



Bericht

**des Landesbeauftragten für den Datenschutz
beim Innenminister des Landes Schleswig-Holstein**

Neunter Tätigkeitsbericht

In der Anlage übersende ich gemäß § 19 Abs. 3 Satz 2 des Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung vom 1. Juni 1978 den neunten Tätigkeitsbericht des Landesbeauftragten für den Datenschutz beim Innenminister des Landes Schleswig-Holstein.

Becker

Neunter Tätigkeitsbericht

des Landesbeauftragten für den Datenschutz
beim Innenminister
des Landes Schleswig-Holstein

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

(Berichtszeitraum: März 1986 – Februar 1987)

Inhaltsverzeichnis	Seite
1. Gesetzliche Absicherung des informationellen Selbstbestimmungsrechts – Datenschutzbeauftragte als Motor oder Bremser?	6
2. Parlamentarische Behandlung des 8. Tätigkeitsberichtes	8
3. Die Schnittstelle zwischen der Leistungs- und der Eingriffsverwaltung macht ein datenschutzrechtliches Grundsatzproblem deutlich	8
4. Sorgen der Bürger, Beratung der Behörden, Feststellungen und Wertungen	10
4.1 Allgemeine und innere Verwaltung	10
4.1.1 Meldewesen	10
4.1.1.1 Das Melderegister als Informationsquelle	10
4.1.1.2 Sind die Meldedaten bei meinem Vermieter in guter Obhut?	11
4.1.1.3 Trotz melderechtlicher Auskunftssperre Adreßdaten in öffentlich ausgelegten Wählerverzeichnissen	12
4.1.2 Personalwesen	12
4.1.2.1 Neue Rechtsprechung zur Telefondatenerfassung	12
4.1.2.2 Befragung von Bewerbern nach schwebenden Strafverfahren	14
4.1.2.3 Wozu braucht der Dienstherr die Urlaubsanschrift?	14
4.1.2.4 Datenerhebungen zur Berechnung des Kindergeldes	14
4.1.2.5 Was muß der Dienstherr über die Gesundheit seiner Mitarbeiter wissen?	15
4.1.3 Datenschutz im Kommunalbereich	16
4.1.3.1 Bewerberdaten im Spannungsfeld zwischen Öffentlichkeitsprinzip und Persönlichkeitsschutz	16
4.1.3.2 Muß der Bürger persönliche Daten für gemeindliche Planungsaufgaben preisgeben?	16

	Seite
4.1.3.3 Die Übernahme von Inkassoaufträgen durch Behörden ist unzulässig	17
4.1.3.4 Überprüfung der Versicherungspflicht ehrenamtlicher Bürgermeister durch die Ortskrankenkassen	18
4.1.3.5 Vernichtung von Unterlagen mit personenbezogenen Daten	18
4.1.4 Personalausweis- und Paßwesen	19
4.1.5 Öffentliche Sicherheit und Ordnung	20
4.1.5.1 Erkenntnisse durch Informanten, V-Leute und verdeckte Ermittler	20
4.1.5.2 Erkennungsdienstliche Unterlagen und „andere Lichtbilder“	21
4.1.5.3 Funkverkehr der Polizei – eine Achillesferse bei der Datensicherung	22
4.1.6 Personenstandswesen – sind die Standesämter Außenstellen der Finanzämter?	24
4.1.7 Statistik – die Vorbereitung zur Volkszählung 1987 läuft	24
4.2 Justizverwaltung	26
4.2.1 Forderungen zur Novellierung der Strafprozeßordnung	26
4.2.2 Justizmitteilungen – Stand der Gesetzgebung	29
4.2.3 Notariatskarteien und Dateienregister	29
4.2.4 Veröffentlichung von Entmündigungsbeschlüssen	30
4.2.5 Die Forschung will Einsicht in Gerichtsakten	30
4.2.6 Datenschutz im Strafvollzug	32
4.2.6.1 Der Landesbeauftragte als Ansprechpartner der Strafgefangenen	32
4.2.6.2 Wenn Gefangene Urlaub machen ...	32
4.3 Steuerverwaltung	33
4.3.1 Rechtsklarheit und Transparenz bei den Kontrollmitteilungen	33
4.3.2 Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung im Rechenzentrum der Steuerverwaltung	34
4.4 Wirtschaft und Verkehr	34
4.4.1 Schulnoten im Ausbildungsregister der Industrie- und Handelskammern	34
4.4.2 Datenschutzfragen im Zusammenhang mit dem Führerschein auf Probe	35
4.4.3 Neufassung des Anhörungsbogens bei Verkehrsordnungswidrigkeiten	35
4.4.4 Die Berufsangabe – ein „unsicheres“ Datum	35
4.4.5 Auskünfte des Kraftfahrt-Bundesamtes sind nur nutzbar, wenn sie aktuell sind	36

	Seite	
4.4.6	Dokumentation der Zugriffe auf das zentrale Verkehrsinformationssystem	36
4.5	Gesundheits- und Sozialdaten	36
4.5.1	Der Umgang mit Patientendaten und die ärztliche Schweigepflicht – es besteht ein erheblicher Regelungsbedarf	36
4.5.2	Schweigepflichtentbindungsklauseln sind weiterhin ein datenschutzrechtliches Sorgenkind	38
4.5.3	Abrechnung von Krankenhausleistungen in Rechenzentren	39
4.5.4	Unterrichtung der Führerscheinstellen über die Unterbringung psychisch Kranker	40
4.5.5	Datenschutz im schulärztlichen Dienst	40
4.5.6	Gesundheitsrechtliche Vorschriften können noch datenschutzgerechter gestaltet werden	41
4.5.7	Der Schutz des Sozialgeheimnisses	42
4.5.7.1	Offenbarung von Sozialdaten gegenüber den Sicherheitsbehörden	42
4.5.7.2	Offenbarung von Sozialdaten gegenüber der Kriminalpolizei	43
4.5.7.3	Offenbarung von Sozialdaten gegenüber den Verkehrsaufsichtsbehörden	43
4.5.7.4	Bekanntgabe von Mitarbeiterdaten einer gesetzlichen Krankenkasse an deren Vorstand	44
4.5.8	Datenschutz bei den Sozialversicherungswahlen	44
4.5.9	Rentenversicherungsnummer – Einstieg in das Personenkennzeichen?	45
4.6	Kultusbereich	45
4.6.1	„Datenschutzunfall“ als Unterrichtsgegenstand	45
4.6.2	Hochschulinterne im Altpapierbehälter	46
4.6.3	Denkmalschutz versus Datenschutz?	47
4.6.4	Datenschutz und Forschungsfreiheit – die Rechtsprechung hat Position bezogen	48
5.	Prüfungen	50
5.1	Umfang und Schwerpunkte der Prüfungsmaßnahmen	50
5.2	Prüfungen im Bereich der Jugend-, Sozial- und Gesundheitsämter	51
5.2.1	Allgemeines	51
5.2.2	Einzelne Feststellungen	53
5.3	Test, Freigabe und ordnungsgemäße Anwendung von Computerprogrammen	55

	Seite
6. Neue Informations- und Kommunikationstechniken	59
6.1 Beherrschbarkeit und Revisionsfähigkeit der Personalcomputer	59
6.2 Datenschutzrechtliche Beurteilung der Telekommunikationsordnung	60
7. Zur Verfassungsmäßigkeit des Rechts der Sicherheitsbehörden auf Auskunftsverweigerung	61
8. Einheitlichkeit des Datenschutzrechts in Gefahr?	64

1. Gesetzliche Absicherung des informationellen Selbstbestimmungsrechts - Datenschutzbeauftragte als Motor oder Bremsen?

Das informationelle Selbstbestimmungsrecht erfordert es, daß auch außerhalb des statistischen Bereiches Konsequenzen aus dem Volkszählungsurteil vom 15. Dezember 1983 gezogen werden. Das hat das Bundesverfassungsgericht deutlich gemacht. Im Melde- und Personalausweisrecht hat der Gesetzgeber bereits gehandelt. In den Bereichen „öffentliche Sicherheit und Ordnung“, „Strafverfahrensrecht“, „Justizmitteilungen“, „Arbeitnehmerdatenschutz“ und bezüglich des eigentlichen Datenschutzrechts sind Absichtserklärungen abgegeben, Vorüberlegungen angestellt und einzelne Gesetzentwürfe vorgelegt worden. In Hearings und in der Öffentlichkeit wurden die geplanten Regelungen ausführlich und kritisch diskutiert. Auch die Datenschutzbeauftragten haben sich geäußert und Verbesserungsvorschläge vorgebracht.

Diese Prozesse demokratischer Willensbildung kosten offenbar immer mehr Zeit. Die Datenschutzbeauftragten - gemäß ihrem gesetzlichen Auftrag zur Kontrolle der Rechtmäßigkeit und Erforderlichkeit der Datenverarbeitung verpflichtet - sehen sich deshalb mit der Frage konfrontiert, welche „Bedenkzeit“ angemessen ist, um verfassungsrechtlich problematische Verfahrensweisen der Verwaltung durch neue gesetzliche Regelungen zu beenden.

Das Bundesverfassungsgericht hat sich mit dieser Frage bereits in mehreren Entscheidungen befaßt. Danach können für eine gewisse Zeit gesetzliche Regelungslücken hingenommen werden, vor allem in den Fällen, in denen sich die Notwendigkeit spezieller Regelungen erst aufgrund neuer verfassungsrechtlicher Erkenntnisse ergeben hat. Es begründet die Zulässigkeit eines solchen „Status quo“ damit, daß „eine sonst eintretende Funktionsunfähigkeit staatlicher Einrichtungen der verfassungsgemäßen Ordnung noch ferner stünde als der bisherige Zustand“. Allgemeingültige Maßstäbe für die Dauer der dem Gesetzgeber eingeräumten Bedenkzeit hat das oberste Gericht nicht gesetzt. Es hat jedoch gewisse Kriterien genannt. So könnten z. B. die Eingriffstiefe der Verwaltungsmaßnahmen, die politischen Kontroversen, die außerordentliche Belastung des Gesetzgebers und die Regelungszusammenhänge mit anderen Materien von Bedeutung sein. Die Dauer einer Legislaturperiode wurde in einigen Fällen als angemessen angesehen.

Diese recht großzügige Betrachtungsweise des Bundesverfassungsgerichts hat den Datenschutzbeauftragten veranlaßt, trotz der zu Ende gehenden Legislaturperiode des Bundestages und der zu erwartenden legislativen Pause bis zu seiner Neukonstituierung noch nicht von schwerwiegenden Verzögerungen bei der Umsetzung des Volkszählungsurteils zu sprechen. Die vorliegenden Absichtserklärungen, Vorüberlegungen und konkreten Gesetzentwürfe sowie die damit in Zusammenhang stehenden Anhörverfahren verdeutlichen seiner Ansicht nach in hinreichendem Maße das Bemühen, die Übergangsfrist nicht zu sehr auszudehnen.

Allerdings dürfen die zutage tretenden Kontroversen gerade über die Regelungen im Sicherheits- und Strafverfolgungsbereich, aber auch im eigentlichen Datenschutzrecht, die Vielschichtigkeit der Problembereiche und deren Regelungszusammenhänge, nicht zu einer Blockade des vom Verfassungsgericht erteilten Auftrags führen. Außerdem empfiehlt er, durch Verwaltungsanweisungen die Befugnisse zu Eingriffen in verfassungsrechtlich geschützte Positionen auf das zu beschränken, was im konkreten Fall für die geordnete Weiterführung eines funktionsfähigen Verwaltungshandelns unerlässlich ist.

Der Landesbeauftragte ist stets von einer sorgfältigen Gesetzgebungsvorbereitung und vom allseitigen Willen, den Datenschutz zu verbessern, ausgegangen. In jüngster Zeit sind hier jedoch auch Zweifel entstanden. Betroffen ist er über Äußerungen zum Datenschutz, die in der Öffentlichkeit den Eindruck entstehen ließen, die Bekämpfung des Terrorismus werde durch die Arbeit der Datenschutzbeauftragten behindert.

Gemeinsam mit seinen Kollegen beim Bund und in den Ländern stellt er hierzu fest, daß sich die Datenschutzbeauftragten grundsätzlich nicht der Notwendigkeit verschließen, die Befugnisse der Sicherheitsbehörden und ihre Informationstechnik den Erfordernissen einer effektiven Verbrechensbekämpfung anzupassen. Sie sehen sich aber veranlaßt, darauf hinzuweisen, daß auch bei der Terrorismusbekämpfung die Anforderungen zu beachten sind, die das Bundesverfassungsgericht an den Schutz des Rechts auf informationelle Selbstbestimmung gestellt hat. Zu diesen Anforderungen gehören vor allem

- normenklare, für den Bürger verständliche Gesetze, deren Eingriffsmöglichkeiten im richtigen Verhältnis zum angestrebten Ziel stehen,
- Beachtung der Zweckbindungsgrundsätze,
- größtmöglicher Schutz Unbeteiligter,
- ausreichende Kontrollierbarkeit der Datenverarbeitung.

Die Aktivitäten der Datenschutzbeauftragten im Sicherheitsbereich unterstützen ihres Erachtens für jeden erkennbar das Bemühen, die Belange der Sicherheitsbehörden mit den verfassungsrechtlichen Grundsätzen in Einklang zu bringen. Die gegenwärtige Situation verlangt Lösungen, die die Bekämpfung des Terrorismus verbessern, ohne wesentliche Elemente des freiheitlichen Rechtsstaates in Frage zu stellen.

Solche konstruktiven Lösungsansätze zu fördern, zu erarbeiten und mitzutragen, hält der Landesbeauftragte für einen wesentlichen Teil seiner Tätigkeit. Er sieht sich nicht als Bremser, sondern als Motor für einen gerechten Ausgleich zwischen den Grundrechten der Sicherheit und Unversehrtheit des Lebens und der informationellen Selbstbestimmung.

2. Parlamentarische Behandlung des 8. Tätigkeitsberichtes

Der Schleswig-Holsteinische Landtag hat auch den 8. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz zeitlich so behandelt, daß die Beratungen im Jahr der Vorlage abgeschlossen werden konnten. Der Landesbeauftragte begrüßt die zeitnahe Beratung in den parlamentarischen Gremien, weil auf diese Weise eine unmittelbare parlamentarische Einflußnahme auf das datenschutzrechtliche Geschehen im Lande am ehesten gewährleistet wird.

Der Bericht ist nicht ohne Widerspruch geblieben. In der Plenardebatte wurde der Landesbeauftragte wegen des in Anspruch genommenen Rechts, zu Verwaltungsvorgängen auch außerhalb der Datenverarbeitung und zu Gesetzentwürfen des Bundes Stellung zu nehmen, wegen seiner geringen Bereitschaft zum Kompromiß und der Berichterstattung über Gesetzentwürfe, die sich noch in der (vertraulichen) Beratungsphase befanden, kritisiert.

Der Datenschutzbeauftragte nimmt die Kritik ernst. Sie gibt ihm Anlaß, seine Amtsführung immer wieder an den ihm durch das Gesetz auferlegten Grenzen unter Berücksichtigung der neuen verfassungsrechtlichen Situation zu messen. Er ist sich bewußt, daß er nur dann von der Verwaltung als Gesprächspartner akzeptiert wird, wenn er nicht nur kompetent argumentiert, sondern auch Kompetenzen einhält und in den gebotenen Fällen die nötige Zurückhaltung bei der Abfassung der Tätigkeitsberichte übt. Dabei hat er aber alles zu vermeiden, was Zweifel an seiner Unabhängigkeit und an seiner Glaubwürdigkeit weckt. Das gilt besonders für Grundpositionen des Datenschutzes. Sie eignen sich wenig für Kompromisse und müssen von ihm mit Nachdruck vertreten werden. Sich hier in „Sprachlosigkeit“ zu üben, wäre zum Nachteil des Datenschutzes! Nach Überzeugung des Landesbeauftragten bewegt er sich auch in seinem 9. Tätigkeitsbericht in diesen Grenzen.

3. Die Schnittstelle zwischen der Leistungs- und der Eingriffsverwaltung macht ein datenschutzrechtliches Grundproblem deutlich

„Was immer ich bei der Behandlung oder außerhalb der Behandlung im Leben der Menschen sehe und höre, werde ich als vertraulich betrachten und darüber schweigen“. Dies ist der Inhalt jener traditionellen Datenschutzvorschrift, die gemeinhin als „hippokratischer Eid“ bekannt ist. Sie soll dem Patienten gewährleisten, daß seine Offenbarungen gegenüber dem Arzt Dritten nicht bekannt werden. Es wird seit jeher als unerträglich empfunden, wenn das sehr subtile Verhältnis zwischen Patient und Arzt durch Indiskretionen gestört wird. Als so abhängig von der Verschwiegenheit des Arztes wird diese Beziehung angesehen, daß selbst der Staat ihr gegenüber seinen Anspruch auf Strafverfolgung eingeschränkt hat. Die Strafprozeßordnung billigt den Ärzten in Strafverfahren ein Zeugnisverweigerungsrecht zu und schließt ärztliche Unterlagen von einer Beschlagnahme und damit von einer Verwertung als Beweismittel aus.

Wie aber, wenn sich der Bürger einer staatlichen Stelle gegenüber offenbart, die ihm in vergleichbarer Weise Beratung, Hilfe und Unterstützung in Aussicht stellt? Auch hier können es körperliche oder psychische, aber auch wirtschaftliche Bedrängnisse sein, die den Menschen zu einer Offenbarung zwingen, die ihn veranlassen, seine Scheu abzulegen, um – wie er meint – im Schutze der Vertraulichkeit aus freiem Willen seine Not zu schildern und durch Beratung und Betreuung Hilfe zu erfahren. Es ist bitter für ihn, wenn er erst im nachhinein erfahren muß, daß in solchen Fällen sein Vertrauen weniger stark geschützt ist. Die nichtärztlichen Berater für Suchtkranke, die Mitarbeiter in der Familienberatung, die Sozialarbeiter usw. können nämlich nicht dafür einstehen, daß das, was ihnen der Betroffene aus seiner Situation heraus anvertraut hat, nicht in einer polizeilichen Vernehmung, in einem Strafverfahren, in einem Zwangsunterbringungsverfahren o. ä. gegen ihn verwendet wird.

Es mag berechtigt sein, solche Beratungen anders zu sehen als das Arzt-Patienten-Verhältnis. Sicher sind für die Staatsanwaltschaft und die Polizei z. B. im Kampf gegen die Rauschgiftkriminalität gerade auch Informationen über Süchtige erforderlich. Der Landesbeauftragte will auch nicht geltendes Recht in Frage stellen. Jedoch zwingt diese Rechtslage seines Erachtens zu vielfältigen Datenschutzüberlegungen:

- Der Berater sollte im Interesse seines Vertrauensverhältnisses zum Betroffenen den Umfang seiner Aufzeichnungen auf das für eine Beratung oder Entscheidung unbedingt erforderliche Maß beschränken. Je weniger Daten, etwa mit gesundheitlichem Bezug, über Kontaktpersonen eines Suchtkranken, über seine wirtschaftlichen, sozialen und psychischen Beziehungen, eine Datei enthält, um so geringer ist die Gefahr einer anderweitigen Nutzung.
- Der Betroffene kann in die Aufnahme seiner Angaben in eine Behandlungs- oder Beratungskartei wirksam nur einwilligen, wenn er vorher über deren Charakter und deren Nutzung informiert wird. Dazu muß ihm transparent gemacht werden, daß ihn keine ärztliche Schweigepflicht schützt und auch die allgemeine Amtsverschwiegenheit gesetzlich besonders geregelte Zugriffe auf die Aufzeichnungen nicht verhindert. Transparenz bedeutet, daß der Betroffene wissen muß, wer was wann und bei welcher Gelegenheit über ihn in Erfahrung bringen kann. Dazu gehört insbesondere die Kenntnis über die gesetzlichen Zugriffsmöglichkeiten auf seine freiwillig gemachten Angaben.
- Freiwillig bereitgestellte Informationen unterliegen im Gegensatz zu Daten, zu deren Preisgabe ein Gesetz verpflichtet, der freien Verfügung des Betroffenen. Ihm ist deshalb ein Lösungsanspruch zuzubilligen. Das gilt allerdings nur solange, wie er noch keine staatlichen Leistungen (z. B. in Form von Sozialhilfe) in Anspruch genommen hat. Die Antragsdaten dienen dann der Dokumentation des Verfahrens.

- Ein Bestand personenbezogener Daten, der auf freiwilliger Basis erhoben wurde, ist von solchen Datensammlungen zu trennen, deren Inhalt auf gesetzlichen Auskunfts- und Angabepflichten beruht. Es ist z. B. nicht zulässig, Informationen über meldepflichtige Krankheiten nach dem Bundesseuchengesetz in der gleichen Datei zu speichern und denselben Zugriffen zu unterwerfen wie die Erkenntnisse einer psychologischen oder Drogenberatungsstelle.

Die Nutzung personenbezogener Daten der Leistungsverwaltung für Zwecke der Eingriffsverwaltung hält der Landesbeauftragte nur in den gesetzlich ausdrücklich bestimmten Fällen für zulässig. Die Voraussetzungen dafür sind zuvor sorgfältig zu prüfen. Er wird diese wichtige datenschutzrechtliche Problemstellung bei seinen Kontrollen in besonderem Maße im Auge behalten.

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

4.1 Allgemeine und innere Verwaltung

4.1.1 Meldewesen

4.1.1.1 Das Melderegister als Informationsquelle

Da das Melderegister eine Fülle von Daten über jeden Bürger enthält, begehren die verschiedenen Institutionen und Stellen immer wieder Auskünfte daraus. Der Landesbeauftragte stößt häufig auf Unverständnis, wenn er unter Hinweis auf das Meldegeheimnis die Preisgabe der gewünschten Daten als unzulässig erachtet. Er begrüßt es daher, daß der Innenminister in seinen „Allgemeinen Verwaltungsvorschriften zum Landesmeldegesetz“ ausdrücklich darauf hingewiesen hat, daß dieses Register nicht als eine für jedermann zugängliche öffentliche Sammlung betrachtet werden darf. Die Meldedaten dienen grundsätzlich behördlichen Zwecken und dürfen neben der eigenen Verwertung durch die Meldebehörde selbst nur dann anderen Personen und Stellen bekanntgegeben werden, wenn eine Rechtsvorschrift dies ausdrücklich zuläßt (vgl. auch Tz. 4.6.4).

Folgende Beispiele verdeutlichen die Grenzen der durch das neue Melderecht zugelassenen Nutzung:

- Vielfach begehren Versandhäuser, Inkassobüros und ähnliche Stellen Informationen über Kunden, die im Zahlungsverzug sind. Dabei geht es um Daten, die über die einfache Melderegisterauskunft hinausgehen, so daß zu jedem einzelnen Datum von der anfragenden Stelle das berechtigte Interesse an der Auskunft konkret glaubhaft zu machen ist. Eine pauschale Erklärung, das berechtigte Interesse liege vor, reicht hierzu nicht aus. Zudem sind in jedem Falle die Auskunftsinteressen gegen die schutzwürdigen Belange der Betroffenen abzuwägen.
- Anhand der Anmeldungen zum Dateienregister hat der Landesbeauftragte festgestellt, daß noch nicht alle Meldebehörden ihre regelmäßigen Datenübermittlungen an die neuen Bestimmungen in der „Landesverordnung über re-

regelmäßige Datenübermittlungen" angepaßt haben. Das Interesse, regelmäßige Informationen über die persönlichen Verhältnisse der Einwohner zu erhalten, mag zwar verständlich sein. Den Meldebehörden ist es jedoch z. B. untersagt, privaten Altenklubs oder örtlichen Polizeistationen regelmäßig Mitteilungen über An- und Abmeldungen zu übersenden.

- Vielfach auf Unverständnis stießen die neuen melderechtlichen Vorschriften bei ehrenamtlichen Bürgermeistern amtsangehöriger Gemeinden, die sich nicht mehr ausreichend über die Bürger ihrer Gemeinde informiert sehen. Sie erhalten zwar Informationen über An- und Abmeldungen sowie Alters- und Ehejubiläen zur Erfüllung ihrer Repräsentationsaufgaben. Darüber hinausgehende Mitteilungen, wie z. B. detaillierte Einwohnerlisten, würden aber eine unzulässige doppelte Registrierung der Bürger bedeuten.
- In einigen Bundesländern wird offenbar ein Verfahren praktiziert, durch das die Gebühreneinzugszentrale der Rundfunkanstalten (GEZ) von den Meldebehörden regelmäßig Informationen über An- und Abmeldungen sowie über Sterbefälle erhält, um diese mit dem eigenen Bestand der Gebühreneinzugszentrale abzugleichen und dadurch nicht gemeldete Rundfunkbenutzer ermitteln zu können. Der Landesbeauftragte begrüßt es, daß die schleswig-holsteinischen melderechtlichen Vorschriften keine entsprechende Befugnis enthalten. Er hält dieses Verfahren für unverhältnismäßig, da die Gebühreneinzugszentrale damit keine säumigen Zahler erfassen kann, die ihre Anschrift nicht ändern, statt dessen aber in den Fällen nicht erforderliche Daten erhält, in denen die Bürger entweder nicht zahlungspflichtig sind oder sich keine Änderung der Zahlungspflicht ergibt.

4.1.1.2 Sind die Meldedaten bei meinem Vermieter in guter Obhut?

Der Landesbeauftragte hat in seinem 8. Tätigkeitsbericht (S. 15) auf die Risiken der künftigen Speicherung amtlicher Meldedaten bei privaten Vermietern und Beherbergungsstätten hingewiesen und gefordert, den Gemeinden in den Verwaltungsvorschriften eine ausdrückliche Pflicht zur Kontrolle aufzuerlegen.

In Anfragen und Beschwerden der Bürger dokumentiert sich nun tatsächlich ein Unbehagen, ob in diesem privaten Bereich die Meldedaten genauso sicher geschützt sind wie bei den Meldebehörden. Die Befürchtungen werden z. B. damit begründet, daß Vermietungsbüros, die Ferienwohnungen vermitteln, auf diesem Wege Daten über mehrere tausend Bürger jährlich erhalten und speichern. Es wird die Frage gestellt, ob diese umfangreichen Datensammlungen nicht z. B. für Werbezwecke mißbräuchlich verwendet werden. Der Innenminister geht allerdings nach wie vor davon aus, daß die privaten Vermieter die Vorschriften des Landesmeldegesetzes kennen und daß die allgemeine Verpflichtung der Meldebehörde, die Beachtung der gesetzlichen Vorschriften im Vermietergewerbe sicherzustellen, ausreicht, um einen angemessenen Schutz der Meldedaten zu gewährleisten.

4.1.1.3 **Trotz melderechtllicher Auskunftssperre Adreßdaten in öffentlich ausgelegten Wählerverzeichnissen**

Bereits früher hat der Landesbeauftragte in Frage gestellt, ob noch immer ein Bedürfnis zur öffentlichen Auslegung von Wählerverzeichnissen besteht. Insbesondere die Tatsache, daß darin auch die Daten derjenigen Bürger aufgeführt werden, für die im Melderegister zum Schutze ihres Lebens, ihrer Gesundheit, ihrer persönlichen Freiheit oder ähnlicher Belange eine Auskunftssperre vermerkt wurde, veranlaßte ihn dazu, dieses Problem erneut anzusprechen. Trotz verschiedener Initiativen, auch der anderen Datenschutzbeauftragten, vertreten der Bundes- und die Landesinnenminister die Auffassung, daß nur durch Beibehaltung der öffentlichen Auslegung eine demokratische Kontrolle der Wahlberechtigung erfolgen könne. Zudem würden die Verzeichnisse überwiegend nicht in alphabetischer Reihenfolge der Familiennamen, sondern nach Ortsteilen sortiert, was einen Mißbrauch schwieriger mache. Diese Argumente vermögen den Landesbeauftragten nicht zu überzeugen. Er regt deshalb an, statistische Erhebungen darüber anzustellen, in welchem Umfang die öffentliche Auslegung der Wählerlisten zur Überprüfung einer Wahlberechtigung geführt hat. Der Fortbestand dieses Verfahrens sollte wegen der damit verbundenen Risiken von seiner Effektivität abhängig gemacht werden.

4.1.2 **Personalwesen**

4.1.2.1 **Neue Rechtsprechung zur Telefondatenerfassung**

Zu dem Problem, ob personenbezogene Daten gespeichert werden dürfen, die bei der automatischen Vermittlung von Telefongesprächen über Dienstanschlüsse anfallen, sind in jüngster Zeit mehrere Entscheidungen der Arbeitsgerichte zu Betriebsvereinbarungen in der privaten Wirtschaft ergangen. Auch im Bereich der öffentlichen Verwaltung stellen sich im Zusammenhang mit der Erfassung, Speicherung und Auswertung der Nummer der Nebenstelle, des Zeitraums eines Telefongesprächs, der Dauer des Gesprächs, der Gebührenhöhe und der Nummer des Angerufenen für Dienst- und Privatgespräche folgende Fragen:

- Führt die Aufzeichnung der Daten zu einer unzulässigen Speicherung dienstlicher Verhaltens- oder Leistungsdaten des Mitarbeiters?
- Liegt eine unzulässige Speicherung von Informationen über das private Verhalten des Mitarbeiters vor?
- Ist die Aufzeichnung der Daten für Anschlüsse der Personalräte, des ärztlichen Dienstes, des Datenschutzbeauftragten usw. unzulässig, weil sie zu einer Kontrolle und Beeinträchtigung der Arbeit ihrer Inhaber führen können?
- Wird durch die Speicherung das informationelle Selbstbestimmungsrecht des Angerufenen beeinträchtigt?

Hierzu hat das Bundesarbeitsgericht in einem Beschluß (1 ABR 48/84 vom 27.05.1986) festgestellt:

- Die Kostenkontrolle und die Unterscheidung von dienstlichen und privaten Gesprächen rechtfertigen aus dem Arbeits- (und Dienst-) Verhältnis heraus die Speicherung von Nebenstellenummer sowie Zeitraum, Dauer und Kosten der Gespräche. Für die Dokumentation dienstlicher Aktivitäten ist auch die Aufzeichnung der Zielnummer erforderlich und zulässig. Das Interesse des Mitarbeiters an Vertraulichkeit von Verhaltensdaten hat bei dienstlichen Gesprächen demgegenüber ein geringeres Gewicht.
- Auch bei Privatgesprächen muß das Interesse des Mitarbeiters an Vertraulichkeit zurücktreten. Hier erfordert die aus der Kostenerstattungspflicht des Mitarbeiters notwendig werdende Kostenabrechnung solche Aufzeichnungen.
- Die Arbeit des Betriebsrats und vergleichbarer Einrichtungen ist nicht eingeschränkt, wenn ihm die Möglichkeit eröffnet wird, Gespräche ohne Aufzeichnung der Zielnummer zu führen. Andererseits wird eine Kostenerfassung auch für die Gespräche des Betriebsrats als legitim angesehen.
- Das informationelle Selbstbestimmungsrecht des Angerufenen wird von einer Aufzeichnung der Zielnummer zwar berührt, jedoch muß bei dienstlichen Gesprächen sein Recht gegenüber dem Dokumentationsinteresse des Gesprächspartners zurücktreten. Wer durch Anschluß an das Telefonnetz anderen die Gelegenheit gibt, mit ihm Fernsprechkontakt aufzunehmen, erklärt sich generell damit einverstanden, daß er angerufen wird. Er hat keinen Anspruch darauf, Aufzeichnungen seines Gesprächspartners - welcher Art auch immer sie sein mögen - zu verhindern.
- Anders kann die Rechtslage bei Privatgesprächen sein. Das Bundesarbeitsgericht brauchte diese Frage im konkreten Fall nicht abschließend zu entscheiden. Es gibt jedoch zu erkennen, daß es in Fällen privater Nutzung dienstlicher Telefonanschlüsse den Verzicht auf eine Speicherung der Zielnummer als datenschutzgerechte Lösung ansehen würde, denn für Zwecke des Dienstherrn sei die Aufzeichnung solcher Daten nicht erforderlich.

Der Landesbeauftragte hat in seiner Stellungnahme zu einem Entwurf von Fernmeldeanschlußrichtlinien des Innenministers auf der Grundlage des genannten Urteils vorgeschlagen, für Privatgespräche und für Gespräche des Personalrats im Interesse eines verstärkten Datenschutzes künftig die Zielnummer nicht mehr zu erfassen oder jedenfalls soweit abzukürzen, daß die angerufene Stelle für Unbeteiligte nicht mehr identifizierbar ist. Darüber hinaus wäre bei konkreten Regelungen für die geplanten neuen Kommunikationssysteme festzulegen, wie die Verbindungsdaten zu speichern sind. Ihre Speicherdauer wäre auf das für die anerkannten Zwecke (z. B. Kostenkontrolle, Kostenabrechnung) unabdingbar erforderliche Maß zu beschränken.

Die aus Gründen des Persönlichkeitsschutzes gebotene Transparenz (vgl. auch 6. TB, S. 17) müßte durch eine umfassende Information der betroffenen Mitarbeiter und des Personalrates gewährleistet werden.

4.1.2.2 **Befragung von Bewerbern nach schwebenden Strafverfahren**

In der datenschutzrechtlichen Diskussion um die Speicherung von Arbeitnehmerdaten stehen immer wieder die Angaben über strafrechtlich relevantes Verhalten im Vordergrund. Als problematisch erscheint es dem Landesbeauftragten z. B., daß Bewerber für den öffentlichen Dienst aufgefordert werden, Angaben über noch schwebende Verfahren zu machen. Da nicht ausgeschlossen werden kann, daß die Betroffenen später freigesprochen werden oder die Verurteilung nicht zu einer Auskunftspflicht aus dem Bundeszentralregister führt, dürften seines Erachtens derartige Angaben nur ausnahmsweise zu einer negativen Bewertung führen. Der Innenminister hat ihm hierzu erläutert, daß die Beantwortung dieser Frage jedem Bewerber freisteht. Entsprechende Hinweise enthält der hierzu in der Landesverwaltung verwendete Fragebogen allerdings nicht. Der Landesbeauftragte befürchtet, daß die Bewerber sich in der Praxis der Freiwilligkeit ihrer Angaben nicht bewußt sind. Er hat daher eine Umgestaltung dieses Vordruckes empfohlen. Die Frage nach schwebenden Verfahren sollte mit einem deutlichen Hinweis auf die Freiwilligkeit, jedoch auch auf die Konsequenzen (eventuelle Beendigung des Dienstverhältnisses nach einer Verurteilung) versehen werden.

4.1.2.3 **Wozu braucht der Dienstherr die Urlaubsanschrift?**

In den Urlaubsanträgen für die Landesverwaltung wurden die Mitarbeiter aufgefordert, dem Dienstherrn ihre Urlaubsanschrift mitzuteilen. Das wurde damit begründet, daß die Dienststellen in der Lage sein müßten, Mitarbeiter im Urlaub zu erreichen und eventuell zur Wiederaufnahme der Dienstgeschäfte aufzufordern. Da nicht von vornherein abzuschätzen sei, ob ein Rückruf erforderlich werde, müßten die Angaben in jedem Fall verlangt werden.

Der Landesbeauftragte vertritt die Auffassung, daß in Einzelfällen z. B. für Verschlussachen-Verpflichtete die dienstliche Notwendigkeit zur Angabe der Urlaubsanschrift anerkannt werden kann. Die anderen Mitarbeiter sollten jedoch nur dann befragt werden, wenn aufgrund ihrer Aufgabenstellung überhaupt ein Rückruf in Betracht kommt. Im übrigen dürfte es ausreichen, wenn für eine Kontaktadresse oder einen Nachsendeauftrag gesorgt wird. Konkrete Angaben über das jeweilige Urlaubsziel scheinen entbehrlich. Der Innenminister hat diesen Vorschlag aufgegriffen und eine entsprechende Handhabung in der Landesverwaltung empfohlen.

4.1.2.4 **Datenerhebungen zur Berechnung des Kindergeldes**

Ein Mitarbeiter der Landesverwaltung beklagte sich darüber, daß das Landesbesoldungsamt telefonisch bei der Ausbildungsfirma seiner Tochter die Höhe der gezahlten Ausbildungsvergütung erfragte, ohne ihn vorab darüber zu unterrichten. Die Nachforschungen des Landesbeauftragten ergaben, daß die Angaben zur Berechnung des beantragten Kindergeldes und kindergeldbezogenen Ortszuschlages verwendet wurden und der Petent auf dem Antragsvordruck eine aller-

dings leicht zu überlesende Einverständniserklärung unterschrieben hatte. Damit hatte die Behörde formal gesehen richtig gehandelt.

Der Landesbeauftragte hat das Landesbesoldungsamt aber darauf hingewiesen, daß derartige Einverständniserklärungen nur dann Wirkung entfalten, wenn sie den darin bezeichneten privaten Arbeitgebern auch vorgelegt werden. Diese haben selbst zu überprüfen, ob und in welchem Umfang sie bei ihnen gespeicherte Arbeitnehmerdaten, für die sie allein die datenschutzrechtliche Verantwortung tragen, preisgeben dürfen. Telefonische Anfragen brauchen aufgrund der Bestimmungen des Bundesdatenschutzgesetzes nicht beantwortet zu werden. Der Arbeitgeber der Tochter des Petenten hätte dem Landesbesoldungsamt also keine Auskünfte erteilen dürfen.

Das Landesbesoldungsamt hat diesen Fall zum Anlaß genommen, künftig von Anfragen bei den Ausbildungsstellen abzusehen. Statt dessen wird es grundsätzlich die Antragsteller auffordern, spezifizierte Bescheinigungen der Arbeitgeber ihrer Kinder selbst beizubringen.

4.1.2.5 Was muß der Dienstherr über die Gesundheit seiner Mitarbeiter wissen?

Von Beamten und anderen Mitarbeitern im öffentlichen Dienst wird verlangt, bei der Einstellung, der Lebenszeitanstellung, der Ausübung besonderer Tätigkeiten usw. ein Gesundheitszeugnis beizubringen und damit nachzuweisen, daß sie nach medizinischer Einschätzung ihre berufliche Tätigkeit dauernd ausüben können.

Auch das Fragerecht des Dienstherrn zur körperlichen Leistungsfähigkeit des Mitarbeiters unterliegt den sich aus dem allgemeinen Persönlichkeitsrecht ergebenden Grenzen. Der Dienstherr kann deshalb den Mitarbeiter nur mit dessen Zustimmung untersuchen lassen. Der Arzt darf nur solche Fragen stellen und Merkmale erheben, die zur Beurteilung der medizinischen Eignung für die künftige Arbeit von Bedeutung sind. Wichtig ist außerdem, daß die Einwilligung des Betroffenen zur Untersuchung den Arzt nur insoweit von der Schweigepflicht entbindet, als er sich zu der medizinischen Eignung für den künftigen Arbeitsplatz äußert. Die Entbindung gilt also nicht für die vom Arzt erhobenen Einzelbefunde. Er ist auch nicht berechtigt, dem Dienstherrn Diagnosen mitzuteilen.

Dem Landesbeauftragten ist bekannt, daß die Gesundheitszeugnisse der Ärzte in der Praxis sehr unterschiedlich aussehen. Einige enthalten bis ins Detail gehende Angaben über den Gesundheitszustand des Untersuchten. Nach seiner Auffassung benötigt die jeweilige Personalstelle im Regelfall lediglich das Ergebnis der Untersuchung. Es würde also die Aussage „geeignet/nicht geeignet“ oder „dienstfähig/-unfähig“ genügen. Weitere medizinische Daten können nur in Ausnahmefällen benötigt werden, wenn für berufliche Tätigkeiten besondere körperliche Voraussetzungen erforderlich sind. Er hat dem Sozialminister seine Auffassung mitgeteilt. Dieser sieht sich jedoch nicht in der Lage, den Amtsärzten konkrete

Handlungsanweisungen zu geben, solange die personalverwaltenden Stellen sich nicht festgelegt haben, welche Daten tatsächlich erforderlich sind.

4.1.3 **Datenschutz im Kommunalbereich**

4.1.3.1 **Bewerberdaten im Spannungsfeld zwischen Öffentlichkeitsprinzip und Persönlichkeitsschutz**

In seinem 8. Tätigkeitsbericht (S. 8, S. 20) empfahl der Landesbeauftragte einen diskreteren Umgang mit Daten von Bewerbern für kommunale Ämter. Er begrüßt, daß seine Verfahrensvorschläge offenbar auf fruchtbaren Boden gefallen sind. Pressemitteilungen konnte er entnehmen, daß in einem Fall die Stadtverordneten anstelle einer schriftlichen Vorlage nur Einsicht in die Bewerbungsunterlagen der Bürgermeisterkandidaten erhielten und daß nur die in die engere Wahl genommenen Kandidaten über ihre persönlichen Verhältnisse detaillierter befragt wurden. In einem anderen Fall traf zunächst jeweils ein Magistrats-/Senatsmitglied für „seine“ Fraktion nach Einsichtnahme in die Bewerbungsunterlagen eine Vorauswahl. Für die danach erforderliche Weiterleitung der ausgewählten Bewerbungsunterlagen an die Fraktionen wurde die Zustimmung der Bewerber eingeholt.

Eine möglichst einheitliche Behandlung der Bewerbungsunterlagen im Lande würde nach Meinung des Landesbeauftragten dem Problem entgegenwirken, daß die Bewerber, die um vertrauliche Behandlung ihrer Unterlagen bitten, möglicherweise schlechtere Chancen haben.

4.1.3.2 **Muß der Bürger persönliche Daten für gemeindliche Planungsaufgaben preisgeben?**

Mit der Frage, inwieweit die Gemeinden für Planungsaufgaben personenbezogene Daten ihrer Bürger erheben, speichern und veröffentlichen dürfen, hat sich der Landesbeauftragte bereits in seinen früheren Tätigkeitsberichten befaßt (vgl. 7. TB, S. 19). Er hat dargelegt, daß aus dem allgemeinen Recht der Selbstverwaltung der Gemeinden noch keine Befugnis zur Heranziehung jedweder privater Daten der Bürger hergeleitet werden kann. Besteht keine konkrete Rechtsnorm, bleibt den Gemeinden lediglich die Möglichkeit, den Bürgern Zweck und Nutzen der geplanten Maßnahme darzulegen und sie um freiwillige Unterstützung zu bitten.

Dies war im Berichtszeitraum z. B. in folgenden Fällen zu fordern:

- Zur Überprüfung, inwieweit Bedarf für eine neue Straßenführung bestand, wurde von einer Stadt eine Umfrage durchgeführt. Die Bürger wurden aufgefordert, Aufzeichnungen über die an einem bestimmten Stichtag durchgeführten Fahrten unter genauer Angabe von Uhrzeit, Art des Verkehrsmittels und des Endzieles zu fertigen. Der Fragebogen wurde zwar nicht mit dem Namen der Betroffenen versehen. Aus den detaillierten Angaben ließ sich jedoch ein Personenbezug herstellen, so daß es sich zum Zeitpunkt

der Erhebung um personenbezogene Daten im Sinne der Datenschutzbestimmungen handelte. Der Fragebogen enthielt weder eine Rubrik, in der die Bürger ihre Einwilligung zur Speicherung erklären konnten, noch einen ausdrücklichen Hinweis auf die Freiwilligkeit der Angaben.

- Eine andere Gemeinde plante, aus bereits vorhandenen Unterlagen, wie Bauleitplänen und im Handel erhältlichen Luftbildaufnahmen, Plänen und Karten sowie aus eigenen Bildaufnahmen Informationen zusammenzutragen und daraus ein Kataster über den Zustand des Gemeindegebietes einschließlich der sich im Privatbesitz befindlichen Grundstücke zu erstellen. Dieses Kataster sollte auch der Öffentlichkeit zugänglich gemacht werden. Es sollte zwar keine Namen enthalten, von Bürgern wurde aber die Befürchtung geäußert, daß bisher nicht bekannte grundstücksbewertende Daten verbreitet würden, aus denen Erkenntnisse über die Nutzbarkeit und Wirtschaftlichkeit von Flächen zu entnehmen wären.

Der Landesbeauftragte stellte fest, daß ein Umweltkataster, das ausschließlich Angaben enthält, die in der Öffentlichkeit ohnehin bekannt sind, nicht zu einer Beeinträchtigung der schutzwürdigen Belange der Bürger führen kann. Wenn allerdings Informationen aus öffentlichen Registern wie z. B. dem Grundbuch (für das ein Einsichtsrecht nur bei Vorliegen eines berechtigten Interesses besteht) einbezogen oder durch Verknüpfungen neue Informationen gewonnen werden, muß die Einwilligung der Betroffenen eingeholt werden.

4.1.3.3 Die Übernahme von Inkassoaufträgen durch Behörden ist unzulässig

Durch eine Beschwerde wurde der Landesbeauftragte auf eine offenbar weit verbreitete Praxis der Energieversorgungsunternehmen aufmerksam, gegen die er erhebliche datenschutzrechtliche Bedenken hat. Ein kommunaler Eigenbetrieb (Stadtwerke) war von einem privatrechtlich organisierten Energieversorgungsunternehmen gebeten worden, im Rahmen einer sogenannten Gegenseitigkeitshilfe einen säumigen Kunden, der zwischenzeitlich in den Bereich der betreffenden Stadtwerke verzogen war, zur Zahlung zu bewegen. Zumindest sollten dessen Einkommensverhältnisse sowie sein Arbeitgeber ermittelt und mitgeteilt werden. Diesem Verfahren liegt wohl die Annahme zugrunde, daß das jeweils örtlich zuständige Energieversorgungsunternehmen über die besseren Kenntnisse und die „wirksameren Möglichkeiten“ verfügt, um die ausstehenden Beträge „hereinzubekommen“.

Das Rechtsberatungsgesetz läßt die Besorgung fremder Rechtsgeschäfte in Form der außergerichtlichen Einziehung fremder Forderungen nur durch Inkassobüros, die hierzu eine ausdrückliche Erlaubnis erhalten haben, zu. Es gehört somit nicht zur Aufgabenerledigung einer öffentlichen Stelle, Forderungen privater Unternehmen einzuziehen. Demzufolge ist nach den Bestimmungen des Landesdatenschutzgesetzes die Speicherung und die Weitergabe von Informationen, die eine

öffentliche Stelle zur eigenen Aufgabenerfüllung nicht benötigt, sondern ausschließlich für Zwecke eines Privatunternehmens ermittelt hat, unzulässig.

4.1.3.4 **Überprüfung der Versicherungspflicht ehrenamtlicher Bürgermeister durch die Ortskrankenkassen**

Um zu prüfen, ob ihre Aufwandsentschädigungen der Sozialversicherungspflicht unterliegen, wurden Bürgermeister ehrenamtlich verwalteter Gemeinden von den Ortskrankenkassen aufgefordert, eine Vielzahl von Angaben zu ihrer Person, zu ihrem beruflichen Werdegang sowie zu ihrer Tätigkeit als Bürgermeister zu machen. Der hierzu verwendete Fragebogen war nach Auffassung der Betroffenen viel zu weitreichend. (Beispiele: „Hatten Sie es früher einmal aufgegeben, regelmäßig als Arbeitnehmer tätig zu sein?“, „Jährlicher und monatlicher Aufwand in Stunden für die gedankliche Sitzungsvorbereitung“.)

Der Landesbeauftragte hat im Zusammenwirken mit dem Schleswig-Holsteinischen Gemeindetag anstelle dieser Totalerhebung ein zweistufiges Verfahren vorgeschlagen, in dem zunächst geprüft werden sollte, ob eine Versicherungspflicht überhaupt in Betracht kommen könnte. Nur in vergleichsweise wenigen Fällen käme es dann zu einer weiteren Befragung der Betroffenen.

Die Ortskrankenkassen haben die Anregungen des Landesbeauftragten zum Anlaß genommen, ihr Verfahren neu zu gestalten.

4.1.3.5 **Vernichtung von Unterlagen mit personenbezogenen Daten**

Der Landesbeauftragte wird immer wieder um datenschutzrechtliche Beratung zu der Frage gebeten, welche Vorkehrungen bei der Vernichtung von vertraulichem, mit personenbezogenen Daten versehenem Altpapier getroffen werden sollten, um das Risiko einer rechtswidrigen Verwertung der Unterlagen auszuschalten (vgl. auch Tz. 4.6.2). Er hat hierzu die nachstehenden Empfehlungen gegeben:

- Zunächst sollten Datenbestände mindestens jährlich durchgesehen und entbehrliche Unterlagen ausgesondert werden, um sie rechtzeitig einer eventuell unzulässigen Verwertung zu entziehen.
- Die Unterlagen sollten bis zu ihrer Vernichtung möglichst gesondert und in verschlossenen Behältnissen aufbewahrt werden, damit auch während dieses Zeitraumes eine unbefugte Kenntnisnahme der Daten unterbleibt.
- Soll das Altpapier zum Zweck des Recyclings veräußert werden, so ist es so zu zerkleinern oder zusammenzupressen, daß daraus keine zusammenhängenden Sätze, Wörter oder Zahlenkolonnen mehr rekonstruiert werden können.
- Sofern Privatunternehmer mit der Entsorgung beauftragt werden, hat die Behörde sie sorgfältig auszuwählen und durch strenge vertragliche Vereinbarungen auf die Einhaltung des Datenschutzes zu verpflichten. Bei der Vertragsgestaltung sollte folgendes beachtet werden:

- Der in einem Praxistest durchgespielte Ablauf einer Entsorgung sollte exakt beschrieben und zum Vertragsinhalt gemacht werden.
- Die maximale Lagerungsdauer der Unterlagen beim Auftragnehmer sollte festgelegt werden.
- Die zusätzliche Einschaltung weiterer Subunternehmer sollte ausgeschlossen werden.
- Der Auftragnehmer ist zu verpflichten, Änderungen in der Art der Auftragsausführung, Störungen und Fehler im Betriebsablauf sowie Verlegungen der Betriebsstätte anzuzeigen.
- Für den Fall von Unregelmäßigkeiten sollte eine Vertragsstrafe vereinbart werden.
- Einer besonderen Geheimhaltung unterliegende Unterlagen wie Steuer- und Sozialdaten dürfen nur unter Aufsicht der speichernden Stelle vernichtet werden.

4.1.4 Personalausweis- und Paßwesen

Die Entscheidung für den neuen fälschungssicheren und maschinenlesbaren Ausweis ist gefallen. Das Gesetz über Personalausweise sieht die Einführung der neuen Ausweise bereits für April 1987 vor. Bis zu diesem Zeitpunkt gilt es, landesspezifische Regelungen zur Konkretisierung der Rahmenbestimmungen zu schaffen. Hierbei wurde der Landesbeauftragte beteiligt. Er hat auf eine Reihe datenschutzrechtlicher Verbesserungen hingewirkt:

- Bei der Feststellung der Identität eines Ausweisbewerbers sollen „verdeckte“ Befragungen Dritter nur in den Fällen erfolgen, in denen eine Überprüfung mit Wissen des Antragstellers nachweislich nicht zum Erfolg führen würde.
- Die erkennungsdienstlichen Unterlagen (z. B. Fingerabdrücke), die bei Zweifeln an der Identität eines Bürgers angefertigt werden, dürfen von der Polizei nicht in kriminalpolizeilichen Sammlungen gespeichert werden.
- Zum Inhalt des Ausweisregisters wird der Innenminister in einer Verwaltungsvorschrift klarstellen, daß ausschließlich die zum Zeitpunkt der Ausweiserstellung gültige Anschrift gespeichert werden darf. Eine Berichtigung findet beim Umzug des Ausweisinhabers nicht statt. Das bedeutet, daß die aktuelle Anschrift ausschließlich aus dem Melderegister entnommen werden kann.
- Um die Gültigkeit eines Ausweises zu überprüfen, wird nicht stets die Polizei eingeschaltet. Dies bleibt zunächst Aufgabe der Ausweisbehörden selbst. Nur bei Verdacht einer strafbaren Handlung bzw. einer mißbräuchlichen Benutzung kann die Kriminalpolizei beteiligt werden.
- Daten über ungültige oder abhanden gekommene Ausweise oder über den Verdacht einer Benutzung durch Nichtberechtigte werden nur dann an die Polizei weitergegeben, wenn dies für die Sachfahndung dienlich ist.

Die Sicherheitsbehörden sind im übrigen gesetzlich verpflichtet worden, ihre Übermittlungersuchen an die Ausweisbehörden aufzuzeichnen. Unbeschadet ihrer Pflicht zur Selbstkontrolle wird auch der Landesbeauftragte die Rechtmäßigkeit und Erforderlichkeit der Auskünfte stichprobenweise überprüfen.

4.1.5 **Öffentliche Sicherheit und Ordnung**

4.1.5.1 **Erkenntnisse durch Informanten, V-Leute und verdeckte Ermittler**

In zunehmendem Maße sehen sich Polizeibehörden veranlaßt, Dritte als Informanten in Anspruch zu nehmen, Vertrauenspersonen einzusetzen oder mit „verdeckten Ermittlern“ zu operieren. Den Einsatz derartiger Personen haben der Justizminister und der Innenminister in gemeinsamen Richtlinien im Februar 1986 neu geregelt. Aus ihnen wird deutlich, daß die besondere datenschutzrechtliche Problematik in der Zusage der Vertraulichkeit liegt.

Informanten und V-Personen können häufig nur dann zur Zusammenarbeit bewogen werden, wenn ihnen die Geheimhaltung ihrer Identität zugesichert wird. Verdeckte Ermittler sind besonders ausgewählte und ausgestattete Polizeivollzugsbeamte, die um Anhaltspunkte für Maßnahmen der Strafverfolgung zu gewinnen, unter einer Legende Kontakte zur kriminellen Szene aufnehmen und deren Identität auch im Strafverfahren geheimgehalten werden soll. Grundsätzlich entscheidet zwar die Staatsanwaltschaft über die Inanspruchnahme bzw. den Einsatz der betreffenden Personen. Deren Identität ist ihr aber nur in Ausnahmefällen, die Ermittlungsergebnisse sind ihr grundsätzlich nicht bekannt. Die Staatsanwaltschaften sind nach den Richtlinien lediglich gehalten, über die Gespräche mit der Polizei ohne Nennung des Namens der betreffenden Personen Vermerke zu den Generalakten zu fertigen. In den Ermittlungs- und Gerichtsakten finden sich mithin keinerlei Hinweise auf diese besonderen Methoden der Informationsgewinnung, weil durch die Akteneinsicht ihrer Verteidiger den Verdächtigten, Beschuldigten oder Angeklagten die „Datenquellen“ und die Informanten bekannt werden könnten.

Bereits im Zusammenhang mit den datenschutzrechtlichen Prüfungsmaßnahmen bei der Verfassungsschutzbehörde im Jahre 1982 (vgl. 6. TB, S. 59) hat der Landesbeauftragte darauf hingewiesen, daß die Speicherung der von dort übermittelten „verdeckten Erkenntnisse“ bei der Polizei ohne eine ausdrückliche gesetzliche Legitimation datenschutzrechtlich nicht unbedenklich ist.

Das gleiche Problem stellt sich seines Erachtens nunmehr hinsichtlich der Erkenntnisse, die durch Informanten, Vertrauenspersonen und verdeckte Ermittler beigebracht werden und die aus Gründen des Quellenschutzes weder dem Staatsanwalt noch dem Richter bekannt werden dürfen. Wenn derartige Daten gleichwohl in polizeilichen Informationssystemen gespeichert oder durch sie erschlossen werden können, entstehen Datenbestände, die einer unmittelbaren gericht-

lichen Kontrolle entzogen sind. Der Datenschutzbeauftragte hat zwar die Möglichkeit, diese Daten einzusehen und ihre Speicherungsrechtfertigung zu beurteilen, er kann aber weder dem Betroffenen noch dem Gericht über seine eventuellen datenschutzrechtlichen Bedenken berichten.

Dies dürfte seit dem Urteil des Bundesverfassungsgerichts zur Volkszählung zumindest bei Personen, die nicht rechtskräftig verurteilt werden (Einstellung des Verfahrens, Freispruch, Daten über „sonstige“ Personen), datenschutzrechtlich und strafprozessual problematisch sein. Die u. U. weitreichenden Konsequenzen für die Betroffenen können wohl kaum im Erlaßwege, sondern nur im Rahmen der Novellierung der Strafprozeßordnung rechtsstaatlich einwandfrei „aufgefangen“ werden. Der Landesbeauftragte hat seine Vorbehalte gegen die Richtlinien dem Justiz- und dem Innenminister dargelegt.

Der Justizminister hat daraufhin die Auffassung vertreten, daß die Richtlinien „auf der Grundlage des geltenden Strafprozeßrechts“ beschlossen seien. Die Bedenken des Datenschutzbeauftragten gegen den „Erlaßweg“ vermochte er nicht zu teilen. Ein Bedürfnis für eine deklaratorische gesetzliche Regelung in der Strafprozeßordnung könnte seines Erachtens aber für einzelne operative Maßnahmen verdeckter Ermittler gegeben sein. Die Überlegungen hierzu seien jedoch noch nicht abgeschlossen.

Auch der Innenminister sieht die derzeitige Regelung durch die Rechtsprechung des Bundesgerichtshofes gedeckt. Er bestätigte jedoch, daß die betreffenden Daten auch in Spurendokumentationssysteme, in zentral geführte Dateien des Bundeskriminalamtes und in kriminalpolizeiliche Sammlungen zur vorbeugenden Bekämpfung von Straftaten einfließen. Einer gerichtlichen Verwertung stünde gleichwohl die Zusage der Vertraulichkeit gegenüber. Dies sei in entsprechender Anwendung des § 54 Strafprozeßordnung gerechtfertigt. Nach dieser Bestimmung könne der Dienstherr einem Mitarbeiter des öffentlichen Dienstes die Genehmigung zur Aussage über Umstände, auf die sich ihre Pflicht zur Amtverschwiegenheit bezieht, versagen. Ferner könne die Vorlage oder Auslieferung von Akten oder anderen Schriftstücken, die sich im amtlichen Gewahrsam befinden, von der obersten Dienstbehörde verweigert werden.

Der Landesbeauftragte für den Datenschutz kann sich dieser Auffassung nicht anschließen, weil seines Erachtens ein so gravierender Eingriff in die Datenschutzrechte der Bürger einer ausdrücklichen gesetzlichen Regelung vorbehalten bleiben muß. Wegen der bundesweit einheitlichen Regelung hat der Landesbeauftragte darauf verzichtet, das Verfahren zu beanstanden, und wird statt dessen im Rahmen der Erörterungen zur Novellierung der Strafprozeßordnung auf entsprechende gesetzgeberische Schritte drängen (vgl. auch Tz. 4.2.1).

4.1.5.2 Erkennungsdienstliche Unterlagen und „andere Lichtbilder“

Bereits in früheren Tätigkeitsberichten hat sich der Landesbeauftragte aufgrund von Beschwerden der Bürger kritisch mit der Aufbewahrung und der Verwertung erkennungsdienst-

licher Unterlagen auseinandergesetzt (vgl. 4. TB, S. 18; 5. TB, S. 27; 8. TB, S. 33). Ein exemplarischer Fall hat auch in diesem Berichtszeitraum deutlich gemacht, daß im nachgeordneten Polizeibereich nach wie vor Regelungsdefizite bestehen.

Ein Petent schilderte, daß von ihm vor vielen Jahren erkennungsdienstliche Unterlagen angefertigt worden seien. Nachdem sich die damals zugrundeliegenden Beschuldigungen als unrichtig erwiesen hatten, seien die Unterlagen auf seinen Antrag hin gelöscht worden. Dies habe ihm der Innenminister bestätigt. Als er dann sechs Jahre später wegen angeblicher Fischwilderei in DDR-Gewässern vernommen worden sei, hätte sich in den Unterlagen ein Foto von ihm befunden. Es läge also der Verdacht nahe, daß sich seine erkennungsdienstlichen Fotos nach wie vor in den polizeilichen Informationssystemen befänden.

Die Untersuchungen des Landesbeauftragten ergaben zwar keine Anhaltspunkte dafür, daß die erkennungsdienstlichen Unterlagen auch nach der bestätigten Löschung noch weiter gespeichert worden waren. Es war allerdings auch nicht möglich, die Herkunft des in den Akten befindlichen Fotos und den Grund für seine Speicherung herauszufinden. Zunächst wurde dem Landesbeauftragten mitgeteilt, es handele sich um ein Foto, das der Datei der örtlichen Paßbehörde entnommen worden sei, um die Identität des Betroffenen zu ermitteln. Auf Vorhalt des Landesbeauftragten, daß die betreffende Behörde eine Herausgabe des Bildes nicht bestätigt und die Identität des Beschuldigten ja wohl bereits festgestanden habe, wurde eingeräumt, daß es sich nicht um das Paßfoto handele. Woher das Foto stamme, konnte nicht geklärt werden. Da es für polizeiliche Zwecke ganz offensichtlich nicht erforderlich war, wurde es zwischenzeitlich vernichtet.

Der Landesbeauftragte hat aufgrund dieses Vorganges dem Innenminister vorgeschlagen, die Polizeibehörden anzuweisen, nur solche Unterlagen in die kriminalpolizeilichen Sammlungen zu übernehmen, deren Herkunft eindeutig nachweisbar ist. In diesem Zusammenhang hat er auch darauf hingewiesen, daß Personenfotos, die zu Beweis Zwecken angefertigt werden, nicht als erkennungsdienstliches Material verwendet werden dürfen, ohne daß sie dann den strengen Regelungen der „Landesverordnung über erkennungsdienstliche Maßnahmen der Polizei“ unterworfen werden. Es ist nach seiner Auffassung stets zu berücksichtigen, daß über einen nicht vorbestraften Bürger mit festem Wohnsitz erkennungsdienstliche Unterlagen nur dann gespeichert werden dürfen, wenn „Tatsachen darauf schließen lassen, daß der Betreffende künftig gewohnheits- oder gewerbsmäßig mit Strafe bedrohte Handlungen begehen wird“. Liegen diese Voraussetzungen nicht vor, kann auch eine längerfristige Aufbewahrung sonstiger „Porträtfotos“ nicht gerechtfertigt werden.

4.1.5.3 Funkverkehr der Polizei - eine Achillesferse bei der Datensicherung

Einer der ersten „Datenschutzunfälle“, der in der Öffentlichkeit bekannt wurde, bestand darin, daß es (in einem anderen

Bundesland) jemandem gelungen war, durch Mithören des Polizeifunks die Abfragemodalitäten für das polizeiliche Informationssystem zu „studieren“. Auf diese Weise war es dem Betreffenden möglich, fingierte telefonische Anfragen zu starten und ungerechtfertigterweise Auskünfte aus den Datenbeständen der Polizei zu erhalten.

Bereits bei seiner datenschutzrechtlichen Überprüfung der polizeiliche Erkenntnisdatei (PED) im Jahre 1980 hat der Landesbeauftragte deshalb gefordert, daß in Anbetracht der sehr hohen Sensitivität der im Polizeibereich gespeicherten Daten die Polizei sich beim Einsatz von „Datensicherungstechnologien“ stets als Vorreiter ansehen sollte. Hierüber wurde in den Gesprächen mit dem Innenminister grundsätzliches Einverständnis erzielt.

Um so überraschender war es für den Landesbeauftragten, als ihm im Jahre 1986 ein Fall im Lande bekannt wurde, in dem ein Bürger mit geringem technischem Aufwand über längere Zeit den polizeilichen Funkverkehr abgehört hatte, was zwar gesetzlich verboten ist, technisch aber nicht verhindert wird. Die gewonnenen Erkenntnisse benutzte auch er, um „in die Identität eines Polizeibeamten zu schlüpfen“. Diese Manipulation konnte er unentdeckt über einen längeren Zeitraum aufrechterhalten, in dem er für Freunde und Bekannte, die wußten, daß sie polizeilich registriert waren, Auskünfte aus der PED einholte. In einem Gerichtsverfahren konnte er aber nur wegen Amtsanmaßung und Verstoß gegen das Fernmeldeanlagengesetz verurteilt werden. Die Strafvorschrift des Landesdatenschutzgesetzes lief ins Leere, weil natürlich keiner der Nutznießer seines Tuns einen Strafantrag stellte.

Der Landesbeauftragte hat daraufhin dem Innenminister empfohlen, kurzfristig das Verfahren zur Identitätsfeststellung der anfragenden Polizeibeamten zu verbessern. Seines Erachtens ist es dringend geboten, individuelle Code-Wörter zu verwenden, die Plausibilitätskontrollen zu verstärken, die Anfragen zu dokumentieren und sie stichprobenweise auf ihre Erforderlichkeit hin zu überprüfen. Da mit diesen Maßnahmen zwar eine wiederholte mißbräuchliche Nutzung der polizeilichen Daten, nicht aber eine Einmalaktion verhindert werden kann, hat er auch gefordert, daß das Mithören des Funkverkehrs durch entsprechende Verschlüsselungen z. B. mit Sprachverschlüsselungsgeräten unmöglich gemacht wird. Er hat darauf hingewiesen, daß es den Unbefugten nicht immer um die Ausforschung von Code-Wörtern gehen müsse, um dann selbst Auskünfte zu erschleichen. Der immer umfangreichere Datenstrom, der auf dem Funkwege zwischen den Polizisten vor Ort und den Zentralen ausgetauscht wird, ermöglicht bei einem systematischen Mithören nicht nur ein weitgehendes Ausforschen der polizeilichen Praktiken, er erbringt im besonderen Maße auch Erkenntnisse über persönliche Verhältnisse von Bürgern. Hierdurch können deren schutzwürdige Belange durchaus beeinträchtigt werden. Der Landesbeauftragte verzichtet wegen der Öffentlichkeit dieses Berichts auf eine detailliertere Beschreibung der Möglichkeiten und Gefahren.

Der Innenminister hat daraufhin angekündigt, daß ein neues zugriffssicheres Abfrageverfahren entwickelt werde. Die Neukonzeption ist dem Landesbeauftragten bisher noch nicht zur Kenntnis gegeben worden. Der Innenminister hat jedoch zugesichert, im Rahmen des technisch und haushaltsmäßig Machbaren nach Lösungsmöglichkeiten zu suchen.

4.1.6 **Personenstandswesen - sind die Standesämter Außenstellen der Finanzämter?**

Die Standesbeamten sind durch Dienstanweisungen verpflichtet, bei jedem Todesfall die Angehörigen nach dem Nachlaß und dem Nachlaßwert zu befragen. Diese Angaben haben sie in sogenannte Totenlisten einzutragen und an das für die Erbschaftssteuerberechnung zuständige Finanzamt weiterzuleiten.

Das Verfahren ist aus datenschutzrechtlicher Sicht bedenklich, weil die Betroffenen aufgefordert werden, den Standesbeamten gegenüber Daten preiszugeben, die diese für personenstandsrechtliche Zwecke nicht benötigen. Zudem werden die Todesfälle zumeist nicht von den Angehörigen selbst, sondern von Bestattungsunternehmen oder Krankenanstalten gemeldet, so daß die Daten auch diesen Institutionen bekannt werden. Die Finanzbehörden treten für eine Beibehaltung des Verfahrens ein. Ihrer Meinung nach liegt es sogar im Interesse der Angehörigen, wenn die Finanzämter anhand der Nachlaßangaben bereits vorab feststellen können, ob überhaupt eine Erbschaftssteuerpflicht besteht.

Der Landesbeauftragte schlägt eine Änderung des Verfahrens vor, die sowohl die Interessen der Betroffenen, der Standesämter als auch der Finanzbehörden abdeckt. Die Standesbeamten, die Bestattungsunternehmen und die Krankenanstalten sollten ein einheitliches, von der Steuerverwaltung herausgegebenes Formblatt vorrätig halten und bei jedem Todesfall den Angehörigen aushändigen. Diese hätten die Möglichkeit, die für die Erbschaftssteuerstelle nötigen Angaben einzutragen und direkt dorthin zu versenden. Durch ihre Unterschrift würden sie sogleich die Richtigkeit der Angaben bestätigen. Er hofft, daß sich die Bundes- und Länderfinanzminister auf dieses Verfahren verständigen können.

4.1.7 **Statistik - die Vorbereitung zur Volkszählung 1987 läuft**

Mit Stichtag 25.05.1987 wird erneut eine Volkszählung durchgeführt. Der Landesbeauftragte will an dieser Stelle auf die Fragen, ob eine Totalerhebung zu Planungszwecken sinnvoll ist, ob das vorgegebene Datenprofil erforderlich ist und ob sie die nötige Akzeptanz bei der Bevölkerung findet, nicht eingehen. Der Gesetzgeber hat eine bindende Entscheidung getroffen. Der Landesbeauftragte ist weder zur Kontrolle des Gesetzgebers befugt noch zur Anfechtung von Rechtsnormen legitimiert.

Das der Volkszählung zugrunde liegende Gesetz vom 08.11.1985 entspricht nach seiner Auffassung den vom Bundesverfassungsgericht formulierten Grundsätzen zur Wahrung des informationellen Selbstbestimmungsrechts der Bürger. Die

Zählung soll erneut als Totalerhebung mit Auskunftszwang durchgeführt werden, da nach der Überzeugung des Gesetzgebers noch keine abschließenden wissenschaftlichen Erkenntnisse über alternative Erhebungsmethoden vorliegen. Das auch von den Datenschutzbeauftragten als überprüfungsbedürftig erachtete, jedoch vom Bundesverfassungsgericht akzeptierte Datenprofil bleibt weitgehend unverändert. Zur Organisation der Befragungen sowie zur Nutzung der Daten hat der Gesetzgeber entsprechend den verfassungsgerichtlichen Forderungen dagegen umfassende Verbesserungen vorgenommen. Er ist dabei auch den Empfehlungen der Datenschutzbeauftragten des Bundes und der Länder gefolgt (vgl. 7. TB, S. 26). Von zentraler Bedeutung ist hierbei die gesetzliche Verpflichtung, die mit der Zählung beauftragten und eigens dafür eingerichteten Erhebungsstellen strikt abzuschotten und so zu verhindern, daß die aus der Erhebung gewonnenen Daten (Erhebungsmerkmale) zu Verwaltungszwecken unzulässigerweise genutzt werden.

Zur Umsetzung dieser Bestimmungen ist vom Innenminister eine Durchführungsverordnung sowie eine Verwaltungsvorschrift zur Durchführung der Volkszählung 1987 erlassen worden. Der Landesbeauftragte hatte Gelegenheit, seine datenschutzrechtlichen Forderungen in die Beratungen einfließen zu lassen. Seinem Wunsch, bereits in die Verordnung konkrete Regelungen zur Ausgestaltung der organisatorischen, räumlichen und personellen Trennung aufzunehmen und damit die Gemeinden stärker zu binden, wurde nur zum Teil entsprochen. Doch finden sich seine Anregungen in der detaillierten Verwaltungsvorschrift wieder. Beispielhaft sei auf folgende Punkte hingewiesen:

- Zur organisatorischen Trennung sind die Erhebungsstellen von anderen Verwaltungsbereichen unabhängig, mit einem eigens dazu bestellten Dienststellenleiter einzurichten. Ihre Mitarbeiter sind unmittelbar den Weisungen des Bürgermeisters bzw. Amtsvorstehers zu unterstellen.
- Für die Erhebungsstellen ist ein eigener Raum verfügbar zu halten, der, je nach örtlicher Gegebenheit, durch geeignete Maßnahmen vor unbefugtem Zutritt zu sichern ist. Daneben sind zur räumlichen Trennung weitere Vorkehrungen zu treffen, um eine unbefugte Einsichtnahme in die dort gelagerten Erhebungsunterlagen von vornherein auszuschließen.
- Die Mitarbeiter der Erhebungsstellen dürfen erst nach Abschluß ihrer dortigen Tätigkeit wieder mit Aufgaben des Verwaltungsvollzuges betraut werden, um auch personell eine Abschottung zu gewährleisten. Stunden- oder tagesweise Parallelbeschäftigung oder der Einsatz als „Springer“ oder „Pendler“ in Zeiten geringerer Arbeitsbelastung in der Erhebungsstelle ist nicht erlaubt. Zudem wird empfohlen, keine Mitarbeiter aus den Einwohnermelde- oder Sozialämtern einzusetzen, um auszuschließen, daß statistische Angaben für diese Verwaltungsbereiche mißbräuchlich verwendet werden.

Diese strengen Vorgaben sind für die Ämter und Gemeinden im Hinblick auf die Bereitstellung geeigneten Personals, auf

die Verfügbarkeit „abgeschotteter“ Räume und wegen der damit verbundenen Kosten nicht leicht zu erfüllen. Sie bilden jedoch die Voraussetzung für eine mit dem informationellen Selbstbestimmungsrecht der Bürger zu vereinbarende statistische Totalerhebung.

Auch der Einsatz der EDV zur Rücklaufkontrolle in den Erhebungsstellen wirft eine Reihe von Fragen auf. Sind es beim PC-Einsatz die Datensicherheit und die Zugangskontrolle, die Schwierigkeiten bereiten können, so entstehen bei Rechenzentren größerer Kommunen Probleme, die Abschottung sicherzustellen. Die Auftragsdatenverarbeitung in externen Rechenzentren setzt wiederum voraus, daß durch klare Vereinbarungen die Anonymität der Zählergebnisse sichergestellt ist und das Verbot der Zweckentfremdung und der Verbindung mit Vollzugsdaten beachtet wird.

Die Möglichkeit, ggf. auch Zwangsmittel einzusetzen, damit der einzelne Bürger der Auskunftspflicht nachkommt, ist wohl unvermeidlich. Bei diesem Verfahren dürfen aber keine „schwarzen Listen“, Verweigererverzeichnisse usw. entstehen.

In den letzten Wochen sind aufgrund wissenschaftlicher Untersuchungen erneut Zweifel an der ausreichenden Anonymisierbarkeit der Erhebungsdaten geäußert worden. Nach den Erkenntnissen des Landesbeauftragten gehen diese Untersuchungen allerdings davon aus, daß ein Zugang zu den Originaldaten besteht und dadurch sehr spezifische Bezüge zwischen den Merkmalsverteilungen hergestellt werden können. Diesen Zugang haben jedoch nur die Statistikbehörden. Anderweitige Nutzungen setzen strafbare Handlungen (Eindringen in Gebäude, Entwendung von Unterlagen, Verstoß gegen das Statistikgeheimnis usw.) voraus.

Nach Auffassung des Landesbeauftragten lassen Volkszählungsgesetz, Durchführungsverordnung und Verwaltungsvorschrift grundsätzlich eine datenschutzgerechte Durchführung der Volkszählung zu. Zur Umsetzung dieser Regelung in die Praxis hat er Hinweise, Anregungen und Denkanstöße gegeben. Die Gespräche werden fortgesetzt, er wird zu gegebener Zeit die Praxis auch durch Kontrollen „vor Ort“ prüfen.

4.2 Justizverwaltung

4.2.1 Forderungen zur Novellierung der Strafprozeßordnung

Bereits mehrfach hat der Landesbeauftragte in seinen Tätigkeitsberichten den Vorrang der Novellierung der Strafprozeßordnung vor einer Neuregelung des Polizeirechts der Länder hervorgehoben (vgl. 8. TB, S. 39). Inzwischen hat der Bundesminister der Justiz den Entwurf eines Gesetzes zur Regelung der rechtlichen Grundlagen für Fahndungsmaßnahmen, für Fahndungshilfsmittel und für die Akteneinsicht im Strafverfahren vorgelegt. Leider sollen darin wichtige Bereiche unregelt bleiben. So fehlen z. B. konkrete Normen für die Befugnis, bei Versammlungen Informationen aufzuzeichnen sowie V-Personen und verdeckte Ermittler einzusetzen, eine normenklare Regelung über die Nutzung von Informationssystemen zur Strafverfolgung, Fristen für die Sperrung und

Löschung von personenbezogenen Daten in Akten und Dateien sowie die Beschreibung der Auskunftsrechte von Beschuldigten, die sich keines Rechtsbeistandes bedienen.

Die Datenschutzbeauftragten des Bundes und der Länder sind der Auffassung, daß nur eine umfassende Gesamtlösung den Anforderungen der Rechtsprechung des Bundesverfassungsgerichts zum Umgang mit personenbezogenen Daten gerecht werden kann. Sie haben deshalb einen Katalog der Themenbereiche erarbeitet, die unter datenschutzrechtlichen Gesichtspunkten neu geregelt werden müßten. Der Landesbeauftragte hat dabei sein besonderes Augenmerk auf folgende Problemfelder, die bisher noch nicht im Vordergrund der Diskussion standen, gerichtet:

- Die Inanspruchnahme von Informanten sowie der Einsatz von V-Personen und verdeckten Ermittlern bedarf wegen der Gefahren für die Rechte des Beschuldigten einer normklaren gesetzlichen Regelung (vgl. auch Tz. 4.1.5.1). Es muß ein angemessener Ausgleich zwischen dem Recht des Informanten auf Vertraulichkeit und dem Recht des Betroffenen auf ein rechtsstaatliches Verfahren (Artikel 2 Abs. 1 i. V. m. Artikel 20 Abs. 3 Grundgesetz) gefunden werden. Diese Art der Informationsgewinnung sollte deshalb grundsätzlich nur im Bereich der Schwerekriminalität, der organisierten Kriminalität und der schweren Staatsschutzdelikte und nur dann zugelassen werden, wenn die Aufklärung der Straftat sonst aussichtslos wäre. Im Bereich der mittleren Kriminalität sollte der Einzelfall besonders gründlich geprüft werden.

Außerdem sollten im Gesetz die Grenzen des zulässigen Einsatzes festgelegt und klargestellt werden, daß alle gesammelten Informationen aufzuzeichnen und an die Staatsanwaltschaft weiterzugeben sind. Bei der Staatsanwaltschaft sollten die geheimzuhaltenden Informationen in gesonderten Akten aufbewahrt und das Gericht sowie die Verteidigung darauf hingewiesen werden.

- Das in der Strafprozeßordnung geregelte Akteneinsichtsrecht der Verteidigung sollte grundsätzlich auch dem Beschuldigten zugestanden werden, der sich keines Rechtsbeistandes bedient. Das ist eine wichtige Voraussetzung für eine wirksame Rechtsverteidigung im Strafverfahren.
- Der Landesbeauftragte hat schließlich Bedenken gegen die Einführung einer generalklauselartigen, allgemeinen Befugnisnorm für staatsanwaltschaftliche/polizeiliche Maßnahmen im Rahmen der Ermittlungsverfahren. Im Hinblick auf die Risiken einer extensiven Auslegung einer Generalklausel sollte in der Strafprozeßordnung am bisherigen Prinzip des gesetzlich abgesicherten Einzeleingriffs festgehalten und zusätzlich eine Regelung der bislang noch nicht erfaßten Bereiche angestrebt werden.

Außerdem haben die Datenschutzbeauftragten des Bundes und der Länder folgende Anregungen gegeben:

- Die Rasterfahndung bedarf einer gesetzlichen Grundlage. Sie sollte auf besonders schwere Straftaten beschränkt und

nur zugelassen werden, wenn die Annahme gerechtfertigt ist, daß der Datenabgleich zur Aufklärung der Straftat führt und die Aufklärung sonst aussichtslos oder wesentlich erschwert wäre. Außerdem ist eine Nutzungsbegrenzung für die gewonnenen Informationen vorzusehen.

- Die Informationserhebung im Rahmen der polizeilichen Beobachtung, der planmäßigen Observation und der Überwachung mit technischen Mitteln sollte in getrennten Vorschriften geregelt werden. Dabei wäre besonderes Gewicht auf die Beschreibung der jeweiligen Zulässigkeitsvoraussetzungen zu legen.
- Auch die Datenerhebung in Versammlungen ist wegen des Eingriffs in das Grundrecht der Versammlungsfreiheit gesetzlich zu regeln. Es dürften unterschiedliche Regelungen für Versammlungen in geschlossenen Räumen und für Veranstaltungen im Freien erforderlich sein.
- Die Verwendung von Abhörgeräten und die Aufnahme des in der Öffentlichkeit gesprochenen Wortes auf Tonträgern sollten nur zulässig sein, wenn dies zur Aufklärung einer in § 100 a Strafprozeßordnung bezeichneten Straftat geboten ist.
- Bezüglich der Auskunfts- und Akteneinsichtsrechte sind neben Regelungen für Behörden, für die Verteidigung, für den verteidigerlosen Beschuldigten, für Privat- und Nebenküßler, vor allem Bestimmungen über das Akteneinsichtsrecht wissenschaftlicher Einrichtungen, von Bedeutung. Nachdem die Rechtsprechung (vgl. Tz. 4.6.4) einen verfassungsunmittelbaren Anspruch der Wissenschaft auf Akteneinsicht verneint hat, sollten personenbezogene Daten nur unter engen Voraussetzungen herausgegeben werden können. Das gilt insbesondere für Daten aus eingestellten Verfahren, aus Verfahren, die mit einem Freispruch beendet wurden, und für Daten der Verfahrensbeteiligten, z. B. der Zeugen und der Opfer (vgl. auch Tz. 4.2.5).
- Für die Unterrichtung der Medien durch Polizei und Justiz vor einer öffentlichen Gerichtsverhandlung sollte eine bereichsspezifische Grundlage geschaffen werden. Um unnötige Bloßstellungen zu vermeiden, müßte festgelegt werden, daß Namen und sonstige Angaben (auch Abkürzungen), die die Opfer von Straftaten, die Beschuldigten und die Angeklagten bestimmbar machen, in Auskünften nicht aufgeführt werden.
- Schließlich sollten auch die Aufbewahrungs- und Löschungsbestimmungen neu geregelt werden. Die zur Zeit geltenden Aufbewahrungsbestimmungen bedürfen einer Überprüfung. Eine Differenzierung unter Berücksichtigung des Verfahrensausgangs, der Verfolgungsverjährung und der Schwere der Tat sollte angestrebt werden.

Der Landesbeauftragte hat diese Forderungen dem Justizminister mit der Bitte um Berücksichtigung im weiteren Gesetzgebungsverfahren übersandt.

4.2.2 Justizmitteilungen - Stand der Gesetzgebung

Nachdem die verwaltungsinternen Richtlinien über die Mitteilungen der Gerichte an andere Stellen in Straf- und Zivilsachen (MiStra und MiZi) von dem Datenschutzbeauftragten kritisiert worden sind (vgl. z. B. 8. TB, S. 40), liegt nunmehr der Entwurf eines „Justizmitteilungsgesetzes“ des Bundesjustizministers vor. Die Übermittlungsregelungen sind darin nicht bis in alle Einzelheiten präzisiert, um eine unerwünschte Gesetzesflut aufgrund der Fülle von denkbaren Mitteilungen zu vermeiden.

Der Landesbeauftragte begrüßt zwar, daß personenbezogene Daten durch die Gerichte und die Staatsanwaltschaften nunmehr nur noch übermittelt werden sollen, wenn zuvor die Notwendigkeit dafür im Einzelfall geprüft wurde. Er weist jedoch darauf hin, daß hier eine Präzisierung erfolgen muß, um der Forderung des Volkszählungsurteils nach Transparenz für den Betroffenen (Normenklarheit) gerecht zu werden.

Unter dem Gesichtspunkt der Verhältnismäßigkeit sollten Strafurteile regelmäßig auf die Urteilsformel beschränkt übermittelt werden. Außerdem dürften Mitteilungen vor Erhebung der öffentlichen Klage nur zulässig sein, wenn ein dringender Tatverdacht besteht und aufgrund der Sachlage Maßnahmen von erheblicher Bedeutung - etwa Ausspruch eines Tätigkeitsverbots - erforderlich sind.

Die im Gesetzentwurf vorgesehene Benachrichtigung des Betroffenen ist grundsätzlich positiv zu bewerten. Allerdings sollte der Betroffene vorab (nicht im nachhinein) unterrichtet werden, damit er ggf. Einwendungen erheben kann, bevor es zu spät ist, unzulässige Maßnahmen zu verhindern.

Der Landesbeauftragte hat den Justizminister gebeten, diese Punkte bei den weiteren Beratungen des Entwurfes zur Geltung zu bringen.

4.2.3 Notariatskarteien und Dateienregister

„Wegen der fehlenden Gesetzgebungszuständigkeit des Landesgesetzgebers kann das Landesdatenschutzgesetz für die Notare nicht gelten. Das Berufsrecht der Notare gewährleistet die den Landesdatenschutzgesetzen zugrundeliegenden gesetzgeberischen Zwecke und den verfassungsrechtlich gebotenen Schutz des informationellen Selbstbestimmungsrechts umfassend, so daß auch im Hinblick auf das Subsidiaritätsprinzip der Datenschutzgesetze kein sinnvoller Anwendungsbereich verbleibt.“ Mit diesen Worten haben die Notarkammern die Anwendbarkeit der Datenschutzgesetze im Notarbereich energisch bestritten.

Die Datenschutzbeauftragten des Bundes und der Länder sahen sich deshalb veranlaßt, in einem Beschluß die rechtliche Situation klarzustellen: Die Notare als Träger eines öffentlichen Amtes sind öffentliche Stellen und in vollem Umfang den Bestimmungen der Datenschutzgesetze unterworfen. Sie haben deshalb ihre automatisierten Dateien zum Dateienregister anzumelden und unterliegen der Kontrolle durch die Datenschutzbeauftragten.

Die Justizminister des Bundes und der Länder folgten der Rechtsansicht der Datenschutzbeauftragten. Die Erwartung, daß durch ein Gespräch des Bundesjustizministers mit der Bundesnotarkammer die bislang ablehnende Haltung der Notarkammern in den Ländern überwunden werden könnte, hat sich leider nicht erfüllt. Der Justizminister des Landes klärt deshalb zur Zeit, ob durch Einschaltung der Notaraufsichtsstellen auf eine Erfüllung der gesetzlichen Meldepflichten hingewirkt werden kann.

4.2.4 **Veröffentlichung von Entmündigungsbeschlüssen**

Die Amtsgerichte veröffentlichen in Entmündigungsbeschlüssen nicht nur den Namen und die Adresse des Entmündigten, sondern auch den Entmündigungsgrund, wenn es sich um Trunksucht oder Verschwendung handelt. Sie folgen damit einem Gesetzesbefehl in der Zivilprozeßordnung, der keine Ausnahmen zuläßt (§ 687). Beschwerden entmündigter Bürger, ihrer gesetzlichen Vertreter, aber auch eine kritische Diskussion im Schleswig-Holsteinischen Landtag bestärken den Landesbeauftragten in seiner schon früher geäußerten Überzeugung, daß die konsequente Anwendung des Gesetzes hier in unverhältnismäßiger Weise in die Persönlichkeitsrechte der Betroffenen eingreift. Es ist zwar nicht zu bestreiten, daß ein Kaufmann wissen muß, ob sein Vertragspartner geschäftsfähig ist. Die Entmündigungsgründe sind dagegen für ihn zwar eine interessante, zur Wahrung seiner Rechtsposition aber überflüssige Information. Nach Auffassung des Bundesverfassungsgerichts im Volkszählungsurteil muß der grundrechtlich verbürgte Persönlichkeitsschutz verhindern, daß Bürger in einer bestimmten Situation „sozial abgestempelt“ werden. Der Landesbeauftragte drängt deshalb auf eine Änderung der Vorschrift. In einer Stellungnahme gegenüber dem Bundesverfassungsgericht zu einem Vorlagebeschluß, in dem die Verfassungsmäßigkeit des § 687 Zivilprozeßordnung angezweifelt wird, hat der Landesbeauftragte insbesondere auf das Unbehagen und die Sorgen der Betroffenen hingewiesen, die eine schwere Beeinträchtigung schutzwürdiger Belange deutlich machen.

4.2.5 **Die Forschung will Einsicht in Gerichtsakten**

Personenbezogene Daten in Gerichtsakten unterliegen zwar nicht unmittelbar dem Schutz des Datenschutzgesetzes. Da in diesen Vorgängen jedoch häufig auch Informationen enthalten sind, die das Ergebnis einer dateimäßigen Aufbereitung darstellen oder einer besonderen Geheimhaltungsvorschrift (z. B. Sozial- oder Steuergeheimnis) unterliegen, mußte der Landesbeauftragte Bedenken gegen einen Zugriff zur wissenschaftlichen Verwertung erheben.

So wurden z. B. bei der Anfertigung einer Doktorarbeit zu dem Thema „Untersuchungshaft an Jugendlichen und Heranwachsenden“ Informationen auch durch Einsichtnahme in die in den Gerichtsakten enthaltenen Jugendgerichtshilfeberichte des örtlichen Jugendamtes gewonnen. Diese enthalten in der Regel sehr sensible Angaben, z. B. über den schulischen Werdegang, die Berufsausbildung, die Freizeitgestaltung, das

Einkommen, die Vorstrafen, den Alkohol- und Drogenkonsum sowie sehr differenzierte Persönlichkeitsdarstellungen und Prognosen. Jugendgerichtshilfeberichte unterliegen dem Sozialgeheimnis, das auch die Gerichte verpflichtet, genauso sorgsam mit den Daten umzugehen, wie die dem Sozialgeheimnis unmittelbar unterliegenden Stellen.

Vorbehaltlich noch zu klärender Detailfragen hat der Landesbeauftragte dem Justizminister seine Rechtsauffassung mitgeteilt:

Eine Herausgabe - vorausgesetzt, daß es tatsächlich nicht zumutbar ist, die Einwilligung der Betroffenen einzuholen - ist nur erlaubt, soweit dies für die wissenschaftliche Forschung im Sozialleistungsbereich erforderlich ist und schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden oder das öffentliche Interesse an der Forschung im Sozialleistungsbereich das Geheimhaltungsinteresse erheblich überwiegt. Mit anderen Worten, die Promotion muß als Forschungsbeitrag im Sozialleistungsbereich zu werten sein.

Der Landesbeauftragte hat nicht nur grundsätzliche Bedenken, ob die Anfertigung einer Doktorarbeit überhaupt unter den Forschungsbegriff des Sozialgesetzbuches fällt, in diesem speziellen Fall bestanden auch Zweifel, ob das Thema als ein Forschungsbeitrag im Sozialleistungsbereich zu werten war. Im übrigen hätte die Offenbarung von Sozialdaten zu Forschungszwecken in jedem Fall der vorherigen Genehmigung durch die zuständige oberste Landesbehörde bedurft. Er hat deshalb den Justizminister darauf hingewiesen, daß das Sozialgeheimnis auch über den eigentlichen Sozialbereich hinaus wirksam ist.

Zweifel mußte der Landesbeauftragte auch an der Rechtmäßigkeit der Einsichtnahme in Daten aus Familiengerichtsverfahren in einem Fall anmelden, der ihm durch eine Beschwerde des Verbandes der Scheidungsgeschädigten bekannt geworden ist. Zwar gibt die Zivilprozeßordnung dem Vorstand des Gerichts die Befugnis, auch ohne Einwilligung der Parteien Einsicht in die Akten zu gestatten, wenn ein „rechtliches Interesse“ glaubhaft gemacht wird. Jedoch betreffen Informationen aus Ehescheidungsakten sehr sensible Daten aus dem privaten Lebensbereich der Ehepartner und weiterer Prozeßbeteiligter, so daß dem Schutz der Persönlichkeit im Verhältnis zu dem wissenschaftlichen Interesse ein deutliches Übergewicht zuzubilligen ist. Sonst droht das sogenannte informationelle Selbstbestimmungsrecht im besonderen Maße beeinträchtigt zu werden. Deshalb erscheint dem Landesbeauftragten die Forderung gerechtfertigt, daß in solchen Fällen die wissenschaftliche Auswertung auf der Basis anonymisierter Daten oder mit Zustimmung der Betroffenen vorgenommen wird. Er sieht sich in seiner Beurteilung auch durch die neue Rechtsprechung des Bundesverfassungsgerichts zum Verhältnis zwischen Persönlichkeitsschutz und Forschungsfreiheit bestätigt (vgl. Tz. 4.6.4). Der Landesbeauftragte hat den Justizminister über seine Rechtsauffassung unterrichtet.

4.2.6 **Datenschutz im Strafvollzug**

4.2.6.1 **Der Landesbeauftragte als Ansprechpartner der Strafgefangenen**

„Datenschutz ist auch Minderheitenschutz!“ Wie ein roter Faden zieht sich diese datenschutzrechtliche Problematik durch die Tätigkeitsberichte der letzten Jahre. Allein die Zugehörigkeit zu einer bestimmten Personengruppe ist nicht selten ausschlaggebend für die Erfassung und Verdattung des einzelnen (6. TB, S. 7).

Auch die „Minderheit“ der Strafgefangenen befindet sich in einer Situation, in der schützenswerte Interessen beeinträchtigt werden können. Anfragen und Beschwerden machten dies deutlich und haben den Justizminister veranlaßt, den Persönlichkeitsschutz der Strafgefangenen in vielen Bereichen zu verbessern (7. TB, S. 32; 8. TB, S. 44).

Von den Strafgefangenen mußte es z. B. als „Störung des Vertrauensverhältnisses zum Datenschutzbeauftragten“ empfunden werden, daß die Justizvollzugsanstalten entsprechend den Regelungen des Strafvollzugsgesetzes ihre Schreiben an den Landesbeauftragten und dessen Antwortschreiben überprüften. Der Landesbeauftragte hatte für dieses „Unbehagen“ Verständnis. Auf seine Empfehlung hin hat der Justizminister inzwischen ein Verfahren eingeführt, das insoweit den Strafgefangenen weitgehend dem in Freiheit befindlichen Bürger gleichstellt. Schreiben des Gefangenen an den Landesbeauftragten werden grundsätzlich, Schreiben des Landesbeauftragten werden immer dann von einer Überprüfung ausgenommen, wenn der Landesbeauftragte in einem gesonderten Anschreiben darum bittet.

4.2.6.2 **Wenn Gefangene Urlaub machen ...**

Justizvollzugsanstalten dürfen Gefangene nicht zu Personen beurlauben, von denen zu befürchten ist, daß sie eine Rückgliederung in die Gesellschaft nach der Entlassung beeinträchtigen. Soweit die Anstalt nicht bereits ausreichende Informationen über die Urlaubsunterkunft hat, war es bisher üblich, Auskünfte über den Gastgeber insbesondere bei Polizeidienststellen und Sozialämtern einzuholen und diese auch um besondere Ermittlungen zu bitten.

Auf Empfehlung des Landesbeauftragten (8. TB, S. 44) hat der Justizminister nunmehr vorgeschrieben, daß Behörden zur Überprüfung des Gastgebers grundsätzlich nur eingeschaltet werden dürfen, wenn dieser zuvor sein Einverständnis schriftlich erklärt hat. Positiv zu beurteilen ist dabei auch, daß die Weigerung, das Einverständnis zu erklären, nicht automatisch die Ablehnung des Urlaubsantrages zur Folge hat. In diesem Fall ist die Anstalt gehalten, alle bekannten Umstände abzuwägen und erst bei nichtausräumbaren Zweifeln den Antrag negativ zu bescheiden.

4.3 **Steuerverwaltung**

4.3.1 **Rechtsklarheit und Transparenz bei den Kontrollmitteilungen**

Seit mehreren Jahren haben zwischen den Finanzministerien des Bundes und der Länder und den Datenschutzbeauftragten Gespräche darüber stattgefunden, wie das sogenannte Kontrollmitteilungsverfahren so umgestaltet werden könnte, daß es datenschutzrechtlichen Anforderungen genügt. Der Landesbeauftragte hat das in seinen früheren Tätigkeitsberichten (vgl. 4. TB, S. 29; 5. TB, S. 35; 6. TB, S. 41) dargestellt. Als Kontrollmitteilungen bezeichnet man Hinweise von Behörden an die zuständigen Wohnsitzfinanzämter, durch die sie über steuerlich relevante Zahlungen an Bürger informiert werden. Die Finanzämter nehmen diese Belege zu den Steuerakten und vergleichen die Beträge nach Eingang der Steuererklärungen mit den dort gemachten Angaben. Hat ein Steuerpflichtiger die Erklärung dieser Einnahmen „vergessen“, wird er darauf aufmerksam gemacht, schlimmstenfalls wird ein Verfahren wegen Steuerhinterziehung gegen ihn eingeleitet.

Die Steuerverwaltung leitet die Notwendigkeit derartiger „Melddienste“ aus der Abgabenordnung ab, nach der sie verpflichtet ist, „die Steuern gleichmäßig festzusetzen und zu erheben“. Die Datenschutzbeauftragten sehen diese Bestimmung nur als eine Aufgabenzuweisung und nicht als eine Befugnisnorm an. Ihres Erachtens bedarf ein Datentransfer zwischen den Behörden ohne Wissen des Betroffenen einer ausdrücklichen gesetzlichen Legitimation. Das gilt um so mehr, als auch das Anfertigen von Kontrollmitteilungen durch die Betriebsprüfung der Finanzämter in der Abgabenordnung speziell geregelt ist.

Nachdem die Aufnahme dieses Problems in den damals bestehenden Novellierungskatalog zur Abgabenordnung zunächst nicht für erforderlich gehalten wurde, ließen die beiden Urteile des Bundesverfassungsgerichts zur Volkszählung und zum Akteneinsichtsrecht parlamentarischer Untersuchungsausschüsse eine entsprechende gesetzliche Regelung dringlich erscheinen, wollte man auf das bisherige Verfahren nicht ganz verzichten. Entscheidend hierfür war die Feststellung des Bundesverfassungsgerichts, daß „die Grundrechte ihren Trägern einen Schutz gegen unbegrenzte Erhebung, Speicherung, Verwendung oder Weitergabe der auf sie bezogenen individualisierten oder individualisierbaren Daten verbürgen. Dieser Schutz darf nur im überwiegenden Interesse der Allgemeinheit und unter Beachtung des Grundsatzes der Verhältnismäßigkeit durch Gesetze oder aufgrund eines Gesetzes eingeschränkt werden; die Einschränkung darf nicht weiter gehen, als es zum Schutz öffentlicher Interessen unerlässlich ist.“

Die nunmehr in § 93 a Abgabenordnung getroffene Regelung wird den bisherigen Umfang des Kontrollmitteilungsverfahrens zwar nicht entscheidend verändern. Es wird aber in Zukunft für die Betroffenen wesentlich mehr Transparenz geben als bisher. In einer Rechtsverordnung sind nämlich

- die mitteilenden Stellen,

- die mitzuteilenden Angaben,
- die für die Entgegennahme der Mitteilungen zuständigen Finanzbehörden und
- die Verpflichtung zur Unterrichtung der Betroffenen

im einzelnen festzulegen bzw. zu regeln. Insbesondere dem letzten Punkt mißt der Landesbeauftragte eine besondere Bedeutung bei. In ihm dokumentiert sich seines Erachtens ein gelungener Kompromiß zwischen dem staatlichen Anspruch auf eine umfassende Besteuerung aller Einkünfte und dem Anspruch des einzelnen darauf, daß staatliche Stellen nicht „hinter seinem Rücken“ vorsorglich Informationen austauschen, um sein späteres Verhalten (Angabe der Einkünfte in seiner Steuererklärung) zu kontrollieren. Wenn alle Bezieher steuerpflichtiger Einnahmen aus staatlichen Quellen von vornherein wissen, daß das Finanzamt über die Einkünfte informiert wird, dürfte es in Zukunft wesentlich weniger ertappte „Steuersünder“ als bisher geben, ohne daß der staatliche Steueranspruch darunter leidet.

Nicht vom Datenschutzbeauftragten, sondern nur vom Gesetzgeber kann allerdings die Frage beantwortet werden, warum ein derartig umfassendes Informationssystem für den öffentlichen Bereich für erforderlich erachtet wird, während die wesentlich umfangreicheren „Nebeneinkünfte“ der Steuerpflichtigen aus nichtöffentlichen Kassen im wesentlichen auf der Grundlage von „Treu und Glauben“ besteuert werden.

4.3.2 **Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung im Rechenzentrum der Steuerverwaltung**

Im Berichtszeitraum ist die Sicherheit und die Ordnungsmäßigkeit der Datenverarbeitung im Rechenzentrum der Steuerverwaltung bei der Oberfinanzdirektion Kiel überprüft worden. Die dort vorgefundenen datenschutzrechtlich bedeutsamen Sachverhalte und Verfahrensweisen sowie deren Bewertung durch den Landesbeauftragten sind unter Tz. 5.3 dargestellt.

4.4 **Wirtschaft und Verkehr**

4.4.1 **Schulnoten im Ausbildungsregister der Industrie- und Handelskammern**

Auszubildende haben sich beim Landesbeauftragten darüber beschwert, daß von den Industrie- und Handelskammern u. a. auch ihre letzten Schulnoten in Deutsch und Rechnen erhoben würden, obwohl hierfür im Berufsbildungsgesetz keine Rechtsgrundlage besteht. Von den Ausbildungsbetrieben würden die Daten aus den Berufsausbildungsverhältnissen den Industrie- und Handelskammern gemeldet, damit diese statistische Erhebungen über die schulischen Leistungen der „Azubis“ anstellen könnten.

Der Verband der Industrie- und Handelskammern hat die entsprechenden Hinweise des Landesbeauftragten aufgegriffen und verzichtet heute auf eine Erfassung der Schulnoten. Außerdem wurde der Erhebungsbogen präzisiert, so daß künftig auf die jeweiligen Bestimmungen des Berufsbildungs- und Berufsbildungsförderungsgesetzes hingewiesen wird.

4.4.2 **Datenschutzfragen im Zusammenhang mit dem Führerschein auf Probe**

Fahranfänger sind besonders häufig an Unfällen beteiligt, der „Führerschein auf Probe“ soll dem entgegenwirken. Dazu ist es erforderlich, daß beim Kraftfahrt-Bundesamt ein zentrales Register aller Fahranfänger geführt wird. Daraus werden die innerhalb der Probezeit begangenen Straftaten und Ordnungswidrigkeiten den Führerscheinstellen mitgeteilt, die dann die entsprechenden Maßnahmen (z. B. Nachschulungen) veranlassen.

Es ist u. a. vorgesehen, daß die Anordnung eines Nachschulkurses dem Kursleiter (Fahrlehrer) vorzulegen ist. Da es sich hierbei um hochsensible Daten handelt (Art des Fehlverhaltens wie z. B. Trunkenheit, Körperverletzung), erscheint es dem Landesbeauftragten erforderlich, daß diese Daten beim Fahrlehrer nur in anonymisierter Form verwendet und keine personenbezogenen Karteien oder Dateien geführt werden. Er hat den Minister für Wirtschaft und Verkehr gebeten, diese Überlegungen bei den Beratungen der betreffenden Rechtsverordnungen zu berücksichtigen.

4.4.3 **Neufassung des Anhörungsbogens bei Verkehrsordnungswidrigkeiten**

Der Landesbeauftragte hat sich bereits seit längerer Zeit dafür eingesetzt, den Anhörungsbogen für Verkehrsordnungswidrigkeiten auf den unbedingt erforderlichen Datenumfang zu reduzieren (vgl. 3. TB, S. 19). Außerdem hat er gefordert, daß aus der Belehrung für den Betroffenen zweifelsfrei zu erkennen sein muß, zu welchen Angaben er verpflichtet ist und welche Angaben er freiwillig machen kann. Das gilt z. B. für die Führerscheindaten und die Angaben zum Familienstand und Beruf.

Der Innenminister hat dem Landesbeauftragten mitgeteilt, daß dessen Forderungen in der Neufassung des Anhörungsbogens Berücksichtigung gefunden haben.

4.4.4 **Die Berufsangabe – ein „unsicheres“ Datum**

Ein Kraftfahrzeughalter hat sich beim Datenschutzbeauftragten darüber beschwert, daß er bei der Anmeldung seines Kraftfahrzeuges bei der Zulassungsstelle Angaben über seinen Beruf machen müsse. Die Berufsausübung unterliege in der heutigen Zeit schnellen Veränderungen und veraltete Daten könnten leicht zu unrichtigen Registerinformationen führen. Im Hinblick darauf, daß das Kraftfahrt-Bundesamt auf die Speicherung der Berufsangabe bei nichtselbständigen Kraftfahrzeughaltern bereits ab Januar 1986 verzichtet, hat der Datenschutzbeauftragte den Minister für Wirtschaft und Verkehr um Überprüfung eines entgegenstehenden Erlasses aus dem Jahre 1985 gebeten. Künftig wird auf die Erhebung der Berufsangabe der nichtselbständigen Kraftfahrzeughalter auch in Schleswig-Holstein verzichtet.

4.4.5 Auskünfte des Kraftfahrt-Bundesamtes sind nur nutzbar, wenn sie aktuell sind

Ein anderer Petent hat sich nach der Ummeldung seines veräußerten Kraftfahrzeuges darüber beklagt, daß dieser Tatbestand erst mehrere Monate später beim Kraftfahrt-Bundesamt in Flensburg eingetragen wurde. Er sei in der Zwischenzeit durch eine Halteranfrage der Polizei in Flensburg Adressat belastender Maßnahmen der Polizei (Vernehmung wegen des Verdachts einer Verkehrsstraftat) geworden.

Die Überprüfung durch den Landesbeauftragten hat ergeben, daß die zuständige Kraftfahrzeugzulassungsstelle die Ummeldung unverzüglich an das Kraftfahrt-Bundesamt gemeldet hatte. Die verspätete Speicherung fiel somit allein in den Zuständigkeitsbereich einer Bundesbehörde, die nicht der Kontrolle des Landesbeauftragten unterliegt.

Der Vorgang verdeutlicht jedoch, daß die Polizeibehörden bei ihren Schlußfolgerungen aus Auskünften des zentralen Verkehrsinformationssystems stets berücksichtigen müssen, daß der Datenbestand nicht immer aktuell ist.

4.4.6 Dokumentation der Zugriffe auf das zentrale Verkehrsinformationssystem

Die Beratungen zum sogenannten Fahrzeugregistergesetz sind unter erheblichem Zeitdruck geführt worden. Der Landesbeauftragte hat im Hinblick auf die Einführung des zentralen Verkehrsinformationssystems (ZEVIS) beim Kraftfahrt-Bundesamt in Flensburg und der Möglichkeit eines Direktabrufs der Daten durch Polizeibehörden empfohlen, auch die örtlichen Zulassungsstellen zu verpflichten, Anfragen auf ihre Datenbestände aufzuzeichnen. Anderenfalls könne bei „problematischen Anfragen“ die Protokollierungspflicht des Kraftfahrt-Bundesamtes durch Rückgriffe auf die Dateien der örtlichen Zulassungsstellen umgangen werden. Außerdem hat er gefordert, beim Kraftfahrt-Bundesamt Verknüpfungsmerkmale zu speichern, die die für den Abruf verantwortliche Person und den Anlaß des Abrufes feststellbar machen.

Diese Forderungen haben nur zum Teil Eingang in das Fahrzeugregistergesetz gefunden. Der Landesbeauftragte hat deshalb nachdrücklich darauf hingewiesen, daß nur die Protokollierung der Zugriffe eine wirksame Kontrolle der Zugriffsberechtigung und der rechtmäßigen Weiterverwendung der Daten bei den anfragenden Stellen ermöglicht. Welche Anforderungen dabei an die Dokumentation im einzelnen zu stellen sind, hat er bereits in seinem 8. Tätigkeitsbericht (S. 63) ausgeführt. Er hat dort insbesondere klargestellt, daß eine Dokumentation wertlos ist, die einen Rückschluß auf Anfrager und anfragende Person nicht zuläßt.

4.5 Gesundheits- und Sozialdaten

4.5.1 Der Umgang mit Patientendaten und die ärztliche Schweigepflicht – es besteht ein erheblicher Regelungsbedarf

Im Berichtsjahr haben sich die Datenschutzbeauftragten des Bundes und der Länder eingehend mit den Auswirkungen des

Volkszählungsurteils auf den Umgang mit Patientendaten befaßt und ihre datenschutzrechtliche Beurteilung in einer Entscheidung dargelegt. Schwerpunkt der Überlegungen war die Frage, wie ein ausreichender Datenschutz im Krankenhaus sicherzustellen ist.

Aus der Sicht des Landesbeauftragten besteht hier insbesondere bei folgenden Problemen ein Regelungsbedarf:

- Die in der Berufsordnung der Ärzte verankerte ärztliche Schweigepflicht, die ergänzt wird durch die entsprechende Strafvorschrift des § 203 Abs. 1 Strafgesetzbuch, sowie die allgemeinen Datenschutzgesetze reichen nicht aus, um alle Fälle, in denen im Bereich des Krankenhauses das Persönlichkeitsrecht des Patienten berührt wird, angemessen zu lösen.
- Konkrete gesetzliche Regelungen sind auch deshalb dringend geboten, weil der zunehmende Einsatz der automatisierten Datenverarbeitung in den Krankenhäusern die Risiken für den Persönlichkeitsschutz des Patienten erhöht. Die EDV wird zunehmend nicht nur für Abrechnungszwecke, sondern auch für die Verarbeitung medizinischer Daten (Anamnese-, Diagnose- und Therapiedaten) eingesetzt.
- Die automatisierte personenbezogene Verarbeitung von Patientendaten in Krankenhausinformationssystemen u. ä. erfolgt in der Regel auf der Grundlage der „Allgemeinen Geschäftsbedingungen“ oder sehr weit gefaßter formularmäßiger Einwilligungserklärungen. Diese müssen konkreter gefaßt werden. Auch in den Fällen, in denen die Informationsmöglichkeiten und die Entscheidungsfreiheit des Patienten eingeschränkt sind, muß sein Recht auf informationelle Selbstbestimmung gewährleistet bleiben.
- Maßstab für die Bestimmung der Grenzen der Verarbeitung und der sonstigen Nutzung von Patientendaten muß stets der Zweck „Behandlung“ sein. Eine vom konkreten Behandlungszweck nicht gedeckte Datenverarbeitung bedarf einer besonderen Legitimation durch Gesetz oder der ausdrücklichen Einwilligung des Betroffenen.
- Zur Wahrung des Patientengeheimnisses ist es geboten, im Krankenhaus den ärztlichen Bereich vom Verwaltungsbereich informationell abzuschotten. Die Weitergabe von Behandlungsdaten an die Verwaltung ist nur insoweit befugt, wie sie für Aufgaben der Verwaltung erforderlich sind. Daraus folgt, daß z. B. die Daten der Krankenhausverwaltung nur getrennt von denjenigen des ärztlichen Bereichs genutzt werden dürfen. Aber auch innerhalb des ärztlichen Bereichs darf der behandelnde Arzt nur auf „seine“ Patientendaten zugreifen, denn die ärztliche Schweigepflicht gilt auch für den Informationsaustausch zwischen Ärzten.
- Die Krankenhäuser sehen sich vielfältigen Informationsanforderungen, z. B. von Sozialleistungsträgern (Sozialämter, Versorgungsämter) und anderen öffentlichen Stellen (Meldebehörde, Standesamt, Polizei), ausgesetzt. Die Übermittlungersuchen sind häufig nicht ausreichend begründet.

- Ihre Notwendigkeit muß überprüft, die gesetzlichen Grundlagen müssen präzisiert werden.
- Bei einer Patientendatenverarbeitung „außer Haus“ (Abrechnung, Mikroverfilmung, Archivierung, externe Labors) muß den Patienten zumindest ein Widerspruchsrecht eingeräumt werden.
 - Wegen der Sensibilität von Patientendaten sollte die Verarbeitung im Auftrag durch nichtöffentliche Stellen nur zulässig sein, wenn anders Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der automatischen Datenverarbeitung hierdurch erheblich kostengünstiger besorgt werden können.
 - Der Patient darf ohne sein Wissen und sein Einverständnis nicht zum Objekt der Forschung gemacht werden.
 - Das informationelle Selbstbestimmungsrecht umfaßt auch das Recht des Patienten, Einsicht in seine Akten und ärztlichen Unterlagen zu nehmen und Auskunft zu erhalten. Dieses Recht darf nur eingeschränkt werden, wenn der Schutz des Patienten selbst oder überwiegende Geheimhaltungsinteressen anderer ihm entgegenstehen.
 - Eine undifferenzierte, zeitlich unbefristete Aufbewahrung von Patientenunterlagen darf es auch im Krankenhaus nicht geben. Deshalb müssen die Krankenhäuser verpflichtet werden, regelmäßig zu überprüfen, wann welche Unterlagen ohne Beeinträchtigung schutzwürdiger Belange der Patienten gesperrt bzw. vernichtet werden können.

4.5.2 **Schweigepflichtentbindungsklauseln sind weiterhin ein datenschutzrechtliches Sorgenkind**

Bereits in seinem 7. und 8. Tätigkeitsbericht (S. 44 bzw. S. 51) hat der Landesbeauftragte die generalklauselartigen Einwilligungserklärungen zur Befreiung von der ärztlichen Schweigepflicht kritisiert, die den Antragstellern vom Landesversorgungsamt und von der Landesversicherungsanstalt abverlangt werden. Den genannten Behörden sind die konkreten Forderungen des Landesbeauftragten bekannt. Ihnen sind auf Wunsch sogar Musterentwürfe für eine Neufassung dieser Schweigepflichtentbindungsklauseln übersandt worden.

Er hat dabei im einzelnen gefordert:

- Unterrichtung des Antragstellers über die gesetzlich geregelten Verwendungsmöglichkeiten der Daten durch die Leistungsträger;
- Begrenzung der von der Einwilligung erfaßten Daten auf den im Einzelfall erforderlichen Umfang;
- Angabe des Zwecks, zu dem die Kenntnis der medizinischen Daten erforderlich ist, um dem Arzt deutlich zu machen, welche Daten von der Entbindungserklärung erfaßt werden;
- Trennung der Erklärung vom Antrag, um die Vorlage bei dem Arzt möglich zu machen;

- Vorlage der Erklärung bei dem Arzt, den der Antragsteller von der Schweigepflicht befreit hat.

Das Landesversorgungsamt hat sich inzwischen bereit erklärt, die von den Patienten unterschriebenen Erklärungen den betreffenden Ärzten zuzuleiten. Dies wird vom Landesbeauftragten begrüßt. Leider konnte in den anderen Fragen keine Annäherung der Standpunkte erreicht werden. Der Landesbeauftragte vertritt dabei mit besonderem Nachdruck die Auffassung, daß es nicht erforderlich und somit datenschutzrechtlich auch nicht zulässig ist, in **allen** Fällen die Entbindung von der Schweigepflicht für **sämtliche** Krankenunterlagen, die im Leben des Antragstellers angefallen sind, zu verlangen. Hier muß abgestuft vorgegangen werden. Es kann nicht der Regel-, sondern nur der Ausnahmefall sein, daß alle Krankenunterlagen (womöglich vom Kindesalter an) herangezogen werden.

Auch mit der Landesversicherungsanstalt fanden im Berichtszeitraum weitere Erörterungen statt. Sie führten zwar zu einer Klärung der unterschiedlichen Positionen, jedoch nicht zu einer Neugestaltung der Schweigepflichtentbindungsklauseln. Der Landesbeauftragte bedauert das um so mehr, als ihm bekannt ist, daß die Landesversicherungsanstalt in der Praxis tatsächlich nicht in jedem Fall alle Unterlagen anfordert. Das zeigt, daß sie durchaus bemüht ist, unnötige Datenübermittlungen zu vermeiden. Der Landesbeauftragte sieht keinen Hinderungsgrund, dieser datenschutzrechtlich zu begrüßenden Praxis auch bei der Gestaltung der Schweigepflichtentbindungsklauseln Rechnung zu tragen.

Die Diskussion über die Neugestaltung der Schweigepflichtentbindungsklauseln wird sowohl beim Bund als auch in den anderen Bundesländern geführt. Es ist zu erwarten, daß dies die Bereitschaft der betroffenen Institutionen zu Veränderungen heben wird, denn in der Vergangenheit wurden die Forderungen des Landesbeauftragten häufig auch mit dem Argument abgelehnt, man könne nicht aus einem bundeseinheitlichen Verfahren ausbrechen.

4.5.3 **Abrechnung von Krankenhausleistungen in Rechenzentren**

Im Berichtsjahr fanden umfangreiche Erörterungen mit der Datenzentrale Schleswig-Holstein statt, die im Auftrag ihrer Kunden Krankenhausleistungen abrechnet. Ziel der Datenzentrale ist es, in den Krankenhausaufnahmeverträgen aller angeschlossenen Anwender eine einheitliche, rechtlich tragfähige Basis für die externe Verarbeitung von Patientendaten zu Abrechnungszwecken zu schaffen. Zu den damit im Zusammenhang stehenden Problemen haben sich sowohl der Justizminister als auch der Sozialminister geäußert. Beide haben darauf hingewiesen, daß zwar unter gewissen Umständen die Offenbarung von Patientendaten zu Abrechnungszwecken mit der „Sozialadäquanz“ oder der „Wahrnehmung berechtigter Interessen“ gerechtfertigt werden könnte. Sie haben jedoch gleichzeitig deutlich gemacht, daß dies keineswegs rechtlich eindeutig und insofern für die Krankenhäuser und die Ärzte risikobehaftet sei. Deshalb haben sowohl der Justizmini-

ster als auch der Sozialminister empfohlen, vor der Weitergabe von Patientendaten an externe Rechenzentren ausdrückliche Einverständniserklärungen der Patienten einzuholen. Diese Empfehlung unterstützt der Landesbeauftragte nachdrücklich.

Die Kunden der Datenzentrale Schleswig-Holstein sind derzeit jedoch nicht bereit, eine förmliche Einwilligungserklärung zur externen Patientendatenverarbeitung in den Krankenhausaufnahmeverträgen vorzusehen. Sie beabsichtigen, statt dessen ausführliche Informationen über den praktizierten Abrechnungsweg zu geben. Der Landesbeauftragte hat deutlich gemacht, daß er hierin zwar einen ersten Schritt in die richtige Richtung sieht, die Forderung nach einer „Einwilligungslösung“ jedoch nach wie vor aufrechterhält. Den Patienten muß in jedem Fall die Möglichkeit zum Widerspruch gegen die Weitergabe ihrer Daten an ein Rechenzentrum gegeben werden.

4.5.4 **Unterrichtung der Führerscheinstellen über die Unterbringung psychisch Kranker**

Die Anregung des Landesbeauftragten, die Unterrichtung der Führerscheinstellen über Unterbringung psychisch Kranker gesetzlich zu regeln oder aber auf die Übermittlung zu verzichten (vgl. 7. TB, S. 50; 8. TB, S. 57), hat der Sozialminister nicht aufgegriffen. In einem Erlaß ist allerdings klargestellt, daß die Führerscheinstellen nur in Ausnahmefällen von einer Unterbringung eines Bürgers in einem Landeskrankenhaus unterrichtet werden dürfen. Die Führerscheininhaber seien während der Zeit ihrer Unterbringung gehindert, am Straßenverkehr teilzunehmen. Im Zeitpunkt ihrer Entlassung aus der stationären Behandlung sei die akute Erkrankung, die unter Umständen eine Fahruntüchtigkeit verursacht hätte, in der Regel abgeklungen. Die leitenden Ärzte der psychiatrischen Krankenhäuser sollten daher dafür sorgen, daß während der Behandlung der Patienten und bei ihrer Entlassung geprüft wird, ob aus ärztlicher Sicht ein begründeter Anhalt für eine Fahruntüchtigkeit besteht. Den Befund und die sich daraus ergebenden Konsequenzen sollen die Ärzte mit den Patienten und ggf. ihren gesetzlichen Vertretern eingehend besprechen. Falls der betreffende Patient nicht einsichtig ist, soll der behandelnde Arzt die Kreisgesundheitsbehörde unterrichten. Kommt diese zum gleichen Ergebnis wie der Arzt, muß sie das Straßenverkehrsamt, das die Fahrerlaubnis erteilt hat, informieren.

Obwohl diese Regelung des Sozialministers eine deutliche Verbesserung gegenüber der bisherigen Praxis darstellt, betrachtet der Landesbeauftragte sie nur als eine Zwischenlösung.

4.5.5 **Datenschutz im schulärztlichen Dienst**

Noch immer Probleme mit dem Schülersgesundheitsbogen

Der Landesbeauftragte erhält nach wie vor Anfragen besorgter Eltern wegen der datenschutzrechtlichen Bewertung schulärztlicher Fragebögen (vgl. auch 7. TB, S. 47; 8. TB, S. 59).

Er sah sich deshalb veranlaßt, in diesem Jahr nochmals deutlich zu machen, daß die Schüler ausschließlich zur Feststellung der Schulreife und zur Früherkennung von Gesundheits- und Entwicklungsstörungen untersucht werden und die Datenerhebungen und -speicherungen nur in dem zur Erfüllung dieser gesetzlichen Aufgabe notwendigen Umfang erfolgen dürfen. Daten, die nur „wünschenswert“ sind (z. B. der Impfstatus des Schülers), dürfen auf der Grundlage des Schulgesetzes nicht erhoben und gespeichert werden. Die über die Aufgaben des schulärztlichen Dienstes hinausgehenden Ziele, wie z. B. die medizinische Beobachtung und die gesundheitspolitische Bewertung ganzer Schülerjahrgänge, können ohne spezialgesetzliche Grundlage nicht verfolgt werden.

Der Landesbeauftragte rechnet damit, daß 1987 ein einheitlicher datenschutzgerechter Schülergesundheitsbogen eingesetzt wird.

Schulärztliche Untersuchungen vor der versammelten Klasse

Ein Bürger wandte sich mit der Beschwerde an den Landesbeauftragten, sein Kind sei vor der versammelten Schulklasse schulärztlich untersucht, der Befund für alle vernehmbar verkündet und dann schriftlich festgehalten worden.

Der Datenschutzbeauftragte sah hier eine unzulässige Offenbarung medizinischer Daten. Ein Arzt darf grundsätzlich ein Gespräch mit seinem Patienten über dessen Krankheit nicht gegen dessen Willen in Gegenwart eines anderen Patienten führen. Was für jeden Patienten gilt, ist auch bei der Untersuchung von Schülern zu beachten.

Vom betreffenden Schularzt wurde betont, daß es aus seiner Sicht sinnvoll sei, den Schülern Erläuterungen und Belehrungen anhand eines konkreten Einzelfalles zu geben. Solche Einzelfälle seien z. B. Schüler mit Gewichtsproblemen, Wirbelsäulenschäden bzw. Farbsinnstörungen.

So löblich die Absicht gewesen sein mag, das Interesse der Kinder dadurch zu wecken, daß ein konkreter Problembezug hergestellt wurde, so legitimiert sie jedoch keinesfalls dazu, über die persönlichen Probleme eines Schülers vor der Klasse zu sprechen. Aus Datenschutzgründen und speziell im Hinblick auf die Beachtung der ärztlichen Schweigepflicht ist daher die Einzeluntersuchung der Schüler organisatorisch derart zu gestalten, daß die medizinischen Befunde Dritten nicht bekannt werden.

Da dem Landesbeauftragten bekannt ist, daß der geschilderte Vorfall keinen Ausnahmefall, sondern eher das übliche Vorgehen darstellt, hat er die zuständigen Ressorts über seine Rechtsauffassung informiert und um künftige Beachtung gebeten.

4.5.6 Gesundheitsrechtliche Vorschriften können noch datenschutzgerechter gestaltet werden

Das am 25.09.1986 beschlossene Gesetz zur Änderung gesundheitsrechtlicher Vorschriften enthält zwar eine Reihe klarer Regelungen über den Umgang mit personenbezogenen

Daten im öffentlichen Gesundheitswesen. Der Landesbeauftragte sieht sich aber veranlaßt, weitergehende datenschutzrechtliche Regelungen anzuregen:

- Neben einer bloßen Beschreibung der Aufgaben der Gesundheitsbehörden sollten auch die Befugnis zur Verarbeitung personenbezogener Daten und der zulässigerweise zu speichernde Datenumfang geregelt werden.
- Für die Statistiken im Gesundheitswesen ist entsprechend den Forderungen des Bundesverfassungsgerichts eine ausreichende normative Grundlage zu schaffen. Ein bloßer Hinweis auf die Freiwilligkeit der Teilnahme an Datenerhebungen zu statistischen Zwecken dürfte in vielen Fällen der besonderen Zwangslage kranker Menschen nicht angemessen sein.
- Die Daten, die über die in Berufen des Gesundheitswesens tätigen Personen zu erfassen sind, sollten im Gesetz oder in einer Verordnung festgelegt werden. Es reicht nicht aus, auf einen jederzeit änderbaren, verwaltungsinernen Fragebogen zu verweisen.
- Es wäre eine gesetzliche Regelung darüber zu treffen, wann von Gesundheitsbehörden personenbezogene Daten anderen öffentlichen Stellen übermittelt werden dürfen (etwa für ordnungsbehördliche Maßnahmen). Auf die Ausführungen zur Übermittlung entsprechender Daten an die Führerscheinstellen wird verwiesen (vgl. Tz. 4.5.4).

4.5.7 Der Schutz des Sozialgeheimnisses

4.5.7.1 Offenbarung von Sozialdaten gegenüber den Sicherheitsbehörden

Im abgelaufenen Jahr hat sich gezeigt, daß in der Praxis oft Unsicherheiten über die Zulässigkeit von Auskünften durch Sozialleistungsträger an Sicherheitsbehörden bestehen. Für solche Auskünfte regelt das Sozialgesetzbuch sowohl das formal einzuhaltende Verfahren als auch das zulässige Datenprofil. Die Offenbarung von Sozialdaten ist zulässig, soweit sie im Einzelfall für die rechtmäßige Erfüllung der Aufgaben der jeweiligen Sicherheitsbehörde erforderlich ist und sich auf Angaben über Vor- und Familiennamen, Geburtsdatum, Geburtsort, derzeitige und frühere Anschriften des Betroffenen sowie Namen und Anschriften seiner derzeitigen und früheren Arbeitgeber beschränkt. Darüber hinausgehende Informationen z. B. über die Höhe der Sozialhilfe oder den Gesundheitszustand eines Sozialhilfeempfängers sind unzulässig.

Abweichend vom allgemeinen Amtshilferecht haben allein die Sicherheitsbehörden die Notwendigkeit der Information zu prüfen und zu beurteilen. Hierüber entscheidet ein vom Leiter der betreffenden Sicherheitsbehörde bestimmter Beauftragter, der die Befähigung zum Richteramt haben muß. Bei der ersuchten Stelle, z. B. dem Sozialamt, entscheidet über die zu erteilende Auskunft der Behördenleiter oder sein Stellvertreter.

Um solche Informationsflüsse überprüfen zu können, sollten die Anfragen nur schriftlich gestellt und beantwortet werden.

Darauf hat der Landesbeauftragte in einem konkreten Fall besonders hingewiesen.

4.5.7.2 **Offenbarung von Sozialdaten gegenüber der Kriminalpolizei**

Die Kriminalpolizei wendet sich häufig mit Fragen an die Jugendämter, die jedoch regelmäßig unter Hinweis auf die im Sozialgesetzbuch abschließend geregelten Offenbarungsbefugnisse die Auskünfte ablehnen. Den zuständigen Mitarbeitern der Kriminalpolizei ist das Verhalten der Kreisjugendämter vielfach unverständlich, da, so wurde wörtlich geäußert, „das Rechtsgut der Strafprozeßordnung höheres Recht ist und deshalb die Bestimmungen des Sozialgesetzbuches einschränkt“.

Hierzu hat der Landesbeauftragte klargestellt, daß auch Jugendämter als Leistungsträger im Sinne des Sozialgesetzbuches das Sozialgeheimnis uneingeschränkt zu beachten haben. Die von der Kriminalpolizei als zu restriktiv empfundenen Regelungen der Offenbarungsbefugnisse sind vom Gesetzgeber so gewollt. Der Auskunftsanspruch, den die Kriminalpolizei im Rahmen des staatsanwaltschaftlichen Ermittlungsverfahrens nach der Strafprozeßordnung hat, wird durch die einschlägigen Regelungen des Sozialgesetzbuches begrenzt.

4.5.7.3 **Offenbarung von Sozialdaten gegenüber den Verkehrsaufsichtsbehörden**

Die Praxis der Gesundheitsämter, die Führerscheinstellen über die Einweisung von Bürgern in Landeskrankenhäuser zu unterrichten, ist vom Landesbeauftragten bereits kritisiert worden (vgl. hierzu auch Tz. 4.5.4). Aber auch Sozialämter haben die Führerscheinstellen offenbar unaufgefordert darüber unterrichtet, daß Sozialhilfeempfänger möglicherweise fahruntüchtig seien. In einem Fall übermittelte das Sozialamt der Führerscheinstelle detaillierte medizinische Daten aus einem Versorgungsbescheid.

Hierfür gibt es im Sozialgesetzbuch keine Übermittlungsbefugnis. Das Sozialamt hat sich auf den rechtfertigenden Notstand als Rechtsgrundlage für derartige Übermittlungen berufen. Der Landesbeauftragte hat Zweifel, ob hier die tatbestandsmäßigen Voraussetzungen des § 34 Strafgesetzbuch – er „rechtfertigt“ nur in Ausnahmesituationen zur Abwendung einer gegenwärtigen Gefahr eine Offenbarung medizinischer Daten – vorgelegen haben, weil die Frage der Fahruntüchtigkeit wohl nur von dem begutachtenden Arzt und nicht vom Sozialamt entschieden werden kann.

Ein anderer Fall – auch hier hatte ein Sozialamt die Führerscheinstelle über Krankheiten eines Sozialhilfeempfängers und die daraus abzuleitende mögliche Fahruntüchtigkeit unterrichtet – wurde vor dem Schleswig-Holsteinischen Verwaltungsgericht verhandelt. Das Gericht hat die Auffassung des Landesbeauftragten bestätigt und deutlich gemacht, daß bloße Eignungszweifel an der Fahrtüchtigkeit weder den Arzt noch die Sozialbehörde berechtigen können, die Verkehrsbehörde über den Zustand des Betroffenen zu informieren. Außerdem ist stets erst der Betroffene selbst darauf hinzuweisen, daß sein

gesundheitlicher Zustand für ihn und die Allgemeinheit eine Gefährdung darstellt, wenn er ein Kraftfahrzeug steuert. Erst wenn das vergeblich ist, darf die Verkehrsbehörde benachrichtigt werden, wenn es gilt, eine akute Gefährdung zu verhindern. Das Gericht vermißte bei dem verhandelten Fall das von der Rechtsprechung geforderte „Zureden“ und sah auch die akute Gefährdung nicht als gegeben an. Es ging daher davon aus, daß die Verkehrsbehörde diese Daten unbefugt erhalten habe und daß sie nicht verwertet werden dürften, solle nicht das Grundrecht der informationellen Selbstbestimmung leerlaufen.

4.5.7.4 **Bekanntgabe von Mitarbeiterdaten einer gesetzlichen Krankenkasse an deren Vorstand**

Die gesetzlichen Krankenkassen legen offenbar Wert darauf, daß ihre Angestellten bei ihnen versichert sind. Der Vorstand einer Kasse wollte deshalb durch Prüfung der Versicherungsdaten die Mitarbeiter ermitteln, die sich einer anderen Kasse angeschlossen hatten. Die Betroffenen befürchteten zu Recht eine unerwünschte Einflußnahme und dienstliche Nachteile.

Die Daten aller Mitglieder der gesetzlichen Krankenkassen unterliegen dem Sozialgeheimnis. Eine Offenbarung, die bereits dann vorliegen kann, wenn die Daten innerhalb der für die Sozialleistungen zuständigen Stelle ausgetauscht werden, ist nur in engem Rahmen zulässig. Um die wirtschaftliche Situation und die Entwicklung des Mitgliederbestandes der Kasse zu beurteilen, sind für den Vorstand sicher keine namentlichen Listen der Mitglieder erforderlich. Ein Vergleich der Mitarbeiterdaten mit den Mitgliederdaten würde daher das Sozialgeheimnis verletzen und außerdem zu einer Zweckentfremdung der Daten durch den Arbeitgeber führen. Der Landesbeauftragte hat der Kasse deshalb empfohlen, dem Vorstand nur anonymisierte Unterlagen über den Mitgliederbestand vorzulegen.

4.5.8 **Datenschutz bei den Sozialversicherungswahlen**

Im Zusammenhang mit den Wahlen in der Sozialversicherung hat sich eine Gewerkschaft beim Landesbeauftragten darüber beschwert, daß eine andere Gewerkschaft durch den örtlichen Wahlausschuß Einsicht in ihre Liste der sogenannten Stützunterschriften erhalten hat. Die dabei gewonnenen Informationen könnten dazu verwendet werden, Druck auf die Sympathisanten der betreffenden Gewerkschaft auszuüben.

Die Überprüfung ergab, daß bei den Sozialversicherungswahlen eine andere rechtliche Situation gegeben ist als bei allgemeinen Wahlen. Während nach dem allgemeinen Wahlrecht Einsichtnahmen durch den politischen Gegner in die Unterschriftensammlungen unzulässig sind, ergibt sich dies keineswegs so eindeutig aus den verfahrensrechtlichen Vorschriften für die Sozialversicherungswahlen.

Der Landesbeauftragte hat beim Sozialminister angeregt, bei einer Novellierung der Sozialwahlordnung für die Aufnahme einer der Bundeswahlordnung entsprechenden Regelung einzutreten. Diese sieht vor, daß Auskünfte über Stützungsunter-

schriften für Wahlvorschläge nur Behörden, Gerichte und sonstige amtliche Stellen des Wahlgebietes und nur dann erhalten dürfen, wenn sie zur Durchführung der Wahl oder eines Wahlprüfungsverfahrens oder zur Aufklärung des Verdachts einer Wahlstraftat erforderlich sind.

Dem Landesbeauftragten ist zugesagt worden, daß diese Anregung aufgegriffen wird.

4.5.9 **Rentenversicherungsnummer – Einstieg in das Personenkennzeichen?**

Die Datenschutzbeauftragten des Bundes und der Länder haben in der Vergangenheit stets die Verwendung von „automationsgerechten Ordnungsbegriffen“ kritisiert, wenn die damit bezweckten Verknüpfungsmöglichkeiten nicht durch ein Gesetz „abgesegnet“ waren. Anderenfalls bestünde die Gefahr, daß doch Stück für Stück der „gläserne Mensch“ entstehe. Der Bund hat nunmehr einen Gesetzentwurf zur Rentenversicherungsnummer vorgelegt, der nicht nur die derzeitige Praxis legalisieren, sondern darüber hinaus noch zusätzliche Verwendungen möglich machen soll. Diese Entwicklung zeigt, wie problematisch es häufig ist, im Interesse der Betroffenen eindeutige gesetzliche Regelungen vom Gesetzgeber zu verlangen. Nicht selten führt dies zwar zu einer nunmehr normenklaren, jedoch objektiv „schlechteren“ Stellung der Betroffenen. Es muß also auch darauf geachtet werden, daß solche, dem Personenkennzeichen ähnlichen Ordnungsmerkmale nicht „durch die Hintertür“ eingeführt werden. Bei der angestrebten breiten Verwendungsmöglichkeit der Versicherungsnummer ist diese Gefahr nicht von der Hand zu weisen, da sie auch für den gesamten Bereich der gesetzlichen Krankenversicherung, der Unfallversicherung und für alle Aufgaben der Arbeitsverwaltung verwendet werden soll.

Der Landesbeauftragte hat seine Bedenken vorgetragen und hofft, daß es hier noch zu einer Einschränkung des vorliegenden Gesetzentwurfes kommt.

4.6 **Kulturbereich**

4.6.1 **„Datenschutzunfall“ als Unterrichtsgegenstand**

Im Rahmen der Auseinandersetzung mit modernen Techniken der Informationsverarbeitung sollten in einer Mittelstufenklasse einer allgemeinbildenden Schule anhand von Fragebögen das persönliche Freizeitverhalten der Schüler (Beschäftigung mit Musik, Sport, anderen Hobbys, Diskothekenbesuch, Gammeln u. a. m.) ermittelt und die Ergebnisse in einem Personalcomputer gespeichert und ausgewertet werden. Durch die Ankündigung einer personenbezogenen Veröffentlichung der Ergebnisse am „Schwarzen Brett“ der Schule sollte sodann eine persönliche Betroffenheit bei den Schülern ausgelöst werden. Sie sollte es erleichtern, die rechtlichen Grundlagen und die Organisation des Datenschutzes im Unterricht zu erläutern.

Der Landesbeauftragte ist der Bitte um Beratung bei der Entwicklung der Unterrichtseinheit gern nachgekommen. Er

hat aber Zweifel angemeldet, ob die Methode, Problembewußtsein durch persönliche Betroffenheit zu erzeugen, in diesem Bereich pädagogisch und rechtlich vertretbar ist. Es schien ihm gefährlich, die Notwendigkeit ausreichenden Datenschutzes anhand einer echten Datenschutzverletzung deutlich zu machen. In jedem Fall muß bei derartigen „Feldversuchen“ die Freiwilligkeit der Teilnahme durch Eltern und Schüler ausdrücklich bestätigt werden.

Dieses Beispiel macht nach Auffassung des Landesbeauftragten aber auch deutlich, daß Datenverarbeitung in Schule und Berufsausbildung nicht nur als eine mathematisch-naturwissenschaftliche Technik dargestellt werden sollte. Es müssen auch ihre darüber hinausgehenden gesellschaftlichen Auswirkungen erörtert werden. Datenschutz ist ein Regulativ unserer Technologiesellschaft und kann nicht rechtzeitig genug als „die andere Seite der Medaille“ erläutert werden. Dieser pädagogischen Aufgabe sollten sich die zuständigen Stellen für die Lehrerausbildung und für die Praxis und die Theorie in der Schule, vor allem aber auch die Schulen selbst annehmen.

4.6.2 Hochschulinterna im Altpapierbehälter

Nicht immer wurden in der Vergangenheit geeignete Maßnahmen getroffen, um die notwendige Sicherheit und Sorgfalt bei der Vernichtung von überflüssigem Datenmaterial zu gewährleisten (vgl. 4. TB, S. 44; 5. TB, S. 45). Es wurden Karteikarten mit sensiblen Versicherungsdaten in offenen Containern transportiert, auf der Müllhalde einfach abgekippt und vom Winde in alle Richtungen herumgewirbelt. Ärztliche Unterlagen aufgelöster Krankenhäuser in offenen Kellern wurden zur interessanten Lektüre für die Handwerker in der Mittagspause. Patientenkarteen aus aufgelösten Arztpraxen waren auf Dachböden und in Vorgärten „zwischenlagert“. Veraltete Dateiausdrucke der Finanzämter mit Steuerdaten der Bürger boten – weil sie auf der Straße lagen – einen sehr informativen Lesestoff. Die Reihe dieser Datenschutzunfälle ließe sich fortsetzen. Im Verlauf der neunjährigen Tätigkeit des Landesbeauftragten hat fast jeder Verwaltungsbereich Anlaß zur Kritik gegeben. Zur Verteidigung beriefen sich die Verantwortlichen zwar nicht auf den frischen schleswig-holsteinischen Wind, aber darauf, daß es sich nur um „einen bedauerlichen Einzelfall“ gehandelt habe und man künftig die Einhaltung der selbstverständlich vorhandenen Anweisungen überwachen werde. Der Datenschutzbeauftragte steht dann jedes Mal vor der Entscheidung, ob er sich mit einer solchen Erklärung zufriedengeben oder ob er wegen eines erheblichen Verstoßes gegen das Gebot der Datensicherheit eine Beanstandung aussprechen und die betreffende Fachaufsichtsbehörde benachrichtigen soll, um seiner Forderung nach mehr Datensicherheit noch mehr Nachdruck zu verleihen.

Vor diese Frage sah sich der Landesbeauftragte auch im Berichtsjahr gestellt, als er der Presse entnehmen konnte, daß eine Hochschule Listen von Seminarteilnehmern, Lebensläufe von Doktoranden und weitere Sammlungen von Studentendaten in einem Container zusammen mit Verpackungsma-

terial, Zeitungen, Broschüren bis zum Abtransport zur Vernichtung so aufbewahrte, daß jedermann Zugriff hatte. Auch dies wieder nur ein bedauerlicher Einzelfall, wie die speichernde Stelle behauptete?

Für den Datenschutzbeauftragten verstärkt sich immer mehr der Eindruck, daß diese „Unfälle“ bei der Vernichtung überflüssiger Datenträger und Datensammlungen nur „die Spitze eines Eisberges“ sind. Er wird deshalb künftig von seinem Beanstandungsrecht stärker Gebrauch machen und die zuständigen Aufsichtsbehörden unterrichten (vgl. auch Tz. 4.1.3.5).

4.6.3 **Denkmalschutz versus Datenschutz?**

Die Denkmalschutzbehörden erfassen eine Vielzahl von Baudenkmalen. Neben einer Abbildung und einer Beschreibung des Objekts werden auch die Belegenheit und die Eigentumsverhältnisse gespeichert. Aus dieser Kartei fließen Informationen an die Gemeinden, die Bauämter und an die obere Denkmalschutzbehörde. Die Daten sollen bei Überlegungen zur Ortsplanung bzw. in Baugenehmigungsverfahren und bei der Entscheidung über die Aufnahme von „Kulturdenkmälern von besonderer Bedeutung“ in das Denkmalsbuch und die Denkmalliste Verwendung finden. Mit den Eigentümern wird zwar üblicherweise Kontakt aufgenommen, jedoch wird zunächst kein förmliches Verfahren durchgeführt und keine Einwilligung zur Datenspeicherung gefordert.

Nach Ansicht des Landesbeauftragten entsprechen die Regelungen im Gesetz zum Schutz der Kulturdenkmale nicht den datenschutzrechtlichen Anforderungen an die Normenklarheit eines Gesetzes, das so tiefgreifende Einwirkungen auf die Rechtssphäre betroffener Bürger vorsieht. Zwar kann aus den Vorschriften hergeleitet werden, daß die Nutzung personenbezogener Grundeigentümerdaten für den Schutz von „Kulturdenkmälern von besonderer Bedeutung“ erforderlich ist. Dagegen hat die praktizierte dateimäßige Erfassung „sonstiger Kulturdenkmale“ mit Personenbezug in den genannten Vorschriften überhaupt keine Rechtsgrundlage. Für die Aufnahme solcher Baulichkeiten in ein „Denkmalkataster“ unter Nennung des Eigentümers bedarf die untere Denkmalschutzbehörde daher der Einwilligung des betroffenen Eigentümers.

Dem kann nicht entgegeng gehalten werden, daß es hier keine Belastung des Eigentümers gebe, weil aus der karteimäßigen Erfassung keinerlei Rechtsschmälerung für den Eigentümer folge. Abgesehen davon, daß nach der neueren Rechtsprechung des Bundesverfassungsgerichts schon jede Speicherung personenbezogener Daten in Dateien in die Rechtssphäre der Betroffenen eingreift, erfolgt hier sowohl die Speicherung als auch die Übermittlung von Informationen gerade zu dem Zweck, in besonderer Weise planen und bei baulichen Änderungen ggf. intervenieren zu können. Damit geht die karteimäßige Erfassung der Baudenkmale über den Charakter einer bloßen Registrierung hinaus.

Der Landesbeauftragte hat sich an den Kultusminister gewandt und gefordert, das Denkmalschutzgesetz unter Einbe-

ziehung von Regelungen zum Schutz der betreffenden Eigentümer normenklar zu gestalten. Sollte die Erfassung der „sonstigen Kulturdenkmale“ auch in Zukunft erforderlich sein, wären auch insoweit einwandfreie Rechtsgrundlagen zu schaffen.

4.6.4 **Datenschutz und Forschungsfreiheit - die Rechtsprechung hat Position bezogen**

„Zwischen Wissenschaftsfreiheit und Datenschutz besteht ein Interessengegensatz. Er ist Ausfluß des Strebens von Wissenschaft und Forschung nach umfassender Information einerseits und dem Ziel des Datenschutzes nach Sicherung des individuellen Persönlichkeitsrechtes andererseits.“

Mit diesen Ausführungen im 2. Tätigkeitsbericht (S. 23) hat der Landesbeauftragte schon im Jahr 1979 auf das Spannungsverhältnis zwischen Datenschutz und Wissenschaftsfreiheit hingewiesen. Veranlaßt durch Beschwerden der Bürger und durch Beratungersuchen von Behörden, die von Forschungsinstituten zur Lieferung von Daten gedrängt wurden, aber auch durch die Kritik von Forschungsstellen an einer „vom Datenschutz verschuldeten Abschottung“ hat der Landesbeauftragte nahezu in jedem Tätigkeitsbericht zu dieser Thematik Stellung nehmen müssen. Oft sah er sich zu dem Hinweis veranlaßt, daß Geheimhaltungs- und Verschwiegenheitspflichten der Übermittlung von Daten zu Forschungszwecken entgegenstehen. Er hat deshalb stets gefordert, daß Daten der Bürger, die an Einrichtungen der Forschung gegeben werden, vorher zu anonymisieren sind oder daß eine schriftliche Einwilligung des Betroffenen nach angemessener Aufklärung einzuholen ist. Der hohe Rang des Zweckbindungsgebotes für zwangsweise erhobene und insbesondere für die dem Staat freiwillig zur Verfügung gestellten Daten ist durch das Bundesverfassungsgericht im Volkszählungsurteil bekräftigt worden. Jede Zweckentfremdung personenbezogener Daten berührt das informationelle Selbstbestimmungsrecht des Bürgers.

Dennoch werden die Stimmen in Forschung und Wissenschaft lauter und kritischer, die den Datenschutzbehörden eine Beeinträchtigung der Forschungsfreiheit vorwerfen. Zwar wird der Datenschutz grundsätzlich als wichtig eingeschätzt. Wenn es aber um die Übermittlung von personenbezogenen Daten der Verwaltung an die Forschungseinrichtung geht, hält man sich für legitimiert, dem eigenen Informationsanspruch ein Übergewicht im Verhältnis zu den Persönlichkeitsrechten der Betroffenen zu verleihen.

Um die Situation der Wissenschaft besser nachvollziehen zu können, hat der Landesbeauftragte ein Gutachten zu den datenschutzrechtlichen Aspekten sozialwissenschaftlicher Forschung auf der Grundlage personenbezogener Ausgangsdaten eingeholt. Der Gutachter kommt zu dem Ergebnis, daß gerade aus der Interessenlage der Sozialwissenschaft heraus (z. B. bei der Stichprobenziehung) die Übermittlung von Adreßdaten und ggf. weiterer personenbezogener Daten aus den Melderegistern und deren anschließende „Bearbeitung“ unverzichtbar

sei. Die vorherige Festlegung der Zielpersonen garantiere am ehesten die Einhaltung der Regeln der Zufallsauswahl, schalte die Willkür des Interviewers bei der Auswahl der endgültigen Zielperson aus, ermögliche eine wirksame Kontrolle des Interviewers und senke die Ausfallquote drastisch. Der vom Landesbeauftragten als Ersatz für die personenbezogene Übermittlung vorgeschlagene „Forschungsbrief“ sei zum Erreichen dieser Ziele nicht geeignet. Solle die ausgewählte Zielperson anschließend befragt werden, könne sich die dafür einzuholende schriftliche Zustimmung negativ auf die Bereitschaft zur Teilnahme auswirken. Das gleiche gelte für die geforderten Begleitinformationen, wenn diese über Zweck, Ziel und Sicherungsmaßnahmen zu detailliert aufklären. Auch die wissenschaftliche Bearbeitung der erhobenen Daten müsse bis zum Abschluß der Primärauswertung in personenbezogener Form vorgenommen werden, nur so seien die notwendigen Ausfallanalysen und Plausibilitätskontrollen durchführbar.

Diese auf den ersten Blick durchaus gewichtigen Argumente stehen in einem nicht unerheblichen Gegensatz zu einer Entscheidung des Bundesverwaltungsgerichts vom 9. Oktober 1985, die durch einen Beschluß des Bundesverfassungsgerichts bestätigt worden ist. Dort heißt es:

„Das Grundrecht der Freiheit von Wissenschaft und Forschung in seiner Funktion als objektivrechtliche Wertentscheidung ... begründet nur die Verpflichtung des Staates, Wissenschaft und Forschung durch Bereitstellung von personellen, finanziellen und organisatorischen Mitteln zu ermöglichen und zu fördern, also funktionsfähige Situationen für einen freien Wissenschaftsbetrieb zur Verfügung zu stellen. ... Das Grundrecht auf Wissenschaftsfreiheit vermittelt keinen verfassungsrechtlichen Anspruch auf Akteneinsicht zu Forschungszwecken.“

Damit hat die Rechtsprechung nach Auffassung des Landesbeauftragten der Diskussion um einen möglicherweise bestehenden Entscheidungsspielraum der Verwaltung bei der Herausgabe personenbezogener Daten zu Forschungszwecken ein Ende gesetzt.

Zwar könnte durch den Gesetzgeber ein Ausgleich zwischen den teilweise in Konflikt zueinander stehenden Grundrechtspositionen des Persönlichkeitsschutzes und der Wissenschaftsfreiheit vorgenommen werden. Dabei kann aber nach Meinung des Landesbeauftragten der hohe Wert des Persönlichkeitsschutzes nicht unberücksichtigt bleiben. Deshalb müssen „Forschungsklauseln“ als verfassungsrechtlich bedenklich angesehen werden, wenn sie die Interessen der Forschung privilegieren und die schutzwürdigen Belange des Betroffenen zu gering gewichten. Der Landesbeauftragte hat daher auch an der im Entwurf zur Novellierung des Bundesdatenschutzgesetzes vorgesehenen Forschungsklausel Kritik geübt, weil die sehr unbestimmte Voraussetzung „berechtigtes Interesse der Allgemeinheit“ ausreichen sollte, um Daten ohne Einwilligung der Betroffenen zu wissenschaftlichen Zwecken zu verarbeiten. Dem verfassungsrechtlichen Rang des Persönlichkeitsrechtes wäre es nach Auffassung des Landesbeauftragten

angemessener, wenn eine Forschungsklausel die Einwilligung zum obersten Prinzip machen und nur in ganz wenigen Einzelfällen unter Einhaltung besonderer Schutzvorkehrungen Ausnahmen zulassen würden. Dieser Grundsatz müßte auch seinen Niederschlag finden in dem noch zu schaffenden Landesarchivgesetz, dem Landesstatistikgesetz, dem Gesundheitsdienstgesetz, einem eventuellen Krankenhausgesetz usw. Damit wären die Wissenschaftsklauseln wirkliche Schutzvorschriften und nicht faktisch Datenübermittlungsnormen, die unter der Überschrift „Datenschutz“ die durch die Rechtsprechung gezogenen Grenzen wieder erweitern.

Die Entscheidung des Bundesverfassungsgerichts zum Vorrang des allgemeinen Persönlichkeitsrechts kann nach Meinung des Landesbeauftragten auch nicht ohne Auswirkungen auf die Anwendung des Landesmeldegesetzes bleiben. Sowohl bei der Prüfung eines „öffentlichen Interesses“ – dann dürfen Meldedaten „über eine Vielzahl nicht namentlich bezeichneter Einwohner“ auch an private Forschungseinrichtungen übermittelt werden – als auch bei der Beurteilung der Frage, wann Meldedaten der rechtmäßigen Aufgabenerfüllung staatlicher Hochschulen dienen, darf nicht auf die pauschale Aussage abgestellt werden, daß wegen der Forschungsaufgabe eines Hochschulinstituts diese Voraussetzungen generell erfüllt seien. Wegen der weitgefächerten und unterschiedlichen Aufgabenstellungen öffentlicher und privater Forschungsinstitute und der immer stärker angestrebten Kooperation zwischen den Hochschulen und der Wirtschaft rät der Landesbeauftragte zu einer zurückhaltenden Praxis. Die Festlegung einheitlicher Kriterien zur Ausfüllung der unbestimmten Rechtsbegriffe „öffentliches Interesse“, „zur rechtmäßigen Aufgabenerfüllung erforderlich“ und „Nichtbeeinträchtigung schutzwürdiger Belange“ erscheint dringend geboten (vgl. auch 8. TB, S. 13 und 15).

Der Landesbeauftragte hält es für einen ersten Schritt in die richtige Richtung, daß der Innenminister die Meldebehörden angewiesen hat, in Zweifelsfällen seine Stellungnahme einzuholen.

5. Prüfungen

5.1 Umfang und Schwerpunkte der Prüfungsmaßnahmen

In seinem letzten Tätigkeitsbericht hat der Landesbeauftragte bedauert, daß er durch verschiedene Umstände daran gehindert war, in ausreichendem Umfang datenschutzrechtliche Prüfungen „vor Ort“ durchzuführen (vgl. 8. TB, S. 60). Um so mehr war ihm in diesem Berichtszeitraum daran gelegen, nicht nur auf „Anstöße von außen“ zu reagieren, sondern durch Kontrollbesuche bei den speichernden Stellen auch unmittelbar zu agieren. Das ist wegen erneut eingetretener personeller Engpässe nicht in einem befriedigenden Umfang gelungen. Die Zielvorstellungen des Landesbeauftragten werden erst dann erreicht werden können, wenn seine Dienststelle mit einem Mitarbeiterstab besetzt ist, der über einen hinreichend großen Erfahrungsschatz nicht nur in daten-

schutzrechtlicher, sondern – wegen der raschen Ausbreitung der Bürokommunikation – auch in technisch-organisatorischer Hinsicht verfügt. Der häufige Personalwechsel in jüngster Zeit wirkte sich wegen der erforderlichen Einarbeitungszeit von ein bis zwei Jahren für neue Mitarbeiter insoweit negativ aus.

Der Landesbeauftragte hat sich deshalb bei seinen Prüfungsmaßnahmen zunächst schwerpunktmäßig auf zwei Komplexe konzentriert. Zum einen wurde bei verschiedenen Gesundheits- und Sozialbehörden die Schnittstelle zwischen der Leistungsverwaltung und der Eingriffsverwaltung untersucht; über die Ergebnisse wird unter Tz. 5.2 berichtet. Zum anderen hat er sich erneut besonders intensiv mit den Fragen im Zusammenhang mit dem Test, der Freigabe und der ordnungsgemäßen Anwendung von Computerprogrammen befaßt (vgl. insoweit Tz. 5.3).

5.2 **Prüfungen im Bereich der Jugend-, Sozial- und Gesundheitsämter**

5.2.1 **Allgemeines**

Was kann mit den Informationen geschehen, die ratsuchende Eltern bei Erziehungsschwierigkeiten den Jugendämtern oder betreuungsbedürftige Suchtkranke den Gesundheitsämtern freiwillig zur Verfügung stellen? Können den Betroffenen aus diesen Offenbarungen Nachteile erwachsen, wenn die Daten in Zwangsverfahren „von Amts wegen“ genutzt werden? Das stellte sich als die zentrale Frage bei Prüfungen heraus, die der Landesbeauftragte im Bereich der Jugend-, der Gesundheits- und der Sozialämter durchführte. Die unter Tz. 3 dargestellten Datenschutzprobleme im Übergangsbereich zwischen Leistungs- und Eingriffsverwaltung sind also nicht nur Theorie.

Die Problematik folgt unmittelbar daraus, daß bei den betreffenden Behörden verschiedene Aufgaben organisatorisch und personell zusammengeführt werden. Es werden durchweg sowohl Funktionen der Beratung wahrgenommen als auch vorbereitende Schritte und endgültige Entscheidungen für zwangsweise Maßnahmen durchgeführt. Beispielsweise können sich aus einer freiwillig in Anspruch genommenen Erziehungsberatung im Jugendamt über schon etwas „institutionalisierte“ Erziehungsmaßnahmen in sozialen Gruppen oder einer Erziehungsbeistandsschaft nach dem Jugendwohlfahrtsgesetz letztlich Anzeigen an das Vormundschaftsgericht ergeben, die unter Umständen sogar in die Entziehung des elterlichen Sorgerechts einmünden. Aus einer freiwilligen sozialpsychologischen Beratung durch ein Gesundheitsamt kann sich bei Gefahr für den Betroffenen oder die Allgemeinheit eine Zwangsunterbringung in einem Landeskrankenhaus nach dem Gesetz für psychisch Kranke entwickeln. Ein Antrag auf Sozialhilfe kann durch bloße Überleitungsanzeige des Sozialamtes den Übergang einer Forderung des Antragstellers gegen Unterhaltsverpflichtete an das Sozialamt zur Folge haben.

Begünstigt wird diese Arbeitsweise auch dadurch, daß oft dieselben Mitarbeiter für die verschiedenen Aufgabenbereiche zuständig sind und außerdem die vorhandenen Informationen einheitlich gespeichert und genutzt werden. So wurden

in einem Jugendamt Angaben, die zunächst freiwillig vom Erziehungsberechtigten für unterstützende Maßnahmen dieser Stelle gegeben wurden, „selbstverständlich“ gegenüber dem Vormundschaftsgericht verwendet. Der Krankheitszustand einer Mutter wurde beispielsweise bei einer Erziehungsberatung bekannt. Er wurde sodann verwendet, um gegen den Willen der Mutter einen Antrag auf Entziehung des Sorgerechts beim Vormundschaftsgericht zu begründen, als die alleinerziehende Mutter einen Kuraufenthalt antreten mußte.

Bei einem Gesundheitsamt wurde eine sog. Zentralkartei geführt, in der, auf die einzelnen Personen bezogen, nahezu alle Erkenntnisse, über die das Gesundheitsamt verfügte, zusammengefaßt waren. Das hatte zur Folge, daß sogar polizeiliches Eingreifen bei einem Familienstreit, der bei einer Beratung bekanntgeworden war, für eine „Gesamtbetrachtung“ des Betroffenen zur Verfügung stand.

Diese Feststellungen bestärken den Landesbeauftragten in seiner Forderung, auch in der Verwaltungspraxis das vom Bundesverfassungsgericht herausgestellte Prinzip der Zweckbindung der personenbezogenen Daten zu beachten. Daraus folgert seines Erachtens:

- Die Speicherung freiwillig offenbarter personenbezogener Daten ist auf das zu beschränken, was für die Beratung oder die Entscheidung über einen Antrag im Einzelfall unbedingt erforderlich ist.
- Dem Betroffenen gegenüber ist deutlich zu machen, für welche Zwecke die Angaben benötigt werden, ob sie noch weiter verwendet werden sollen und ob sie ggf. weitergegeben werden (müssen). Nur wenn er über das Schicksal seiner Daten informiert ist, kann er rechtswirksam in ihre Nutzung einwilligen.
- Aus datenschutzrechtlichen Gründen ist anzustreben, die Aufgaben der gewährenden Verwaltung und die der eingreifenden Verwaltung zu trennen. Wenn das aus fachlichen, organisatorischen oder personellen Gründen nicht möglich ist, sollten jedenfalls die Datenbestände der einzelnen Aufgabenbereiche voneinander getrennt werden.
- Informationen im Bereich der Leistungsverwaltung sollten möglichst immer freiwillig erhoben werden. Muß die Behörde ausnahmsweise von Amts wegen, z. B. durch Auskünfte Dritter, ermitteln (was im Rahmen der Sozialhilfe zugelassen ist), so sollte sie von dieser Befugnis erst Gebrauch machen, wenn der Betroffene nicht in der Lage ist, die erforderlichen Angaben zu machen. Er sollte von der beabsichtigten Maßnahme vorher unterrichtet werden.
- Ist eine anderweitige (zweckfremde) Nutzung freiwillig gegebener Daten notwendig, so setzt das eine Einwilligung oder eine gesetzliche Grundlage voraus. Letztere muß den Grundsätzen der Normenklarheit und der Verhältnismäßigkeit entsprechen und den Betroffenen bekanntgegeben werden.

- Bei der Beurteilung der Rechtslage und der Sachverhalte muß stets eine gewissenhafte Güterabwägung zwischen dem Eingriffszweck und dem Geheimhaltungsinteresse des Betroffenen vorgenommen werden.

5.2.2 Einzelne Feststellungen

Die bei den Prüfungen festgestellten Sachverhalte haben einmal mehr auf bekannte Schwächen im Umgang mit personenbezogenen Daten hingewiesen. Sie lassen sich drei Bereichen zuordnen:

- Datenspeicherung und -austausch über das Maß des im Einzelfall Erforderlichen hinaus,
 - Datenspeicherung und -austausch ohne erkennbare oder den Beteiligten bekannte Rechtsgrundlage und
 - Mängel bei der Verwahrung personenbezogener Daten.
- Sowohl im geprüften Gesundheitsamt als auch im Sozialamt werden Vordrucke verwandt, mit denen eine Fülle von Informationen bei den Betroffenen abgefragt werden können. Selbst einem Amtsarzt erschienen viele Fragen (z. B. nach dem Namen, dem Beruf und der Staatsangehörigkeit des Partners im Vordruck zur Schwangerenberatung nach § 218 b Strafgesetzbuch) zu weitgehend. Weil der Vordruck aber nun einmal so gestaltet war, hielt er die Erhebung dieser Daten für verbindlich.
 - Sozialhilfeanträge müssen nur selten vollständig ausgefüllt werden, weil mit ihnen eine Vielzahl von sehr unterschiedlichen Fallgestaltungen abgedeckt wird. Sehr leicht kommt es daher zur Offenbarung von überflüssigen Informationen (z. B. zur Offenlegung der Vermögensverhältnisse nicht unterhaltspflichtiger Schwiegerkinder in einer „Erklärung zur Feststellung der finanziellen Leistungsfähigkeit von Unterhaltspflichtigen“). Es muß eine sorgfältige Beratung der Betroffenen bei der Ausfüllung des Vordrucks verlangt werden, wenn eine Beschränkung des Datenprofils nicht erfolgen kann.
 - Im Jugendamt waren es Mitteilungen aus Strafverfahren, die nach den „Richtlinien über Mitteilungen in Strafsachen (MiStra)“ zulässigerweise zu den Beratungsvorgängen gelangten, dort aber ein Eigenleben entwickelten. Während nach den Richtlinien die Informationen zu vernichten sind, sobald das Gerichtsverfahren abgeschlossen und die gerichtliche Entscheidung vollzogen ist – Auskünfte fließen dann nur noch aus dem Bundeszentralregister –, blieben diese Mitteilungen auf Dauer Bestandteil der Vorgänge. Der Landesbeauftragte hat darauf gedrängt, diese Mitteilungen in einem gesonderten Teil des Vorgangs zu halten und termingerecht zu löschen.
 - Weiter wurde festgestellt, daß alle Informationen – fachlich und organisatorisch gesehen durchaus zweckmäßig – im Familienzusammenhang gesammelt wurden. Die Entwicklungseinflüsse, die elterliches oder geschwisterliches Verhalten auf ein Kind ausüben, sind zum Erkennen und Überwinden von Erziehungsschwierigkeiten sicher von Be-

deutung. Aber es ist wohl kaum zu vertreten, daß Informationen über einen längst verheirateten und aus dem Familienverband ausgeschiedenen Bruder noch immer auf dessen frühkindliche Probleme hinweisen, weil die Eltern heute Erziehungsschwierigkeiten mit der 15 Jahre jüngeren Schwester haben. Auch dürfte es kaum dem Willen der Eltern entsprechen, wenn sich aus einem Beratungsgespräch über ein Kind negative Stellungnahmen im Gutachten über ein anderes ihrer Kinder in einem Jugendgerichtsverfahren ergeben. Auch um die individuellen Ansprüche auf Sperrung und Löschung von Informationen befriedigen zu können, bedarf es hier einer anderen Organisationsform der Vorgänge.

- Vom Gesundheitsamt gingen bei bestimmten Krankheiten regelmäßig Mitteilungen an den „Beauftragten für die systematische Bekämpfung des Typhus, Paratyphus B, sonstiger Salmonellosen sowie der Hepatitis und der Meningitis“. (Diese Aufgabe wird vom jeweiligen Leiter der Abteilung Mikrobiologie am Hygiene-Institut in Kiel wahrgenommen.) Nach dem Bundesseuchengesetz sind meldepflichtige Krankheiten nur dem Gesundheitsamt anzuzeigen. Weitermeldungen an andere Stellen sind im Gesetz nicht vorgesehen.
- Ebenso selbstverständlich war es, jeweils einen Durchschlag der Anträge auf Unterbringung psychisch Kranker in einer Anstalt an das zuständige Sozialamt zu senden. Eine Rechtsgrundlage hierfür besteht nicht. Diese Praxis wurde damit begründet, daß unter Umständen das Sozialamt die Unterbringungskosten übernehmen müsse. Die bloße Möglichkeit einer Kostenübernahme im Einzelfall kann nicht zu einer regelmäßigen Datenübermittlung berechtigen. Selbst in den Fällen, in denen die Kosten übernommen werden, braucht das Sozialamt nicht die ausführliche Begründung für die Unterbringung zu erhalten.
- Schließlich führte auch der wohlmeinende Eifer eines Beraters zu unzulässigen Offenbarungen. Er bemühte sich im Rahmen der Beratung einer psychisch Kranken, bei den Nachbarn um Verständnis für ihre besondere Situation zu werben. Die Nachbarn hatten sich durch das eigentümliche Verhalten der Betroffenen belästigt gefühlt. In diesem Zusammenhang unterrichtete er die Hausbewohner schriftlich von dem Aufenthalt der Betroffenen in einer psychiatrischen Klinik und bat um Rücksichtnahme nach ihrer Entlassung.
- Daß auch das Bestreben nach Verfahrensvereinfachung zum Widerstreit mit Datenschutzerfordernissen führen kann, zeigt die Technik, die ein Sozialamt anwandte, um Bankauskünfte über Sozialhilfeempfänger zu erhalten. Gestützt auf die formularmäßig vom Antragsteller erklärte Freistellung aller seiner Banken vom Bankgeheimnis, fragte das Sozialamt in einem Rundbrief alle Kreditinstitute des Ortes nach Geschäftsbeziehungen mit dem Antragsteller. Es bat, nach entsprechenden Vermerken auf dem Rundbrief, diesen dem nächsten im Verteiler vorgesehenen Bank-

institut zuzuleiten. Daß dieses Verfahren nicht mehr praktiziert wird, betrachtet der Landesbeauftragte als selbstverständliche Folge des geschärften Datenschutzbewußtseins.

- Schließlich mußte der Landesbeauftragte rügen, daß Vorgänge und Archivgut der geprüften Bereiche nicht so verwahrt wurden, daß nur die zuständigen Bearbeiter Zugriff hatten. Unverschlossene Schränke, offene Aufbewahrung in nicht verschlossenen Räumen und gemeinsame Unterbringung mit Unterlagen anderer Verwaltungsbereiche wurden dem besonderen Rang des Patienten- und Sozialgeheimnisses nicht gerecht. Ungeordnete Archivierungen machten darüber hinaus die planmäßige und vorschriftsmäßige Sperrung und Löschung personenbezogener Daten unmöglich.

5.3 **Test, Freigabe und ordnungsgemäße Anwendung von Computerprogrammen**

Die vom Landesbeauftragten in seinem 8. Tätigkeitsbericht (S. 61) vorgebrachten Zweifel an der Wirksamkeit der in der Praxis üblichen Maßnahmen zur Gewährleistung eines ausreichenden Tests, einer kontrollierenden Freigabe und einer ordnungsgemäßen Anwendung von Computerprogrammen haben in den Kreisen der Datenverarbeiter ein unterschiedliches Echo gefunden. Die Resonanz reichte von uneingeschränkter Zustimmung und Bestätigung der geschilderten Schwachstellen bis hin zu Attributen wie „weit übertrieben“. In Gesprächen mit einzelnen Rechenzentrumsleitern wurde ihm zwar bestätigt, es komme immer wieder einmal vor, daß schlecht dokumentierte und unzulänglich getestete Programme eingesetzt würden, für das eigene Rechenzentrum gelte dies jedoch nicht. Im eigenen Zuständigkeitsbereich sei man sehr darauf bedacht, „alles Vertretbare“ zu tun, um eine sichere und richtige automatisierte Datenverarbeitung zu gewährleisten. Schwierig wurden die Gespräche aber stets dann, wenn es um die Frage ging, welche Maßnahmen im konkreten Einzelfall noch als vertretbar und welche als unangemessen zu bezeichnen waren.

Da auch in den Erörterungen mit den Vertretern der Automationskommissionen des Landes und der kommunalen Landesverbände keine übereinstimmende Bewertung der praktizierten Verfahrensweisen erreicht werden konnte, hat sich der Landesbeauftragte entschlossen, eine Art datenschutzrechtliche Bestandsaufnahme für die Bereiche „Test“, „Freigabe“ und „ordnungsgemäße Anwendung“ der Computerprogramme durchzuführen. Er beabsichtigt, bei ca. 8 bis 10 Rechenzentren, EDV-Abteilungen und Anwendern von automatisierten Verfahren die Aufbau- und Ablauforganisation, die bestehenden Verwaltungsanweisungen und die tatsächlichen Verfahrensweisen zu analysieren und datenschutzrechtlich zu beurteilen. Er wird in diesen Querschnitt möglichst alle Organisationsformen und Sachbereiche der automatisierten personenbezogenen Datenverarbeitung im Lande einbeziehen. Im abgelaufenen Berichtszeitraum hat er zunächst das Rechenzentrum der Steuerverwaltung und die EDV-Abteilung einer

mittelgroßen Kommunalverwaltung geprüft. Hierbei sind folgende signifikante Sachverhalte festgestellt worden:

– **Unzureichende Anpassung der Organisationsstrukturen**

Die Organisationsstrukturen der Behörden berücksichtigten nicht hinreichend die Besonderheiten, die bei der Erstellung und dem Betrieb von arbeitsteiligen automatisierten Verfahren auftreten. Wenn auf der sachbearbeitenden Ebene neue technische Spezialfunktionen wie z. B. Systemprogrammierung, Anwendungs- und Organisationsprogrammierung, Datenerfassungs- und Rechenzentrumsbetrieb angesiedelt werden, bedarf es auf den leitenden Verwaltungsebenen adäquater Kontrollfunktionen. Nicht immer war gewährleistet, daß die Fachabteilungen die Maßnahmen des Rechenzentrums bzw. daß die Leiter der EDV-Abteilungen die Arbeit ihrer Programmierer auf ihre sachliche Richtigkeit hin überprüften.

– **Unklarheiten bei der Verfahrensverantwortung**

Obwohl in vielen Verwaltungsbereichen seit nunmehr fast 20 Jahren Verfahrensabläufe automatisiert werden, haften der Datenverarbeitung nach wie vor die Attribute des Außergewöhnlichen, des nicht Beeinflussbaren und des nicht Nachvollziehbaren an. Das führt dazu, daß die Fachabteilungen, die meist nicht über technisch ausgebildetes Personal verfügen, sich im allgemeinen recht wenig um die Inhalte und Formen automatisierter Verfahren kümmern. Faktisch übertragen sie stillschweigend weite Teile ihrer Verfahrensverantwortung auf die Datenverarbeiter. Auch in den bisherigen Prüfungen ließ sich dies feststellen. Bezeichnenderweise war der allgemeine Trend des „Sich-aus-der-Verantwortung-Schleichens“ im Bereich des Kassenwesens aber kaum anzutreffen. Offenbar haben sich hier die seit jeher praktizierten Verfahren der Kassenprüfung, der Rechnungsprüfung und der Innenrevision auch gegenüber den vermeintlichen „technischen Zwängen“ der Datenverarbeitung behaupten können.

– **Technische Systeme schaffen vollendete Tatsachen**

Die Entscheidungsprozesse bei der Einführung neuer technischer Systeme oder automatisierter Abläufe liefen häufig in der verkehrten Reihenfolge ab. Zunächst wurden die Hard- und die Software angeschafft und in der Regel in sogenannten Pilotprojekten eingesetzt und erst dann wurde über die erforderlichen technischen und organisatorischen Maßnahmen entschieden. Die dabei entstehenden Übergangsfristen erstreckten sich meist über Jahre, vorläufige Regelungen erhielten stillschweigend den Status des Endgültigen, vorsorglich besonders streng ausgestaltete Sicherungsmaßnahmen wurden ohne eingehende Risikoanalysen nach und nach immer weiter abgeschmolzen.

– **Rentabilität kontra Verfahrenssicherheit**

Gleichwohl war bei allen Prüfungen die Sorge der Verantwortlichen um einen sicheren und ordnungsgemäßen Ablauf der EDV-Verfahren festzustellen. Es fehlte weder an

Problembewußtsein noch an der Absicht, die bereits bekannten oder durch die Prüfungen aufgedeckten Schwachstellen zu beseitigen. Da aber die betreffenden Änderungen in der Regel nicht ohne Auswirkungen auf die Personal- oder Sachkosten blieben, wurde immer wieder mit den „haushaltsmäßigen Sachzwängen“ argumentiert. Auch wenn sich automatisierte Verfahren in einer kostenmäßigen Konkurrenz zu den von ihnen verdrängten konventionellen Verfahrensabläufen befinden, darf die Rentabilität nicht als wichtiger angesehen werden als die Verfahrenssicherheit; darauf hat der Landesbeauftragte auch im Rahmen der Prüfungen nachdrücklich hingewiesen.

- Verfahrensregelungen werden nicht beachtet

In einem wichtigen Punkt fühlt sich der Landesbeauftragte in seinen bereits früher geäußerten Bedenken bestätigt (vgl. 6. TB, S. 61): Die für die Landesverwaltung verbindliche und von der Kommunalverwaltung als Maßstab akzeptierte „Gemeinsame Geschäftsanweisung für die elektronische Datenverarbeitung“ und die sogenannten „Mindestanforderungen zur Verfahrenssicherheit“ aus den Jahren 1969/1971 werden nicht uneingeschränkt beachtet. Die Regelungen für die Bereiche „Test“, „Freigabe“ und „Dokumentation“ wurden – womöglich weil die Bestimmungen tatsächlich veraltet sind – so „frei interpretiert“, daß dem Landesbeauftragten noch bei keiner Prüfung Programm- und Verfahrensakten vorgelegt wurden, die in jeder Hinsicht den formalen Vorschriften der o. a. Geschäftsanweisungen entsprachen. Er hat die speichernden Stellen deshalb erneut darauf hingewiesen, daß dieser Zustand der „geduldeten Nichtbeachtung“ an sich verbindlicher Verwaltungsanweisungen auf Dauer datenschutzrechtlich nicht hinnehmbar ist.

- Dauerhafte „Vorläufigkeit“ von Dienstanweisungen

Die spezifischen Dienstanweisungen der geprüften Behörden waren – soweit sie überhaupt schriftlich vorlagen – dadurch geprägt, daß viele Regelungen nur einen vorläufigen Charakter hatten, weil an der endgültigen Fassung „noch gearbeitet“ wurde. In einem Fall dauerte der Zustand der Vorläufigkeit bestehender Regelungen und deren Ergänzungsbedürftigkeit schon seit 1974 an. Da die Dienstanweisungen in der Regel gerade von den Mitarbeitern entwickelt wurden, deren Arbeit reglementiert werden sollte, lag es nahe, daß besonders „schmerzhaft“ Komplexe ungeregelt blieben bzw. so formuliert waren, daß ausreichende „Interpretationsmöglichkeiten“ bestanden.

- Privilegien für die Systemprogrammierung

Auffällig war außerdem, daß für die besonders sensiblen Bereiche der Systemprogrammierung und Systemsteuerung im allgemeinen keine umfassenden Dienstanweisungen bestanden. Ein Grund hierfür könnte sein, daß die weisungsbefugten Verwaltungsebenen nur unzureichend über die Aktivitäten und die damit verbundenen Risikofaktoren der

technischen Seite der elektronischen Datenverarbeitung informiert sind. Das würde auch die Tatsache erklären, daß in der Praxis erhebliche Unterschiede zwischen der Dokumentation von Anwendungs- und Systemsoftware bestehen. Wann aus welchem Grund welche Veränderungen an Betriebs-, Datenbank- und Datenfernverarbeitungssystemen vorgenommen wurden, konnte anhand der während der Prüfungen vorgelegten Unterlagen nur sehr viel schwerer nachvollzogen werden als bei den Anwendungsprogrammen.

– Nicht ausreichende Testbestände

Ein immer wieder anzutreffender Mißstand ist der Test der EDV-Programme mit sogenannten „echten Fällen“. Aus „Vereinfachungsgründen“ wurden anstelle von speziellen Testfällen Datensätze aus den Originalbeständen benutzt, um die Richtigkeit der Programme zu überprüfen. Da die Zusammensetzung dieser Daten ganz zufällig war und somit nicht alle denkbaren Fallgestaltungen geprüft werden konnten, blieben Fehler bei den Produktionsläufen nicht aus.

– Unklarheiten über die Funktion der Programmfreigabe

Über die Funktion der Programmfreigabe herrscht bei den datenverarbeitenden Stellen nach wie vor eine weit verbreitete Unsicherheit. Der Landesbeauftragte hat bei seinen Prüfungen Verfahrensregelungen und konkrete Maßnahmen vermißt, die zum Ziel hatten, die Datenverarbeitungsabteilung zu kontrollieren und sie von der Verantwortung der sachlich/rechtlich richtigen Programmgestaltung zu entlasten. Im Rahmen der Programm-/Verfahrensfreigabe muß seines Erachtens

- von einem „EDV-sachverständigen“ Mitarbeiter (wie bei einer Innenrevision) geprüft werden, ob die Computerprogramme in formaler Hinsicht entsprechend den Vorgaben entwickelt und dokumentiert worden sind und
- von der „verfahrenssachverständigen“ Fachabteilung dahin gehend kontrolliert werden, ob sie richtige Ergebnisse erbringen.

– Fehlende Kontrollen

Erfreulicherweise haben beide geprüften Behörden den Zugriff auf die Programme und Daten durch sogenannte Passwords geregelt und gesichert. Leider hat man es dabei bewenden lassen und keine Kontrollen dahin gehend vorgenommen, wie im praktischen Betrieb mit diesen Codewörtern umgegangen wurde. Es ist allgemein bekannt, daß die meisten Versuche, ein EDV-System zu „knacken“, dadurch erfolgreich waren, daß ein Password erraten oder „ausgekundschaftet“ wurde. Trotzdem wurde weder das regelmäßige Wechseln der Passwords noch deren Struktur kontrolliert, noch wurde überprüft, ob nicht z. B. der Mitarbeiter mit der weitestgehenden Zugriffsbefugnis frühmorgens sein Password eingab, um den Kollegen tagsüber das lästige Eingeben ihrer Codewörter zu ersparen.

Als vorläufiges Fazit der Prüfungen in diesem Bereich ist festzustellen, daß bei dem Test, der Freigabe und der Anwendung von Computerprogrammen trotz einer positiven Entwicklung noch nicht der Sicherheitsstandard erreicht ist, der aus datenschutzrechtlicher Sicht wünschenswert wäre. Dies kann aber nur zum Teil den Datenverarbeitern angelastet werden, gefordert sind insoweit auch diejenigen, für die die automatisierten Verfahren entwickelt worden sind. Ob dies als eine allgemeine „Softwarekrise“, die auch zu Lasten der schutzwürdigen Belange der betroffenen Bürger geht, bezeichnet werden muß, werden die nächsten Prüfungen zeigen.

6. Neue Informations- und Kommunikationstechniken

6.1 Beherrschbarkeit und Revisionsfähigkeit der Personalcomputer

Unter Datenverarbeitern gilt die Regel, daß sich die Technik immer vom Primitiven über das Komplizierte zum Einfachen entwickelt. Viele Anzeichen deuten darauf hin, daß sich die Datenverarbeitung im Augenblick in der Übergangsphase vom Komplizierten zum Einfachen befindet. Eines von vielen Merkmalen dafür ist die Tatsache der geradezu explosionsartigen Ausbreitung der Personalcomputer bzw. der gleichartigen, lediglich anders bezeichneten technischen Geräte. Nach einer Diebold-Studie wird erwartet, daß bis Ende der 80er Jahre mehr als 2,6 Millionen Mikrocomputer in der Preisklasse bis 25 000 DM in der Bundesrepublik im Einsatz sein werden. Man könnte fast sagen: „Wir stehen am Vorabend der zweiten Datenverarbeitungsrevolution“. So wie 1967/68 die dritte Computergeneration die damaligen Lochkartenverfahren abgelöst hat, so können in den nächsten Jahren die Techniken und die Software rund um die Begriffe „Officeautomation“ und „Bürokommunikation“ eine neue Dimension in der Datenverarbeitung eröffnen.

Dies ist an sich eine positive Entwicklung. Sie stellt den Datenschutzbeauftragten jedoch vor die Aufgabe, die neuen Gefahrenmomente zu erkennen und zu bewerten. So wie jede Medizin neben dem gewollten therapeutischen Effekt auch schädliche Nebenwirkungen hat, birgt auch die dezentralisierte automatisierte Informationsverarbeitung Risiken des Mißbrauchs und der ungewollten Fehlentwicklungen in sich.

Die Anforderungen an die sicherheitstechnischen Maßnahmen werden maßgeblich durch die Art und den Inhalt der zu verarbeitenden Daten bestimmt. Deshalb kann man auch nicht schematisch feststellen: „Alle Personalcomputeranwendungen sind risikobehafteter als andere EDV-Verfahren“. Den Personalcomputer als Mittel der automatisierten Informationsverarbeitung grundsätzlich abzulehnen, hieße, ein technisches System nur deshalb zu verbieten, weil man sich nicht der Mühe unterziehen will, anwendungsorientierte Sicherungsmechanismen zu entwickeln. Diese müssen allerdings abgestimmt sein auf die Anwendungen, die mit dem Personalcomputer betrieben werden. Dabei ist nicht das grobe Raster gefragt, sondern das feine Filigran. Einige Beispiele: Die Personalcomputeranwendung in einem städtischen Fremden-

verkehrsbüro ist anders zu gewichten als die eines Krankenhauses. Eine Finanzkasse muß bereits aus Gründen der Abwehr von Betrugsversuchen andere Sicherungsmaßnahmen ergreifen, als die Stadtreinigung. Von einem großen Service-Rechenzentrum für das Land und die Kommunalverwaltungen muß man bei Einsatz vernetzter Personalcomputer ein differenzierteres Konzept erwarten als von der öffentlichen Waage, in der abends die Disketten mit den Wiegedaten zusammen mit der Gebührenkasse verschlossen werden.

Auf der anderen Seite ist es denkbar, daß man in bestimmten Bereichen auf den Personalcomputereinsatz ganz verzichtet, weil das nötige Maß an Sicherheit nur mit der Groß-EDV und zentraler „Datenverarbeitungsintelligenz“ zu erreichen ist. Das gilt unter Umständen für die Gesundheits-, Sozial-, Steuer- oder Sicherheitsbehörden oder im militärischen Bereich.

Mit den technischen Voraussetzungen, unter denen Personalcomputer in diesen besonders „sensiblen“ Bereichen eingesetzt werden können, hat sich der Landesbeauftragte bereits in seinem 7. Tätigkeitsbericht (S. 55) beschäftigt. Im abgelaufenen Berichtsjahr hat er sich schwerpunktmäßig mit den Fragen der Beherrschbarkeit und der Revisionsfähigkeit komplexer Personalcomputeranwendungen befaßt. Die Ergebnisse dieser Überlegungen sind in einem Merkblatt zusammengefaßt, das „Praktische Hinweise zur Methodik und Zielrichtung der Prüfung der Sicherheit und Ordnungsmäßigkeit von Personalcomputeranwendungen“ gibt. Dieses Merkblatt stellt der Landesbeauftragte allen Behörden zur Verfügung, die sich mit dem Gedanken tragen, im größeren Umfang Personalcomputer einzusetzen. Es enthält einen Katalog präventiver und repressiver Maßnahmen, deren Ziel es ist, Fehlentwicklungen entgegenzuwirken und bei bereits bestehenden Systemen den Standard der Sicherheits- und Ordnungsmäßigkeitsvorkehrungen auf das erforderliche Maß anzuheben.

6.2 **Datenschutzrechtliche Beurteilung der Telekommunikationsordnung**

In den letzten Jahren hat die Deutsche Bundespost mehrere neue Postdienste eingeführt. Sie plant, künftig alle Dienste auf einem einheitlichen Netzwerk abzuwickeln, so daß sich die Verantwortung für Information und Kommunikation, für ihre Sicherheit und den Schutz personenbezogener Daten im Netz und in den Vermittlungsanlagen mehr und mehr zur Bundespost hin verlagert.

Die Datenschutzbeauftragten von Bund und Ländern haben daher immer wieder ausreichende Datenschutzregelungen bei der Bundespost gefordert (vgl. 7. TB, S. 58). Weil diese Postdienste in steigendem Maße auch von öffentlichen Stellen im Lande Schleswig-Holstein genutzt werden, hat sich der Landesbeauftragte an diesen Gesprächen beteiligt.

Eine Reihe von Anregungen hat der Bundespostminister inzwischen aufgegriffen und 1986 eine Telekommunikationsordnung (TKO) erlassen. Der Landesbeauftragte begrüßt es, daß das bisher zersplitterte und unübersichtliche Fernmelde-recht zusammengeführt worden ist. Für den Bürger werden

die Regelungen übersichtlicher und die Verantwortlichkeit der Bundespost deutlicher. Daß viele bereichsspezifische und damit problemnähere Datenschutzregelungen getroffen worden sind, ist ebenfalls positiv zu bewerten.

Dennoch sind einige Forderungen der Datenschutzbeauftragten nicht berücksichtigt worden. Dazu gehören u. a.:

- Regelung des Datenschutzes direkt im Postverwaltungsgesetz statt in einer Rechtsverordnung. (Es erscheint zweifelhaft, ob die Verordnungsermächtigung in § 14 Postverwaltungsgesetz ausreicht, um grundsätzliche Datenschutzstrukturen zu definieren.)
- Übersichtliche Begriffsbestimmungen für den Datenschutz im Telekommunikationsbereich. (Einige sehr allgemeine Formulierungen in der TKO, z. B. „andere Art der Verarbeitung“, müssen präzisiert werden.)
- Eindeutige Unterscheidung der Datennutzung nach der Art der in Anspruch genommenen Dienste. (Telefondaten dürfen nur für den Fernsprechkreis, Datex-Daten nur für Datex-Dienste, Btx-Daten nur für Bildschirmtext verwendet werden; eine allgemeine Verwendung „für Telekommunikationszwecke“ schafft keine ausreichende Abgrenzung.)
- Aufklärungspflicht der Bundespost über Risiken bei der Benutzung der Postdienste. (Kein technisches System kann verbleibende Risiken aus technischen Pannen, menschlichem Versagen oder strafbaren Handlungen ausschließen; die Bundespost muß auf die spezifischen Gefahren schon bei der Beratung von Interessenten hinweisen.)
- Weitere Detailregelungen zum Datenschutz von Nachrichteninhalten, zur sog. „Fangschaltung“, für Gebührendaten, aber auch im Btx-Dienst erscheinen erforderlich.

Der Landesbeauftragte hat seine Verbesserungsvorschläge dem Chef der Staatskanzlei, dem Innenminister und dem Minister für Wirtschaft und Verkehr als Mitglied des Postverwaltungsrates vorgetragen. Er wird darüber hinaus Risiken, die bei der Nutzung von Postdiensten durch die Datenverarbeitung von Landes- und Kommunalverwaltungen entstehen, beobachten und gegebenenfalls vor einem Anschluß warnen müssen.

7. Zur Verfassungsmäßigkeit des Rechts der Sicherheitsbehörden auf Auskunftsverweigerung

Von grundsätzlicher Bedeutung auch über Schleswig-Holstein hinaus ist die Klärung der Frage, die das Verwaltungsgericht Schleswig dem Bundesverfassungsgericht vorgelegt hat.

Eine Klägerin hatte aus der Presse von Äußerungen erfahren, die den Schluß zuließen, daß die Verfassungsschutzbehörde personenbezogene Daten über sie gespeichert hat. Sie beantragte, über den Inhalt der gespeicherten Daten informiert zu werden, um ihren Lösungsanspruch durchsetzen zu können. Die Behörde lehnte dies unter Hinweis auf ihr Auskunftsverweigerungsrecht nach dem Landesdatenschutzgesetz (§ 14 Abs. 2) ab. Der Landesbeauftragte hat zwar auf Antrag der Betroffenen die Rechtmäßigkeit und Erforderlich-

keit der einzelnen Datenspeicherungen geprüft, war aber durch das Landesdatenschutzgesetz auch an einer Auskunft über den Inhalt der gespeicherten Daten und das Ergebnis seiner Untersuchungen gehindert. Das von der Klägerin ange-rufene Verwaltungsgericht Schleswig, dem die Verfassungs-schutzbehörde wegen des Akteneinsichtsrechts des Klagever-treters ebenfalls nicht mitteilen konnte, um welche Daten es sich handelte, hat schließlich das Verfahren ausgesetzt und die Sache dem Bundesverfassungsgericht vorgelegt. Es soll die Frage entschieden werden, ob § 14 Abs. 2 und 3 Landesdaten-schutzgesetz (dieser Regelung entsprechen Vorschriften im Bundesdatenschutzgesetz und in anderen Länderdatenschutz-gesetzen) mit dem Grundgesetz (Artikel 2 Abs. 1, Artikel 1 Abs. 1, Artikel 19 Abs. 4) vereinbar ist.

In einer vom Bundesverfassungsgericht erbetenen Stellung-nahme hat der Landesbeauftragte Zweifel an der Verfassungs-mäßigkeit der Bestimmung geäußert. Nach der bisherigen Rechtsprechung des Gerichts ist das Recht des Bürgers, selbst zu bestimmen, welche Stelle welche personenbezogenen In-formationen über ihn erhält (informationelles Selbstbestim-mungsrecht), die Konkretisierung der Grundrechte aus Arti-kel 2 Abs. 1 und Artikel 1 Abs. 1 Grundgesetz. Diese Grundrechte kann der einzelne nur dann geltend machen und durchsetzen, wenn er Kenntnis von Eingriffen in seine Rechte erhält. Diese Kenntnis kann er aber oft nur durch eine Auskunft der Behörden über die zu seiner Person gespeicher-ten Daten erlangen. Verweigern die Stellen eine Auskunft, so kann darin ein zusätzlicher Eingriff in seine Rechte liegen.

Deshalb wirft die Anwendung des § 14 Landesdatenschutzge-setz in der Praxis Probleme auf. Aufgrund der Gesetzesmate-rialien und der Kommentierung zu den entsprechenden Vor-schriften der Datenschutzgesetze könnte man zwar zu dem Ergebnis gelangen, daß diese Vorschrift kein generelles Verbot der Auskunft ist, sondern bestimmten Behörden nur die Möglichkeit eröffnen will, eine Auskunft zu versagen. Nach den Erfahrungen des Landesbeauftragten wird sie von den schleswig-holsteinischen Sicherheitsbehörden aber so gehand-habt, daß die Auskunftsanträge zumindest dann grundsätzlich abgelehnt werden, wenn tatsächlich Daten gespeichert sind. Dem Betroffenen gegenüber wird die Entscheidung außerdem nur mit dem Hinweis auf die Rechtslage nach dem Landesda-tenschutzgesetz begründet.

Es gibt zwar Entscheidungen höherer Gerichte in vergleichba-ren Fällen, nach denen bei Auskunftsverweigerungen die maßgeblichen Gründe jedenfalls glaubhaft zu machen sind. Die Sicherheitsbehörden meinen jedoch, daß dies nicht in allen Fällen erforderlich sei und der Wortlaut der Bestimmun-gen im Landesdatenschutzgesetz nicht zu einer Begründung zwingt.

Hier setzen die verfassungsrechtlichen Überlegungen des Da-tenschutzbeauftragten an. Er vermag nicht zu erkennen, warum die Sicherheitsbehörden mit **allen** ihren Aufgaben von einer Auskunftsverpflichtung freigestellt werden müssen und eine Begründung für eine Auskunftsverweigerung nicht zu geben

brauchen. Schon der unterschiedliche Rang der zu schützenden Rechtsgüter zwingt seines Erachtens zu einer Unterscheidung zwischen der Steuerfahndung, der Polizei und dem Verfassungsschutz. Auch innerhalb dieser Stellen erscheint es erforderlich zu unterscheiden, ob z. B. personenbezogene Daten zur Aufklärung eines besonders komplizierten und schweren Steuervergehens oder zur Verfolgung einer relativ belanglosen Steuerstraftat gespeichert werden. Vergleichbare Maßstäbe müßten im Polizeibereich angelegt werden zur Unterscheidung zwischen Fällen der Schwerstkriminalität und fahrlässig begangener Verkehrsdelikte. Im Bereich des Verfassungsschutzes ist schließlich nicht einzusehen, warum einem Bürger die Auskunft über Daten verweigert wird, die im Rahmen einer Sicherheitsüberprüfung, auf seinen eigenen Antrag hin, erhoben worden sind. Eine Gleichbehandlung mit den Fällen, in denen im Bereich der Spionageabwehr verdeckte Beobachtungen erforderlich sind, um Waffengleichheit der Sicherheitsorgane mit den Feinden der demokratischen Staatsordnung zu haben, erscheint unverhältnismäßig. Auch sind innerhalb der verschiedenen Bereiche je nach Situation des Betroffenen noch Unterscheidungen denkbar. Insbesondere nicht gespeicherte Personen könnten aus einer besonderen Situation heraus eine Auskunft erwarten, etwa Bewerber um eine Arbeitsstelle, die wiederholt abgewiesen worden sind und daraus – meist unberechtigterweise – schließen, daß Eintragungen in Dateien der Sicherheitsbehörden dafür maßgeblich gewesen sind. Auch das Alter des Menschen (etwa über 70jährige) kann eine Differenzierung der Auskunftspraxis rechtfertigen. Besonders mißtrauische oder ängstliche Bürger könnten sicher ohne besonderes Sicherheitsrisiko zufriedengestellt werden, wenn ihnen mitgeteilt würde, daß Erkenntnisse über sie nicht vorliegen.

Darüber hinaus bleibt ein Rest von Fällen denkbar, in denen im überwiegenden Interesse der Allgemeinheit eine Auskunft absolut unterbleiben muß und auch eine Begründung für die Auskunftsverweigerung nicht in Betracht gezogen werden darf. Das gilt z. B. immer dann, wenn der begründete Verdacht besteht, daß das Auskunftsrecht nur zum Zwecke der Ausforschung der Sicherheitsbehörden in Anspruch genommen wird.

Aber auch diese Fälle bedürfen einer über § 14 Landesdatenschutzgesetz hinausgehenden gesetzlichen Klärung. Dabei sind unterschiedliche Lösungsansätze denkbar. Das neue hessische Datenschutzgesetz zwingt die Behörden in jedem Fall zu einer Abwägung zwischen dem Grundrecht des einzelnen und dem öffentlichen Interesse (vgl. Tz. 8). Es wäre aber auch eine Organisationsform denkbar, die in anderer Weise die Grundrechte des Betroffenen schützt, wie es etwa das Gesetz zu Artikel 10 Grundgesetz zeigt. Eine andere Alternative könnte darin bestehen, daß die Gerichte, die über Klagen gegen abgelehnte Auskunftersuchen zu entscheiden haben, ein spezielles Einsichtsrecht in die Datenbestände der Sicherheitsbehörden erhalten, wobei sie nicht zu verpflichten wären, die dabei gewonnenen Erkenntnisse in den Gerichtsakten festzuhalten. Damit wäre gewährleistet, daß es keine Datenbestände gibt, die einer richterlichen Kontrolle entzogen sind,

ohne daß die Sicherheitsbelange des Staates beeinträchtigt werden (vgl. insoweit auch Tz. 4.1.5.1 und 4.2.1).

Das Bundesverfassungsgericht hat eine Entscheidung noch nicht getroffen. Sie kann von grundsätzlicher Bedeutung für das Datenschutzrecht über Schleswig-Holstein hinaus sein und wertvolle Hinweise auf den verfassungsmäßigen Rang und die Grenzen des Rechtes auf informationelle Selbstbestimmung bringen.

8. Einheitlichkeit des Datenschutzrechts in Gefahr?

Die Datenschutzgesetze des Bundes und der Länder sind in ihren Grundzügen so ähnlich gestaltet, daß den meisten Bürgern gar nicht bewußt geworden ist, daß es nicht nur ein einziges Datenschutzgesetz, sondern deren zwölf gibt. Die Einheitlichkeit des Datenschutzrechts ist nicht nur für die Arbeit der Datenschutzbeauftragten sehr hilfreich, sie ist schlechthin die Grundvoraussetzung für einen wirksamen Datenschutz. Da die einschlägigen gesetzlichen Bestimmungen als eine Ausprägung der verfassungsmäßig garantierten Persönlichkeitsrechte anzusehen sind, erschiene es dem Landesbeauftragten undenkbar, wenn aufgrund des föderativen Aufbaus der Bundesrepublik diese Rechte in den Datenschutzgesetzen der einzelnen Bundesländer eine unterschiedliche Interpretation erfahren würden. Es ließe sich den Bürgern gegenüber nicht begründen, wenn bei gleichen Datenverarbeitungsprozessen die Risikopotentiale unterschiedlich beurteilt würden und die Kontroll- und Abwehrrechte nicht gleichermaßen wirksam ausgestaltet wären.

Trotz einer Reihe von „Detailnovellierungen“ in einigen Bundesländern hat sich die notwendige Rechtseinheitlichkeit bis jetzt erhalten. Sie droht allerdings auseinanderzubrechen, weil einige Länder von ihrem Recht Gebrauch machen, die von ihnen erkannten Schwachstellen im Datenschutzrecht kurzfristig durch gesetzgeberische Maßnahmen zu beheben, während der Bundestag und die Parlamente anderer Länder einen Handlungsbedarf noch nicht sehen. Insofern ist die Tatsache, daß das Land Hessen im Jahre 1986 ein neues Datenschutzgesetz beschlossen hat, das mit Wirkung vom 1. Januar 1987 in Kraft treten wird, von erheblicher Bedeutung.

Dem Landesbeauftragten liegt es fern, darüber zu befinden, ob der Zeitpunkt und die Art einer Gesetzesnovellierung als richtig und angemessen zu bezeichnen ist. Er sieht es jedoch als seine Pflicht an, den Schleswig-Holsteinischen Landtag über die Konsequenzen zu unterrichten, die sich aus der Entwicklung des Datenschutzrechts beim Bund und in den anderen Bundesländern ergeben. Deshalb werden nachstehend die wesentlichen Neuerungen im hessischen Datenschutzgesetz dargestellt.

- Als grundlegende Änderung gegenüber dem bisher geltenden Datenschutzrecht ist der Wegfall der Beschränkung auf die dateimäßige Verarbeitung der personenbezogenen Daten anzusehen. Die Bürger werden ihre Rechte in Zukunft ungeachtet der Verarbeitungsform der Daten durchsetzen

können. Der Datenschutzbeauftragte braucht seine Kontrolle nicht mehr auf bestimmte Verwaltungsabläufe zu beschränken.

- Dem Ziel einer größeren Transparenz bei der Datenverarbeitung soll der grundsätzliche Anspruch auf Akteneinsicht und Dateiauskunft dienen. Die Akteneinsicht ist nur dann eingeschränkt, wenn z. B. in einer Akte auch Angaben über Dritte enthalten sind und diese Daten nicht abgetrennt werden können. Die Dateiauskunft ist kostenlos. Eine Ablehnung der Einsicht bzw. der Auskunft ist nur im Einzelfall zulässig, wenn „die Rechte des Betroffenen hinter dem öffentlichen Interesse an der Geheimhaltung oder im überwiegenden Interesse Dritter zurücktreten müssen“. Eine generelle Ausnahme für Sicherheits- und Strafverfolgungsbehörden besteht also in Hessen nicht mehr.
- Als ein Kernpunkt der Neuregelung wird die Verpflichtung der Behörden angesehen, grundsätzlich Daten nur beim Betroffenen und stets mit seiner Kenntnis zu erheben. Bevor sich eine Behörde an eine andere öffentliche oder private Stelle wendet, hat sie daher zu prüfen, ob es nicht doch möglich ist, die Angaben vom Betroffenen selbst zu bekommen. Daraus folgt unter anderem, daß künftig in den Formularen nicht wie bisher nur auf die zugrunde liegende Rechtsvorschrift hinzuweisen ist, sondern auch auf den Erhebungszweck und auf eventuelle Datenempfänger. Damit verbunden wurde auch eine wesentliche Verstärkung des Zweckbindungsgrundsatzes.
- Das Gesetz schreibt weiterhin vor, daß die Bürger von der erstmaligen dateimäßigen Speicherung ihrer Daten durch die betreffende Behörde schriftlich zu unterrichten sind.
- Schließlich wird die Berichtigungspflicht der Behörden strenger geregelt. Ist die Berichtigung von Daten bei einer Behörde erforderlich, so müssen von ihr unverzüglich auch sämtliche Stellen unterrichtet werden, die - in welchem Zusammenhang auch immer - die unzutreffenden Informationen erhalten haben. Undokumentierte automatisierte Datenübermittlungen wird es aus diesem Grunde in Zukunft nicht mehr geben können.

Während diese und einige weitere Regelungen in dem neuen Gesetz die Rechte der Betroffenen stärken und die Befugnisse des Datenschutzbeauftragten erweitern, kann nicht übersehen werden, daß im Vergleich zu dem bislang in Schleswig-Holstein geltenden Datenschutzrecht auch Restriktionen eingeführt wurden. Zum einen wird bei Datenübermittlungen an Personen und Stellen außerhalb des öffentlichen Bereichs nur noch eine Globalprüfung der schutzwürdigen Belange anstelle der in Schleswig-Holstein obligatorischen Einzelfallprüfung gefordert. Zum anderen enthält das Gesetz eine sogenannte „Wissenschaftsklausel“, die unter Verwendung recht unbestimmter Rechtsbegriffe letztendlich Datenübermittlungen ohne Einwilligung des Betroffenen an öffentliche und private Forschungsstellen erlaubt. In Schleswig-Holstein unterliegen auch Datenübermittlungen zu Forschungszwecken

der Einzelfallprüfung schutzwürdiger Belange, was auch durch die unter Tz. 4.6.4 dargestellte Rechtsprechung bestätigt wird.

Der Landesbeauftragte wird die Erfahrungen mit den neuen datenschutzrechtlichen Vorschriften in Hessen und die Novellierungsbestrebungen in anderen Bundesländern weiter beobachten.

**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

A

Abgabenordnung s. Steuerverwaltung

Adoptionsdaten VII/13, VIII/65

Adreßbücher

- über Berufsgruppen VI/50
- Straßenverzeichnisse in - IV/11, V/14, VI/10, VII/7
- Veröffentlichung von Einwohnermeldedaten in - s. Meldedaten

Amtshilfe II/9, III/9, V/38, VI/43, VI/57, VII/8

Anschriftenfelder s. Datensicherungsmaßnahmen

Archivwesen

- gesetzliche Regelung des - IV/14, V/29, VI/32, VIII/35
- Nutzungsmöglichkeiten für archivierte Daten II/24, III/12, IV/13, IV/35, V/15, V/29, V/30, VIII/14, VIII/53

Aufsichtsbehörde für den Datenschutz

- Gleichartigkeit datenschutzrechtlicher Problemstellungen bei der III/43, V/44, V/50
- Kontrollanspruch der - in bezug auf privatrechtliche kirchliche Einrichtungen IV/36

Auftragsdatenverarbeitung

- Datensicherungsmaßnahmen bei - II/28, IV/38, IV/41
- Dokumentation von Aufträgen s. Dokumentation
- Einbindung automatisierter Verfahren in die Organisation des Auftraggebers IV/38, IV/41
- Fachamt als behördeninterner Auftraggeber IV/38
- beim Statistischen Landesamt s. Statistisches Landesamt
- Verantwortung der Auftraggeber s. Verantwortung

Aushänge am „Schwarzen Brett“ s. Schüler-, Eltern- und Studentendaten

Auskunftsersuchen mit Begründung VI/19, VI/57, VII/35

Ausländerdaten

- Zentralregister VI/25, VII/18

Ausschüsse s. kommunale Vertretungskörperschaften

Automationskommissionen

- Freigabe von Verfahren durch die - IV/39, VIII/66
- Kontakte des Landesbeauftragten zu den - I/9, II/7

B

- Bausparkassen
- Datenerhebungen der - IV/44
- Beihilfe s. Personaldaten
- Beobachtende Fahndung der Polizeibehörden s. polizeiliche Tätigkeit
- Bereichsspezifischer Datenschutz
- Anforderungen an gesetzliche Regelungen VII/10, VII/14, VII/18, VII/21, VII/51, IX/7, IX/50
- vorrangige Geltung V/5
- Berufsständische Vereinigungen s. Kammern
- Besondere Vertragsbedingungen s. Vertragsgestaltung
- Bewerberkarteien s. Grundstücksinteressenten
- Bildschirmtext s. Medien
- Bundeskriminalamt s. polizeiliche Informationssysteme
- Bundeszentralregister
- Auskunft aus dem - VIII/47
- Löschung von Daten im - II/12
- Mitteilungen der Staatsanwaltschaften s. Staatsanwaltschaften

C

Computerviren VIII/62

D

- Daktyloskopische Daten s. polizeiliche Informationssysteme
- Dateibegriff s. Novellierung des Datenschutzrechts
- Dateienregister I/18, II/26, III/5, III/26, III/38, III/41, IV/32, IV/50, IV/58, V/8, IX/29
- Datenschutzbeauftragte
- im Sozialbereich III/29, IV/31, V/10, V/37, VII/55
- allgemein in den Verwaltungen V/8, VII/55
- Datensicherungsmaßnahmen s. a. Ordnungsmäßigkeit der Datenverarbeitung
- bei Auftragsdatenverarbeitung s. Auftragsdatenverarbeitung
- Begrenzung des Datenprofils bei Datenübermittlungen III/40, IV/22, VII/14, VII/46
- Dokumentation automatisierter Anfragen s. Dokumentationspflichten
- durch Technologiewandel erforderliche Fortschreibung der - I/4, III/45, VII/55, VIII/67, IX/59
- bei neuen Medien s. Medien
- durch organisatorische Maßnahmen IV/38, IV/41, V/9, IX/56
- im Schalterbereich V/21, VIII/46
- Kontrolle der Datenverarbeitung IV/39, IV/40, IX/58
- Versand von Schriftstücken I/11, III/40, IV/28, V/20
- Aufbewahrung und Vernichtung von Unterlagen II/16, IV/40, IV/43, V/45, VIII/45, IX/18, IX/46
- Legitimationsprüfung bei mündlichen Anfragen II/16, III/14, III/32, V/20, V/36
- Vorkehrungen gegen unbefugte Datennutzung und Datenweitergabe IV/44, V/20, V/21, VI/31, VIII/58, IX/23, IX/52, IX/53
- Datenzentrale Schleswig-Holstein
- Vertragsgestaltung bei der Auftragsdatenverarbeitung durch die s. Vertragsgestaltung
- Verantwortung für Programmentwicklung, -pflege und -sicherung s. Verantwortung
- Denkmalschutz IX/47

Dokumentationspflichten

- bei einem automatisierten Datenaustausch III/28, IV/21, IV/30, VI/9, VII/39, VIII/14, VIII/49, VIII/63
- bei eigenem Einsatz von EDV-Systemen III/29, IV/39, VI/62, IX/57
- bei nichtautomatisierter Einsichtnahme in Dateibestände I/15, V/12, VI/59, VIII/14
- bei regelmäßigen Datenübermittlungen VIII/13
- bei der 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

Erkennungsdienstliche Daten s. polizeiliche Informationssysteme

F

Familienverbund im Melderecht s. Kinder

Forschung

- Adressenziehen aus Melderegistern V/12, VII/12, VIII/13, IX/50
 - Verarbeitung medizinischer Daten III/31, V/41, V/49, VI/47, VII/6, VII/35, VIII/55, IX/38
 - Auswertung von Gerichtsakten I/12, IX/30
 - Genehmigung bei der Verwertung von Sozialdaten III/30, IV/31
 - Stellungnahmen zum Spannungsverhältnis zwischen dem Datenschutz und der – II/23, III/31, IV/34, IV/57, IX/48
 - Hinweis auf die Freiwilligkeit bei der Teilnahme an Forschungsvorhaben I/12, II/24, VI/45, VI/50
 - Krankheitsregister V/49, VI/7, VI/47, VII/6, VII/8, VII/53
 - Nutzung von archivierten Verwaltungsdaten s. Archivwesen
 - Verfahren bei der Erhebung von Daten I/12, II/23, IV/34, IV/47
 - Verwertung gesperrter Daten I/12, II/23, III/32, IV/35, V/15, V/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 für Fahrschulen II/18, IX/35
- Funkverkehr VI/31, IX/23

G

Geburtsdaten

- im postalischen Anschriftenfeld I/11
- Veröffentlichung von Jubiläen s. Jubiläumsdaten
- in Wählerverzeichnissen II/10, III/12, VI/24, VII/7
- auf Wahlbenachrichtigungskarten V/22, VI/23, VII/7

Gesundheitsbogen in Schulen s. Schüler-, Eltern- und Studentendaten

Gewerbebeanmeldungen

- Auskünfte aus dem Gewerberegister II/16, VII/36
- Verhältnis des Gewerberegisters zum Handelsregister II/17
- Verwendung der Daten aus Gewerbebeanmeldungen VII/37
- Auskünfte über Reisegewerbetreibende an Berufsgenossenschaften 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

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
- Nutzung für den Denkmalschutz s. Denkmalschutz

Grundstücksinteressenten

- Bewerberkarteien IV/24
- öffentliche Grundstücksvergabe IV/25

H

Hinweise zur Durchführung des Landesdatenschutzgesetzes I/16
Heimatsforschung 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 Anwaltsachen VII/31
- Datenschutz im Strafvollzug VII/32, VIII/44, IX/45, IX/46
- Mitteilungen an die Polizei VII/30
- Grundbuchführung s. Grundbuch
- Mitteilungen in Zivil- und Strafsachen III/25, IV/26, V/33, VI/38, VII/29, VII/30, VIII/40, VIII/41, IX/29
- Schuldnerverzeichnis II/13, II/14, III/25, IV/26, V/33, VIII/41
- Tätigkeit der Staatsanwaltschaften s. Staatsanwaltschaften
- Veröffentlichung von Entmündigungsbeschlüssen IX/30

K

Kammern (berufsständische)

- Datenübermittlungen der - II/26, III/37, VI/50
- Einsichtsrecht in die Handwerksrolle III/37
- Verwertung von Daten aus dem Schuldnerverzeichnis II/13, III/43, IV/26
- gesetzliche Grundlagen III/38
- Ausbildungsregister IX/34

Katasterbuchwerk s. Grundstückseigentümerdaten

Kaufpreissammlung s. Grundstückseigentümerdaten

Kinder

- Auflösung des melderechtlichen Familienverbundes nach Volljährigkeit II/9, V/11
- Speicherung von Daten über - in kriminalpolizeilichen Sammlungen IV/15
- Vernehmung von - VIII/34

Kindergarten

- Umfang zu erhebender Daten V/17

Kindergeld

- Berechnung bei Angehörigen des öffentlichen Dienstes s. Personal-
daten
- Datenabgleich der Arbeitsverwaltung mit öffentlichen Stellen II/9,
VII/16

Kirchen

- kirchliche Einrichtungen II/25, III/35, IV/36
- Sonderstatus der - II/25
- Suchdienst der Kirchen IV/36
- Übermittlung von kirchlichen Daten an die Meldebehörden VI/12,
VII/7, VII/14
- Übermittlung von Meldedaten an die Kirchen II/9, II/25
- Übermittlung von Patientendaten an die - III/36, IV/35
- verfassungsrechtliche Autonomie der - III/36, IV/36

Kommunale Erhebungen auf freiwilliger Basis VII/19, IX/16

Kommunale Vertretungskörperschaften

- Beratung der Fraktionen der - durch den Landesbeauftragten III/8
- Datenübermittlungen zwischen der Kommunalverwaltung und den
IV/12, IV/43, VI/22, VII/17, VIII/8, VIII/18, VIII/19, IX/16
- öffentliche Erörterung von Verwaltungsdaten VI/23, VIII/8
- Veröffentlichung von Stellenplänen VIII/15, VIII/19

Kompetenzgrenzen des Landesbeauftragten II/15, III/7, III/26, III/29,
V/34, VI/40, VII/10, VII/59

Kontrollmitteilungen s. Steuerverwaltung

Kraftfahrt-Bundesamt s. Kraftfahrzeugzulassungsdaten

Kraftfahrzeugzulassungsdaten

- Auskünfte V/36, VII/7, VII/39, IX/36
- Novellierung des Straßenverkehrsgesetzes VII/38, VIII/48
- Einwilligung zur Veräußerung von - I/10
- Anfragen der Polizeibehörden II/18, III/28, IV/21, IV/30, VII/39,
VIII/48, VIII/63
- Umfang zu erhebender Daten V/16, VII/38, VIII/48
- Übermittlung an das Kraftfahrt-Bundesamt III/27
- ZEVIS VII/38, VIII/48, IX/36

Krebsregister s. Forschung

Kriminalpolizeiamt s. a. polizeiliche Informationssysteme und
polizeiliche Tätigkeit

- datenschutzrechtliche Einordnung des - III/13

Kriminalpolizeiliche Sammlungen s. polizeiliche Informationssysteme

Kurgäste s. Fremdenverkehr

L

Landesarchivgesetz s. Archivwesen

Landesmeldegesetz III/8, IV/9, V/11, V/14, VI/8, VI/16, VI/33,
VII/10, VIII/11, VIII/13

- Verwaltungsvorschriften zum - II/8, VIII/13, IX/10

Lehrerdaten III/23, VII/16

Leistungsverwaltung

- Nutzung freiwillig gegebener Daten IX/9, IX/51
- Aufbewahrung IX/10, IX/52, IX/53
- Umfang der Speicherung IX/9, IX/52, IX/53

Liegenschaftskataster s. Grundstückseigentümerdaten

M

Medien

- Bildschirmtext V/52, VI/65, VII/58
- Breitbandkabelnetze VI/66, VII/59
- datenschutzrechtliche Beurteilung der neuen – III/47, IV/46, VI/64, VII/59
- Datensicherungsmaßnahmen VI/64, VII/59
- Datenschutzkontrolle VI/66
- Fernwirk- und Fernmeßdienste VI/68, VII/60
- Telekommunikation allgemein III/46, VII/58, IX/60

Medizinische Daten s. a. Leistungsverwaltung

- Offenbarung an Dritte zu Abrechnungszwecken – VIII/40, VIII/42, IX/38, IX/39
- Auskunft aus eigenen Krankenunterlagen V/40, VII/42, IX/38
- automatisierte medizinische Informationssysteme II/19
- Einwilligung zur Verarbeitung IV/33, V/30, VI/43, VII/41, VII/43, VII/53, VIII/50, VIII/56, IX/37, IX/38, IX/39, IX/52
- gesetzliche Regelungen im Gesundheitsdienstgesetz I/15, IX/41
- medizinische Untersuchungen von Schülern s. Schüler-, Eltern- und Studentendaten
- Mikroverfilmung VIII/54
- Übermittlungen an die Kirchen s. Kirchen
- Mitteilungen an Dritte IX/54
- Übermittlung von Ergebnissen der Röntgenreihenuntersuchungen an den Hausarzt II/20
- Umfang der Übermittlung an Dritte bei Einwilligung VII/42, VII/44, VIII/51
- Übermittlung an die Krankenhausseelsorge III/36, IV/35
- Übermittlung an soziale Leistungsträger und andere Behörden IV/33, VII/6, VII/41, VII/42, IX/37, IX/38, IX/54
- Daten für die Krankenkassen VI/44, VII/45
- Übermittlung von – auf Überweisungsträgern VIII/45
- Verarbeitung in Krankenhäusern V/50, VII/41, VII/49, VIII/54, IX/37
- Verwaltung von Krankenakten VII/48, VIII/52, VIII/53, IX/38, IX/52
- Meldung der Unterbringung psychisch Kranker an die Führerscheinstelle VII/50, VIII/57, IX/40
- Verwertung zu Forschungszwecken s. Forschung
- Erhebung bei den Beratungsstellen nach § 218 Strafgesetzbuch III/30

Melddaten

- Abgleich mit Kindergelddaten s. Kindergeld
- Adressenziehen für Forschungsvorhaben s. Forschung
- Allgemeines zu Auskünften aus den Melderegistern I/14, II/7, III/9, III/41, IV/10, VII/11, VIII/60, IX/10
- Anfragen von Auskunfteien, Versandhäusern und Inkassobüros III/43, IX/10
- Daten der Kinder s. Kinder
- Mitteilungen an Wehrersatzbehörden II/8, III/9
- kirchliche Daten s. Kirchen
- Übermittlung an Parteien VI/13, VII/12
- Sperrung von Altdateien V/15, VI/14, VII/7
- Weitergabe an Bürgermeister und -vorsteher II/9, III/11, IX/11
- Veröffentlichung in Adreßbüchern I/14, II/8, IV/11, V/14, VII/10
- Zugriff der Polizei I/15, III/9, V/12, VI/59, VIII/12, VIII/14

- Zusammenarbeit mit der Presse s. Presse
- Gruppenauskünfte III/10, III/11, VIII/13
- Datensatz IV/9, VI/11, VII/10, VII/11, VIII/11
- regelmäßige Datenübermittlungen VIII/11, IX/10
- Wahrung des Adoptionsgeheimnisses s. Adoptionsdaten
- Melderechtsrahmengesetz II/8, III/8, V/11, VI/17, VII/10
- Meldescheinverordnung VIII/6, VIII/12
- Meldescheine
- Aufbewahrung in Beherbergungsstätten und bei privaten Vermietern VI/10, VII/10, VIII/12, IX/11
- Grenzen des Familienverbundes s. Kinder
- Weitergabe von – an ehrenamtliche Bürgermeister II/9
- Mieterdaten
- gerichtliche Verwertung von – II/15, IV/23
- Mitteilungen an Sozialbehörden VI/38
- Mietwagen
- Personalien der Fahrgäste VII/40
- Mitteilungen in Straf- und Zivilsachen s. Justizverwaltung

N

- Nachrichtendienstliche Informationssysteme s. Sicherheitsbehörden
- Namensnennung
- des Angeklagten auf Zeugenladungen VIII/43
- Novellierung des Datenschutzrechts
- in bezug auf die Datenverarbeitung der Steuerverwaltung s. Steuerverwaltung
- Entwürfe der Bundestagsfraktionen 1980 III/44
- Entwurf der Bundesregierung 1983 VI/69
- Erfahrungen des Landesbeauftragten mit dem Landesdatenschutzgesetz IV/48
- Änderung des Dateibegriffs IV/48, VII/61, VIII/67, IX/64
- Verhältnis zu bereichsspezifischen Lösungen III/44, V/34, VII/62
- Wissenschaftsklausel VI/46, VIII/67, IX/49
- Zeitpunkt der – II/4, II/30, IV/47, VI/69, IX/64
- Zielrichtung der – VII/61, VIII/66, IX/64
- Anpassung an technischen Wandel VII/61, VIII/67

O

- Online-Anschlüsse IV/21, IV/30, IV/50, VI/9, VII/38
- Ordnungsmäßigkeit der Datenverarbeitung s. a. Auftragsdatenverarbeitung, Datensicherungsmaßnahmen und Verwaltungsanweisungen
- allgemeine Feststellungen V/50, VI/60, VII/54, VII/55, VIII/61, IX/55, IX/56
- Aufträge zur Erstellung von Software IV/38
- Test und Freigabe von EDV-Verfahren s. a. Automationskommissionen IV/37, V/50, VI/63, VII/56, VIII/62, VIII/64, IX/57, IX/58
- Fremdsoftware IV/39
- Forderungen an neue EDV-Verfahren VII/16, VII/55
- Ordnungswidrigkeiten
- Inhalt und Aufbau des Anhörungsbogens bei Verkehrs- II/17, III/18, IX/35

P

Parlament

- parlamentarische Behandlung der Tätigkeitsberichte s. Tätigkeitsberichte

- Stellung des Landesbeauftragten gegenüber den Fraktionen des - III/7
- Unterrichtung/Beratung des - V/48, VIII/6
- Patientendaten s. medizinische Daten
- Personalausweisrecht VI/5, VI/14, VI/17, VI/26, VII/14, VIII/40, VIII/49, IX/19
- Personaldaten
 - Abgleich zwischen - und Studentendaten VIII/17
 - Erhebung von Bewerber- und Mitarbeiterdaten IV/26, IV/41, VI/19, VI/20, VI/21, VII/16, VIII/18, IX/14, IX/15
 - Sperrung von - IV/42
 - Grenzen der Speicherung von - IV/25, VI/18, VIII/17
 - Übermittlung IV/25, VI/19
 - Verarbeitung durch automatisierte Verfahren s. Personalinformationssysteme und Telefondatenerfassung
 - Veröffentlichung von - IV/25, VIII/19
 - Zweckbindung der Beihilfedaten VI/18, VII/7
- Personalinformationssysteme
 - datenschutzrechtliche Zulässigkeit von - IV/26
 - Zugangskontrollsysteme IV/26
 - Risiken automatisierter Verfahren VII/15, VIII/16
- Polizeiliche Informationssysteme
 - daktyloskopische Sammlung III/16
 - Grundsätze und Richtlinien für die Führung der - II/12, II/13, III/16, III/17, III/20, IV/15, IV/16, IV/18, IV/55, V/27, VI/30, VII/7, VII/21, VII/23, VII/26, VIII/27, VIII/31
 - erkennungsdienstliche Unterlagen IV/18, V/27, VIII/33, IX/21
 - Löschung von Daten VIII/32, IX/28
 - Kriminalaktennachweis IV/17, V/24
 - Meldedienst „gewalttätiger Störer“ V/24
 - polizeiliche Erkenntnisdatei II/13, III/13, VI/29, VII/26, VIII/34
 - Neukonzeption INPOL III/16
 - Speicherung von Daten über Kinder s. Kinder
 - Spurendokumentationssysteme IV/17, V/23
 - Versetzerkartei VI/7, VI/28, VII/7, VII/24, VIII/31
 - zentrale Sammlungen beim Bundeskriminalamt III/16, III/20, IV/16, IV/17, V/24
 - Speicherung von Suizidversuchen VI/29, VII/7, VII/25, VIII/29
 - Auskünfte an die Betroffenen III/18, IV/16
- Polizeiliche Tätigkeit
 - beobachtende Fahndung II/11, III/15, VIII/27
 - Fehlen konkretisierter Rechtsgrundlagen II/11, IV/15, V/27, VI/17, VI/26, VII/6, VII/20, VIII/25, IX/21, IX/27
 - Informationsgewinnung III/19, IV/20, VIII/26, IX/20, IX/27
 - polizeiliche Auskünfte und deren Verwertung II/17, III/19, III/21, V/26, VII/23, VIII/27, IX/28
 - polizeiliche Befragung nach § 161 Strafprozeßordnung IV/20
 - Rasterfahndung II/11, IV/15, IV/20, VII/22, VIII/27, IX/27
 - Zugriffe auf Kraftfahrzeugregister s. Kraftfahrzeugzulassungsdaten
 - Zugriffe auf Melderegister s. Meldedaten
 - Zusammenarbeit mit der Presse s. Presse
 - Überprüfung von Edelmetallverkäufen VIII/31
- Presse
 - Übermittlung aus Standesamtsregistern IV/12
 - Datenübermittlung der Kommunalverwaltung an die - VIII/14, VIII/20

- Datenübermittlungen der Polizei an die – IV/19, IX/28
- Übermittlung von Jubiläumsdaten s. Jubiläumsdaten
- Übermittlung von Meldedaten IV/10
- Veröffentlichung von Sozialdaten VI/44
- Prüfungsmaßnahmen des Landesbeauftragten
- Allgemeines zur Konzeption der – I/19, IV/37, IV/45, V/44, VIII/60
- im kommunalen Bereich IV/37
- Kompetenz im Bereich der Steuerverwaltung s. Steuerverwaltung
- im Zuständigkeitsbereich des Kriminalpolizeiamtes II/12, III/13
- im Bereich des Klinikums der Christian-Albrechts-Universität V/7, V/48, VI/60
- bei der Verfassungsschutzbehörde V/45, VI/51
- hinsichtlich der datenschutzrechtlichen Verpflichtungen nach § 16 Landesdatenschutzgesetz VII/54
- in der Sozialverwaltung IX/50
- Test, Freigabe und Anwendung von Computerprogrammen IX/50

R

- Rasterfahndungen der Polizeibehörden s. polizeiliche Tätigkeit
- Religionsgesellschaften s. Kirchen
- Reisepaß VI/18
- Röntgenreihenuntersuchungen s. medizinische Daten

S

- Schleppnetzfangung VIII/40
- Schulärztliche Untersuchungen s. Schüler-, Eltern- und Studentendaten
- Schüler-, Eltern- und Studentendaten
- Datenweitergabe an Eltern II/22, III/34, VIII/60
- für Statistikzwecke III/23, III/33
- Gutachten III/35, VI/48, VII/8
- Verkündung von – III/32, V/43
- zur Aufgabenerfüllung der Schule verarbeitete – II/21, III/34, V/42, VI/48, VII/8, VII/51, VIII/58
- Schulfragebogen II/22, III/34, V/42
- Studenten-Operations-Systeme III/33
- schulärztlicher Dienst II/21, III/35, V/42, VII/8, VII/47, VIII/59, IX/40
- Datenaustausch zwischen den Schulen VII/51
- im Unterricht abgefragte Daten VII/52, IX/45
- Schuldnerverzeichnis s. Justizverwaltung
- „Schwarze Listen“
- im Steuerbereich V/35
- über Verkehrssünder III/28
- Sicherheitsbehörden (für den Polizeibereich s. polizeiliche Tätigkeit)
- nachrichtendienstliche Informationssysteme III/21, III/22
- Anfragen aus anderen Ländern VI/53
- Auskünfte an private Stellen VI/57, VIII/22
- Auskünfte über Datenspeicherungen der – I/13, V/47, IX/61
- Datensicherungsmaßnahmen bei – VI/52
- Datenspeicherung und -weitergabe durch – III/21, IV/22, V/45, V/46, VI/51, VI/57, VIII/21, VIII/24, VIII/28
- Löschung von Daten I/13, VIII/23
- Informationsgewinnung der – V/45, VIII/23, VIII/29
- Sicherheits- und Verfassungstreueüberprüfungen durch – V/47,

- VI/53, VI/55, VII/8, VIII/21, VIII/28
- Transparenz bei der Datenverarbeitung der – II/11, IV/22, V/47
- Überwachung der – durch den Landesbeauftragten IV/22, V/45, VI/51, VIII/24
- verdeckte Erkenntnisse VI/59, VIII/26
- Sicherheitsgesetze VIII/6, VIII/21, VIII/24, VIII/28, IX/7
- Software s. Ordnungsmäßigkeit der Datenverarbeitung
- Sozialdatenschutz s. a. Leistungsverwaltung und medizinische Daten
- Befragung von Banken IX/54
- Einwilligung zur Verarbeitung in Sozialleistungsverfahren IV/33, VI/43, VII/44, VII/46, VIII/57, IX/52
- Weitergabe der Daten von Flüchtlingen, Vertriebenen und Aussiedlern zum Zwecke der Betreuung III/31
- Datenspeicherung in privaten Frauenhäusern III/30
- Auskunftspflicht der Antragsteller IV/34, IV/42, VI/43, VII/46
- Übermittlung an Verkehrsaufsichtsbehörden IX/43
- Ausgabe von Warengutscheinen V/39
- Veröffentlichung von Sozialdaten in der Presse s. Presse
- Offenbarung gegenüber Versicherungen VIII/57, IX/44
- Weitergabe von Sozialdaten zu Forschungszwecken s. Forschung
- Auskünfte an Sicherheitsbehörden IV/23, V/38, IX/42, IX/43
- allgemeine Ausführungen zum Sozialgesetzbuch III/29, IV/30, V/7, V/37, VI/43
- Übermittlung von Sozialdaten an Kreiswehrrersatzämter VI/43
- Sozialhilfe s. Sozialdatenschutz
- Staatsanwaltschaften
- Geschäftsstellenautomation der – IV/28
- Mitteilungen an das Bundeszentralregister VII/33
- zentrale Namensdateien der – IV/27
- Standesamtsdaten
- Bekanntgabe von – in der Presse s. Presse
- Berufsbezeichnung in Aufgebotsaushängen IV/10, VI/37
- Datenerhebungen aufgrund von Aufgebotsniederschriften IV/11
- Einwilligung zur Veröffentlichung von – IV/12
- Mitteilungspflichten der Standesbeamten VI/37, VIII/36, IX/24
- Statistiken
- Agrarberichterstattung VI/37
- Arbeitskräftestichprobe VII/28
- Bereinigung V/32
- Handels- und Gaststättenzählung VIII/37, VIII/46
- Hochschulstatistik III/23, VII/28, VIII/38
- Lehrerstatistik III/23, VII/16
- Mikrozensus V/32, VII/27, VIII/36
- Volkszählung V/32, VI/5, VI/7, VI/33, VII/26, VIII/6, IX/24
- Wanderungsstatistik VII/28
- Strafverfolgungsstatistik VII/33, VIII/44
- Datenweitergabe zu Statistikzwecken I/14, VII/28, VII/34, VII/24
- Statistikgesetze III/23, V/32, VI/37, VII/28, VIII/39, IX/24
- Statistisches Landesamt
- Funktion des – als Auftragnehmer und speichernde Stelle III/22
- Steuerverwaltung
- Auskünfte an den Betroffenen II/15, III/26
- Berücksichtigung der Probleme bei der Novellierung des Bundesdatenschutzgesetzes IV/49
- Datenerhebungen und -übermittlungen der – III/26, VI/41, VI/42, VII/35, VIII/46

- Kontrollrecht des Landesbeauftragten II/15, III/26, IV/29, IV/49, V/34, VI/40, VII/34
- Datenabgleich mit kommunalen Steuerbehörden II/16
- Datenaustausch zur Kindergeldberechnung s. Kindergeld
- Veröffentlichung der Dateien der – II/15, V/34
- Kontrollmitteilungen von öffentlichen Stellen an Finanzämter IV/29, V/35, VI/41, IX/33

Strafgefangene s. Justizverwaltung

Strafprozeßordnung VIII/25, VIII/39, VIII/50, IX/26

Studentendaten s. Schüler-, Eltern- und Studentendaten

Suchdienst s. polizeiliche Informationssysteme

Suizidversuch s. polizeiliche Informationssysteme

T

Tätigkeitsberichte des Landesbeauftragten

- parlamentarische Behandlung der – III/6, IV/7, V/7, VI/6, VII/6, VIII/7, IX/8

Technischer Wandel VII/55, VII/62, VIII/67

Telefondatenerfassung IX/12

Telefonische Auskünfte s. Datensicherungsmaßnahmen

Tumorregister s. Forschung

U

Übersicht über gespeicherte Daten III/40, VII/54

V

Verantwortung

- der Anbieter und Hersteller IV/46, V/50
- des Auftraggebers I/19, IV/6, VI/60
- der Fachaufsicht oder des Fachamtes IV/54, V/7, IX/56
- für Freigabe von Programmen s. Ordnungsmäßigkeit der Datenverarbeitung
- der speichernden Stelle V/8, V/50, VII/54
- für Patientendaten in Krankenhäusern s. medizinische Daten
- der Datenzentrale für Programmentwicklung, -pflege und -sicherung VII/62, VIII/65

Verfassungsschutzrecht s. Sicherheitsgesetze

Verkehrsordnungswidrigkeiten s. Ordnungswidrigkeiten

Verkehrszentralregister s. Kraftfahrzeugzulassungsdaten

Verpflichtung auf das Datengeheimnis III/40, IV/32, V/8, V/21

Verschwiegenheitspflichten V/21, V/49, VI/22, VII/31, VIII/10

Versetzerkartei s. polizeiliche Informationssysteme

Versicherungen

- Offenbarung von Sozialdaten s. Sozialdatenschutz
- Versicherungspflicht ehrenamtlicher Bürgermeister IX/18
- Sozialversicherungswahlen IX/44
- Rentenversicherungsnummer IX/45

Vertragsgestaltung

- zwischen Staat und Bürger IV/50
- besondere Vertragsbedingungen für Verträge mit Software-Häusern IV/38, VI/61
- rechtliche und tatsächliche Verhältnisse zwischen Auftragnehmern und Auftraggebern I/19, II/28, IV/40, V/50, IX/18
- schriftliche Fixierung der Datensicherungsmaßnahmen II/29, IV/43, VI/63
- über die Verwaltung personenbezogener Daten bei Auflösung/Zusammenlegung von öffentlichen Stellen VII/49

– mit der Datenzentrale III/14, III/40, IV/40, VII/57

Verwaltungsanweisungen

– bereichsspezifische II/18, IV/32, V/37, VII/18, VIII/6

– interne V/8, VI/52, VI/62, IX/57

Videoaufzeichnungen VIII/60

Volkszählung s. Statistiken

Vordruckgestaltung

– Hinweis auf die Freiwilligkeit der Angaben II/24, III/24, IV/33,
IV/42, V/16, VII/20, VII/47, IX/14, IX/16

– inhaltliche Bestimmtheit aufgrund klarer Rechtsnormen V/16, VI/19

– Umfang des Datenkataloges II/22, V/42, VI/45, VII/36, VII/45,
VII/46, IX/53

W

Wahlen

– Datenübermittlungen an Parteien s. Meldedaten

– Unterstützungsunterschriften VI/24

– Verschwiegenheit der Wahlhelfer V/21

– Wahlbenachrichtigungskarten s. Geburtsdaten

Wählerverzeichnisse

– Auslegung der – 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

ZEVIS s. Kraftfahrzeugzulassungsdaten

Zugangskontrollsysteme s. Personalinformationssysteme

Zusammenarbeitsgesetz s. Sicherheitsgesetze

Zwangsversteigerung

– Namensnennung in der Terminbestimmung VIII/42

Zweckentfremdung von Daten

– Verbot der – IV/49, V/12, VI/18, VII/39