; IX/59
– Kontrolle der Datenverarbeitung IV/39, 40; IX/58; XI/64, 67
– Legitimationsprüfung bei mündlichen Anfragen II/16; III/14, 32; V/20, 36; XI/19
– organisatorische Maßnahmen IV/38, 41; V/9; IX/56; XI/54, 61
– Schalterbereiche mit starkem Publikumsverkehr V/21; VIII/46
– Versand von Schriftstücken I/11; III/40; IV/28; V/20
– Vorkehrungen gegen unbefugte Datennutzung und Datenweitergabe IV/44; V/20, 21; VI/31; VIII/58; IX/23, 52, 53

Datenübersicht XI/61
Datenzentrale Schleswig-Holstein
– Verantwortung für Programmentwicklung, -pflege und -sicherung s. Verantwortung
– Vertragsgestaltung bei der Auftragsdatenverarbeitung s. Vertragsgestaltung
Denkmalschutz IX/47
Dokumentationspflichten
– automatisierter Datenaustausch III/28; IV/21, 30; VI/9; VII/39; VIII/14, 49,63
– Datenübermittlungen VIII/13
– Einsatz von EDV-Systemen III/29; IV/39; VI/62; IX/57
– Einsichtnahme in Dateibestände I/15; V/12; VI/59; VIII/14
– Grundbuchauskünfte XI/32
– Melderegisterauskünfte XI/12
– Überwachung der Auftragsdatenverarbeitung II/29; IV/41; VI/60
Dokumentationszentrale der Landeskrankenhäuser s. Forschung

E

Eigentümerverzeichnis s. Grundbuch
Einsatzleitstellen s. Funkverkehr
Energieversorgungsunternehmen VIII/47; IX/17
Entmündigungsverfahren XI/34
Erkennungsdienstliche Daten s. polizeiliche Informationssysteme

F

Familienverbund im Melderecht s. Kinder
Forschung
– Adressenziehen aus Melderegistern V/12; VII/12; VIII/13; IX/50
– Auswertung von Gerichtsakten I/12; IX/30; X/33
– Genehmigung bei der Verwertung von Sozialdaten III/30; IV/31; X/42
– Hinweis auf die Freiwilligkeit bei der Teilnahme an Forschungsvorhaben I/12; II/24; VI/45, 50; X/44
– Krankheitsregister V/49; VI/7, 47; VII/6, 8, 53; XI/50
– Nutzung von archivierten Verwaltungsdaten s. Archivwesen
– Spannungsverhältnis zwischen Datenschutz und Forschung II/23; III/31; IV/34, 57; IX/48
– Verarbeitung medizinischer Daten III/31; V/41, 49; VI/47; VII/6, 35; VIII/55; IX/38; XI/64
– Verfahren bei der Erhebung von Daten I/12; II/23; IV/34, 47
– Verwertung gesperrter Daten I/12; II/23; III/32; IV/35; V/15, 49
– Verwertung medizinischer Daten in der Dokumentationszentrale der Landeskrankenhäuser III/32; V/41; VII/8
– wissenschaftliche Auswertung einer Fremdarbeiterkartei II/24; III/6
Fragebogen s. Vordruckgestaltung
Frauenhäuser s. Sozialdatenschutz
Freigabe s. Ordnungsmäßigkeit der Datenverarbeitung
Fremdarbeiterkartei s. Forschung
Fremdenverkehr II/16; III/24; V/19; VI/10
Führerscheindaten II/18; IX/35; X/40; XI/28
Funkverkehr VI/31; IX/23

G

Geburtsdaten
– postalisches Anschriftenfeld I/11
– Veröffentlichung von Jubiläen s. Jubiläumsdaten
– Wählerverzeichnisse II/10; III/12; VI/24; VII/7
– Wahlbenachrichtigungskarten V/22; VI/23; VII/7
Gesundheitsbogen in Schulen s. Schüler-, Eltern- und Studentendaten
Gesundheitsreform XI/42
Gewerbeanmeldung/erlaubnis
– Auskünfte aus dem Gewerberegister II/16; VII/36
– Auskünfte über Reisegewerbetreibende an Berufsgenossenschaften VII/37
– Heranziehung von Ermittlungsakten der Staatsanwaltschaft X/38
– Verwendung der Daten aus Gewerbeanmeldungen VII/37
Grundbuch
– Datenumfang bei Grundbuchabschriften II/14; VII/31
– Einsicht in das Eigentümerverzeichnis VI/39; VII/31
– Nachweis des berechtigten Interesses bei Einsicht II/14; V/44; VIII/43
– Protokollierungspflicht bei Auskünften XI/32
Grundrecht auf Datenschutz III/45; VIII/8
Grundstückseigentümerdaten
– Datenumfang bei Auszügen aus dem Katasterbuchwerk III/25
– Einsicht in die Liegenschaftsbücher III/24
– Kaufpreissammlung V/31
– Listen der Grundstückskäufer IV/25; XI/31
– Nutzung für den Denkmalschutz s. Denkmalschutz
Grundstücksinteressenten
– Bewerberkarteien IV/24
– öffentliche Grundstücksvergabe IV/25

H

Handelsregisterauskünfte XI/33
Hinweise zur Durchführung des Landesdatenschutzgesetzes I/16
Heimatforschung s. Forschung

I/J

Internationaler Datenschutz I/20; II/31; IV/51
Innerbehördliche Datenweitergabe VII/18
Jubiläumsdaten I/11; III/11; IV/10; VI/9
Jugendamtstätigkeit s. Sozialdatenschutz
Justizverwaltung
– Austausch von Entscheidungen der Ehrengerichtshöfe in Anwaltssachen VII/31
– Datenschutz im Strafvollzug VII/32; VIII/44; IX/45, 46; X/36
– Datenübermittlung an die Polizei VII/30
– Grundbuchführung s. Grundbuch
– Mitteilungen in Zivil- und Strafsachen III/25; IV/26; V/33; VI/38; VII/29, 30; VIII/40, 41; IX/29
– Schuldnerverzeichnis II/13; III/25; IV/26; V/33; VIII/41; X/34, 52
– Tätigkeit der Staatsanwaltschaften s. Staatsanwaltschaften
– Veröffentlichung von Entmündigungsbeschlüssen IX/30

K

Kammern (berufsständische)
– Ausbildungsregister IX/34
– Datenerhebungen der – XI/38
– Datenübermittlungen der – II/26; III/37; VI/50; XI/38
– Einsichtsrecht in die Handwerksrolle III/37
– gesetzliche Grundlagen III/38
– Verwertung von Daten aus dem Schuldnerverzeichnis II/13; III/43; IV/26; X/52
Katasterbuchwerk s. Grundstückseigentümerdaten
Kaufpreissammlung s. Grundstückseigentümerdaten
Kinder
– Auflösung des melderechtlichen Familienverbundes nach Volljährigkeit II/9; V/11
– Speicherung von Daten in kriminalpolizeilichen Sammlungen IV/15
– Vernehmung durch die Polizei VIII/34
Kindergarten
– Umfang der Datenerhebung V/17
Kindergeld
– Berechnung bei Angehörigen des öffentlichen Dienstes s. Personaldaten
– Datenabgleich der Arbeitsverwaltung mit öffentlichen Stellen II/9; VII/16
Kirchen
– kirchliche Einrichtungen II/25; III/35; IV/36
– Kontrollrecht des Landesbeauftragen im Rahmen der Übermittlung von Meldedaten X/13
– Sonderstatus II/25
– Suchdienst IV/36
– Übermittlung von kirchlichen Daten an die Meldebehörden VI/12; VII/7, 14
– Übermittlung von Meldedaten II/9, 25
– Übermittlung von Patientendaten III/36; IV/35
– verfassungsrechtliche Autonomie III/36; IV/36
Kommunale Abgaben XI/16
Kommunale Erhebungen auf freiwilliger Basis VII/19; IX/16
Kommunale Vertretungskörperschaften
– Beratung der Fraktionen durch den Landesbeauftragten III/8
– Datenübermittlung zwischen Kommunalverwaltung und den – IV/12, 43; VI/22; VII/17; VIII/8, 18, 19; IX/16; XI/15
– öffentliche Erörterung von Verwaltungsdaten VI/23; VIII/8; XI/15
– Veröffentlichung von Stellenplänen VIII/15, 19
Kompetenzgrenzen des Landesbeauftragten II/15; III/7, 26, 29; V/34; VI/40; VII/10, 59; X/13
Kontrollmitteilungen s. Steuerverwaltung
Kraftfahrzeugzulassungsdaten
– Anfragen der Polizeibehörden II/18; III/28; IV/21, 30; VII/39; VIII/48, 63
– Auskünfte V/36; VII/7, 39; IX/36
– Novellierung des Straßenverkehrsgesetzes VII/38; VIII/48
– Übermittlung an das Kraftfahrt-Bundesamt III/27
– Umfang zu erhebender Daten V/16; VII/38; VIII/48
– Veräußerung von – I/10
– ZEVIS VII/38; VIII/48; IX/36; X/39; XI/59
Krebsregister s. Forschung

Kriminalpolizeiamt s. a. polizeiliche Informationssysteme und polizeiliche Tätigkeit
Kriminalpolizeiliche Sammlungen s. polizeiliche Informationssysteme
Kurgäste s. Fremdenverkehr

L

Landesarchivgesetz s. Archivwesen
Landesmeldegesetz III/8; IV/9; V/11, 14; VI/8, 16, 33; VII/10; VIII/11, 13
Legitimationsprüfung XI/19
– Verwaltungsvorschriften II/8; VIII/13; IX/10
Lehrerdaten III/23; VII/16; X/45
Leistungsverwaltung
– Aufbewahrung IX/10, 52, 53
– Nutzung freiwillig gegebener Daten IX/9, 51
– Umfang der Speicherung IX/9, 52, 53
Liegenschaftskataster s. Grundstückseigentümerdaten

M

Medien
– Bildschirmtext V/52; VI/65; VII/58
– Breitbandkabelnetze VI/66; VII/59
– datenschutzrechtliche Beurteilung III/47; IV/46; VI/64; VII/59
– Datenschutzkontrolle VI/66
– Datensicherungsmaßnahmen VI/64; VII/59
– Fernwirk- und Fernmeßdienste VI/68; VII/60
– Telekommunikation III/46; VII/58; IX/60; XI/66
Medizinische Daten s. a. Leistungsverwaltung
– Auskunft aus Krankenunterlagen V/40; VII/42; IX/38; XI/62
– automatisierte medizinische Informationssysteme II/19
– Daten für die Krankenkassen VI/44; VII/45
– Einwilligung zur Verarbeitung IV/33; V/30; VI/43; VII/41, 43, 53; VIII/50, 56; IX/37, 38, 39, 52; X/41; XI/47, 48, 61
– Erhebung bei den Beratungsstellen nach § 218 Strafgesetzbuch III/30
– Gesundheitsdienstgesetz I/15; IX/41
– Meldung der Unterbringung psychisch Kranker an die Führerscheinstelle VII/50; VIII/57; IX/40
– Mikroverfilmung VIII/54
– Offenbarung an Dritte VIII/40, 42; IX/38, 39, 54; X/41, 67; XI/44, 63
– Röntgenreihenuntersuchungen II/20
– Speicherung von "AIDS"-Daten X/26, 36; XI/46, 47, 59
– Tumornachsorgeverfahren X/43
– Übermittlungen an die Kirchen s. Kirche
– Übermittlung an die Krankenhausseelsorge III/36; IV/35
– Übermittlung an soziale Leistungsträger und andere Behörden IV/33; VII/6, 41, 42; IX/37, 38, 54; XI/20, 44, 48
– Übermittlung auf Überweisungsträgern VIII/45
– Umfang der Übermittlung an Dritte bei Einwilligung VII/42, 44; VIII/51
– Untersuchung von Schülern s. Schüler-, Eltern- und Studentendaten
– Verarbeitung in Krankenhäusern V/50; VII/41, 49; VIII/54; IX/37; X/47; XI/60
– Vernichtung von – XI/45
– Verwaltung von Krankenakten VII/48; VIII/52, 53; IX/38, 52
– Verwertung zu Forschungszwecken s. Forschung

Meldedaten
– Abgleich mit Kindergelddaten s. Kindergeld
– Adressenziehen für Forschungsvorhaben s. Forschung
– Adreßbücher I/14; II/8; IV/11; V/14; VII/10
– Anfragen von Auskunfteien, Versandhäusern und Inkassobüros III/43; IX/10
– Auskünfte aus dem Melderegister I/14; II/7; III/9, 41; IV/10; VII/11; VIII/60; IX/10; XI/12, 56
– Daten der Kinder s. Kinder
– Datensatz IV/9; VI/11; VII/10, 11; VIII/11
– Gruppenauskünfte III/10, 11; VIII/13
– kirchliche Daten s. Kirchen
– regelmäßige Datenübermittlungen VIII/11; IX/10
– Sperrung von Altdaten V/15; VI/14; VII/7
– Übermittlung an Bürgermeister und -vorsteher II/9; III/11; IX/11
– Übermittlung an Parteien VI/13; VII/12
– Übermittlung an Wehrersatzbehörden II/8; III/9
– Wahrung des Adoptionsgeheimnisses s. Adoptionsdaten
– Zugriff der Polizei I/15; III/9; V/12; VI/59; VIII/12, 14
– Zusammenarbeit mit der Presse s. Presse
Melderechtsrahmengesetz II/8; III/8; V/11; VI/17; VII/10
Meldescheinverordnung VIII/6, 12

Meldescheine
– Aufbewahrung in Beherbergungsstätten und bei privaten Vermietern VI/10; VII/10; VIII/12; IX/11
– Grenzen des Familienverbundes s. Kinder
– Weitergabe an ehrenamtliche Bürgermeister II/9
Mieterdaten
– gerichtliche Verwertung II/15; IV/23
– Übermittlung an Sozialbehörden VI/38
Mietwagen
– Personalien der Fahrgäste VII/40
Mitteilungen in Straf- und Zivilsachen s. Justizverwaltung

N

Nachrichtendienstliche Informationssysteme s. Sicherheitsbehörden
Normenklarheit X/20
Novellierung des Datenschutzrechts
– bereichsspezifische Lösungen III/44; V/34; VII/62
– Bundesdatenschutzgesetz III/44; VI/69; X/60; XI/71
– Dateibegriff IV/48; VII/61; VIII/67; IX/64
– Dateienregister X/55
– Datenverarbeitung der Steuerverwaltung s. Steuerverwaltung
– Erfahrungen mit dem Landesdatenschutzgesetz IV/48; X/5; XI/7
– Rechtstellung des Landesbeauftragten XI/7
– technischer Wandel VII/61; VIII/67
– Vorschläge des Landesbeauftragten X/72; XI/73
– Wissenschaftsklausel VI/46; VIII/67; IX/49
– Zeitpunkt II/4, 30; IV/47; VI/69; IX/64
– Zielrichtung VII/61; VIII/66; IX/64

O

Online-Anschlüsse IV/21, 30, 50; VI/9; VII/38
Ordnungsmäßigkeit der Datenverarbeitung s. a. Auftragsdatenverarbeitung, Datensicherungsmaßnahmen und Verwaltungsanweisungen
- Allgemeines V/50; VI/60; VII/54, 55; VIII/61; IX/55, 56
- Aufträge zur Erstellung von Software IV/38
- Einsatz von Personal-Computern X/55
- Forderungen an neue EDV-Verfahren VII/16, 55
- Fremdsoftware IV/39; X/57
- Test und Freigabe von EDV-Verfahren s. a. Automationskommissionen IV/37; V/50; VI/63; VII/56; VIII/62, 64; IX/57, 58; X/51, 58

Ordnungswidrigkeiten
- Anhörungsbogen II/17; III/18; IX/35

P

Parlament
- parlamentarische Behandlung der Tätigkeitsberichte s. Tätigkeitsberichte
- Stellung des Landesbeauftragten III/7; XI/7
- Unterrichtung/Beratung V/48; VIII/6; XI/25

Patientendaten s. medizinische Daten
Personalausweis- und Paßrecht VI/5, 14, 17, 26; VII/14; VIII/40, 49; IX/19; XI/18, 19
Personalcomputer XI/52, 65, 67
Personaldaten
- Abgleich mit Studentendaten VIII/17
- Eignungstests XI/13
- Erhebung von Bewerber- und Mitarbeiterdaten IV/26, 41; VI/19, 20, 21; VII/16; VIII/18; IX/14, 15; X/15, 21; XI/13, 26
- Grenzen der Speicherung IV/25; VI/18; VIII/17; XI/14, 21, 55
- Sperrung IV/42
- Übermittlung IV/25; VI/19; XI/15
- Verarbeitung durch automatisierte Verfahren s. Personalinformationssysteme und Telefondatenerfassung
- Veröffentlichung IV/25; VIII/19
- Zweckbindung der Beihilfedaten VI/18; VII/7

Personalinformationssysteme
- Risiken automatisierter Verfahren VII/15; VIII/16
- Zugangskontrollsysteme IV/26
- Zulässigkeit IV/26; XI/14

Planfeststellungsverfahren XI/31
Polizeiliche Informationssysteme
- Amtspflichtverletzung durch unzulässige Speicherung X/25
- Auskünfte III/18; IV/16; X/67; XI/26
- daktyloskopische Sammlung III/16
- Datensicherung X/29
- erkennungsdienstliche Unterlagen IV/18; V/27; VIII/33; IX/21
- Grundsätze und Richtlinien II/12, 13; III/16, 17, 20; IV/15, 16, 18, 55; V/27; VI/30; VII/7, 21, 23, 26; VIII/27, 31; XI/25
- Kriminalakten IV/17; V/24; XI/56
- Kriminalpolizeiamt III/13
- Löschung von Daten VIII/32; IX/28; X/23
- Meldedienst „gewalttätiger Störer" V/24
- Neukonzeption INPOL III/16

– polizeiliche Erkenntnisdatei II/13; III/13; VI/29; VII/26; VIII/34; XI/24, 25
– Speicherung von „AIDS"-Hinweisen X/26; XI/28
– Speicherung von Daten über Kinder s. Kinder
– Speicherung von Suizidversuchen VI/29; VII/7, 25; VIII/29
– Speicherung von Volkszählungsgegnern X/27; XI/24
– Spurendokumentationssysteme IV/17; V/23; X/31
– Versetzerkartei VI/7, 28; VII/7, 24; VIII/31
– zentrale Sammlungen beim Bundeskriminalamt III/16, 20; IV/16, 17; V/24
Polizeiliche Tätigkeit
– beobachtende Fahndung II/11; III/15; VIII/27
– Edelmetallverkauf VIII/31
– Fehlen konkretisierter Rechtsgrundlagen II/11; IV/15; V/27; VI/17, 26; VII/6, 20; VIII/25; IX/21, 27
– Informationsgewinnung III/19; IV/20; VIII/26; IX/20, 27
– polizeiliche Auskünfte und deren Verwertung II/17; III/19, 21; V/26; VII/23; VIII/27; IX/28; X/21; XI/27, 28
– polizeiliche Befragung nach § 161 Strafprozeßordnung IV/20
– Rasterfahndung II/11; IV/15, 20; VII/22; VIII/27; IX/27
– Zugriffe auf Kraftfahrzeugregister s. Kraftfahrzeugzulassungsdaten
– Zugriffe auf Melderegister s. Meldedaten Presse
– Übermittlung von Jubiläumsdaten s. Jubiläumsdaten
– Übermittlung von Meldedaten IV/10
– Übermittlung aus Standesamtsregistern IV/12
– Veröffentlichung von Daten aus Ermittlungsverfahren durch die Polizei/Staatsanwaltschaft IV/19; IX/28; X/64, 67; XI/27
– Veröffentlichung von Daten durch die Kommunen VIII/14, 20
– Veröffentlichung von Sozialdaten VI/44
– Veröffentlichung von sonstigen personenbezogenen Daten XI/39
Prüfungsmaßnahmen des Landesbeauftragten
– AIDS-Beratungsstelle XI/59
– Barschel-Pfeiffer-Affäre X/63
– Klinikum der Christian-Albrechts-Universität V/7, 48; VI/60; X/46; XI/60
– kommunaler Bereich IV/37; XI/54
– Kompetenz bei der Steuerverwaltung s. Steuerverwaltung
– Konzeption I/19; IV/37, 45; V/44; VIII/60
– Kraftfahrzeugzulassungsstelle XI/59
– Kriminalpolizei II/12; III/13; XI/56
– Schuldnerverzeichnisdaten bei einer IHK X/52
– Sozialverwaltung IX/50
– Test, Freigabe und Anwendung von Computerprogrammen IX/50; X/51
– Verfassungsschutzbehörde V/45; VI/51
– Verpflichtung nach § 16 Landesdatenschutzgesetz VII/54
– Volkszählung 1987 X/46; XI/58

R

Rasterfahndungen der Polizeibehörden s. polizeiliche Tätigkeit
Religionsgesellschaften s. Kirchen
Röntgenreihenuntersuchungen s. medizinische Daten

S

Schleppnetzfahndung VIII/40
Schulärztliche Untersuchungen s. Schüler-, Eltern- und Studentendaten
Schüler-, Eltern- und Studentendaten
– Abfrage von Daten VII/52; IX/45; XI/43
– Datenaustausch zwischen den Schulen VII/51
– Datenweitergabe an Eltern II/22; III/34; VIII/60
– Datenweitergabe innerhalb der Schule X/53
– Forschung X/44
– Gutachten III/35; VI/48; VII/8
– Öffentliche Bekanntgabe III/32; V/43
– schulärztlicher Dienst II/21; III/35; V/42; VII/8, 47; VIII/59; IX/40
– Schulfragebogen II/22; III/34; V/42; XI/51
– Schulgesetz XI/52
– Statistik III/23, 33; X/45
– Studenten-Operations-Systeme III/33
– Verarbeitung von Daten zur Aufgabenerfüllung II/21; III/34; V/42; VI/48; VII/8, 51; VIII/58; XI/51, 52
Schuldnerverzeichnis s. Justizverwaltung
"Schwarze Listen"
– Steuerbereich V/35
– Verkehrssünder III/28
Schweigepflicht X/45; XI/44
Sicherheitsbehörden (für den Polizeibereich s. polizeiliche Tätigkeit)
– Anfragen aus anderen Ländern VI/53
– Auskünfte über Datenspeicherungen I/13; V/47; IX/61
– Auskünfte an private Stellen VI/57; VIII/22
– Datensicherungsmaßnahmen VI/52
– Datenspeicherung und -weitergabe III/21; IV/22; V/45, 46; VI/51, 57; VIII/21, 24, 28; XI/22, 25
– Informationsgewinnung V/45; VIII/23, 29
– Löschung von Daten I/13; VIII/23; XI/22
– nachrichtendienstliche Informationssysteme III/21, 22
– Sicherheitsgesetze VIII/6, 21, 24, 28; IX/7; X/68
– Sicherheits- und Verfassungstreueüberprüfungen V/47; VI/53, 55; VII/8; VIII/21, 28; X/19; XI/21
– Transparenz bei der Datenverarbeitung II/11; IV/22; V/47
– Überwachung durch den Landesbeauftragten IV/22; V/45; VI/51; VIII/24; XI/23
– verdeckte Erkenntnisse VI/59; VIII/26
SISY X/ 32; XI/33
Software s. Ordnungsmäßigkeit der Datenverarbeitung
Sozialdatenschutz s. a. Leistungsverwaltung und medizinische Daten
– Auskünfte an Sicherheitsbehörden IV/23; V/38; IX/42, 43
– Auskunftsverpflichtung der Antragsteller IV/34, 42; VI/43; VII/46; XI/40, 43
– Befragung von Banken IX/54
– Datenspeicherung in privaten Frauenhäusern III/30
– Einwilligung zur Verarbeitung in Sozialleistungsverfahren IV/33; VI/43; VII/44, 46; VIII/57; IX/52
– Kostenübernahmeanträge XI/40
– Offenbarung gegenüber Versicherungen VIII/57; IX/44
– Sozialdatenschutzbeauftragter XI/41
– Sozialgesetzbuch III/29; IV/30; V/7, 37; VI/43
– Sozialversicherungsausweis XI/42

– Übermittlung der Daten von Flüchtlingen, Vertriebenen und Aussiedlern zum Zwecke der Betreuung III/31
– Übermittlung von Sozialdaten an Kreiswehrersatzämter VI/43
– Übermittlung an Verkehrsaufsichtsbehörden IX/43
– Veröffentlichung von Sozialdaten in der Presse s. Presse
– Warengutscheine V/39
– Weitergabe von Sozialdaten zu Forschungszwecken s. Forschung
Sozialhilfe s. Sozialdatenschutz
Staatsanwaltschaften
– Geschäftsstellenautomation IV/28; X/32
– Mitteilungen an das Bundeszentralregister VII/33
– Veröffentlichung von Daten aus Ermittlungsverfahren X/64,67
– zentrale Namensdatei IV/27; X/32; XI/33
Standesamtsdaten
– Bekanntgabe in der Presse s. Presse
– Berufsbezeichnung in Aufgebotsaushängen IV/10; VI/37
– Datenerhebungen aufgrund von Aufgebotsniederschriften IV/11
– Einwilligung zur Veröffentlichung IV/12
– Mitteilungspflichten der Standesbeamten VI/37; VIII/36; IX/24; XI/11, 20
Statistiken
– Agrarberichterstattung VI/37
– Arbeitskräftestichprobe VII/28
– Bereinigung V/32
– Datenweitergabe zu Statistikzwecken I/14; VII/28, 34
– Handels- und Gaststättenzählung VIII/37, 46
– Hochschulstatistik III/23; VII/28; VIII/38; XI/51
– Lehrerstatistik III/23; VII/16
– Mikrozensus V/32; VII/27; VIII/36
– Statistikgesetze III/23; V/32; VI/37; VII/28; VIII/39; IX/24
– Strafverfolgungsstatistik VII/33; VIII/44
– Volkszählung V/32; VI/5, 7, 33; VII/26; VIII/6; IX/24; X/11, 15, 27; XI/17, 58
– Wanderungsstatistik VII/28
Statistisches Landesamt
– Funktion als Auftragnehmer und speichernde Stelle III/22
Steuerverwaltung
– Auskünfte an den Betroffenen II/15; III/26
– Datenabgleich mit kommunalen Steuerbehörden II/16
– Datenaustausch zur Kindergeldberechnung s. Kindergeld
– Datenbank XI/37
– Datenerhebungen und -übermittlungen III/26; VI/41, 42; VII/35; VIII/46; X/38; XI/
– Kontrollmitteilungen von öffentlichen Stellen an Finanzämter IV/29; V/35; VI/41; IX/33; X/37; XI/37
– Kontrollrecht des Landesbeauftragten II/15; III/26; IV/29, 49; V/34; VI/40; VII/34; XI/35
– Novellierung des Bundesdatenschutzgesetzes IV/49
– Steuergeheimnis X/65
– Veröffentlichung von Dateien II/15; V/34
Strafgefangene s. Justizverwaltung
Strafprozeßordnung VIII/25, 39, 50; IX/26
Studentendaten s. Schüler-, Eltern- und Studentendaten
Suchdienst s. polizeiliche Informationssysteme
Suizidversuch s. polizeiliche Informationssysteme

T

Tätigkeitsberichte des Landesbeauftragten
– parlamentarische Behandlung III/6; IV/7; V/7; VI/6; VII/6; VIII/7; IX/8; X/9; XI/9
– Sonderbericht nach § 19 Abs. 3 S. 1 LDSG X/64
Technischer Wandel VII/55, 62; VIII/67; XI/10
Telefondatenerfassung IX/12; X/13, 66; XI/12, 55
Telefonische Auskünfte s. Datensicherungsmaßnahmen
Telekommunikation XI/66
Trennungsgebot zwischen Polizei und Verfassungsschutz X/29
Tumorregister s. Forschung

U

Übersicht über gespeicherte Daten III/40; VII/54
Urteile XI/12, 14, 31, 37, 45

V

Verantwortung
– Anbieter und Hersteller IV/46; V/50
– Auftraggeber I/19; IV/6; VI/60
– Datenzentrale für Programmentwicklung, -pflege und -sicherung VII/62; VIII/65
– Fachaufsichtsbehörde oder Fachamt IV/54; V/7; IX/56
– Freigabe von Programmen s. Ordnungsmäßigkeit der Datenverarbeitung
– Patientendaten in Krankenhäusern s. medizinische Daten
– speichernde Stelle V/8, 50; VII/54
Verfassungsschutzrecht s. Sicherheitsgesetze
Verkehrsordnungswidrigkeiten s. Ordnungswidrigkeiten
Verkehrszentralregister s. Kraftfahrzeugzulassungsdaten
Veröffentlichung von Urteilen XI/14
Verpflichtung auf das Datengeheimnis III/40; IV/32; V/8, 21; XI/55
Verschwiegenheitspflichten V/21, 49; VI/22; VII/31; VIII/10
Versetzerkartei s. polizeiliche Informationssysteme
Versicherungen
– Offenbarung von Sozialdaten s. Sozialdatenschutz
– Rentenversicherungsnummer IX/45
– Sozialversicherungswahlen IX/44
– Versicherungspflicht ehrenamtlicher Bürgermeister IX/18
Vertragsgestaltung
– Datenzentrale III/14, 40; IV/40; VII/57
– privatrechtliche Verträge zwischen Bürger und Staat IV/50
– schriftliche Fixierung der Datensicherheitsmaßnahmen II/29; IV/43; VI/63
– Verhältnis zwischen Auftragnehmern und Auftraggebern I/19; II/28; IV/40; V/50; IX/18
– Vertragsbedingungen für Verträge mit Software-Häusern IV/38; VI/61
– Verwaltung personenbezogener Daten bei Auflösung/Zusammenlegung von öffentlichen Stellen VII/49
Verwaltungsanweisungen
– bereichsspezifische II/18; IV/32; V/37; VII/18; VIII/6
– interne V/8; VI/52, 62; IX/57

Videoaufzeichnungen VIII/60; XI/50
Volkszählung s. Statistiken
Vordruckgestaltung
– Hinweis auf die Freiwilligkeit der Angaben II/24; III/24; IV/33, 42; V/16; VII/20, 47; IX/14, 16
– inhaltliche Bestimmtheit aufgrund klarer Rechtsnormen V/16; VI/19
– Umfang des Datenkataloges II/22; V/42; VI/45; VII/36, 45, 46; IX/53; X/41

W

Wahlen
– Datenübermittlungen an Parteien s. Meldedaten
– Unterstützungsunterschriften VI/24
– Verschwiegenheit der Wahlhelfer V/21
– Wahlbenachrichtigungskarten s. Geburtsdaten
Wählerverzeichnisse
– Auslegung II/10; III/12; IX/12
– Streichung der Geburtsdaten s. Geburtsdaten
Wissenschaft s. Forschung
Wohngeldverfahren s. Sozialdatenschutz

Z

Zeugnisverweigerungsrecht des Landesbeauftragten II/30; IV/49
Zeugenladung VIII/43; X/34
ZEVIS s. Kraftfahrzeugzulassungsdaten
Zugangskontrollsysteme s. Personalinformationssysteme
Zusammenarbeitsgesetz s. Sicherheitsgesetze
Zwangsversteigerung
– Namensnennung in der Terminsbestimmung VIII/42
Zweckentfremdung von Daten IV/49; V/12; VI/18; VII/39; XI/16