BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG Drucksache **15/5258**

15. Wahlperiode 24.01.96

Der Hamburgische Datenschutzbeauftragte

An die
Frau Präsidentin der Bürgerschaft

Betr.: 14. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten

Gemäß § 23 Hamburgisches Datenschutzgesetz übersende ich der Bürgerschaft den 14. Tätigkeitsbericht*.

Dem Senat leite ich den Tätigkeitsbericht gleichzeitig zu.

Wegen der Haushaltssituation ist der Tätigkeitsbericht im Vergleich zu den Vorjahren aus Kostengründen diesmal um ein Drittel kürzer.

Dr. Schrader

* Verteilt nur an die Abgeordneten der Bürgerschaft

Bürgerschaftsdrucksachen — außer Senatsvorlagen — sind — gedruckt auf chlorfrei gebleichtem Papier — zu beziehen bei: Druckerei Wartenberg & Söhne GmbH, Theodorstraße 41 w, 22761 Hamburg, Telefon 89 97 90-0

14. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten zugleich Tätigkeitsbericht der Aufsichtsbehörde für den nicht-öffentlichen Bereich

vorgelegt im Januar 1996
(Redaktionsschluß: 1. Dezember 1995)

Dr. Hans-Hermann Schrader

Herausgegeben vom Hamburgischen Datenschutzbeauftragten
Baumwall 7, 20459 Hamburg, Tel.: 3504 2044
Auflage: 3.000 Exemplare

Druck: Lübbe & Wulff, 2057 Hamburg

INHALTSVERZEICHNIS

Einzelne Probleme des Datenschutzes im öffentlichen Bereich

14. Tätigkeitsbericht 1995 HmbDSB

14. Tätigkeitsbericht 1995 HmbDSB

Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich

14. Tätigkeitsbericht 1995 HmbDSB

Zusammenfassung wichtiger Punkte

Grundrecht auf Datenschutz Senat und Bürgerschaft haben übereinstimmend erklärt, daß in den Gesetzesbegründungen künftig auf Einschränkungen des Grundrechts auf Datenschutz besonders hingewiesen wird (1.1).

Einwilligung Verwaltung und Wirtschaft weichen vielfach auf die Einwilligung des Bürgers aus, um leichter und umfassender an seine Daten zu gelangen. Bei den Risiken von Fremdbestimmung und Selbstpreisgabe sind Einwilligungen nur dann als rechtswirksam anzuerkennen, wenn sie den rechtsstaatlichen Anforderungen genügen (1.2).

Netzinfrastruktur Den Gefahren, die mit einer flächendeckenden Vernetzung der hamburgischen Verwaltung verbunden sind, muß durch geeignete Sicherheitskonzepte begegnet werden. Ein Anschluß von behördlichen Rechnern an das Internet erfordert den Einsatz von Firewall-Systemen. Sensible Daten dürfen nur verschlüsselt übertragen werden (3.1).

Patientenverwaltungssystem Das System SAP IS-H wird in allen staatlichen Krankenhäusern eingeführt. Der Umfang, in dem Patientendaten erfaßt werden, und die Vergabe der Zugriffsrechte sind problematisch (3.2 und 19.2).

Online-Dienste Durch ein Mediennutzungsgeheimnis im Grundgesetz und durch einen Staatsvertrag sollten die Nutzer von Online-Diensten gegen den Mißbrauch ihrer Daten geschützt werden. Bis zu einer ländereinheitlichen Regelung sind die Landesmediengesetze und damit die Vorschriften des Hamburgischen Mediengesetzes über rundfunkähnliche Dienste einschlägig (4.2).

Sozialdaten auf Überweisungsträgern Die Verwaltung darf nach einer Entscheidung des Bundesverwaltungsgerichts vom Juni 1994 Sozialleistungen auf Überweisungsträgern nicht kenntlich machen (5.8).

Lernausgangslagenuntersuchung bei Schülern Für alle 15.000 Fünftklässler wird durch Testverfahren und Befragungen einschließlich Elternbefragung eine Untersuchung der Lernausgangslage z. B. hinsichtlich Kenntnissen und sozialem Hintergrund vorbereitet. Anstelle des bei der Vorstudie gewählten Verfahrens wäre es datenschutzfreundlicher, wenn die erhobenen Daten den jeweiligen Schülern wesentlich schwerer zugeordnet werden können. Nach geltendem Recht ist für die Hauptstudie ein Gesetz erforderlich (7.2).

Zentrales Fahrerlaubnisregister Die geplante zentrale Registrierung von 50 Millionen Bürgern, die einen Führerschein besitzen, ist abzulehnen. Die Kontrolle von Fahrern ohne Fahrerlaubnis und die Zusammenarbeit zwischen den zuständigen Behörden in der Europäischen Union ist auch ohne dieses Zentralregister möglich (14.2.2).

Parlamentarischer Untersuchungsausschuß „Hamburger Polizei" Das Hamburgische Verfassungsgericht hat in einem Grundsatzurteil, das durch

normative Regelungen umzusetzen ist, die Grenzen einer personenbezogenen Aktenvorlage an Parlamentarische Untersuchungsausschüsse festgelegt (15.1).

Telefonüberwachung Die Staatsanwaltschaft macht von ihrer Befugnis, Telefone abzuhören, großzügig Gebrauch und vernachlässigt dabei die Pflichten zum Schutz der Betroffenen. Trotz der eindeutigen gesetzlichen Anordnung, zur Strafverfolgung nicht erforderliche Unterlagen unverzüglich zu vernichten, werden Überwachungsprotokolle teilweise über ein Jahrzehnt aufbewahrt und sogar an andere Stellen versandt (16.1.2).

Zwangsvollstreckungsnovelle Die Pfändung und Zwangsversteigerung von EDV-Anlagen erfordern bereichsspezifische Vorkehrungen zum Schutz von personenbezogenen Daten des Schuldners und Dritter, die auf den Datenträgern der Anlage gespeichert sind (17.3).

Briefkontrolle im Strafvollzug Die Mitwirkung von Praktikanten an der Briefkontrolle im Strafvollzug muß zum Schutz sensibler Kommunikationsinhalte eingeschränkt werden (18.2).

Chipkarten im Gesundheitswesen Das Selbstbestimmungsrecht der Patienten und die Freiwilligkeit der Nutzung von Chipkarten müssen respektiert werden. Über die Datenschutzanforderungen werden die Bürger mit einem Faltblatt informiert (19.1).

Übermittlung von Patientendaten Eine Abrechnung von Krankenhauskosten mit dem Sozialamt ist nur zulässig, wenn hinreichende Anhaltspunkte für eine Sozialhilfebedürftigkeit vorliegen (19.4).

Elektronische Geldbörse Bei Einführung der elektronischen Geldbörse sollten umfangreiche personenbezogene Datensammlungen in sogenannten Schattenkonten der Kreditwirtschaft vermieden werden. Aus Datenschutzgründen sollte die Kreditwirtschaft auch anonyme Karten einführen (25.1).

BahnCard Gegen die zum 1. Juli 1995 herausgegebenen Antragsformulare der BahnCard mit Kreditkartenfunktion wurden massive datenschutzrechtliche Einwände erhoben. Die Deutsche Bahn AG hat daraufhin die Datenerhebung wesentlich eingeschränkt (26.).

Videoüberwachung in der Wirtschaft Die private Videoüberwachung öffentlicher Wege ist regelmäßig unzulässig und nur bei Gefahren im Einzelfall gerechtfertigt. In keinem Fall dürfen private Stellen die Bürger mit versteckten Kameras überwachen (27.).

1. Zur Lage des Datenschutzes

1.1 Grundrecht auf Datenschutz

Nach den Bemühungen, das Grundrecht auf Datenschutz ausdrücklich in das Grundgesetz aufzunehmen (s. zuletzt 13. TB, 1.1), hatte die Bürgerschaft in ihrem Ersuchen vom 1./2. Februar 1995 an den Senat bedauert, daß die Einigung über dieses Vorhaben bisher gescheitert ist. Sie hat den Senat ersucht, bei geeigneter Gelegenheit seinen Vorstoß wieder aufzunehmen. Außerdem ersuchte die Bürgerschaft den Senat, in allen künftigen Gesetzentwürfen in der Begründung Auskunft über eventuelle Einschränkungen des Datenschutzes zu geben.

Der Senat hat in seiner Stellungnahme vom 25. April 1995 erklärt, daß er zu gegebener Zeit die Frage einer ausdrücklichen Aufnahme des Grundrechts auf informationelle Selbstbestimmung wieder aufgreifen werde. Außerdem hat er angekündigt, daß er gemäß dem bürgerschaftlichen Ersuchen „künftig in der Begründung zu Entwürfen von Landesgesetzen auf etwaige Einschränkungen des Rechts auf informationelle Selbstbestimmung besonders hinweisen" werde (Bürgerschafts-Drucksache 15/3212).

Senat und Bürgerschaft sind damit meinem Vorschlag weitgehend gefolgt. Künftig ist in hamburgischen Gesetzentwürfen ausdrücklich auf Einschränkungen des Datenschutzgrundrechts hinzuweisen. In der Bürgerschaftsdebatte ist dazu erwähnt worden, daß der Senat im jeweiligen Gesetzesvorhaben einen zusätzlichen Abschnitt über den Datenschutz aufnehmen solle, um das Parlament über eventuelle Einschränkungen zu unterrichten.

1.2 Schwerpunkt Datenschutz bei Einwilligung

Der Datenschutz war bisher vorrangig darauf ausgerichtet, den Bürger vor einer unzulässigen Datenverarbeitung von Staat und Wirtschaft aufgrund von Rechtsvorschriften zu schützen. Die gesetzlich geregelten Eingriffsbefugnisse von staatlichen Stellen und die ebenfalls gesetzlich geregelten Befugnisse der Wirtschaft zur Datenverarbeitung standen im Vordergrund, weil sich daraus in erster Linie Gefährdungen für das Recht des einzelnen ergeben konnten, selbst über die Verwendung seiner Daten zu bestimmen. Aufgabe des Datenschutzes war und ist es insbesondere, bei dem Erlaß von Rechtsvorschriften auf eine verfassungskonforme Beschränkung der Eingriffsbefugnisse hinzuwirken und die Anwendung bestehender Vorschriften auf die Einhaltung der datenschutzrechtlichen Grenzen zu kontrollieren. Dabei ist die Durchsetzung von Schutzrechten der Betroffenen (z. B. Auskunftsansprüche) sicherzustellen.

Inzwischen hat sich herausgestellt, daß Verwaltung und Wirtschaft angesichts der gesetzlichen Grenzen für die Datenverarbeitung vielfach auf die Einwilligung des Bürgers ausweichen, um damit leichter und umfassender an seine

Daten zu gelangen. Wir haben deshalb dieses Thema als Schwerpunkt gewählt, um den Datenschutz auch dann zu wahren, wenn sich der Bürger bei seiner täglichen, zunehmend technisierten Datenweitergabe auf allen Lebensgebieten mit der Datenverarbeitung einverstanden erklärt.

An verschiedenen Beispielen im öffentlichen und nicht-öffentlichen Bereich wird das Thema in diesem TB dargestellt (siehe dazu auch im Stichwortverzeichnis unter „Einwilligung"). Auf einige Beispiele wird im folgenden hingewiesen.

1.2.1 Selbstbestimmung

Verfassungsrechtlicher Ausgangspunkt ist in sämtlichen Fällen die Selbstbestimmung des Bürgers.

Mit der Einwilligung nimmt der Bürger seine informationelle Selbstbestimmung wahr, wenn er selbst verantwortlich entscheidet (Art. 2 Abs. 1 und Art. 1 GG). Die Einwilligung ist aber problematisch, wenn der Bürger seine Daten unter faktischem Zwang an Verwaltung und Wirtschaft weitergibt oder von sich aus persönliche Daten preisgibt, ohne die Tragweite zu überblicken. Den Gefährdungen der Selbstbestimmung einerseits durch Fremdbestimmung oder andererseits durch Selbstpreisgabe hat der Datenschutz soweit wie möglich entgegenzuwirken.

Die Einwilligung unterliegt dabei nicht einfach dem freien Spiel der Kräfte. Vielmehr sind Einwilligungen nur dann als rechtswirksam anzuerkennen, wenn sie rechtsstaatlichen Anforderungen genügen. Als Maßstab für die rechtliche Beurteilung der Einwilligung kann der 2. Leitsatz des Volkszählungsurteils des Bundesverfassungsgerichts mit der Folge herangezogen werden, daß auch die Datenverarbeitung aufgrund einer Einwilligung einer verfassungsmäßigen gesetzlichen Grundlage bedarf. Hierbei gelten die Grundsätze der Normenklarheit und Verhältnismäßigkeit. Zur Gewährleistung einer wirksamen Einwilligung sind außerdem organisatorische und verfahrensmäßige Vorkehrungen zum Schutz der Persönlichkeitsrechte der Betroffenen zu treffen.

Bei den bestehenden Risiken von Fremdbestimmung und Selbstpreisgabe ist es für eine wirksame Einwilligung erforderlich, zunächst einmal sicherzustellen, daß für den Bürger eine klare, transparente Informationslage über Inhalt, Zweck und Umfang der Einwilligung besteht. Diese Informationslage ist in allen Abschnitten der weiteren Datenverarbeitung, beispielsweise durch nachträgliche Unterrichtung bei Zweckänderung, aktuell zu gewährleisten.

Insgesamt gilt der Grundsatz, daß Zweifel und sonstige Defizite hinsichtlich der Einwilligung zu Lasten des Datenempfängers, der die Einwilligung einholt, und aller weiteren datenverarbeitenden Stellen gehen. Wenn der Bürger nicht wirksam einwilligt, ist die Datenverarbeitung unzulässig. Der Bürger darf wegen

der Tatsache, daß keine wirksame Einwilligung vorliegt, nicht benachteiligt werden.

1.2.2 Unterschiede zwischen Verwaltung und Wirtschaft

Die gesetzlichen Regelungen für die Einwilligung gelten zwar grundsätzlich übereinstimmend für Verwaltung und Wirtschaft, wie sich aus §§ 1 und 4 BDSG und nunmehr auch aus Art. 2, 3, 7, 8 und 10 der EG-Datenschutzrichtlinie ergibt. Grundrechtlich ist die Einwilligung jedoch im öffentlichen und nicht-öffentlichen Bereich ganz unterschiedlich zu bewerten:

Öffentlicher Bereich

Das Grundrecht auf informationelle Selbstbestimmung ist im öffentlichen Bereich ein Abwehrrecht gegen den Staat, der regelmäßig dem Bürger überlegen ist. Deshalb kommt dem Institut der Einwilligung, das eine Ausgestaltung der informationellen Selbstbestimmung darstellt und nicht etwa einen Grundrechtsverzicht bedeutet, in diesem Bereich von vornherein nur eine begrenzte Anwendung zu.

In der Eingriffsverwaltung und in der Leistungsverwaltung sind Voraussetzungen und Grenzen der Datenverarbeitung durch öffentliche Stellen regelmäßig durch Rechtsvorschriften abschließend festzulegen. Die Befugnisse des Staates sind grundsätzlich nicht über individuelle Einwilligungen zu erweitern. Soweit überhaupt eine Einwilligung in Betracht kommt, gilt auch dafür der Grundsatz der Erforderlichkeit, weil der Umfang der Aufgaben des öffentlichen Bereichs nicht durch Einwilligungen ausgedehnt werden kann.

Es gibt außerdem Fälle, in denen – wie bei der Sicherheitsüberprüfung – eine Einwilligung gesetzlich gefordert wird, um eine umfassende Aufklärung der Betroffenen über die Reichweite der staatlichen Maßnahme zu dokumentieren. Eine Aufforderung der öffentlichen Stellen an die Betroffenen, persönliche Daten mitzuteilen, ist aber nur zulässig, wenn die Daten für eine gesetzmäßige Entscheidung wirklich erforderlich sind. Für den Bürger verbleibt dann als Alternative nur noch die Möglichkeit, daß ohne seine Mitwirkung z. B. bei der Sicherheitsüberprüfung keine Einstellung erfolgt.

Ferner gibt es im öffentlichen Bereich „schlichtes Verwaltungshandeln", das sich nicht im einzelnen gesetzlich festlegen läßt, z. B. im Bereich der Forschung und Planung. Denkbar sind hier Einwilligungen – etwa in die Teilnahme an einer Befragung durch Universitätsforscher –, die ohne jede nachteilige Auswirkung abgelehnt werden können.

Nicht-öffentlicher Bereich

Im nicht-öffentlichen Bereich stehen sich auf beiden Seiten Grundrechte gegenüber, die gesetzlich abzusichern sind. In Art. 1 Abs. 1 der EG-Datenschutzrichtlinie wird bekräftigt, daß gerade auch für den nicht-öffentlichen Bereich

der Schutz der Grundrechte zu gewährleisten ist. Hier geht es um die Drittwirkung des informationellen Selbstbestimmungsrechts mit entsprechender Interessenabwägung. Die Datenverarbeitung ist im Rahmen der Zweckbestimmung eines Vertragsverhältnisses grundsätzlich zulässig.

Dabei muß die Datenverarbeitung für die Erfüllung des Vertrags erforderlich sein, wie in Art. 7 Buchstabe b der EG-Datenschutzrichtlinie verdeutlicht wird. Für die übrige gesetzlich zugelassene Datenverarbeitung im nicht-öffentlichen Bereich gilt ebenfalls der Grundsatz der Erforderlichkeit gemäß § 28 BDSG, wie durch Art. 7 Buchstaben c bis f der EG-Datenschutzrichtlinie bestätigt wird.

Für weitergehende Verarbeitungen muß eine Einwilligung eingeholt werden. Eine umfassende Aufklärung und im übrigen die Beachtung der gesetzlichen Formvorschriften sind für eine wirksame Einwilligung notwendig.

Dabei ist zu unterscheiden zwischen Massenverträgen mit Formular-Einwilligungen einerseits und Einzel-Einwilligungen andererseits. Bei massenweisen Einwilligungen insbesondere durch Formular-Verträge mit Großunternehmen ist die Situation des Bürgers ähnlich der im öffentlichen Bereich, da der Vertragspartner häufig eine Vormachtstellung innehat und die Vertragsgestaltung weitgehend bestimmt, z. B. gegenüber Versicherungen, Banken, Arbeitgebern, Vermietern. Eine wirklich freiwillige Einwilligung in die Verarbeitung der eigenen Daten ist hier meist Illusion. Bei Formular-Einwilligungen hat der Verwender die erforderlichen Daten eindeutig anzugeben und die Verfahrensanforderungen gemäß den Rechtsvorschriften einzuhalten.

In diesem Sinne gibt es Schutznormen für den Bürger gegenüber einseitigen Geschäftsbedingungen vor allem im Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen (AGB-Gesetz); anhand der EG-Richtlinie über mißbräuchliche Klauseln in Verbraucherverträgen von 1993 werden nun diese Vorschriften nicht mehr allein massenvertraglich, sondern auch einzelvertraglich auszulegen und anzuwenden sein (siehe auch 17.1).

Bei Einzelfall-Einwilligungen ist die Gleichberechtigung der Vertragspartner und damit die Freiwilligkeit der Einwilligung eher zu erwarten. Ob tatsächlich eine Einwilligung im Einzelfall vorliegt, bestimmt sich nicht nach formalen Kriterien, sondern danach, ob Inhalt und Grenzen der Einwilligung wirklich zwischen gleichwertigen Partnern individuell festgelegt wurden.

1.2.3 Schlußfolgerungen und Handlungsbedarf

Zur Verwirklichung der Selbstbestimmung reicht es nicht aus, auf die freien Entfaltungsmöglichkeiten des Bürgers zu verweisen. Gemäß der Rechtsprechung des Bundesverfassungsgerichts besteht eine staatliche Schutzpflicht, die Grundrechte aus Art. 2 und 1 GG zu sichern. Diese Schutzpflicht besteht auch gegenüber Risiken der Datenverarbeitung durch Private.

- Datenvermeidung

  Der beste Datenschutz besteht nach wie vor darin, daß keine oder möglichst wenige personenbezogene Daten erhoben werden. Deshalb ist z. B. verstärkt darauf zu achten, daß dem Bürger die Wahlmöglichkeit eingeräumt wird, ein datenfreies Verfahren zu verwenden oder jedenfalls ein Verfahren mit wenigen, nur vorübergehend gespeicherten Daten.

  Ein Beispiel dafür ist die datenfreie Fahrt im Nahverkehr durch Barzahlung statt Chipkarten oder wenigstens die Verwendung nur einer Guthabenkarte. Beim bevorstehenden interaktiven Fernsehen könnten Guthabenkarten anstelle einer Abrechnung über Kontoverbindung verwendet werden, damit personenbezogene Nutzungsdaten bei dem Betreiber des Dienstes oder bei den Anbietern gar nicht erst entstehen; damit könnten Mediennutzungsprofile vermieden werden. Auf vielen weiteren Lebensgebieten können Guthabenkarten als Inhaberkarten statt Namenskarten zur Datenvermeidung beitragen.

- Volle Anwendung des geltenden Rechts

  Das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze enthalten eine Reihe von wichtigen Einzelregelungen über die Einwilligung, die sich als Auslegungshilfe gegenseitig ergänzen. Diese verschiedenen Bestimmungen konkretisieren die verfassungsmäßigen Anforderungen an die Wahrung des Selbstbestimmungsrechts bei der Einwilligung; sie gelten deshalb auch, soweit sie in das jeweilige Gesetz nicht ausdrücklich aufgenommen wurden.

  Die bestehenden Rechtsvorschriften mit den jeweiligen Absicherungen des Bürgers stehen nicht zur Disposition der öffentlichen Stellen. Auf seine gesetzlichen Rechte kann der betroffene Bürger - wie auch sonst nach § 6 BDSG und den entsprechenden Vorschriften in den Landesdatenschutzgesetzen - nicht im Vorwege rechtswirksam verzichten.

  Eine generelle Grenze bilden Treu und Glauben und in besonders krassen Fällen die Sittenwidrigkeit und das Schikaneverbot. Eine Einwilligung kann auch mit der Menschenwürde unvereinbar sein. Der staatliche Schutz kann dann bis zu einer gesetzlichen Regelung gehen, daß die Einwilligung unbeachtlich ist, wie es nunmehr im Rundfunkstaatsvertrag für Reality TV-Aufnahmen bestimmt ist.

  Für eine wirksame Einwilligung sind folgende Punkte wichtig:

  Freiwilligkeit

  In den Rechtsvorschriften wird die Freiwilligkeit zwar nur selten direkt erwähnt, wie z. B. bei der Regelung der Datenerhebung in § 12 Abs. 3 Satz 3 HmbDSG. In der Begriffsbestimmung der Einwilligung in Art. 2 Buchstabe h

der EG-Datenschutzrichtlinie wird die Freiwilligkeit aber vorausgesetzt, indem die Einwilligung als „Willensbekundung ohne Zwang" definiert wird.

Unverzichtbar ist, daß Verwaltung und Wirtschaft die Freiwilligkeit der vorgesehenen Einwilligung ausdrücklich hervorheben. Diese Anforderung wird oft nicht eingehalten. Verpflichtet eine Rechtsvorschrift den Bürger zu einzelnen Angaben und sieht sie weitere freiwillige Angaben vor – wie bei Befragungen für statistische Zwecke –, ist diese Unterscheidung auch bei der verwaltungsmäßigen Umsetzung deutlich zu kennzeichnen.

Daher haben z. B. - anders als wiederholt geschehen - behördliche Aufforderungen zur Teilnahme an Befragungen oder zur Beteiligung an öffentlichen Planungsvorhaben klare Aussagen über die Freiwilligkeit zu enthalten (siehe 6.2).

Im nicht-öffentlichen Bereich waren die neuen BahnCard-Anträge ein drastisches Beispiel dafür, wie der Bürger ohne jeden Hinweis auf Freiwilligkeit vielfältige persönliche Daten angeben sollte (siehe 26.). Eine ausdrückliche Aussage zur Freiwilligkeit enthält nach langen Bemühungen der Aufsichtsbehörden die Allfinanz-Klausel zur Nutzung von Versicherungsdaten für versicherungsfremde Zwecke (13. TB, 23.4).

Zur Freiwilligkeit gehört auch der Hinweis, daß der Betroffene die Einwilligung verweigern kann und welche Folgen die Verweigerung hat (siehe § 5 Abs. 2 Satz 2 Halbsatz 2 HmbDSG). Nach Art. 10 Buchstabe c der EG-Datenschutzrichtlinie ist die betroffene Person zu informieren, „ob die Beantwortung der Fragen verpflichtend oder freiwillig ist", und „auf mögliche Folgen einer unterlassenen Beantwortung" hinzuweisen. Im Sinne dieser Regelung ist die Einschränkung in § 4 Abs. 2 BDSG, daß der Betroffene nur „auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen" ist, nicht mehr beizubehalten.

In diesem Zusammenhang ist außerdem das Widerrufsrecht des Bürgers wichtig. Insoweit gilt z. B. die in vielen, aber nicht in allen Datenschutzgesetzen enthaltene Regelung, daß der Bürger die Einwilligung mit Wirkung für die Zukunft widerrufen kann.

Frageverbote und Selbstauskünfte

Die Frageverbote z. B. im Arbeitsrecht gegenüber Bewerbern gelten auch für öffentliche Stellen als Arbeitgeber. Bekanntestes Beispiel hierfür ist das grundsätzliche Verbot der Frage nach einer Schwangerschaft im Einstellungsgespräch. Zulässig sind nur Fragen, die für das angestrebte Vertragsverhältnis nach objektivem, an den Wertentscheidungen des Grundgesetzes ausgerichtetem Verständnis unmittelbar von Bedeutung sind; der Grundsatz der Erforderlichkeit wirkt sich auch hier aus. Es kann z. B. nicht für ein Arbeitsverhältnis generell nach Vorstrafen oder anhängigen Strafverfahren gefragt werden, sondern nur nach einschlägigen Verurteilungen. Es sind keine Daten zu verlangen und anzugeben, soweit sich der Betroffene nach den Bestimmungen des Bundeszentralregistergesetzes im Rechtsverkehr als unbestraft bezeichnen darf.

Wenn auf diese Weise das Fragerecht begrenzt ist, darf diese Einschränkung nicht durch die Einholung von weitergehenden Selbstauskünften ausgehöhlt werden. Deshalb dürfen Arbeitgeber entgegen häufiger Übung keine weitergehenden Selbstauskünfte von Bewerbern verlangen – z. B. aus polizeilichen Dateien (vgl. 15.3.1), von der Schufa oder über Stasi-Unterlagen. Der Arbeitgeber darf nur die zulässigen Auskünfte von den jeweiligen Stellen unmittelbar einholen.

Eine Notlösung gegenüber unzulässigen Selbstauskünften besteht darin, daß der Bewerber falsche oder unvollständige Angaben als Notlüge machen darf, ohne daß ihm daraus später rechtliche Nachteile entstehen dürfen. Dieser Ausweg ist allerdings nicht gangbar, wenn im Wege der Selbstauskunft amtliche Unterlagen verlangt werden; dann ist es Sache der zuständigen Stellen und der Kontrollinstanzen, die Anforderung von Selbstauskünften zu unterbinden und die Beteiligten über die Unzulässigkeit des Verfahrens aufzuklären.

Zweckbindungen

Wenn Zweckbindungen für die Datenverarbeitung gesetzlich abschließend festgelegt sind – insbesondere in bereichsspezifischen Vorschriften –, wird damit zugleich die Grenze der zugelassenen Datenverarbeitung geregelt. Diese Grenzen dürfen nicht im Wege der Einwilligung umgangen werden, da die gesetzliche Beschränkung sonst gegenstandslos würde.

Als Beispiel gehören dazu die Protokolldaten, die nur im Rahmen der Maßnahmen zur Datensicherung verwendet werden dürfen. Eine Einwilligung in eine Datenverarbeitung zu Zwecken der Verhaltens- oder Leistungskontrolle der Beschäftigten wäre demnach unwirksam.

Unter die Zweckbindung fallen auch die Regelungen über die begrenzte Einwilligung bei Telekommunikationsdaten. Im Bildschirmtext-Staatsvertrag heißt es z. B., daß der Anbieter personenbezogene Daten von Teilnehmern nur abfragen und speichern darf, soweit dies für die Leistung, den Abschluß oder die Abwicklung des Vertragsverhältnisses erforderlich ist. In der amtlichen Begründung wird dazu betont, daß die „strikte Regelung auch nicht durch die in den allgemeinen Datenschutzgesetzen vorgesehene Einwilligung verdrängt werden" kann.

Ähnliche Regelungen gibt es in den neueren Mediengesetzen und in den bundesrechtlichen Bestimmungen über Telefondaten, um das Risiko zu vermeiden, daß Kommunikationsprofile der Bürger anhand ihres Medienver-

haltens anderen zugänglich werden. Aufweichungen dieses Grundsatzes z. B. im Entwurf eines neuen Telekommunikationsgesetzes, wonach Telefondaten mit Einwilligung „für das bedarfsgerechte Gestalten von Telekommunikations- und Informationsdienstleistungen" verwendet werden dürfen, ist entschieden entgegenzutreten.

Die abschließende Wirkung derartiger gesetzlicher Regelungen über die Zweckbindung wird durch Art. 8 Abs. 2 Buchstabe a der EG-Datenschutzrichtlinie bekräftigt. Danach ist die Einwilligung bei besonders sensiblen Daten nicht wirksam, wenn nach einer Rechtsvorschrift eine bestimmte Datenverarbeitung untersagt ist und nach dieser Vorschrift dieses Verbot auch nicht „durch die Einwilligung der betroffenen Person aufgehoben werden" kann. Es würde im Sinne dieser Bestimmung der Rechtsklarheit dienen, wenn die Zulässigkeit der Einwilligung jeweils ausdrücklich in der Rechtsnorm geregelt würde.

AGB-Grundsätze

Das AGB-Gesetz enthält im Vergleich zu den Datenschutzgesetzen eine Reihe von Konkretisierungen, die ebenfalls auf dem Grundsatz beruhen, einem sozialen Ungleichgewicht – hier bei Allgemeinen Geschäftsbedingungen – rechtlich entgegenzuwirken. Daher sind die Bestimmungen des AGB-Gesetzes nicht nur unmittelbar bei Allgemeinen Geschäftsbedingungen anzuwenden. Folgende Regelungen können generell als Auslegungshilfe herangezogen werden:

Nach § 3 AGB-Gesetz werden überraschende Klauseln mit ungewöhnlichen und unerwarteten Bestimmungen nicht Vertragsbestandteil. Gemäß § 5 AGB-Gesetz gehen Zweifel bei der Auslegung Allgemeiner Geschäftsbedingungen zu Lasten des Verwenders; dieser Grundsatz ist nun – unabhängig von Geschäftsbedingungen – in Art. 7 Buchstabe a der EG-Datenschutzrichtlinie enthalten, wonach die betroffene Person ihre Einwilligung „ohne jeden Zweifel" gegeben haben muß. Im Sinne von § 6 Abs. 2 und 3 AGB-Gesetz sind zu weitreichende Erklärungen nicht auf das gerade noch zulässige Maß zurückzuführen, sondern bleiben insgesamt unzulässig. Nach § 9 AGB-Gesetz ist das Transparenzgebot einzuhalten; eine mit Treu und Glauben nicht zu vereinbarende unangemessene Benachteiligung kann anhand dieser Vorschrift überprüft werden.

Stufenweise Einwilligung

Unnötig weitreichende oder pauschale Einwilligungen können dadurch vermieden werden, daß zunächst nur die unmittelbar notwendige Datenverarbeitung in die Einwilligung einbezogen wird. Daher dürfen bei einer Bewerbung zwar die wesentlichen Daten für das Einstellungsgespräch, nicht aber bereits die für ein späteres Vertragsverhältnis relevanten Daten verlangt werden.

Daten anderer Personen

Eine besondere Bedeutung kommt dem informationellen Selbstbestimmungsrecht und der Einwilligung zu, wenn durch eine freiwillige Befragung auch Daten anderer Personen offenbart werden. So werden bei der Befragung für einen Mietenspiegel regelmäßig Daten aus Mietverträgen mit Angaben zu Wohnungsgröße, Ausstattung und Mietpreis erhoben, die sowohl den Mieter als auch den Vermieter betreffen.

In diesem Falle ist grundsätzlich die Einwilligung sämtlicher Betroffener erforderlich. Falls Mieter eine Befragung aus datenschutzrechtlichen Gründen ablehnen, muß infolgedessen auf Ersatzbefragungen bei ihren Vermietern verzichtet werden (12. TB, 12.3).

– Bereichsspezifische Vorschriften

Bei besonders sensiblen Daten z. B. über gesundheitliche Verhältnisse oder bei besonders intensiven Eingriffen z. B. mit einer Sicherheitsüberprüfung werden die allgemeinen gesetzlichen Regelungen über die Einwilligung nicht ausreichen, soweit es um bereichsspezifische Fragen geht. Dann kann insoweit nur eine gezielt bereichsspezifische Regelung den sozialen Zwängen für eine Einwilligung entgegenwirken, indem die Transparenz und Kalkulierbarkeit der Verarbeitung sichergestellt wird.

Ergänzend kann auf die allgemeinen Regelungen zur Einwilligung zurückgegriffen werden, soweit sie nicht gerade durch die bereichsspezifische Bestimmung ausgeschlossen werden sollen. Aktuelle Beispiele sind dafür die bereichsspezifischen Regelungen im Medienbereich.

– Datenschutz durch Technik

Durch einen datenschutzfreundlichen Technikeinsatz kann gerade auch bei der freiwilligen Datenweitergabe erreicht werden, daß die Rechtslage des Bürgers nicht etwa verschlechtert, sondern möglichst verbessert wird.

Ein aktuelles Beispiel zur Datensicherung bei sensiblen Daten sind die Überlegungen, bei der freiwilligen Gesundheitskarte durch technische Vorkehrungen eine Nutzung nur im Einvernehmen zwischen Patient und Arzt zuzulassen. Wenn die Daten nur mit Zustimmung von beiden freigegeben werden können, lassen sich Mißbräuche bei einem Zugriff anderer Personen, z. B. des Arbeitgebers, durch die technische Ausgestaltung einer derartigen Doppelsicherung abwenden (siehe 19.1).

Ein weiteres Beispiel sind die Bemühungen, z. B. bei Krankenkassen und Krankenversicherungen den vollen Datenzugriff gemäß der Einwilligung des Bürgers nur bei der Zweigstelle zu ermöglichen, die ihn ständig betreut, und bei anderen Zweigstellen den Zugriff auf Stammdaten zu beschränken (siehe 5.3 und auch 5.4 sowie 22.4).

Bei den Risiken durch Fremdbestimmung und Selbstpreisgabe ist es Sache der Datenschutzbeauftragten und der Aufsichtsbehörden für den nicht-öffentlichen Bereich, für die Umsetzung der bestehenden Handlungsmöglichkeiten und Handlungsbedarfe zu sorgen. Dazu gehört eine intensive Beratung der Bürger, die ihre Datenschutzrechte nicht ohne weiteres kennen.

Voraussetzung ist dafür, daß die öffentlichen Stellen ihre Einwilligungs-Konzepte mit den Datenschutzbeauftragten rechtzeitig umfassend beraten. Im nicht-öffentlichen Bereich kann eine frühzeitige Beteiligung der Aufsichtsbehörden den Datenschutz gewährleisten, z. B. bei der Abstimmung von Verhaltensregeln mit Interessenverbänden, wie dies in der EG-Datenschutzrichtlinie nun ausdrücklich vorgesehen ist.

Wichtig ist außerdem eine vielfältige Öffentlichkeitsarbeit in Zusammenarbeit mit den Medien, dem Verbraucherschutz, den Kammern usw. Dadurch kann wiederum das Selbstbewußtsein der Bürger gestärkt werden, ihr Grundrecht auf Datenschutz wahrzunehmen und damit ihre Selbstbestimmung zu verwirklichen.

Die Datenschutzbeauftragten haben auf ihrer Konferenz vom 9./10. November 1995 die Thematik anhand meiner Vorlage behandelt. Es bestand Einvernehmen, daß die Problematik aufmerksam weiter zu verfolgen ist und der Bürger vor einer unzulässigen Einholung und Verwendung der Einwilligung geschützt werden muß.

1.3 Hamburgische Datenschutzvorschriften

1.3.1 Hamburgisches Datenschutzgesetz

Nach den vorangegangenen Referentenentwürfen (13. TB, 1.5.1) hatte die Justizbehörde einen fortgeschriebenen Entwurf eines Gesetzes zur Änderung des Hamburgischen Datenschutzgesetzes mit Stand 25. August 1995 zur abschließenden Stellungnahme bis Ende September 1995 an die Behörden übermittelt. Zu den Verbesserungen gehört insbesondere der Fortfall der Rechtsaufsicht des Senats über meine Tätigkeit. Die Bestimmung, daß der Tätigkeitsbericht mindestens alle zwei Jahre zu erstellen ist, läßt eine flexible Berichterstattung zu. Wie in anderen Landesgesetzen soll nun ausdrücklich geregelt werden, daß im Tätigkeitsbericht auch über den nicht-öffentlichen Bereich und die Aufgabenerfüllung der Aufsichtsbehörde berichtet wird.

Andererseits enthält der neue Entwurf erstmals eine wesentliche Einschränkung für den Geltungsbereich des Hamburgischen Datenschutzgesetzes. Nunmehr ist vorgesehen, daß sämtliche öffentlichen Unternehmen in privater Rechtsform unabhängig von ihrer Aufgabenerfüllung und ihrer Beherrschung durch den öffentlichen Bereich einheitlich den Regelungen des Bundesdatenschutzgesetzes für nicht-öffentliche Stellen zugeordnet werden sollen. Eine

derartige pauschale Regelung, die es in keinem anderen Datenschutzgesetz gibt, halte ich nicht nur für sachlich verfehlt, sondern für rechtlich unzulässig.

Der Landesgesetzgeber hat keine Befugnis und verstößt zugleich gegen den Grundsatz der Bund-Länder-Treuepflicht, wenn er öffentliche Unternehmen, die eindeutig öffentliche Stellen sind – z. B. beherrschte öffentliche Unternehmen zur Daseinsvorsorge –, entgegen der Konzeption des Bundesdatenschutzgesetzes und der ständigen Rechtsprechung dem nicht-öffentlichen Bereich zuordnen will. Eine Differenzierung allein nach der Rechtsform des Unternehmens, die nach § 2 BDSG gerade nicht der Maßstab für die rechtliche Unterscheidung ist, wäre auch im Hinblick auf die Gleichbehandlung nach Art. 3 Abs. 1 GG problematisch. Der Bürger wäre dann in einer unterschiedlichen Rechtsposition gegenüber öffentlichen Unternehmen allein deshalb, weil im einen Fall eine öffentlich-rechtliche Organisationsform und im anderen Fall eine privat-rechtliche Rechtsform für das Unternehmen gewählt wurde.

Die im Gesetzentwurf vorgesehene pauschale Regelung würde außerdem zu erheblichen Einschnitten in das Datenschutzgrundrecht führen. Bei jeder Privatisierung würde es keine Gesetzesregelung für den Datenschutz in Akten mehr geben, weil das Bundesdatenschutzgesetz dafür ausdrücklich keine Regelung enthält. Es würde auch der besondere gesetzliche Datenschutz für Mitarbeiter entfallen, weil es im Bundesdatenschutzgesetz auch dafür keine besonderen Bestimmungen gibt. Schließlich würde die Daueraufsicht durch den Hamburgischen Datenschutzbeauftragten nach jeder Privatisierung nicht mehr fortgeführt werden können, weil das Bundesdatenschutzgesetz nur eine sehr viel schwächere Anlaßaufsicht vorsieht.

Der Bundesbeauftragte für den Datenschutz hält in seiner Stellungnahme, die wir erbeten hatten, eine derartige Regelung durch Landesgesetz kompetenzrechtlich aus der Sicht des Bundesdatenschutzgesetzes zwar grundsätzlich für zulässig. Er hat aber gegen das Anknüpfen an die private Rechtsform der Stellen erhebliche Bedenken, wenn dabei die öffentliche Beherrschung und die Erfüllung öffentlicher Aufgaben durch die Stelle nicht als maßgeblich berücksichtigt werden. Eine einheitliche datenschutzrechtliche Behandlung der öffentlichen Aufgabenerfüllung sei dann nicht mehr gegeben. Der Bundesbeauftragte für den Datenschutz kommt zu dem Ergebnis, daß eine Regelung dieses Inhalts „so keine sinnvolle Fortentwicklung und Ergänzung des Datenschutzes darstellt".

Auch aus diesen Gründen habe ich eine Regelung in Übereinstimmung mit fast allen Datenschutzgesetzen vorgeschlagen. Demnach sind diejenigen öffentlichen Unternehmen als öffentliche Stellen ungeachtet ihrer Rechtsform zu behandeln, die Aufgaben der öffentlichen Verwaltung erfüllen und keine öffentlichen Stellen des Bundes nach § 2 Abs. 3 BDSG sind. Daraus würden sich in der Praxis auch keine besonderen Schwierigkeiten ergeben, weil die begriffliche Abgrenzung zwischen öffentlichen und nicht-öffentlichen Stellen wie bei

der Auslegung des Bundesdatenschutzgesetzes und der anderen Landesdatenschutzgesetze vorzunehmen wäre. Außerdem würde für die meisten privatisierten öffentlichen Unternehmen als Wettbewerbsunternehmen überwiegend das Bundesdatenschutzgesetz mit den Vorschriften für die nicht-öffentlichen Stellen gelten; allerdings würde es gerade bei der Geltung des Arbeitnehmerdatenschutzes und der Daueraufsicht durch die Datenschutzkontrolle bleiben.

Der Senat hat den Gesetzentwurf am 21. November 1995 behandelt; in der Senatsdrucksache ist meine Auffassung mit der entgegenstehenden Auffassung der Justizbehörde dargestellt. Gemäß dem Vorschlag der Justizbehörde hat der Senat den Gesetzentwurf der Bürgerschaft zur Beratung und Beschlußfassung zugeleitet. Die von mir genannten offenen Punkte werden bei der bürgerschaftlichen Beratung näher zu erörtern sein.

1.3.2 Bereichsspezifische Datenschutzvorschriften

Das Hamburgische Verfassungsschutzgesetz wurde von der Bürgerschaft am 7. März 1995 beschlossen. Unsere Auffassung zum Gesetzentwurf ist aus den früheren TB ersichtlich (13. TB und 12. TB jeweils 18.1). Bei den abschließenden bürgerschaftlichen Beratungen konnte erreicht werden, daß sich die von mehreren Fraktionen vorgeschlagenen Änderungen, soweit sie in das Gesetz aufgenommen wurden, schließlich in datenschutzrechtlich vertretbaren Grenzen hielten (13.2).

Aus dem Bereich der Rechtsverordnungen ist erwähnenswert, daß der Senat am 28. März 1995 eine neue Mietenspiegelbefragungsverordnung beschlossen hat. Die von uns für notwendig gehaltenen Datenschutzvorkehrungen werden dort weitgehend berücksichtigt.

Nach wie vor fehlen wichtige gesetzliche Datenschutzvorschriften in Hamburg. Wie bereits im letzten TB angemahnt (13. TB, 1.5.3), ist insbesondere der Erlaß eines hamburgischen Gesetzes über das öffentliche Gesundheitswesen überfällig; es fehlt weiterhin ein hamburgisches Sicherheitsüberprüfungsgesetz, und auch die Schulgesetznovellierung läßt weiter auf sich warten. Ebenso fehlt ein hamburgisches Untersuchungsausschußgesetz (siehe auch 1.5.3 und 15.1.4). Damit wird der Zeitraum immer knapper, bis der sog. Übergangsbonus mit Ende der Legislaturperiode dieser Bürgerschaft endgültig abgelaufen sein wird.

1.3.3 Richtlinien

Gemäß der seinerzeitigen Ankündigung (13. TB, 3.2.4) ist die UNIX-Richtlinie mit Wirkung vom 1. Juni 1995 in Kraft getreten. Die bereits vorliegenden Richtlinien (12. und 13. TB, jeweils 1.5.4) haben sich im wesentlichen bewährt, so daß sie nur in wenigen Punkten inzwischen geändert wurden.

1.4 EG-Datenschutzrichtlinie und Bundesdatenschutzgesetz

Nach schwierigen abschließenden Beratungen während des deutschen Vorsitzes im EG-Ministerrat konnte die EG-Datenschutzrichtlinie unter Leitung des Bundesdatenschutzbeauftragten fertiggestellt werden (siehe zuletzt 13. TB, 1.8). Der Ministerrat hat die Richtlinie am 24. Juli 1995 angenommen. Damit beginnt die Dreijahresfrist zu laufen, in der die Mitgliedstaaten ihr Datenschutzrecht an die Richtlinie anzupassen haben.

Bis Mitte 1998 ist demnach insbesondere das Bundesdatenschutzgesetz zu aktualisieren. Da der öffentliche und der nicht-öffentliche Bereich in der EG-Datenschutzrichtlinie gleichbehandelt werden, wird für das Bundesdatenschutzgesetz hinsichtlich der Regelung für den nicht-öffentlichen Bereich ein ähnlich hoher Standard wie für den öffentlichen Bereich anzustreben sein.

Die Datenschutzbeauftragten wollen das Datenschutzgesetz – über den unerläßlichen Anpassungsbedarf aufgrund der EG-Datenschutzrichtlinie hinaus – grundlegend modernisieren. Demgegenüber sieht das Bundesministerium des Innern bisher nur einen begrenzten Änderungsbedarf.

Auf ihrer 50. Konferenz sind die Datenschutzbeauftragten im November 1995 übereingekommen, nach näherer Erörterung in den nächsten Monaten eine Entschließung über ihre gemeinsamen Vorstellungen zu fassen. Sie wollen ihre Zielsetzung auch öffentlich in offensiver Weise vertreten, damit entsprechend den weitgehenden sozialen und technischen Veränderungen ein modernes Datenschutzrecht zum Schutz der Bürger erreicht wird. Dies stimmt mit dem hohen Anspruch in den Erwägungsgründen der EG-Datenschutzrichtlinie überein:

- „Die Datenverarbeitungssysteme stehen im Dienste des Menschen; sie haben ... deren Grundrechte und Freiheiten und insbesondere deren Privatsphäre zu achten und zum wirtschaftlichen und sozialen Fortschritt, zur Entwicklung des Handels sowie zum Wohlergehen der Menschen beizutragen."

1.5 Verhältnis zum Bürger

Bei der Behandlung von Eingaben, in den Bürgersprechstunden und in der Öffentlichkeitsarbeit haben wir uns wiederum dafür eingesetzt, die verschiedenen Anliegen der Bürger zu berücksichtigen.

Soweit wir, wie im Bereich der Rechtspflege, gesetzlich an einer eigenen Prüfung der Bürgeranliegen gehindert waren, konnten wir zumindest geeignete Wege zur Interessenwahrung aufzeigen. In besonderen Einzelfällen haben wir den Gerichten unsere Auffassung beratend zur Kenntnis gegeben.

1.5.1 Eingaben

Aus dem öffentlichen und dem nicht-öffentlichen Bereich richteten die Bürger wieder zahlreiche Eingaben an uns. Bis Ende November 1995 gingen 333 schriftliche Eingaben zu folgenden Themen ein:

Öffentlicher Bereich	163
davon Inneres und Justiz	72
Gesundheit und Soziales	34
Sonstiges	57
Nicht-öffentlicher Bereich	170
davon Versandhandel	6
Versicherungswirtschaft	18
Kreditwirtschaft	22
Werbung	15
Arbeitnehmer-Datenschutz	8
Schufa und Auskunfteien	26
Gesundheitswesen	14
Wohnungswirtschaft	11
Verkehrswesen	7
Markt- und Meinungsforschung	4
Sonstiges	39

1.5.2 Öffentlichkeitsarbeit

Die Veranstaltungsreihe im Auditorium von Gruner + Jahr in Zusammenarbeit mit dem Kommunikationsverein Hamburger Juristen haben wir fortgesetzt. Zum Thema „Datenschutz auf der Datenautobahn? Interaktive Medien und Datenschutz" fand eine Diskussion mit Vertretern aus dem Medienbereich und der Wissenschaft über „Hamburg im Datennetz mit Video on Demand, Teleshopping und Infodiensten" statt. Dieses aktuelle Thema stieß auf großes Interesse und wurde vorher – wie in den Vorjahren – in einer internen Runde zwischen den norddeutschen Datenschutzbeauftragten erörtert.

Die neuen technischen Möglichkeiten wurden auch auf den vierteljährlichen Pressekonferenzen in der Dienststelle mit Vertretern der Hamburger Zeitungen und des Rundfunks behandelt. Dazu gehörte u.a. das von den Medien erheblich beachtete Thema Videoüberwachung auf öffentlichen Straßen und Plätzen (siehe auch 27.). Wir veröffentlichten zum Thema Datenschutz bei elektronischen Geldbörsen die Entschließung, die die Datenschutzbeauftragten des Bundes und der Länder anhand unserer Vorschläge gefaßt hatten (25.1). Bundesweites Interesse fand die gesonderte Pressekonferenz zur unzulässigen Volksbefragung durch die neuen BahnCard-Anträge (siehe auch 26.). Die internationale Entwicklung wurde anhand des Themas erörtert, daß Europol keine undurchschaubare und unkontrollierbare europäische Zentralpolizei werden darf (siehe auch 15.6).

Wenn in den Medien gelegentlich unzutreffend über den Datenschutz berichtet wurde, haben wir in wichtigen Fällen die Rechtslage mit eigenen Beiträgen – z. B. durch Presseerklärungen – klargestellt. Die Medien haben dann unsere Klarstellung durchweg aufgegriffen. So wurde z. B. schließlich zutreffend berichtet, daß der Datenschutz nicht die effektive Öffentlichkeitsfahndung der Polizei mit aktuellen Fotos verhindert.

Gemeinsam mit den Datenschutzbeauftragten von Berlin und Bremen wurde die Broschüre über Mobilfunk und Datenschutz herausgegeben. Damit wurde dem Bürger als Nutzer ermöglicht, sich über die besonderen Datenschutzrisiken dieses Kommunikationsdienstes unmittelbar zu informieren.

Zusammen mit der Verbraucher-Zentrale Hamburg haben wir außerdem ein Faltblatt über „Die Gesundheits-Chipkarte: Alles auf eine Karte setzen?" herausgegeben. Die Bürger sollten damit über die Vor- und Nachteile der neuen Chipkarten unterrichtet werden, die in großem Umfang sensible medizinische Daten enthalten und bis zu einer vollständigen Krankenakte in Checkkartenformat ausgebaut werden können (siehe auch 19.1).

Zur Öffentlichkeitsarbeit gehörte es auch, daß in einer der Pressekonferenzen über Datenschutz im Internet berichtet wurde. Außerdem soll es zur Information über Datenschutzfragen beitragen, daß der Hamburgische Datenschutz im Oktober 1995 selbst ins Internet gegangen ist und dort eine Vielzahl von Datenschutzhinweisen zum Abruf bereithält (4.1).

1.5.3 Zusammenarbeit mit Verwaltung und Justiz

Die intensive Zusammenarbeit mit den hamburgischen Behörden und Kammern sowie der Justiz wurde wiederum fortgesetzt. Das Datenschutz-Jahrestreffen fand zum vierten Mal als Meinungsaustausch mit Vertretern der Bürgerschaft, Justiz, Verwaltung, Kammern, Gewerkschaften und Bürgervereine statt. Dabei habe ich verdeutlicht, daß bei der hamburgischen Verfassungsreform die Datenschutzrechte der Bürger stärker abzusichern sind. Zu den notwendigen Verfassungsbestimmungen über die Tätigkeit der bürgerschaftlichen Ausschüsse, die Aktenvorlage des Senats und die Rechte und Pflichten der Untersuchungsausschüsse sind gesetzliche Ausführungsvorschriften erforderlich, insbesondere ein hamburgisches Untersuchungsausschußgesetz.

Auch die Verwaltungsreform ist untrennbar mit Datenschutzfragen verbunden. Abzulehnen sind dabei Überlegungen, als „Bürgerservice" allen Bezirksämtern und nicht nur dem örtlich zuständigen Bezirksamt den Zugang zu personenbezogenen Daten zu eröffnen, soweit diese automatisiert verarbeitet werden. Falls hierfür überhaupt ein nachweisbares Bürgerinteresse besteht, wäre der Zugriff auf solche Daten durch andere Bezirksämter strikt an die Einwilligung des Bürgers zu binden.

Angesichts dieser generellen Entwicklung wird im vorliegenden TB erneut näher auf die Netzinfrastruktur der hamburgischen Verwaltung eingegangen

(3.1). Die Datenschutzfragen bei dem Projekt Personalwesen (PROPERS) bedürfen noch eingehender Erörterung (6.1). Bei dem Projekt Automation der Stellenplanung ergaben sich ebenfalls – wenn auch in geringerem Umfang – datenschutzrechtliche Fragen.

Eine förmliche Beanstandung war nur in einem Fall gegenüber der Handelskammer Hamburg notwendig, weil die rechtliche Zulässigkeit zunächst unterschiedlich beurteilt wurde, Prüfungsergebnisse von Auszubildenden regelmäßig an die Ausbildungsbetriebe auf deren Verlangen weiterzugeben. Die Problematik konnte einvernehmlich dadurch gelöst werden, daß die Handelskammer nunmehr von den Auszubildenden eine ausdrückliche Einwilligung einholt (7.1).

2. Entwicklung der Dienststelle

Auch im Jahr 1995 gab es nur wenige personelle Veränderungen. Stelleneinsparungen werden bei der begrenzten Mitarbeiterzahl wegen der ständig quantitativ und qualitativ wachsenden Aufgaben nicht möglich sein.

Nach dem Berliner Modell wäre es zu begrüßen, wenn aus den Stelleneinsparungen bei großen IuK-Projekten der Behörden uns eine Stelle zur Verfügung gestellt wird. Zugleich wäre bei derartigen Einsparungen der Stellenbestand zur Datenschutzprüfung in den Behörden selbst zu verstärken.

Auf diese Weise könnten Zeit und Kosten für die Einführung und Änderung von IuK-Vorhaben eingespart werden. Durch einen derartigen vorgezogenen Datenschutz werden insbesondere zeitaufwendige und kostspielige Nachbesserungen vermieden, die sonst aufgrund späterer Datenschutzprüfungen notwendig werden können (vgl. 11. TB und auch 3.1.1).

3. Informations- und Kommunikationstechnik

3.1 Netzinfrastruktur der hamburgischen Verwaltung

Die Vernetzung ist das beherrschende Datenschutzthema der neunziger Jahre – diese Leitaussage unseres Berichts über den Datenschutz bei Automation und Vernetzung der hamburgischen Verwaltung (IuK-Datenschutzbericht – Berichte und Dokumente Nr. 949) aus dem Jahr 1993 hat sich inzwischen bestätigt. Notwendige Bedingung für eine umfassende Vernetzung ist die Ausstattung der Arbeitsplätze mit IuK-Technik, die in den letzten Jahren stark zugenommen haben.

Eine Erhebung der Finanzbehörde hat ergeben, daß von den rund 30.000 für die DV-Unterstützung geeigneten Büroarbeitsplätzen in der hamburgischen Verwaltung Mitte 1995 ca. 15.500, also mehr als die Hälfte, mit IuK-Technik ausgerüstet waren. Damit hat sich die Ausstattung in den letzten zwei Jahren um 6.500 Bildschirmarbeitsplätze erhöht.

Netze bringen verschiedene datenschutzrechtliche Probleme mit sich, die von uns wiederholt problematisiert wurden (insbes. im IuK-Datenschutzbericht). An dieser Stelle soll auf zwei dieser Probleme noch einmal hingewiesen werden:

- Durch die umfassende Vernetzung besteht die Gefahr, daß die Verwaltung sich zu einem informationellen Ganzen entwickelt, dem der Bürger weitgehend machtlos gegenübersteht. Die technische Infrastruktur könnte für umfassende Datenübermittlungen, Online-Zugriffe und die Zweckentfremdung personenbezogener Daten genutzt werden. Es sind bereits Tendenzen erkennbar, sachliche und örtliche Zuständigkeiten der hamburgischen Verwaltung aufzuheben und unter Nutzung der Netzinfrastruktur auf Datenbestände anderer Stellen zuzugreifen. Die hiermit verbundenen rechtlichen und technischen Probleme sind ausführlich im 13. TB (1.4, 3.9) erörtert worden (siehe auch oben 1.5.3).

- Die Vertraulichkeit der über Netze übertragenen Daten und der auf vernetzten Systemen gespeicherten Daten wird dadurch gefährdet, daß Externe, aber auch unberechtigte Insider aus dem Kreis der Verwaltungsmitarbeiter die Möglichkeit haben könnten, Daten unbemerkt abzuhören und aufzuzeichnen und ggf. auch zu verändern.

Für die Netzinfrastruktur ergeben sich daraus folgende Forderungen:

- Die Nutzungsmöglichkeiten des Behördennetzes sind strikt nach Erforderlichkeitsgrundsätzen festzulegen. Verbindungen und Dienste, die sich nicht aus dem Aufgabenprofil eines Mitarbeiters begründen lassen, sind technisch zu unterbinden; organisatorische Maßnahmen, insb. Nutzungsverbund -gebote, reichen insoweit nicht aus.

- Es sind Maßnahmen gegen Angriffs- und Manipulationsversuche zu treffen. Dies gilt gleichermaßen für interne wie für externe Angriffe.

Im folgenden werden für die verschiedenen technischen Ebenen der behördlichen Netz-Infrastruktur Lösungen aufgezeigt, um diesen Anforderungen gerecht zu werden.

3.1.1 Flächendeckende Vernetzung von behördlichen DV-Systemen

Die weitaus meisten DV-Systeme sind Bestandteile von lokalen oder übergreifenden Netzen und haben somit die Möglichkeit, personenbezogene Daten auch über die Behördengrenzen hinaus zu übermitteln oder auf Datenbestände zuzugreifen, die außerhalb des eigenen Zuständigkeitsbereichs gespeichert sind.

Die Vernetzung findet dabei auf unterschiedlichen Ebenen statt:

- Innerhalb von Gebäuden werden die mit Arbeitsplatzcomputern (PC) oder mit Bildschirmterminals ausgestatteten Arbeitsplätze lokal vernetzt. So sind

z. B. im Neubau der Umweltbehörde sämtliche Räume mit Anschlußmöglichkeiten ausgestattet.

- Mit einem Datenübertragungsdienst gemäß der Norm X.25 können Daten zwischen räumlich entfernten Dienststellen, Ämtern und Behörden übertragen werden (vgl. 13. TB, 3.3). Für diesen reinen Transportdienst besteht ein mit uns abgestimmtes Sicherheitskonzept, das eine mißbräuchliche Inanspruchnahme erschwert, jedoch unsere Forderung nach verschlüsselter Datenübertragung nicht erfüllt.

- Auf dem X.25-Protokoll setzt ein weiteres Transport- und Vermittlungssystem auf, das sich des TCP/IP-Protokolls (Transmission Control Protocol/ Internet Protocol) bedient (vgl. unsere Broschüren mit dem Datenschutzkonzept für UNIX-Mehrplatzanlagen, 6.6, sowie Datenschutz in Netzen, 6.1). Durch den Einsatz dieses Vermittlungssystems werden verschiedene, für den X.25-Dienst vereinbarte Sicherungsmaßnahmen unterlaufen. So müssen diejenigen Rechner, die auf IP- Ebene kommunizieren sollen, auch auf der X.25-Ebene entsprechende Berechtigungen bekommen. Dies ist bei solchen Anwendungen problematisch, die weitgehend unabhängig von fachlichen Aufgaben vorgesehen sind, etwa bei elektronischer Post (vgl 3.3).

- Schließlich findet eine Vernetzung auf Anwendungsebene (Vorgangsverwaltung, Personalwesen, Mittelbewirtschaftung, elektronische Post – vgl. 3.3) statt. Derartige Anwendungen erfordern nicht nur einen lokalen Zugriff, sondern sie setzen eine behördenübergreifende Vernetzung auf den unteren Netzebenen voraus. Dies führt insbesondere in solchen Verwaltungsbereichen zu Datenschutzproblemen, deren Netze aufgrund der Sensibilität der dort verarbeiteten Daten von den übrigen Verwaltungsnetzen getrennt sein sollten.

Die Sicherheitsmechanismen auf allen beschriebenen Ebenen beruhen im wesentlichen auf der Adreßstruktur der angeschlossenen Systeme. Die Datenübertragung wird durch Informationen gesteuert, die den Nutzdaten vorangestellt sind, über den Sender und den Empfänger (Adreßdaten). Da jedoch die Adreßdaten nicht physikalische Eigenschaften der Systeme ausdrücken, sondern auf logischen Strukturen beruhen, können Adreßdaten ggf. durch Software manipuliert werden. Damit könnten die darauf aufbauenden Sicherheitsmechanismen außer Kraft gesetzt werden.

Die behördenübergreifenden Netze werden durch das Landesamt für Informationstechnik (LIT) betrieben. Das LIT betreibt darüber hinaus auch wesentliche weitere Komponenten der IuK-Infrastruktur der hamburgischen Verwaltung. Zu nennen ist hier insbesondere das zentrale Rechenzentrum; ein UNIX-Rechenzentrum ist im Aufbau.

Angesichts der Komplexität der Vernetzung, die auf den verschiedenen Ebenen stattfindet, sind umfassende Sicherheitskonzepte erforderlich, um die Gefährdungen für den Datenschutz auszuschließen. Diese Aufgabe könnte behördenübergreifend ebenfalls beim LIT angesiedelt werden, das ja als umfassendes Kompetenzzentrum für die Verwaltung in Fragen der Informations- und Kommunikationstechnik konzipiert war.

Leider haben die Aspekte des Datenschutzes und der Technikfolgenabschätzung beim LIT bisher nicht den Stellenwert erhalten, den wir uns bei seiner Gründung erhofft hatten (vgl. 11.TB, 3.2.1). Hier besteht dringender und zunehmender Handlungsbedarf. Bei der Verteilung personeller und sächlicher Ressourcen muß den Anforderungen des Datenschutzes und der Datensicherheit ein angemessenes Gewicht eingeräumt werden.

Von den Verantwortlichen wird bisweilen bezweifelt, daß es überhaupt eine nennenswerte Nachfrage für ein entsprechendes Angebot gibt. Wir können dem entgegenhalten, daß nach unserer Erfahrung ein erheblicher Nachholbedarf in der Konzeption und Umsetzung von Risikoanalysen und Sicherheitskonzepten besteht. Dies wird z. B. deutlich an der stark zunehmenden Zahl der technischen Beratungswünsche, die an unsere Dienststelle gestellt werden, und an unzureichenden Vorarbeiten für Sicherheitskonzepte, die uns von verschiedenen Projekten zur Beurteilung vorgelegt wurden. Zudem offenbaren auch die bei Prüfungen vorgefundenen Mängel erhebliche Defizite in den Bereichen Datenschutz und -sicherheit (siehe auch 2.).

Die umfassende Vernetzung erzeugt ferner den Bedarf nach zentral angebotenen Datenschutz- und Datensicherheitsdienstleistungen (z. B. Schlüsselgenerierung und -verwaltung, Authentifizierung zugelassener Benutzer, Konzeption und Betrieb von Firewall-Systemen, vgl. 3.1.3), die ansonsten system- oder anwendungsbezogen von den jeweils zuständigen Behörden selbst entwickelt oder teuer extern eingekauft werden müssen. Auch hier ist das LIT gefordert.

3.1.2 Datenschutzanforderungen an die Routeradministration

Das technische Rückgrat der dargestellten flächendeckenden Vernetzung bilden sog. Router, die für die zielgerichtete Übermittlung der Datenströme zwischen räumlich entfernten lokalen Netzen sorgen. Diesen Routern kommt als zentralen Elementen der behördenübergreifenden Netzinfrastruktur auch unter Datenschutz- und -sicherheitsaspekten besondere Bedeutung zu. Maßnahmen auf Ebene der Router betreffen das Netzwerk als solches und sind unabhängig von dem Sicherungsstand der angeschlossenen Endgeräte.

Router heute üblicher Ausstattung verfügen über verschiedene Sicherheitselemente, die geeignet sind, den oben dargestellten Forderungen nachzukommen. Dazu ist eine entsprechende Konfiguration und Administration dieser Geräte erforderlich. Im einzelnen sind folgende Sicherheitsmaßnahmen zu treffen:

- Kontrolle der zulässigen Verbindungen auf Adress- und Dienstebene durch Konfiguration von Filtertabellen. Damit ist z. B. einstellbar, ob die Nutzung des Dateiübertragungsdienstes „ftp" generell oder nur von einem bestimmten Arbeitsplatz aus erlaubt oder verboten ist.

- Kontrolle der erreichbaren Subnetze durch statisches Routen. Beim statischen Routen kann der Verbindungsaufbau nur in fest definierte Subnetze erfolgen. Die Erreichbarkeit ist dabei bedarfsorientiert festzulegen.

- Bedingter Schutz vor aktiven Angriffen wie Maskerade, Adress-Spoofing und Source-Routing. Diese Form von Angriffen basiert auf der Möglichkeit, durch Änderungen von Netzwerkadressen und durch Ausnutzen bestimmter Routereigenschaften die eigenen Rechte zu erweitern. Moderne Router können hier Abhilfe schaffen.

- Schutz vor Manipulation der Router und somit Umgehung der vorgenannten Maßnahmen. Bei der Implementation von Sicherheitsmaßnahmen in den Routern werden diese zum vorrangigen Ziel eventueller Angriffe. Sie selbst sind daher entsprechend zu schützen.

Die genannten Sicherheitsmaßnahmen sind dabei ohne dauerhaften administrativen Mehraufwand realisierbar. Maßnahmen wie Filterung und statisches Routing wirken sich zudem positiv auf die Netzlast und die Netztransparenz aus und sind daher für den Netzbetreiber auch aus anderen Gründen von Vorteil.

Allerdings ist das Potential der Maßnahmen auf Routerebene begrenzt. Höheren Anforderungen hinsichtlich Filterung und Zugriffsschutz können Router nicht genügen. In solchen Fällen sind Firewall-Systeme erforderlich, die einen wesentlich besseren Schutz vor allem gegen Zugriffe von außen ermöglichen (siehe 3.1.3). Auch hinsichtlich der Sicherung von Vertraulichkeit und Integrität der übertragenen Daten sind Routern Grenzen gesetzt. Zwar kann durch statisches Routen ausgeschlossen werden, daß Datenströme beliebig umgelenkt werden können, doch ist ein effektiver Schutz gegen Kenntnisnahme und Manipulation von Daten nur durch deren Verschlüsselung möglich (siehe 3.1.4).

Das Landesamt für Informationstechnik hat ein Konzept für die Routeradministration vorgelegt, in dem auch Datenschutz- und Datensicherheitsaspekte berücksichtigt sind. Dieser begrüßenswerte Ansatz hat jedoch im Sinne der genannten Maßnahmen Ergänzungsbedarf. Die Abstimmung mit dem LIT ist noch nicht beendet.

3.1.3 Anforderungen an Firewall-Systeme

Der Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder hat unter Federführung des Hamburgischen Datenschutzbeauftragten eine Orientierungshilfe erarbeitet, die sich mit Datenschutzproblemen bei der Anbindung öffentlicher Stellen an globale Datennetze, speziell an das Internet, auseinandersetzt.

Mit der Netzanbindung verfolgen öffentliche Stellen mehrere Ziele:

- die Informationsgewinnung für die Wahrnehmung ihrer Aufgaben soll erleichtert werden,

- Bürger sollen zusätzliche Kommunikationsmöglichkeiten mit der Verwaltung erhalten (etwa über elektronische Post) und

- die Verwaltung will ihrerseits den Bürgern Informationen (z. B. Behördenwegweiser) auf elektronischem Wege zur Verfügung stellen.

Auch in der hamburgischen Verwaltung gibt es – insbesondere im Zusammenhang mit dem Vorhaben eines interaktiven Bürgerinformationssystems – entsprechende Bestrebungen. Dabei ist darauf hinzuweisen, daß der Anschluß an das Internet risikobehaftet ist und Strategien entwickelt werden müssen, wie diesen Gefahren zu begegnen ist (vgl. hierzu auch 4.1).

Wir sind mit dem Landesamt für Informationstechnik über Möglichkeiten des Anschlusses hamburgischer öffentlicher Stellen an das Internet im Gespräch. Solange eine den Anforderungen aus Sicht des Datenschutzes und der Datensicherheit entsprechende Lösung noch nicht realisiert ist, muß sich der Zugriff auf das Internet auf Rechner beschränken, die nicht in das Verwaltungsnetz eingebunden sind und auf denen keine sensiblen personenbezogenen Daten verarbeitet werden.

Im folgenden sollen die Kernaussagen der Orientierungshilfe dargestellt werden (die vollständige Orientierungshilfe kann bei Bedarf vom Hamburgischen Datenschutzbeauftragten abgefordert werden):

Wichtigstes Element von Sicherungskonzepten sind sogenannte „Firewalls" („Brandschutzmauern"). Darunter werden Schwellen zwischen zwei Netzen verstanden, die überwunden werden müssen, um Systeme im jeweils anderen Netz zu erreichen. Die Hauptaufgabe einer Firewall besteht darin, zu erreichen, daß jeweils nur zugelassene netzübergreifende Aktivitäten möglich sind und daß Mißbrauchsversuche frühzeitig erkannt werden. Üblicherweise wird dabei davon ausgegangen, daß die Teilnehmer des internen Netzes (hier: des Verwaltungsnetzes) vertrauenswürdiger sind als die Teilnehmer des externen Netzes (hier: des Internet). Gleichwohl sind Firewall-Lösungen auch geeignet, die „grenzüberschreitenden" Aktivitäten der internen Nutzer, d. h. den Übergang zwischen verschiedenen Teilnetzen (z. B. Ressortnetze) innerhalb eines Verwaltungsnetzes zu begrenzen.

Firewalls weisen die folgenden Charakteristika auf:

- die Firewall ist die definierte und kontrollierte Schnittstelle zwischen dem zu schützenden und dem nicht vertrauenswürdigen Netz;

- im internen Netz besteht jeweils ein einheitliches Sicherheitsniveau; eine weitere Differenzierung nach Sicherheitsstufen geschieht – zumindest auf der Ebene des Netzes – nicht;
- die Firewall setzt eine definierte Sicherheitspolitik für das zu schützende Netz voraus; in diese Sicherheitspolitik müssen die Anforderungen aller vernetzten Stellen einfließen;
- es besteht die Notwendigkeit einer firewallbezogenen Benutzerverwaltung derjenigen internen Teilnehmer, die mit Rechnern in dem externen Netz kommunizieren dürfen.

Zu unterscheiden sind zentrale und gestaffelte Firewall-Lösungen dadurch, daß bei gestaffelten Firewalls zusätzlich zu einem kontrollierten zentralen Netzübergang in das Internet besonders schützenswerte Bereiche (etwa Krankenhäuser) durch eigene Firewalls abgesichert werden.

Sofern ein Netz der öffentlichen Verwaltung mit dem Internet verbunden werden soll, müssen aus Datenschutzsicht folgende Voraussetzungen erfüllt sein:

- Der Anschluß von Verwaltungsnetzen muß dem datenschutzrechtlichen Erforderlichkeitsgrundsatz entsprechen, d.h. die Kommunikationsmöglichkeiten haben sich am Kommunikationsbedarf zu orientieren. Dabei ist auch zu prüfen, inwieweit das Behördennetz in anschließbare, nicht anschließbare und bedingt anschließbare Teile segmentiert werden muß.
- Die Sicherheit des Verwaltungsnetzes und der Schutz von personenbezogenen Daten, die auf vernetzten Systemen verarbeitet werden, ist durch geeignete Firewall-Systeme sicherzustellen, die eine differenzierte Kommunikationssteuerung und Rechtevergabe unterstützen. Dabei sind die Anforderungen, die von den Firewall-Komponenten zu erfüllen sind, vorab zu definieren.
- Der ausschließliche Einsatz einer zentralen Firewall-Lösung ist nur dann vertretbar, wenn eine Orientierung am höchsten Schutzbedarf erfolgt, auch wenn dies Nachteile für weniger sensible Bereiche mit sich bringt. Die Frage der Kontrolle interner Verbindungen bleibt bei einer solchen Lösung offen. Ferner ist eine ausschließlich zentrale Lösung mit der Maxime der lokalen Haltung und Verwaltung von sicherheitsrelevanten Daten (Pflege von Benutzerprofilen) schwer vereinbar. Werden solche Daten nicht durch diejenigen verwaltet, die den verwalteten Bereich direkt überschauen können, besteht die Gefahr erheblicher Differenzen zwischen Realität und sicherheitstechnischem Abbild.
- Das Konzept gestaffelter Firewalls kommt den Datenschutzanforderungen an Verwaltungsnetze entgegen, die aus einer Vielzahl verschiedener Teilnetze bestehen. Dort werden Daten unterschiedlicher Sensibilität von unterschiedlichen Stellen für unterschiedliche Aufgaben verarbeitet; dementsprechend bestehen jeweils unterschiedliche Sicherheitsanforderungen. Allerdings sollte die Anbindung des Gesamtnetzes an das Internet stets über ein zentrales Gateway erfolgen, das durch eine Firewall geschützt wird.
- Der personelle und sachliche Aufwand für Firewall-Lösungen ist generell hoch. Es ist gleichwohl unverzichtbar, hochspezialisierte Kräfte einzusetzen, um gegen mindestens ebenso spezialisierte Angreifer gewappnet zu sein. Dieser Aufwand ist stets dann gerechtfertigt, wenn Verwaltungsnetze an das Internet angeschlossen werden sollen, in denen sensible personenbezogene Daten verarbeitet werden.
- Der Betrieb von Firewall-Systemen muß klaren Richtlinien folgen. Diese Richtlinien müssen neben Zuständigkeitsregelungen auch Vorgaben über die Protokollierung, die Behandlung von sicherheitsrelevanten Ereignissen und Sanktionen bei Sicherheitsverstößen enthalten.
- Auch bei Einsatz von Firewalls bleiben Restrisiken bestehen, die anwendungsbezogen aufgefangen werden müssen. So bleibt es auch beim Einsatz von Firewalls notwendig, sensible Daten nur verschlüsselt zu übertragen (vgl. 3.1.4); hierzu gehören neben besonders sensiblen personenbezogenen Daten auch Paßwörter und sonstige Authentifikationsdaten. Bei einem unvertretbaren Restrisiko muß auf einen Anschluß des jeweiligen Netzes an das Internet verzichtet werden.

Firewall-Konzepte entlasten die dezentralen Verwalter von vernetzten Systemen nicht von ihrer Verantwortung zur Gewährleistung des Datenschutzes. Vielmehr erhöhen sich mit der Vernetzung die Anforderungen an die lokale Systemverwaltung, da Administrationsfehler ungleich schwerwiegendere Konsequenzen haben könnten als bei stand alone betriebenen Rechnern.

3.1.4 Verschlüsselte Datenkommunikation

Bei der Benutzung eines komplexen und vermaschten Behördengesamtnetzes kann eine unberechtigte Kenntnisnahme schützenswerter Daten nicht ausgeschlossen werden. Es ist deshalb notwendig, sensible personenbezogene Daten verschlüsselt zu übertragen.

Wir stoßen jedoch immer wieder auf Vorbehalte gegen die Einführung von Verschlüsselungsdiensten. Sowohl von Verfahrensverantwortlichen als auch vom Landesamt für Informationstechnik als Betreiber des Behördennetzes wird der erwartete Aufwand häufig als unverhältnismäßig groß dargestellt. Eine vorbehaltslose Prüfung des Aufwands ist dabei jedoch zumindest nicht immer erkennbar.

Doch auch in den Fällen, in denen der Aufwand für die Einführung von Verschlüsselungsdiensten gering ist, sind bislang keine entsprechenden Aktivitäten erkennbar. Dies verdeutlichen die folgenden Beispiele:

- Beim Versand von elektronischer Post ist es wünschenswert, eine fallweise Verschlüsselung von Dokumenten durchführen zu können. Dazu ist im Prinzip jedes Offline-Verschlüsselungsprogramm geeignet, solange dessen Verfügbarkeit beim Empfänger sichergestellt ist und Schlüsselaustauschverfahren etabliert sind. Daher könnte durch die Definition eines Produktstandards und die Festlegung organisatorischer Maßnahmen mit geringem Aufwand die Sicherheit deutlich verbessert werden (siehe auch 3.3).
- Bei der Nutzung des Telnet-Dienstes zur Anmeldung auf vernetzten UNIX-Hosts werden Authentifizierungs- und Inhaltsdaten ungeschützt über das Netzwerk übertragen. Die Verwendung von verschlüsselnden Telnet-Versionen bietet einen sehr guten Schutz gegen das eventuelle Abhören der Datenkommunikation. Solche Versionen sind frei verfügbar und könnten ohne großen Aufwand implementiert werden. Dennoch werden derartige Verfahren in der hamburgischen Verwaltung unseres Wissens nicht eingesetzt.

Aufgrund unserer durchweg positiven Erfahrungen mit Verschlüsselungstechniken und dem Mangel an gleichwertigen Alternativmaßnahmen werden wir in entsprechend gelagerten Fällen weiter auf eine verschlüsselte Übertragung im Netz drängen. Dabei kommen dem LIT als zentralem Anbieter eine besondere Bedeutung und neue Aufgaben zu. So weist die Stellung des LIT als Konzerndienstleister für die Freie und Hansestadt Hamburg dieses als besonders geeignet für die Errichtung eines sog. Trust Centers aus. Ein solches Trust Center ist als schlüsselverwaltende Stelle bei einer effektiv nutzbaren umfassenden Sicherheitsinfrastruktur unverzichtbar.

3.2 Datenschutz bei SAP

Kaum ein anderer Software-Hersteller in Europa hat im Augenblick derartige Zuwachsraten zu verzeichnen wie die Walldorfer Firma SAP. So ist es nicht verwunderlich, wenn SAP mittlerweile zum größten deutschen Softwarehaus aufgestiegen ist. Zwar werden SAP-Produkte immer noch hauptsächlich zur Unterstützung innerbetrieblicher oder verwaltungsinterner Abläufe eingesetzt, beispielsweise im Bereich Logistik, im Rechnungswesen und bei der Personalplanung. SAP ist jedoch dabei, neben ihren traditionellen Einsatzgebieten weitere Märkte zu erschließen.

Dementsprechend bezog sich die datenschutzrechtliche Diskusion um SAP in früheren Jahren fast ausschließlich auf den Bereich des Arbeitnehmer-Datenschutzes. Von Personal- und Betriebsräten wurde vor allem problematisiert, inwieweit die im Rahmen der Personalplanung erfaßten Arbeitnehmer-Daten zu Leistungs- und Verhaltenskontrollen zweckentfremdet genutzt werden können. Dabei galt es vor allem zu verhindern, daß Betriebsdaten, die beispielsweise in der Fertigung oder im Lager erhoben werden, aufgrund der hohen Integrationsdichte des Systems unbemerkt an anderer Stelle wieder auftauchen und mit Hilfe der SAP-Abfragesprache ABAP/4 beliebig ausgewertet werden.

Durch den Einzug von SAP in Bereiche, in denen über betriebliche Daten hinaus auch sensible Kunden- oder Patientendaten verwaltet werden, erhält die Auseinandersetzung um den Datenschutz eine neue Dimension.

3.2.1 Anpassung von Standardsoftware

Der SAP-Erfolg basiert nicht zuletzt auf der Strategie, Standard-Software anzubieten, die sämtliche betrieblichen Funktionen integriert abdeckt. Betriebsdaten müssen nur einmal erfaßt werden, Schnittstellenprobleme tauchen kaum auf. Da SAP-Software in fast allen Betrieben und Verwaltungen einsetzbar ist, besteht insbesondere für Großunternehmen die Chance, konzernübergreifend zu automatisieren.

Die ingenieurmäßige Sichtweise, sämtliche betrieblichen Funktionen aller Unternehmen durch eine Standard-Software abdecken zu wollen, setzt systemtechnisch einen hohen Grad von Modularisierung und Parametrisierung voraus. Jede betriebliche Funktion wird bei SAP in einem eigenen Modul abgebildet. Die Module werden wiederum über betriebs- bzw. anwendungsbezogene Parameter gesteuert. Die Verwaltung der Parameter erfolgt in nicht weniger als 600 verschiedenen Tabellen, die in einer Datenbank (der sogenannten "SAP") verwaltet werden. Wie komplex SAP-Software ist, zeigt sich schon darin, daß für die Lohn- und Gehaltsabrechnung allein hundert Tabellen existieren. Die Anpassung an betriebliche und verwaltungsspezifische Besonderheiten ist daher sehr aufwendig.

Das datenschutzrechtliche Problem liegt hauptsächlich darin, daß Standard-Software wie SAP eine Vielzahl von standardisierten Datenkatalogen beinhaltet, die in der praktischen Anwendung ohne genaue Anpassung an betriebliche oder verwaltungsspezifische Besonderheiten übernommen werden. Statt anwendungsorientiert zu spezifizieren, welche personenbezogenen Daten zur eigentlichen Aufgabe benötigt werden, wird eher umgekehrt vorgegangen. Die Standardlisten werden nur noch dahingehend geprüft, ob personenbezogene Daten existieren, die aufgrund besonderer personal- oder datenschutzrechtlicher Regelungen auf gar keinen Fall erhoben werden dürfen. Eine derartige Vorgehensweise läßt sich jedoch schwer mit dem Datenschutzrecht vereinbaren, das grundsätzlich zum Schutz des einzelnen vor möglichen Gefährdungen und Beeinträchtigungen seines Rechts auf informationelle Selbstbestimmung von einem Verarbeitungsverbot mit Erlaubnisvorbehalt ausgeht.

Bei der Anpassung der Datenbestände an betriebliche oder verwaltungsspezifische Besonderheiten erfolgt keine Optimierung der Masken. Zum einen werden nicht mehr benötigte Daten lediglich durch eine andere farbliche Codierung des Eingabefeldes gekennzeichnet, so daß die entsprechenden Datenfelder weiterhin sichtbar sind. Zum anderen werden bei einer Reduzierung der Eingabefelder keine Masken zusammengefaßt, wie es wünschenswert wäre.

3.2.2 Berechtigungskonzept

Die Zugriffskontrolle erfolgt bei SAP-Produkten durch das Berechtigungskonzept, das Bestandteil des zentralen Basissystems ist. Das Basissystem, das für die Anpassung an die jeweilige Hardware und das eingesetzte Rechner-Betriebssystem sorgt und die Verbindung zwischen Programmodulen und ATAB-Datenbank herstellt, liefert u.a. Grundfunktionen für die Benutzerverwaltung, die Protokollierung und den Zugriffsschutz. Als Basissysteme sind die Produkte R/2 und R/3 auf dem Markt.

Während R/2 ein traditionelles, transaktionsorientiertes Großrechnersystem ist, das speziell für die Betriebssysteme MVS bzw. BS 2000 konzipiert wurde, basiert das Basissystem R/3 auf einer Client-Server-Architektur mit UNIX als Server-Betriebssystem. Obwohl R/2 langfristig durch das Basissystem R/3 abgelöst werden soll, hat es immer noch sehr große Bedeutung. So existieren zahlreiche SAP-Module, die bislang nur unter R/2 verfügbar sind. R/3 ist im Gegensatz zu R/2 kein proprietäres System mehr, das eine vollständige SAP-Umgebung im Betrieb voraussetzt und auf einer SAP-spezifischen Datenverwaltung aufbaut. Es ist als offenes System konzipiert, so daß zwischen mehreren SQL-Datenbanksystemen wie beispielsweise INFORMIX oder ORACLE ausgewählt werden kann. Der Vorteil für SAP-Anwender besteht u.a. darin, daß Datenbank-Auswertungen nicht mehr zwingend die SAP-eigene Abfragesprache ABAP voraussetzen, sondern auch in anderen Programmiersprachen geschrieben werden können.

Es existieren zwei Versionen des Berechtigungskonzepts, die sich qualitativ deutlich unterscheiden. So weist das ältere Berechtigungskonzept, das in der R/2-Version 4.3 zum Einsatz kommt, zahlreiche Schwachstellen auf: Dort können die Zugriffsrechte weder zeitlich begrenzt noch differenziert mit getrennter Lese- und Schreibberechtigung für unterschiedliche Bereiche vergeben werden. Statt dessen sind für eine einzelne Person mehrere Kennungen mit jeweils eigenen Benutzerstammsätzen anzulegen. Auch benötigt der für die Vergabe der Zugriffsrechte zuständige Administrator für seine Aufgabe umfangreiche Zugriffsrechte, die weit über das für die SAP-Verwaltung erforderliche Maß hinausgehen.

Hauptsächlich aus der Kritik an dem Berechtigungskonzept der R/2-Version 4.3 resultierend ist von SAP vor einigen Jahren mit der R/2-Version 5.0 ein neues Konzept vorgelegt worden, das auch für das Basissystem R/3 übernommen wurde. Das Berechtigungskonzept, das sich bei näherem Hinsehen als ein transaktionsorientiertes System zur Vergabe von Zugriffsrechten darstellt und fast alle Kombinationen zuläßt, besteht insgesamt aus folgenden Komponenten (die Erläuterungen entsprechen weitgehend der SAP-Originalsprache):

- Ein Feld definiert zu schützende SAP-Elemente (z. B. Buchungskreise, Tabellen) sowie zu schützende Aktivitäten bzw. Transaktionscodes (z. B. Ändern, Hinzufügen, Löschen).
- Ein Objekt stellt eine Kombination von max. 10 Feldern dar und kann sich auf mehrere SAP-Elemente beziehen.
- Berechtigungen beziehen sich auf ein Objekt und stellen die Zuordnung von Werten zu den Feldern eines Objekts dar. Die Prüfung der Berechtigung erfolgt gegenüber den Feldinhalten.
- Sammelberechtigungen fassen mehrere Berechtigungen zusammen, die sich auf dasselbe Objekt beziehen.
- Ein Profil ist eine Auflistung von Berechtigungen bzw. Sammelberechtigungen und bezieht sich auf einen Arbeitsplatz bzw. Anwendungsbereich. Sammelprofile fassen wiederum mehrere Profile zusammen, können jedoch auch aus mehreren Sammelprofilen bestehen.
- Benutzerstammsätze beinhalten schließlich die für einen Benutzer zugelassenen Profile bzw. Sammelprofile. Änderungen, die sich innerhalb eines Sammelprofils vollziehen, wirken sich auf alle Benutzer aus, die das Sammelprofil besitzen.

Darüber hinaus können innerhalb einer Anwendung Mandanten gebildet werden, auf die mit unterschiedlichen Rechten zugegriffen wird. Ebenfalls positiv zu bewerten ist die Tatsache, daß die Verwaltung von Berechtigungen und Profilen durch eine getrennte Pflege- und Aktivversion unterstützt wird, so daß veränderte Zugriffsberechtigungen ausführlich getestet werden können. Da das neue Berechtigungskonzept im Unterschied zum alten Konzept auch eine Funktionstrennung im Bereich der Systemverwaltung ermöglicht, kann die Aktivierung der Testversion zudem arbeitsteilig durch einen sogenannten Aktivierungsadministrator durchgeführt werden. Die Vergabe neuer Paßwörter und anderer Benutzerstammdaten kann durch einen sogenannten Benutzeradministrator erfolgen, während der sogenannte Berechtigungsadministrator die (Sammel-)Profile und (Sammel-)Berechtigungen pflegt.

Die Vielzahl von Möglichkeiten der Rechtevergabe ist jedoch nicht uneingeschränkt positiv zu bewerten. Eine Schwäche des Berechtigungskonzepts liegt vor allem in der Gefahr einer möglichen Fehlanwendung, die in der Komplexität des Systems ihre Ursache haben kann.

Nicht durch entsprechende SAP-Funktionen unterstützt wird der Wechsel auf andere Benutzerkennungen, der erforderlich ist, falls sich mehrere Benutzer einen Arbeitsplatzrechner teilen. Statt den Benutzerwechsel auf Maskenebene durchzuführen, muß sich zunächst der angemeldete Benutzer am System abmelden, bevor der nächste Benutzer das System neu starten und seine Anwendungsmaske anwählen kann. Da ein solches Verfahren in vielen Fällen, beispielsweise auf Krankenhaus-Stationen, nicht praktizierbar ist, sind Gruppenpaßwörter häufig der einzige Ausweg. Gruppenpaßwörter sind problematisch, da sie zum einen erheblich schwieriger geheim gehalten werden

können. Zum anderen ist der regelmäßige Wechsel von Gruppenpaßwörtern kaum realisierbar. Falls Gruppenpaßwörter dennoch vergeben werden sollen, ist zumindest sicherzustellen, daß der Aufruf von Gruppenkennungen auf einzelne, einer räumlichen Zugangskontrolle unterliegende Arbeitsplatzrechner beschränkt bleibt. Leider kann auch diese Datenschutzanforderung durch SAP nicht realisiert werden, da die Zugriffsrechte durch das Berechtigungskonzept nicht terminalbezogen vergeben werden können.

Insgesamt bleibt festzustellen, daß das neue Berechtigungskonzept von SAP trotz zahlreicher Vorzüge gegenüber der alten Version noch einige Schwachstellen aufweist. Während die mit der Systemanpassung zusammenhängenden Datenschutzprobleme weitgehend vom Anwender zu lösen sind, sollte SAP gerade im Bereich des Basissystems weitere Verbesserungen vornehmen.

3.3 Elektronische Post gemäß X.400

Im letzten Tätigkeitsbericht (13.TB, 3.4) hatten wir über das Projekt Elektronische Post in der hamburgischen Verwaltung gemäß X.400 berichtet und datenschutzrechtliche Anforderungen für den Betrieb von elektronischen Postsystemen formuliert.

Inzwischen hat – nach mehr als fünfjährigen Vorarbeiten – das Landesamt für Informationstechnik (LIT) am 1. Oktober 1995 seinen X.400-Dienst in Betrieb genommen, obwohl der vorangegangene Testbetrieb, an dem auch der Hamburgische Datenschutzbeauftragte beteiligt war, gravierende Datenschutzmängel der eingesetzten Mail-Produkte ergeben hatte:

- Die eingesetzte Software erzwingt nicht durchgängig die Vergabe eines Paßworts und entspricht insofern nicht dem Stand der Technik. Im Test konnten wir feststellen, daß mehrere Benutzer ihre elektronischen Postfächer ungesichert ließen und somit die an sie gerichtete Post von Dritten problemlos gelesen, gelöscht oder geändert werden konnte.
- Das Mail-Produkt unterstützt nicht die verschlüsselte Übertragung elektronischer Post.

Entsprechend der Forderung des Bund-/Länder-/Gemeinden-Kooperationsausschusses für ADV (KoopA-ADV) halten wir verwaltungsübergreifende Verschlüsselungs- und Authentifizierungsverfahren für dringend erforderlich, damit den mit dem Einsatz elektronischer Post verbundenen Risiken wirksam begegnet werden kann (ein entsprechender Dienst wäre durch das LIT anzubieten – vgl. 3.1.4). Solange keine Verschlüsselungsmöglichkeiten bestehen, kann elektronische Post in Bereichen, in denen sensible Daten verarbeitet werden, nicht eingesetzt werden.

Soweit die Mängel nicht abgestellt sind, bleibt es den Anwendern überlassen, den Problemen durch einen vorsichtigen Umgang zu begegnen (Durchsetzung

Paßwortvergabe durch organisatorische Maßnahmen, Verzicht auf den sensibler Daten).

LIT als Anbieter und auch die Behörden als Nutzer des Dienstes haben zudem an die Vorgaben der ergänzten Durchführungsbestimmungen zur kommunikationsrichtlinie (Anlage 1 zu den TK-DB) zu halten, die detaillierte Sicherungsanforderungen für die Inanspruchnahme des X.400-Dienstes

Prüfung der Datenverarbeitung der Behörde für Arbeit, Gesundheit und Soziales

Hamburgische Datenschutzbeauftragte hat im Berichtsjahr die Sicherheit tzes der Behörde für Arbeit, Gesundheit und Soziales (BAGS) sowie die heit der auf Personalcomputern, lokalen Netzen und Abteilungsrechnstallierten Verfahren geprüft. Trotz einiger Kritikpunkte kann die Sicherheit der Datenverarbeitung in der BAGS als ausreichend bezeichnet werden.

Kritik sowie Verbesserungsvorschläge bezogen sich hauptsächlich auf figuration der für die Netzsicherheit wichtigen Netzwerkrechner sowie Administration der vernetzten und unvernetzten Personalcomputer. Die BS hat zugesagt, die Netzwerksicherheit sowie die PC-Administration zu essern.

elne Probleme des Datenschutzes öffentlichen Bereich

Neue Medien/Telekommunikation

weite Vernetzung durch das Internet

ternet umfaßt z. Zt. mehr als 4 Millionen Knotenrechner und hat mehr als llionen Nutzer. Über direkt ans Internet angeschlossene Rechner oder Online-Dienste, von denen einige ihren Sitz in Hamburg haben, können mehr Benutzer auf ein breites Informationsangebot zugreifen, elektroche Post versenden oder empfangen und Programme von entfernten Rechnladen. Ferner haben sie die Möglichkeit, selbst als Informationsanbieter treten, z. B. durch Veröffentlichung von Artikeln in sogenannten newsoder durch persönliche Seiten innerhalb des WorldWideWeb.

gs ist darauf hinzuweisen, daß die Nutzung des Internet mit datenschutzrechtlichen Risiken verbunden ist:

Im Internet, das bislang im wesentlichen wissenschaftlichen Zwecken dient, ist eine vertrauliche Kommunikation nicht gewährleistet, da dieses Netz keine Sicherheitsmaßnahmen vorsieht. An beliebiger Stelle (etwa bei einem der vielen Netzknoten, über die eine Nachricht geleitet wird) kann „ab-

gehört" und mitgeschnitten werden. Zudem können Nachrichten unberechtigt verändert, gefälscht, unterdrückt oder verzögert werden. Es gibt keinen Betreiber, der für die Sicherheit des Internet verantwortlich wäre. Gleichwohl wird das Netz zunehmend auch für geschäftliche Zwecke genutzt, bei denen personenbezogene und andere sensible Daten übertragen werden.

- Die Inanspruchnahme von Internet-Diensten ist im Regelfall nicht anonym. Jeder Nutzer hinterläßt eine Datenspur, d.h. es kann im Prinzip festgestellt werden, wer wann welche Informationen abgerufen hat oder wer mit wem elektronisch korrespondiert. Diese Datenspuren können – ohne Wissen der Betroffenen – zu Kommunikationsprofilen verdichtet werden.
- Es ist möglich, daß Teilnehmer mit gefälschten Kennungen arbeiten. Diese Schwäche ist bereits mehrfach dazu benutzt worden, um in unzureichend gesicherte entfernte Rechner einzudringen, dort gespeicherte Informationen auszuspionieren, zu manipulieren oder zu löschen.
- Schließlich eignet sich das Internet zur schnellen Übertragung von großen Datenmengen zu beliebigen anderen, an das Netz angeschlossenen Rechnern. Damit erhöht sich die Gefahr, daß personenbezogene Daten gezielt in solche Länder übertragen werden, in denen der Datenschutz nicht gewährleistet ist.

Angesichts der begrenzten Reichweite nationaler Gesetze besteht die Notwendigkeit, das internationale Datenschutzrecht den neuen technischen Gegebenheiten anzupassen, damit die Nutzer von Informationsdienstleistungen nicht schutzlos werden (vgl. 4.2.3). Unabhängig hiervon sind die Benutzer angesichts der Datensicherheitsmängel gut beraten, die Dienste mit Bedacht zu gebrauchen und insbesondere keine vertraulichen Mitteilungen – etwa Kreditkartenangaben – über das Internet zu versenden. Einen gewissen Schutz gegen die unberechtigte Kenntnisnahme bieten zwar Verschlüsselungsverfahren, die jedoch nicht überall verfügbar sind. Sie schützen zudem nicht gegen die Bildung von Kommunikationsprofilen. Die Anbieter von Diensten und Netzen müssen daher die Benutzer über die Risiken aufklären.

4.2 Datenschutzrechtliche Probleme bei Online-Diensten

Die Frage, wie Menschen vor der Registrierung ihres Mediennutzungsverhaltens geschützt werden können, beschäftigt die Datenschutzbeauftragten schon seit langem (vgl. 2. TB, 2.6.4). Sie ist heute mit dem Aufkommen von Online-Diensten und Multimediaanwendungen aktueller denn je.

4.2.1 Grundrecht auf unbeobachtete Mediennutzung

Da die Nutzung von Online-Diensten für immer mehr Menschen alltäglich wird und immer weitere Angebote in elektronischer Form zur Verfügung gestellt werden (neben elektronischen Informationsangeboten auch und vor allem elektronische Unterhaltung, Video usw.), sollte der Schutz der Nutzungsdaten

auf eine Ebene mit dem Schutz des Fernmeldegeheimnisses gestellt und strafrechtlich bewehrt werden.

Deshalb sollte ein Mediennutzungsgeheimnis in Art. 5 oder in Art. 10 Grundgesetz aufgenommen werden. Dies hätte zur Konsequenz, daß grundrechtsbeschränkende Maßnahmen nur unter gesetzlich definierten Voraussetzungen zulässig wären.

4.2.2 Datenschutz- und medienrechtlicher Rahmen

Anfang der 80er Jahre wurde das Regelungskonzept entwickelt, das die Grundlage für den Bildschirmtext-Staatsvertrag von 1984 bildete und mit wenigen Änderungen auch bei der Neufassung 1991 beibehalten wurde. Durch den Btx-Staatsvertrag wird die zulässige Verbindungsdatenspeicherung stark begrenzt und die Verarbeitung von Verbindungs- und Gebührendaten einer strikten Zweckbindung unterworfen.

Auch wenn der Btx-Staatsvertrag hinsichtlich seiner Regelungsziele und der engen Begrenzung der Verarbeitung von Verbindungsdaten im Grundsatz durchaus als geeignet erscheint, den datenschutzrechtlichen Rahmen für Online-Dienste abzustecken, besteht die Notwendigkeit zu seiner Anpassung an die seitherige Entwicklung, insbesondere an den technischen Fortschritt.

Anpassungsbedarf besteht nicht nur im Hinblick auf neue Online-Dienste, sondern auch für den von der Deutschen Telekom AG unter dem Namen „T-Online" betriebenen Bildschirmtextdienst selbst, der sich hinsichtlich seiner Angebote und seines Betriebs seit 1984 deutlich weiterentwickelt hat.

Bestimmungen, die sich auf den Abruf von „Bildschirmtextseiten" beziehen, müssen überarbeitet werden, da eine seitenorientierte Betrachtungsweise angesichts der vielfältigen Präsentationsformen von Online-Angeboten heute nicht mehr angemessen ist. Außerdem sollte das integrierte Angebot von Bewegtbildern und Audiodateien auf Abruf, das bisher überwiegend dem Rundfunk zugeordnet wird, in die rechtlichen Regelungen für Online-Dienste einbezogen werden.

Ferner muß darauf reagiert werden, daß moderne Online-Dienste ihren Nutzern viele Angebote unter eigener Regie und auf eigene Rechnung zur Verfügung stellen. Damit wird ein zentraler Aspekt des Btx-Staatsvertrages tangiert, der von einer Trennung zwischen dem Betreiber des Dienstes und den Anbietern ausgeht, die den Inhalt liefern. So dürfen gemäß § 10 Abs. 3 Btx-Staatsvertrag die Btx-Betreiber den Anbietern Abrechnungsdaten nur übermitteln, soweit eine Forderung auch nach Mahnung nicht beglichen wird. Dabei sind die Abrechnungsdaten grundsätzlich so zu speichern, daß Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter in Anspruch genommener Angebote nicht erkennbar sein dürfen.

Bei der Neuregelung ist zu gewährleisten, daß Online-Dienste auch bei eigenen Angeboten nicht mehr Daten speichern, als Anbieter nach dem Btx-Staatsvertrag zulässigerweise erhalten dürften. Daten, die bei dem Betrieb des Dienstes entstehen, jedoch für die Abrechnung des Angebotes nicht erforderlich sind, unterliegen nach § 10 Abs. 2 Btx-Staatsvertrag ohnehin einer strikten Zweckbindung.

Soweit nutzungsbezogene Entgelte erhoben werden, müssen die Teilnehmer die Möglichkeit bekommen, die Angebote auch anonym in Anspruch zu nehmen. Dies wäre z. B. durch den Einsatz von Guthabenkarten – ähnlich wie Telefonkarten – als Prepaid-Verfahren zu realisieren (vgl. 13. TB, 4.2).

4.2.3 Internationale Online-Dienste

Probleme ergeben sich auch daraus, daß die Datenverarbeitung bei Online-Diensten häufig geographisch vom Ort des Zugangs getrennt erfolgt, teilweise sogar auf einem anderen Kontinent. So wird z. B. ein elektronischer Brief, den ein deutscher Teilnehmer eines amerikanischen Datendienstes an einen anderen deutschen Teilnehmer desselben Dienstes sendet, stets über die Zentrale in den USA geleitet. Der Zugriff auf das Internet oder auf andere nicht zum Dienst selbst gehörende Angebote wird ebenfalls über den jeweiligen zentralen Rechner des Dienstes geleitet.

Da die in Deutschland aktiven Online-Dienste – auch jene mit Schwerpunkt in anderen Ländern – jeweils über inländische Geschäftsstellen verfügen, haben sie das deutsche Medien- und Datenschutzrecht zu beachten und künftig die Vorgaben der EG-Datenschutzrichtlinie einzuhalten.

Soweit ein Dienst mit Sitz in Deutschland personenbezogene Daten im Ausland verarbeitet und nutzt, muß er die Einhaltung der datenschutzrechtlichen Vorgaben zumindest vertraglich gegenüber seinen deutschen Kunden sicherstellen und sich durch die Aufsichtsbehörde im jeweiligen Bundesland kontrollieren lassen. Die deutsche Geschäftsstelle hat auch die Rechte der Betroffenen auf Auskunft, Sperrung und Löschung gegenüber ihrer ausländischen Muttergesellschaft sicherzustellen, soweit dort Daten verarbeitet werden.

Wenn ein Dienst seinen Sitz nicht im Inland hat und personenbezogene Daten im Ausland verarbeitet und nutzt, muß er einen Beauftragten im Inland bestellen, wie sich aus § 2 Abs. 3 Bildschirmtext-Staatsvertrag ergibt. Eine ähnliche Bestimmung enthält nun auch die EG-Datenschutzrichtlinie.

Eine deutsche staatsvertragliche Regelung und eine internationale Regelung in Europa und über den EU-Bereich hinaus ist – auch aus Gründen der Wettbewerbsgleichheit für die Unternehmen – anzustreben. Dabei wird die Eigenart der neuen interaktiven und multimedialen Online-Dienste angemessen zu berücksichtigen sein. Für die Regelungen wäre es wiederum sachgerecht,

liche Bestimmungen aus dem Bildschirmtext-Staatsvertrag gerade zum schutz zu übernehmen und fortzuentwickeln.

tere Liberalisierung der Telekommunikation

Schwelle zum 21. Jahrhundert zeichnet sich eine grundlegende Verän- der globalen Informations- und Kommunikationsinfrastruktur ab. Die zung von elektronischen Medien zur Unterhaltung, Information und Kom- on nimmt explosionsartig zu.

über der heutigen Situation werden unvergleichlich mehr personenbe- Daten durch mehr Stellen registriert und ausgewertet werden können. sind alle, die fernsehen, telefonieren, fernkopieren, Texte und Do- über Datenleitungen schicken oder Telebanking oder Teleshopping be- Die Risiken für den Einzelnen durch die vermehrten Möglichkeiten der s- und Umfeldkontrolle oder der Ausforschung persönlicher Lebens- heiten und Eigenschaften vergrößern sich entsprechend (vgl. 4.1, 4.2).

chen nimmt auch der rechtliche Regelungsrahmen für den Bereich der mmunikation Gestalt an. Im Jahr 1995 überschnitten sich die Bemühun- Konsequenzen aus der Postreform II durch eine „Verordnung über den schutz für Unternehmen, die Telekommunikations- und Informations- leistungen erbringen" (TIDSV) zu ziehen, mit den Arbeiten an einer Post- , bei der – europarechtlichen Vorgaben folgend – nun auch das Tele- und das Netzmonopol der Deutschen Telekom abgeschafft werden

en Rechtsetzungsvorhaben wird leider die Tendenz deutlich, den chutzstandard gegenüber dem bisherigen Niveau abzusenken.

nschutzbeauftragten des Bundes und der Länder haben sowohl zum der TIDSV als auch zum Telekommunikationsgesetz (TKG), das den en Kern der Postreform III bildet, in Entschließungen kritisch Stellung en. Sie haben darauf hingewiesen, daß ein wirksamer Datenschutz berechtigtes Regulierungsziel bleiben muß.

technischen Gestaltung der kommunikationstechnischen Infrastruktur die Datenvermeidung und die strikte Begrenzung der Datenverarbei- das erforderliche Ausmaß Vorrang behalten. Netzbetreiber und Dien- ieter sollten verpflichtet werden, überall dort, wo dies technisch möglich anonyme Zugangs- und Nutzungsformen für ihre Leistungen bereit- n. Für eine sichere Datenübertragung sind ohne prohibitive Zusatz- wirksame Verschlüsselungsverfahren erforderlich (vgl. 3.1.4).

ht auf informationelle Selbstbestimmung und das Fernmeldegeheim- issen für alle Netzbetreiber und Diensteanbieter ungeachtet ihrer form und ihrer Kundenstruktur (z. B. sog. Corporate Networks) einheit- einem hohen Niveau gesichert werden.

Entscheidend für die Wirksamkeit des Grundrechtsschutzes ist die strikte Einhaltung der Zweckbindung der Verbindungs- und Rechnungsdaten.

Für den Kunden bzw. Teilnehmer ist es von größter Bedeutung, die Verarbeitungsvorgänge im TK-Bereich überschauen zu können. Er muß über die Nutzungsrisiken bestimmter Kommunikationstechniken (z. B. Mobilfunk) ebenso wie über seine Widerspruchsmöglichkeiten umfassend aufgeklärt werden. Keinesfalls darf die Einwilligung des Betroffenen mißbraucht werden, um bereichsspezifische Schutznormen oder effiziente Datensicherungsvorkehrungen zu umgehen.

Um auch und gerade für das besonders schutzwürdige Fernmeldegeheimnis einen durchgängig hohen Schutzstandard zu sichern, braucht es eine unabhängige Kontrolle nach bundesweit einheitlichen Kriterien. Die Zuweisung dieser Überwachungsaufgabe an die im TKG-Entwurf vorgesehene Regulierungsbehörde ist aber wegen deren mangelhafter Unabhängigkeit und der von ihr wahrzunehmenden Regulierungsaufgaben, die mit Interessenkonflikten verbunden sein werden, nicht akzeptabel.

5. Sozialwesen

5.1 Unfallversicherung

Besonders intensiv hat uns im Berichtszeitraum das Recht der gesetzlichen Unfallversicherung beschäftigt. Ein wesentlicher Gegenstand unserer Tätigkeit war insoweit der Gesetzentwurf der Bundesregierung zu einem Unfallversicherungs-Einordnungsgesetz (UVEG). Das Feststellungsverfahren der Landesunfallkasse haben wir im Januar 1995 einer datenschutzrechtlichen Prüfung unterzogen.

5.1.1 Feststellungsverfahren der Landesunfallkasse (LUK)

Etwa 70 % der entstehenden Versicherungsfälle bei der LUK sind Bagatellfälle, in denen die LUK von sich aus keine weiteren Ermittlungen vornimmt. Das Feststellungsverfahren bei Berufsunfällen und -krankheiten in den anderen Fällen haben wir unter datenschutzrechtlichen Gesichtspunkten geprüft und sind dabei auf mehrere verbesserungsbedürftige Verfahrensweisen gestoßen.

Der Gesetzgeber hat in § 67a Abs. 2 Sozialgesetzbuch/Zehntes Buch (SGB X) bestimmt, daß Daten in der Regel beim Betroffenen und nur unter bestimmten Ausnahmen bei anderen Stellen zu erheben sind. Dies gilt auch für die gesetzliche Unfallversicherung. Die bislang bekannt gewordenen Entwürfe zum UVEG (5.1.2) enthalten keinen Ansatz, bereichsspezifisch für die gesetzliche Unfallversicherung eine Modifizierung oder gar Umkehrung dieses Regel-Ausnahme-Verhältnisses vorzunehmen.

Bei der LUK ist es aber die klare Ausnahme, daß Daten unmittelbar beim Betroffenen erhoben werden. Die LUK ist insoweit der Auffassung, daß die Besonderheiten des Feststellungsverfahrens eine überwiegende Datenerhebung bei Dritten bedingen. Nach unserer Auffassung kann die LUK gleichwohl in stärkerem Maße als bislang Daten unmittelbar beim Betroffenen erheben und sich weniger häufig an Dritte wenden, zu denen Arbeitgeber und Krankenkassen gehören. Die LUK will den Ersterhebungsgrundsatz daher in Zukunft verstärkt beachten.

Bei der Datenerhebung wurden bislang zudem die gesetzlichen Hinweispflichten nach § 67a Abs. 3 und 4 SGB X zu wenig berücksichtigt. Nach diesen Vorschriften muß der Betroffene bei der Datenerhebung darauf hingewiesen werden, zu welchem Zweck die Erhebung erfolgt, welche Rechtsvorschrift ihn ggf. zur Auskunft verpflichtet, ob die Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen ist, welche Folgen die Verweigerung von Angaben hat und (sonst) daß die Angaben freiwillig sind. Nicht-öffentliche Stellen sind auf eine Rechtsgrundlage, die sie zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen. Unsere Verbesserungsvorschläge dazu hat die LUK inzwischen weitgehend aufgegriffen.

Zu unvollständig wurden die Betroffenen bislang darüber informiert, von wem und wohin im Feststellungsverfahren ärztliche Daten übermittelt werden. Diese Information ist für den Betroffenen deshalb wichtig, weil er der Übermittlung nach § 76 Abs. 2 Nr. 1 SGB X widersprechen darf. Dieses Widerspruchsrecht kann qualifiziert aber nur bei vorheriger Kenntnis der Übermittlungsadressaten wahrgenommen werden. Auch diesbezüglich hat die LUK unsere Verbesserungsvorschläge weitgehend aufgegriffen.

Erstaunt hat uns, daß die LUK Angaben über Berufskrankheitenfälle in personenbezogener Form an ihren Bundesverband übermittelt, der damit eine Statistik (sog. BK-DOK) aufbauen soll. Wir haben die LUK darauf hingewiesen, daß dies unzulässig ist und diese Übermittlungen nur in anonymisierter Form erfolgen dürften. Die LUK hat dieses Verfahren bislang aber nicht eingestellt, sondern lediglich eine Stellungnahme ihres Bundesverbandes erbeten, die noch aussteht.

Datenschutzrechtlich bedenklich ist es im übrigen, daß die LUK dem staatlichen Gewerbearzt routinemäßig vollständige Berufskrankheitenakten übersendet. Denn damit einhergehend erfolgt stets eine Übermittlung sämtlicher personenbezogenen Daten über den Versicherten, einschließlich erstellter Gutachten.

Die Beteiligung des staatlichen Gewerbearztes durch den Unfallversicherungsträger hat sich im wesentlichen nach den Bestimmungen der Berufskrankheiten-Verordnung (BKVO) zu richten. Nach der BKVO ist der Unfallversicherungsträger verpflichtet,

- der für den medizinischen Arbeitsschutz zuständigen Stelle Gelegenheit zur Äußerung zu geben, wenn beabsichtigt ist, einem Versicherten eine bestimmte Tätigkeit zu untersagen (§ 3 Abs. 1 Satz 3 BKVO),

- der für den medizinischen Arbeitsschutz zuständigen Stelle eine Ausfertigung der von Ärzten oder Unternehmern erstatteten Berufskrankheitenanzeige zu übersenden (§ 7 Abs.1 Satz 1 BKVO),

- von der für den medizinischen Arbeitsschutz zuständigen Stelle gemachten Beweiserhebungsvorschlägen grundsätzlich zu entsprechen (§ 7 Abs. 2 Sätze 2 und 3 BKVO),

- der für den medizinischen Arbeitsschutz zuständigen Stelle Kenntnis von der Einleitung und dem Ergebnis seiner Ermittlungen zu geben (§ 7 Abs. 3 Satz 2 BKVO).

Eine regelmäßige Übersendung der vollständigen Akte ist damit nicht vorgesehen und muß danach unterbleiben. Sie geht insbesondere über die Mitteilung der Einleitung und des Ergebnisses der Ermittlungen deutlich hinaus. Nach unserer Auffassung stellen im übrigen auch § 70 SGB X und § 69 Abs. 1 Nr. 1 SGB X keine ausreichende Rechtsgrundlage für die routiemäßige Übersendung der vollständigen Akten dar. Ehe diese Praxis eingestellt wird, sollte aber zunächst abgewartet werden, ob hierzu eine Klärung im UVEG erfolgt.

5.1.2 Unfallversicherungs-Einordnungsgesetz (UVEG)

Das UVEG (zuletzt Bundestagsdrucksache 13/2204) haben wir in einer Arbeitsgruppe mit dem Bundesdatenschutzbeauftragten und einem weiteren Landesdatenschutzbeauftragten begleitet und die datenschutzrechtlich kritischen Punkte herausgearbeitet. Auf dieser Grundlage hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf ihrer Konferenz am 9./10. März 1995 folgende Entschließung gefaßt:

Verfassungsgemäßer Datenschutz für Unfallversicherte erforderlich

Durch die Träger der gesetzlichen Unfallversicherung werden oft Daten der Versicherten hinter deren Rücken oder zumindest ohne deren konkrete Kenntnis erhoben und weitergegeben. Der vorliegende Entwurf des Bundesministers für Arbeit und Sozialordnung zum Unfallversicherungs-Einordnungsgesetz – SGB VII sieht dazu keine Änderungen vor.

Aus dem Recht auf informationelle Selbstbestimmung der Versicherten, insbesondere auf Transparenz der einzelnen Verfahrensschritte, ergeben sich mehrere grundlegende Forderungen, die bei einer Überarbeitung des Gesetzentwurfes berücksichtigt werden müssen:

[redacted]spflicht behandelnder Ärzte gegenüber Unfallversicherungsträ-

[redacted]delnde Ärzte sollte eine gesetzliche Auskunftspflicht gegenüber Un-[redacted]cherungsträgern nur festgelegt werden, soweit dies erforderlich ist für [redacted]chgerechte und schnelle Heilung (§ 557 Abs. 2 RVO – § 34 Referenten-[redacted] SGB VII). Die gesetzliche Auskunftspflicht ist daher auf Angaben über [redacted]handlung und den Zustand des Verletzten zu beschränken. Danach dür-[redacted]erkrankungen, die aus Sicht des Arztes mit dem aktuellen Status in kei-[redacted]sammenhang stehen oder keine Bedeutung im Zusammenhang mit [redacted]beitsunfall oder der Berufskrankheit haben, nicht übermittelt werden [redacted] Handverletzung und Salmonellenerkrankung).

[redacted]erhebung, -verarbeitung und -nutzung durch Durchgangsärzte und [redacted]skrankheitenärzte

[redacted] von Unfallversicherungsträgern bestellte Durchgangsärzte personenbezogene Daten über den Unfallverletzten erheben und Unfallversicherungsträgern und anderen Stellen mitteilen, muß dies auf eine normenklare gesetzliche Grundlage gestellt werden; die bisherige Regelung in dem zwischen den [redacted]en der Kassenärzte und der Unfallversicherungsträger geschlossenen „Heilabkommen" reicht für die damit verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht der Betroffenen nicht aus. Entsprechendes gilt für die geplante Einführung eines Berufkrankheitenarztes.

[redacted]ung personenbezogener Patientendaten durch Unfallversicherungsträger an ärztliche Gutachter

[redacted]blick auf das Recht der Betroffenen, der Bestellung eines bestimmten [redacted]ters im Einzelfall aus wichtigem Grund – z. B. wegen möglicher Befangenheit – zu widersprechen, haben die Betroffenen ein besonderes berechtigtes [redacted]resse an der Transparenz dieser Datenübermittlungen.

[redacted]lich festzulegen ist daher, daß dem Betroffenen vor Übermittlung seiner [redacted] an einen Gutachter der Zweck des Gutachtens und die Person des [redacted]ters unter Hinweis auf sein Widerspruchsrecht nach § 76 Abs. 2 SGB X [redacted]en sind.

[redacted]e der Unfallversicherungsträger und ihrer Verbände in das Recht auf [redacted]tionelle Seibstbestimmung

[redacted]n der Unfallversicherungsträger und ihrer Verbände und ihre Befugnisse zur Datenerhebung, -verarbeitung und -nutzung – einschließlich der Aufbewahrungsfristen – sind differenziert in der verfassungsrechtlich gebotenen Weise gesetzlich zu regeln. Der vorliegende Referentenentwurf erscheint in diesem Punkt weitgehend unzureichend. So werden undifferenziert Unfallversicherungsträger und ihre Verbände behandelt, die Fachaufgaben dieser Stellen [redacted]t oder nicht hinreichend deutlich genannt und andererseits Selbstver-

ständlichkeiten wie das Führen von Dateien über erforderliche Daten aufgeführt. Außerdem beschränkt sich die Regelung auf die Datenverarbeitung in Dateien und übergeht die gerade im Bereich der Berufsgenossenschaften mit Gutachten und ähnlichen Unterlagen stark ausgeprägte Datenverarbeitung in Akten.

Die Zuweisung von Aufgaben und Befugnissen an Verbände der gesetzlichen Unfallversicherung muß zudem wie bei allen anderen Verbänden von Leistungsträgern durch die Einrichtung einer staatlichen Aufsicht ergänzt werden.

Soweit Vorschriften der Unfallversicherungsträger und ihrer Verbände (z. B. Unfallverhütungsvorschriften) durch Regelungen über die Erhebung, Verarbeitung und Nutzung sensibler medizinischer Daten in das Recht auf informationelle Selbstbestimmung eingreifen, sind diese Eingriffe gesetzlich zu regeln.

5. Anzeige eines Berufsunfalls und einer Berufskrankheit

Bei Datenschutzkontrollen der bisherigen Anzeigen von Berufsunfällen und -krankheiten hat sich gezeigt, daß der Umfang der an die verschiedenen Stellen übermittelten Daten zum Teil dem Grundsatz der Verhältnismäßigkeit, insbesondere der Erforderlichkeit nicht Rechnung trägt. Der Inhalt dieser Anzeigen muß an diesen Grundsätzen gemessen neu festgelegt werden.

6. Zentraldateien mehrerer Unfallversicherungsträger oder ihrer Verbände

Zweck und Inhalt zentral geführter Dateien sind in angemessenem Umfang gesetzlich präzise zu regeln. Dasselbe gilt für die Datenverarbeitung und -nutzung sowie die Festlegung der jeweils speichernden Stelle.

Die rechtzeitige Beteiligung des jeweils zuständigen Bundes- oder Landesbeauftragten für den Datenschutz vor Einrichtung einer Zentraldatei ist vorzusehen.

7. Anforderung medizinischer Unterlagen bei anderen Sozialleistungsträgern

Der in § 76 Abs. 2 SGB X vorgesehene Hinweis auf das Widerspruchsrecht gegen die Übermittlung medizinischer Daten geht stets dann ins Leere, wenn bei der speichernden bzw. übermittelnden Stelle kein Verwaltungsverfahren läuft.

Es ist daher festzulegen, daß ein Unfallversicherungsträger vor der Anforderung von Sozialdaten im Sinne des § 76 SGB X bei anderen Sozialleistungsträgern den Versicherten auf dessen Widerspruchsrecht nach § 76 Abs. 2 SGB X gegenüber der übermittelnden Stelle hinzuweisen hat.

8. Akteneinsichtsrecht der Versicherten

Hinsichtlich des gesetzlichen Akteneinsichtsrechts nach § 25 SGB X treten in der Praxis seitens der Unfallversicherungsträger Unsicherheiten auf, ob zum Schutz von Betriebs- und Geschäftsgeheimnissen oder Urheberrechten das Einsichtsrecht beschränkt werden muß. Hierzu ist eine gesetzliche Klarstellung geboten, daß diese Rechte dem Akteneinsichtsrecht nicht entgegenstehen.

Hinsichtlich einzelner dieser Anforderungen ist der Gesetzentwurf inzwischen verbessert worden. Es bleibt abzuwarten, ob die notwendigen weiteren Verbesserungen erfolgen.

5.2 Unzulässige Übermittlungen der Betriebskrankenkasse der Freien und Hansestadt Hamburg (BKK-FHH)

Bei der Prüfung der LUK (5.1.1) sind uns Übermittlungsersuchen der LUK an die BKK-FHH aufgefallen, die von der BKK-FHH in übermäßiger Weise beantwortet wurden. So wurde z. B. eine Anfrage zu Vorerkrankungen im Zusammenhang mit Schultergelenksbeschwerden in der Weise beantwortet, daß gleichzeitig auch ein früherer Brustkrebs und eine frühere Mandelentzündung mitgeteilt wurden. Die BKK-FHH hat ihre Mitarbeiter inzwischen aufgefordert, bei der Beantwortung solcher Ersuchen nur noch Daten mitzuteilen, die in einem Zusammenhang mit dem Grund der Anfrage stehen.

5.3 Zugriffssperren für Beitrags- und Leistungsdaten bei Krankenkassen

Im Anschluß an die Berichterstattung im 13. TB (6.4) hat die Konferenz der Datenschutzbeauftragten am 9./10. März 1995 eine Entschließung gefaßt, wonach die Geschäftsstellen landesweiter oder überregionaler gesetzlicher Krankenkassen ohne schriftliches Einverständnis des Versicherten nur auf einen „Stammdatensatz" zugreifen dürfen. Dieser soll nur den Namen, das Geburtsdatum, die Anschrift, die Krankenversichertennummer und die betreuende Geschäftsstelle des Versicherten umfassen. Auf den vollständigen Datensatz eines Versicherten darf nur eine vorher bestimmte Geschäftsstelle zugreifen, es sei denn, der Versicherte hat ausdrücklich und schriftlich in Zugriffsmöglichkeiten durch weitere Geschäftsstellen eingewilligt.

Inzwischen hat der AOK-Bundesverband angekündigt, diesen Anforderungen künftig besser entsprechen zu wollen. Noch nicht abschließend geklärt ist allerdings insbesondere, wie der Zugriff technisch/organisatorisch unterbunden wird, wenn keine Einwilligung des Versicherten vorliegt. Insoweit wird die Diskussion mit dem AOK-Bundesverband federführend durch den Bundesdatenschutzbeauftragten fortgeführt.

5.4 Überregionale Datenzugriffsmöglichkeiten in der Rentenversicherung

Mit dem Problem bundesweit möglicher Online-Datenzugriffe sind wir in der Rentenversicherung konfrontiert. Über 20 Rentenversicherungsträger, unter ihnen die Landesversicherungsanstalt Hamburg (LVA), haben sich zusammengeschlossen, um losgelöst von ihren Zuständigkeiten die Erstellung, Anforderung, Aushändigung und Erläuterung von Versicherungsverläufen, Rentenauskünften, Lückenauskünften und Auskünften über Beitragserstattungen vornehmen zu können.

Strittig ist, ob diese Zusammenarbeit rechtlich als Auftragsdatenverarbeitung oder als Funktionsübertragung einzuordnen ist. Unabhängig davon müssen aber die schutzwürdigen Belange der Versicherten gewahrt bleiben. Dementsprechend muß durch technisch/organisatorische Maßnahmen sichergestellt sein, daß der Zugriff nur aktiviert werden darf, wenn die Vorsprache eines Versicherten dies erfordert. Auch diese Klärung (s. auch 5.3) wird federführend durch den Bundesbeauftragten für den Datenschutz betrieben.

5.5 Rehabilitationsverfahren der Landesversicherungsanstalt (LVA)

Kurz vor Redaktionsschluß haben wir eine datenschutzrechtliche Prüfung bei der LVA vorgenommen, die die Einhaltung datenschutzrechtlicher Bestimmungen bei der Durchführung von Rehabilitationsmaßnahmen zum Gegenstand hatte.

Als problematisch ist die Unterbringung der zuständigen Abteilung in einem Großraumbüro anzusehen. Dafür ist eine Lösung allerdings erst mittelfristig durch einen Umzug der LVA zu erwarten.

Im übrigen erwiesen sich einzelne Verfahrensschritte als erörterungs- und voraussichtlich änderungsbedürftig. Dazu gehören Übermittlungen von Versichertendaten an ein Reisebüro und fehlende Löschungsfristen für die EDV. Der Diskussionsprozeß ist noch nicht abgeschlossen.

5.6 Rückforderung überzahlter Renten

Seit der Berichterstattung im 12. TB (6.6) hat es sowohl seitens der Bundesregierung als auch des Bundesrates Initiativen gegeben, § 118 Sozialgesetzbuch/Sechstes Buch (SGB VI) und die parallelen Regelungen im Unfallversicherungsrecht und im Bundesversorgungsgesetz zu ändern. Danach soll ein Geldinstitut künftig Auskunft darüber geben müssen, wer über zuviel gezahlte Renten verfügt hat. Damit zeichnet sich eine Lösung der a. a. O. beschriebenen Problematik für die Zukunft ab.

5.7 Gutscheinvergabe in der Sozialhilfe

Wenn Sozialhilfedienststellen im Einzelfall Lebensmittelgutscheine ausgegeben haben, lassen sie sich von dem einlösenden Geschäft einen Kassenbon geben, auf dem die gekauften Waren aufgeführt sind. Diese Bons wurden

bislang in der Sozialhilfeakte aufbewahrt, so daß sich über einen längeren Zeitraum das Konsumverhalten des Sozialhilfeempfängers kontrollieren ließ. Auf unsere Intervention hin hat uns die Behörde für Arbeit, Gesundheit und Soziales mitgeteilt, daß die Bons zwar auch künftig einmal kontrolliert, aber anschließend nicht mehr aufbewahrt werden sollen.

5.8 Sozialdaten auf Überweisungsträgern

Für die Kenntlichmachung von Sozialleistungen auf Überweisungsträgern hatte die Behörde für Arbeit, Gesundheit und Soziales (BAGS) nach unseren langjährigen Bemühungen einen Kompromißvorschlag erarbeitet, der gleichwohl nicht von allen betroffenen Stellen umgesetzt wurde (10. TB, 6.3). Der Senat hielt im übrigen an seiner Auffassung fest, die konkrete Bezeichnung von Sozialhilfe auf Überweisungsträgern sei nicht rechtswidrig (Bürgerschaftsdrucksache 14/1516). Dazu mußte sich der Senat (wie schon in seiner Auffassung zur Auskunftspflicht nach § 116 BSHG; vgl. 12. TB, 6.8.1) durch eine Entscheidung des Bundesverwaltungsgerichts (BVerwG) eines Besseren belehren lassen.

Das BVerwG hat am 23. Juni 1994 entschieden, daß die Kennzeichnung von Sozialhilfe auf Überweisungsträgern als „Sozialleistung" unzulässig ist, wenn nicht der Betroffene darin eingewilligt hat oder im Einzelfall besondere Umstände für die Erforderlichkeit gesprochen haben. Es hat deutlich gemacht, daß diese Einschätzung auch für andere Sozialleistungen gilt. Auf unsere Bitte um Stellungnahme zur künftigen Praxis stehen abschließende Antworten der BAGS, der Baubehörde, der Behörde für Schule, Jugend und Berufsbildung, der Behörde für Wissenschaft und Forschung sowie des Senatsamts für Bezirksangelegenheiten noch aus.

6. Personalwesen

6.1 Projekt Personalwesen (PROPERS)

Das Projekt Personalwesen hat mittlerweile die Ausstattung der Behörden mit der erforderlichen technischen Infrastruktur und der Nutzung von Textbausteinen weitgehend abgeschlossen. Die bereits für Anfang 1995 geplante Pilotierung der zweiten Stufe mit der Durchführung der Stammdatenverarbeitung und der Bezügeabrechnung nebst den dazugehörigen statistischen Auswertungen hat sich jedoch verzögert und wird nun voraussichtlich Anfang 1996 starten.

Wie in den vorangegangenen Jahren (vgl. 11. bis 13. TB, 7.1) haben wir uns gegenüber dem Projekt zu verschiedenen datenschutztechnischen und datenschutzrechtlichen Fragestellungen geäußert.

6.1.1 Weiterentwicklung des technischen Konzepts

Abweichend von den ursprünglichen Planungen sollen im Rahmen des Personalverfahrens auch Personalcomputer als Endgeräte eingesetzt werden. Zunächst war PROPERS davon ausgegangen, daß die Sachbearbeiter nur mit Terminals auf die Daten, die in den Abteilungsrechnern gespeichert werden, zugreifen können.

Wir hatten frühzeitig darauf hingewiesen, daß mit dem PC-Einsatz und der Integration des Personalverfahrens in die heterogene technische Infrastruktur der Behörden erhebliche Risiken für den Datenschutz und die Datensicherheit verbunden sind, denen durch technische und organisatorische Maßnahmen vorgebeugt werden muß.

So ist insbesondere zu gewährleisten, daß das Personalverfahren sicher von den übrigen Anwendungen der Behörden abgeschottet ist. Risiken ergeben sich vor allem dann, wenn auf den für PROPERS eingesetzten PC auch andere Verfahren abgewickelt werden und wenn behördliche Netze, die broadcastorientiert angelegt sind, genutzt werden (vgl. unsere Broschüre „Datenschutz in Netzen", 2 und 5.1).

Im Hinblick auf die Sicherheit der Endgeräte hat das LIT eine Musterkonfiguration entwickelt, bei der die Benutzer jeweils alternativ nur auf das Personalverfahren oder auf sonstige Anwendungen zugreifen können. Durch eine spezielle Sicherheitssoftware wird dabei ausgeschlossen, daß Daten unberechtigt lokal gespeichert werden.

Für die Netzproblematik wurde bislang noch keine Lösung gefunden. Wir hatten PROPERS mehrfach darauf hingewiesen, daß bei der Anbindung von PC über lokale Netze an die Abteilungsrechner dafür Sorge zu tragen ist, daß sensible Daten (hierzu gehören insbesondere auch Paßwörter, die bei der Anmeldung übertragen werden) nicht abgehört oder ausgewertet werden. Sofern keine leitungsbezogene Filterung erfolgt, ist ein angemessener Schutz nur durch kryptographische Verschlüsselung zu realisieren (vgl. 3.1.4 und 6.1.2).

Diese Problematik tritt in der Behörde für Schule, Jugend und Berufsbildung (BSJB) auf, in deren Personalabteilung ab Januar 1996 die Stammdatenverwaltung mit der PROPERS-Software pilotiert werden soll. Wir hatten bereits im Februar 1995 darauf hingewiesen, daß das Netz der BSJB aufgrund konzeptioneller Schwächen in seiner jetzigen Form nicht für die Verarbeitung von sensiblen Personaldaten geeignet ist. Das Netz, an das mehrere hundert PC angeschlossen sind und das sich auf mehrere Dienstgebäude verteilt, ist nicht segmentiert und entspricht auch hinsichtlich der Verkabelung nicht der Richtlinie zur Gestaltung der IuK-Architektur in der hamburgischen Verwaltung.

PROPERS teilt unsere seit langem bekannte Einschätzung im Grundsatz. Im Dezember 1995 sollen die notwendigen Maßnahmen zur Abhilfe abschließend

mit uns erörtert werden. Das Projekt hält bislang an seinem Ziel fest, die Pilotierung in der BSJB planmäßig im Januar 1996 zu beginnen. Wir haben darauf hingewiesen, daß die vorgesehene Verarbeitung von sensiblen Personaldaten in der BSJB nur dann vertretbar ist, wenn bis zum Pilotierungsbeginn der Datenschutz durch technische und organisatorische Maßnahmen gewährleistet wird.

6.1.2 Einstufung des Schutzbedarfs

Die gemäß § 8 HmbDSG zu treffenden Maßnahmen zur Sicherstellung des Datenschutzes richten sich nach der Schutzbedürftigkeit der Daten. PROPERS hat im Herbst 1995 eine Einstufung des Personalverfahrens nach dem Grundschutzkonzept (vgl. 13. TB, 3.1) vorgenommen. Es kommt dabei zu dem Ergebnis, daß die verarbeiteten Daten überwiegend einem „mittleren" Schutzbedarf entsprächen und allenfalls für einzelne Daten ein hoher Schutzbedarf bestehe.

Diese Einordnung des Personalverfahrens hätte zur Konsequenz, daß die im Rahmen eines Grundschutzes zu treffenden Maßnahmen im Regelfall für ausreichend gehalten werden. Insbesondere wird aus der Einordnung die Konsequenz gezogen, daß weder die Personaldaten selbst noch Authentifizierungsmerkmale (speziell Paßwörter) bei ihrer Übertragung über das behördliche Datennetz verschlüsselt werden müßten (vgl. 3.1.4).

Dagegen vertritt der Hamburgische Datenschutzbeauftragte seit langem die Auffassung, daß für Personaldaten ein hoher Schutzbedarf besteht. Diese Einschätzung hat zur Folge, daß eine gesonderte Risikoanalyse erstellt werden muß und Sicherungsmaßnahmen getroffen werden müssen, die über die Anforderungen nach dem Grundschutzkonzept hinausgehen.

In Literatur und Rechtsprechung ist seit langem unumstritten, daß Personaldaten und insbesondere Personalaktendaten besonders schutzbedürftig sind: Entsprechend dem Grundsatz der Vertraulichkeit, der jetzt seinen Niederschlag in §§ 56 Abs. 3 Beamtenrechtsrahmengesetz (BRRG), 96 a Abs. 1 und 3 Hamburgisches Beamtengesetz (HmbBG) gefunden hat, gehören Personalaktendaten von jeher grundsätzlich zu den Vorgängen, die ihrem Wesen nach geheimgehalten werden müssen. Das Personalaktengeheimnis ist als ein besonderes Amtsgeheimnis anerkannt, dessen Schutz noch über das allgemeine Amtsgeheimnis nach beamtenrechtlichen Vorschriften hinausgeht. Es unterfällt somit auch dem Schutzbereich von § 203 StGB.

Dementsprechend hat der Gesetzgeber in § 28 BDSG auch für den nichtöffentlichen Bereich die Schlußfolgerung gezogen, daß schon bei der Übermittlung von Grunddaten (Name, Anschrift, Berufszweig, Branche, Geburtsdatum) ein schutzwürdiges Interesse der Betroffenen zu berücksichtigen ist, wenn diese Übermittlung aus arbeitsrechtlichen Verhältnissen heraus erfolgt.

Die automatisierte Verarbeitung dieser Daten hat nach dem Willen des Gesetzgebers nur Hilfsfunktion. Sie muß daher der generellen Einstufung der Personal(akten)daten als besonders sensible Daten folgen.

Außerdem geht der Entwurf von PROPERS davon aus, daß verschiedene Anwendungen innerhalb eines Systems auch unterschiedliche Schutzniveaus aufweisen können. Dies ist mit der datenschutzrechtlichen Einordnung der Personalaktendaten jedoch nicht in Einklang zu bringen:

Entsprechend den Ausführungen im Volkszählungsurteil ist zu berücksichtigen, daß scheinbar unsensible Daten je nach Verknüpfung zu empfindlichen Aussagen über den Betroffenen führen können. Auch im hamburgischen Personalverfahren soll der Personalstammdaten-Katalog im Rahmen der Personalwirtschaft und -verwaltung zu unterschiedlichen Zwecken herangezogen werden können; eine einheitliche Betrachtung dieser Daten ist zur Sicherung des Rechts auf informationelle Selbstbestimmung erforderlich. Für ein einheitliches Schutzniveau für Personalaktendaten haben sich die Datenschutzbeauftragten des Bundes und der Länder zuletzt im September 1995 ausgesprochen.

Unbestritten ist ein solches einheitliches Schutzniveau zum Beispiel auch beim Arzt- und beim Steuergeheimnis (z. B. keine geringere Schutzwürdigkeit bei Informationen über Schnupfen; einheitliches Geheimnis auch über die Art der Einreichung von Steuererklärungen).

Nach alledem ist eine gesonderte Risikoanalyse erforderlich, die dem schon aufgrund der Vertraulichkeit erforderlichen hohen Schutzbedarf einheitlich gerecht wird und die Anforderungen an die Abschottung von anderen Bereichen hinreichend gewährleistet.

Darüber hinaus besteht Einigkeit darüber, daß auch die Abschottung einzelner Zuständigkeitsbereiche im Personalwesen voneinander zu gewährleisten ist.

Die Einschätzung von PROPERS, daß Versuchen, unberechtigt in das Personalverfahren einzudringen, keine praktische Relevanz zukomme, wird von uns nicht geteilt. Angesichts der Tatsache, daß perspektivisch alle Büroarbeitsplätze in der hamburgischen Verwaltung mit vernetzten Arbeitsplatzcomputern ausgestattet sein werden, stellt sich die Sicherheitslage heute anders dar als noch vor einigen Jahren, als nur eine kleine, überschaubare Anzahl von Mitarbeitern online auf zentrale Datenbestände zugreifen konnte.

Die Wahrscheinlichkeit, daß in einem tiefgegliederten vielstufigen Netz an nur einer Stelle Berechtigungsdaten abgehört bzw. ausgespäht werden – etwa aufgrund eines Administrationsfehlers in einem lokalen Netz, wegen der Manipulation eines Netzrechners oder wegen Sicherheitsmängeln auf einem Router oder Gateway – ist vor diesem Hintergrund als hoch einzuschätzen.

Daraus ergibt sich die Notwendigkeit, zumindest die Authentifikationsdaten besonders gegen ein Abhören bzw. elektronisches Ausspähen der übertragenen Daten (also insbesondere auch von Kennungen und Paßwörtern) zu schützen.

Insofern wird unsererseits eine Ende-zu-Ende-Verschlüsselung zumindest der Authentifikationsdaten im Personalverfahren für unumgänglich gehalten. Eine Verschlüsselung von Inhaltsdaten ist darüber hinaus dann notwendig, wenn die noch vorzunehmende Risikoanalyse ergibt, daß dies erforderlich ist.

6.1.3 Positivkataloge und Datenkataloge

Bereits in der Sitzung der Lenkungsgruppe PROPERS vom 23. September 1992 ist der Beschluß gefaßt worden, einen Positivkatalog über die Zulässigkeit der Informationsspeicherung und -auswertung aller verwendeten Daten zu erstellen und im Rahmen einer Vereinbarung nach § 94 Hamburgisches Personalvertretungsgesetz (HmbPersVG) festzuschreiben. Hierfür sind bereits im letzten Berichtszeitraum verschiedene Datenkataloge entworfen worden (vgl. 13. TB, 7.1; 7.6.2). Sie wurden zum Teil weiterentwickelt und um den Entwurf einer Dokumentation und eines Verfahrens für einen Katalog personenbezogener Auswertungen ergänzt.

Über alle Kataloge ist noch nicht abschließend entschieden worden. Wir haben wiederholt auf generelle und katalogbezogene Defizite und Bedenken hingewiesen. Zur Sicherstellung der Pilotierung in der BSJB sollen alle offenen Punkte noch im Dezember 1995 geklärt werden.

Generell gehen wir davon aus, daß personalwissenschaftlich begründete Organisationsentscheidungen nur dann verbindlich getroffen werden können, wenn sie sich im Rahmen der rechtlichen Vorgaben, insbesondere der beamten- und datenschutzrechtlichen Bestimmungen, bewegen. Beispielhaft gehört hierzu die Abschottung des Personalstatistik- vom Personalverwaltungsbereich, wenn darin mehr oder historisch tiefergehende Daten verwaltet werden.

Auch haben wir wiederholt darauf hingewiesen, daß die Historikzeiträume der einzelnen Datenfelder für jeden Verwendungszweck gesondert auszuweisen sind, um dem datenschutzrechtlichen Erforderlichkeitsgrundsatz zu genügen.

Daneben hat sich als schwierig erwiesen, daß allgemein übliche statistische Auswertungen entgegen der ursprünglichen Beschlußlage nicht über ein gesondertes Verfahren „Statistisches Informationssystem" (SIS) anonymisiert abgewickelt werden sollen. Vielmehr sollen die Auswertungen überwiegend aus wirtschaftlichen Gründen personenbezogen im Rahmen der Abrechnungs- und Verwaltungsverfahrens Paisy erstellt werden, weil Paisy diese Auswertungen bereits unterstützt. Auch hier werden datenschutzrechtliche Einschränkungen zu beachten sein, wenn statistische Auswertungen im Vollzugsbereich durchgeführt werden sollen.

Im wesentlichen haben wir uns mit folgenden Katalogen beschäftigt:

- Datenkatalog Berichtswesen

Zum Datenkatalog Berichtswesen haben wir über unsere bereits im letzten TB geschilderten Bedenken hinaus eine grundsätzliche Stellungnahme zu den Anforderungen an ein statistisches Personalberichtswesen abgegeben. Wir sind dabei auch auf die Möglichkeiten der statistischen Auswertung spezieller Daten zur Personalentwicklung sowie zur dezentralen Nutzung von SIS eingegangen.

Auch danach kommen wir zu dem Ergebnis, daß ein statistisches Personalberichtswesen in der angedachten Form nur abgeschottet vom Vollzugsbereich zulässig ist, besonders sensible Daten darin nicht frei verknüpfbar verarbeitet werden dürfen und alle Daten frühestmöglich wirksam zu anonymisieren sind. Hierfür reicht es nicht aus, nur die primär identifizierenden Daten wie Name, Personalnummer usw. wegzulassen.

Alternativ sehen wir nur die Möglichkeit, entsprechend der jetzt in Schleswig-Holstein angedachten Regelung das Personalberichtswesen wie eine Geschäftsstatistik auf den Datenumfang zu beschränken, den die personalverwaltende Stelle selbst verwaltet. Durch Organisationsentscheidungen könnte eine zuständige Stelle für zentrale Auswertungen bestimmt werden, die dann allerdings nur bereits anonymisierte Daten einzelner Beschäftigungsbehörden zur weiteren zentralen Auswertung erhalten kann.

- Katalog personenbezogener Auswertungen im Rahmen des Positivkatalogs (Dokumentation und Verfahren)

Mit diesem Katalog soll die zulässige Verarbeitung der in den Datenkatalogen enthaltenen Daten dokumentiert werden; dies gilt allerdings nur, soweit die Daten zentral personenbezogen ausgewertet werden. Dafür sind verschiedene Kategorien entworfen worden, die unterschiedliche Formen der Verarbeitung ermöglichen sollen. Daneben bestimmen die Kategorien das Verfahren zur Freigabe künftiger Auswertungen durch das Projekt und für spätere Zeiten. Zur Vorgehensweise bei Änderung der maßgeblichen Datenkataloge haben wir verschiedene Anregungen und Hinweise gegeben.

Werden in Paisy statistische Auswertungen in personenbezogener bzw. personenbeziehbarer Form vorgenommen, müssen dieselben Anforderungen eingehalten werden, wie sie im Rahmen des Berichtswesens mit SIS behandelt wurden. Werden mit Paisy besonders sensible Daten ausgewertet, so muß zusätzlich, z. B. durch Maskenführung, sichergestellt werden, daß die Daten nicht für andere als die vorgegebenen Auswertungen zur Verfügung stehen.

6.2 Mitarbeiterbefragungen

Im letzten Tätigkeitsbericht (13. TB, 7.6.2; 7.6.3) hatten wir über unsere Erfahrungen und die rechtliche Einschätzung von Mitarbeiterbefragungen berichtet. Wir hatten schwerpunktmäßig auf die Freiwilligkeit von Meinungsäußerungen verwiesen und auf die daraus folgenden Anforderungen an eine wirksame Ausgestaltung der Einwilligungserklärung. Außerdem hatten wir hierzu eine Datenschutzrichtlinie zur Personalentwicklung angeregt. Dem hat sich ein Erfahrungsaustausch mit den Datenschutzbeauftragten des Bundes und der Länder angeschlossen.

Nach den diesjährigen Erfahrungen sehen wir unsere bereits im letzten Jahr vorgetragene Einschätzung im Ergebnis bestätigt. Wesentlich ist jedoch die Unterscheidung, ob die Befragung durch Tatsachen- oder Meinungsfragen geprägt ist; im ersten Fall findet das Hamburgische Statistikgesetz und im zweiten Fall das Hamburgische Datenschutzgesetz Anwendung. In den Kernbereichen schreiben beide Gesetze dieselben Anforderungen vor.

6.2.1 Anwendungsbereiche

Auch im Berichtsjahr haben wir eine Reihe von Fragebogenerhebungen überprüft, die überwiegend im Rahmen von Organisationsuntersuchungen erfolgten. Dabei wurden oft Interviews zur Vor- oder Nachbereitung der Fragebogenerhebungen eingesetzt. Daneben wurden uns aber auch fachspezifische Erhebungen vorgelegt, so z. B. zur Fortbildungsausgestaltung in der Behörde für Arbeit, Gesundheit und Soziales und zur Betroffenheit von Frauen durch den geplanten Personalabbau, die von der Frauenbeauftragten der Finanzbehörde initiiert wurde.

Es hat sich gezeigt, daß die Freiwilligkeit der Angaben nicht nur bei Meinungsäußerungen erforderlich ist, sondern auch bei sog. harten Fakten. Dies betrifft insbesondere Umstände, die dem Arbeitgeber bisher nicht bekannt sind, aber auch bekannte Umstände, die durch die Befragung in einen anderen Kontext geraten und dadurch einen anderen Aussagegehalt erlangen. Dies traf besonders auf den Fragebogen der Frauenbeauftragten zu: Neben der Kenntnis und der Betroffenheit von Maßnahmen zum Personalabbau sollten Angaben zum Alter, Besoldungsgruppe, Familienstand und Kinderzahl gemacht und die Fragestellung nach wirtschaftlichen Abhängigkeiten beantwortet werden.

6.2.2 Rechtsgrundlagen

Mitarbeiterbefragungen gehören typischerweise nicht zu den Angaben, die die Beschäftigungsbehörden als erforderliche Daten über einzelne Beschäftigte im Sinne von § 28 Abs. 1 Hamburgisches Datenschutzgesetz (HmbDSG) verarbeiten dürfen. Es handelt sich um empirische Erhebungen, für die die §§ 5, 12 ff. HmbDSG maßgeblich sind, wenn es sich um Meinungsäußerungen handelt. Wenn die Mitarbeiterbefragung durch die Erhebung von Fakten geprägt

ist, ist sie als Statistik zu qualifizieren, auf die das Hamburgische Statistikgesetz (HmbStatG) anzuwenden ist. Wesentlich ist in beiden Fällen die Freiwilligkeit der Angaben. Hierauf sind die Mitarbeiter nach § 12 HmbDSG bzw. nach § 4 Abs. 1 Nr. 7 HmbStatG i. V. m. § 17 Bundesstatistikgesetz (BStatG) hinzuweisen, ebenso wie auf den Umstand, daß ihnen keine Nachteile erwachsen, wenn sie sich nicht beteiligen. Diese Hinweise und die Bereitschaft zu freiwilligen Angaben sind bei der Mitarbeiterbefragung zu dokumentieren.

Werden primär Meinungsäußerungen abgefragt, bedarf es neben des Hinweises auf die Freiwilligkeit auch einer wirksamen, in der Regel schriftlichen Einwilligungserklärung nach § 5 HmbDSG. Dies setzt eine umfassende Aufklärung voraus. Von der schriftlichen Einwilligung kann nur abgesehen werden, wenn die Aufklärung in anderer Weise hinreichend dokumentiert ist, z. B. durch Abzeichnung im Umlaufverfahren oder durch Anwesenheitslisten über Informationsveranstaltungen.

Der Inhalt der Fragen muß gemäß § 13 HmbDSG durch den Zweck der Erhebung und durch die Einwilligungserklärung abgedeckt sein. Zweifelhaft sind dabei Fragen nach der eigenen Mobilität, nach der Einschätzung des Betriebsklimas und sog. Kontrollfragen gewesen. Daneben dürfen keine Fragen gestellt werden, die den einzelnen Mitarbeiter oder Dritte in ihrem Persönlichkeitsrecht beeinträchtigen. Dies gilt insbesondere für Selbst- und Fremdeinschätzungen und für Fragen nach der eigenen Motivation.

Freiwillige statistische Datenerhebungen sind außerdem nur zulässig, wenn sie durch Gesetz oder Rechtsverordnung angeordnet worden sind (§ 2 Abs. 3 HmbStatG). Um die Verfahrensweise künftig zu erleichtern, haben wir der Behörde für Inneres generell vorgeschlagen, eine Änderung des Hamburgischen Statistikgesetzes vorzubereiten. Dabei könnte die Streichung von § 2 Abs. 3 HmbStatG vorgesehen und zugleich geregelt werden, daß es in den bisherigen Fällen des § 2 Abs. 3 HmbStatG auch keiner Anordnung der Statistik durch Gesetz bedarf. Alternativ wären Mitarbeiterbefragungen von der Anforderung auszunehmen, daß sie jeweils nur aufgrund einer Rechtsvorschrift durchgeführt werden dürfen.

Wesentlich für die Mitarbeiterbefragung ist eine möglichst anonyme Verarbeitung der Daten. Dabei ist zu berücksichtigen, daß die Anonymisierungskriterien der empirischen Sozialforschung – mit dem Verzicht auf primär identifizierende Merkmale wie Namen oder Personalnummer – nicht immer ausreichen. Es muß vielmehr gewährleistet sein, daß ein Personenbezug oder auch eine Personenbeziehbarkeit nur mit unverhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft hergestellt werden kann. Dies bedeutet zunächst, daß schon durch die Fragestellungen möglichst nur aggregierte Daten erfaßt werden sollten. Bei der Auswertung ist sicherzustellen, daß Angaben unter 3 Betroffenen unterdrückt oder mit anderen Fällen zu einer größeren Gruppe zusammengefaßt werden.

Die Durchführung von Mitarbeiterbefragungen muß gemäß § 30 HmbDSG bzw. § 7 HmbStatG organisatorisch und personell abgeschottet sein von der Personalverwaltung und der eigenen Abteilung der Mitarbeiter, um einen unzulässigen Rückfluß der aus der Erhebung stammenden Informationen in den Vollzugsbereich zu verhindern. Dies betrifft auch Informationen darüber, ob einzelne Mitarbeiter an einer Erhebung teilgenommen haben oder nicht.

Werden Dritte mit der Durchführung der Befragung beauftragt, so ist gemäß § 3 HmbDSG bzw. § 5 HmbStatG sicherzustellen, daß sie die datenschutzrechtlichen Anforderungen auch nach diesen Gesetzen erfüllen und daß sie sich der Kontrolle durch den Hamburgischen Datenschutzbeauftragten unterwerfen. Daneben ist vertraglich Sorge zu tragen, daß die Auftragnehmer für eine frühzeitige Anonymisierung verantwortlich sind und daß personenbezogene Unterlagen dem Auftraggeber nicht übermittelt werden dürfen.

In jedem Fall obliegt dem Auftraggeber die verantwortliche Prüfung und Entscheidung hinsichtlich der Fragenkataloge und Interviewleitfäden. Nur so kann sichergestellt werden, daß die Einhaltung aller einschlägigen personaldatenschutzrechtlichen Vorschriften gewährleistet ist. Insgesamt darf der Auftraggeber die Verantwortung für die Befragung nicht dem beauftragten Unternehmen überlassen.

Zur Sicherstellung eines ordnungsgemäßen Verfahrens sollte der Hamburgische Datenschutzbeauftragte rechtzeitig vor Durchführung der Befragungen beteiligt werden. Außerdem ist die Beteiligung des Personalrats angezeigt. Nach unserer Auffassung besteht gemäß der neueren Rechtsprechung Mitbestimmungspflicht über den Inhalt von Personalfragebögen. Zumindest sollte aber von der Möglichkeit zum Abschluß einer Dienstvereinbarung Gebrauch gemacht werden, die das Personalamt auch bei nicht mitbestimmungspflichtigen Angelegenheiten für zulässig hält.

6.2.3 Empfehlungen

Unsere vorgenannten Bewertungen haben wir in einem Entwurf einer Arbeitshilfe „Empfehlungen zum Datenschutz bei Mitarbeiterbefragungen" zusammengefaßt. Wir werden diese zunächst mit dem Personalamt, der Justizbehörde und der Behörde für Inneres erörtern.

Auch das Projekt PROVI wird informiert, um die Behörden im Rahmen ihrer Bemühungen zur Verwaltungsmodernisierung bei Bedarf auf unsere Bewertungen verweisen zu können.

Dem Organisationsamt haben wir Vorschläge zur Ergänzung des Muster-Beratervertrages gemacht.

6.3 Kostenstellenrechnung und Zeitanschreibungen

Im Zuge der Diskussion um die Verwaltungsmodernisierung und die Einführung des Neuen Steuerungsmodells sind wir wiederholt mit der Auffassung konfrontiert worden, daß hierfür Daten der Beschäftigten erforderlich seien und daher auch personenbezogen zu verschiedenen Auswertungen herangezogen werden dürften. Aber auch hierfür gilt der allgemeine Erforderlichkeitsgrundsatz, daß personenbezogene oder personenbeziehbare Daten nur dann verarbeitet werden dürfen, wenn die Aufgabenwahrnehmung ansonsten mit unverhältnismäßig großen Schwierigkeiten verbunden ist. Je sensibler die dafür erhobenen oder verwendeten personenbezogenen Daten sind, desto höhere Anforderungen sind an alternative, weniger belastende Maßnahmen zu stellen.

Ein letztlich gelungenes Beispiel für eine solche Güterabwägung ergab sich in der Baubehörde:

Durch eine Eingabe wurden wir darauf aufmerksam, daß in einer Abteilung des Amtes für Wasserwirtschaft ein betriebswirtschaftliches Abrechnungssystem eingeführt worden war. Dafür mußten die Mitarbeiter Arbeitsnachweise erstellen, in denen unter Angabe von Namen und Vergütungs- bzw. Besoldungsgruppe jeweils täglich Einsatzort, Kostenstelle, Tätigkeit, Auftragsnummer, Datum, Fahrzeit und Stunden festzuhalten waren. Diese Angaben orientierten sich an Nachweisen, die die gewerblichen Arbeitnehmer seit jeher zur Lohnabrechnung erstellen mußten. Die Nachweise waren in der Abteilung monatlich vorzulegen und wurden zentral automatisiert erfaßt. Eine Auswertung war noch nicht erfolgt.

Unsere ersten Gespräche ergaben, daß sich die Anschreibungen entgegen der Verfügung des Amtsleiters noch in der Erprobungsphase befanden, da man sich über die Erforderlichkeit der einzelnen Angaben noch keine abschließende Meinung gebildet hatte. Wir haben bemängelt, daß diese lückenlosen Arbeitsnachweise viele Angaben enthielten, die für die reine Kostenrechnung nicht erforderlich waren. An sich wäre hierfür ein Personenbezug nicht erforderlich; aufgrund der Anzahl der betroffenen Mitarbeiter einerseits und der Kleinteiligkeit der Angaben andererseits war eine wirksame Anonymisierung aber nicht möglich.

Wir haben deshalb darauf hingewiesen, daß die Datenerhebung nur mit einer wirksamen Einwilligung der Betroffenen erfolgen könnte und die Voraussetzungen hierfür benannt. Außerdem ist für die Erhebung die Zustimmung des Personalrats nach § 86 Abs. 1 Nr. 4 (technische Einrichtung, die zur Überwachung geeignet ist) und § 87 Abs. 1 Nr. 23 (Personalfragebogen) Hamburgisches Personalvertretungsgesetz (HmbPersVG) oder eine Dienstvereinbarung erforderlich.

Dies gilt erst recht in der Erprobungsphase. Wir haben die Datenerhebung schon deshalb als rechtswidrig einstufen müssen, weil die Betroffenen aufgrund der Einsetzungsverfügung fälschlicherweise davon ausgehen mußten, daß die Anschreibungen bereits verbindlich vorgeschrieben seien.

Nach intensiven Erörterungen wurden die erhobenen Daten gelöscht. Das Amt hat nunmehr folgenden Vorschlag zur Leistungserfassung für die Kostenrechnung vorgelegt, den wir für datenschutzgerecht halten:

- Personen, die überwiegend auf einer Kostenstelle arbeiten, erbringen Leistungsnachweise nur in dem Umfang, wie sie für eine fremde Kostenstelle Leistungen erbringen; Personen, die überwiegend oder ausschließlich für fremde Kostenstellen arbeiten, erbringen regelmäßig Leistungsnachweise.
- Das Anschreibungsformular wird in zwei Teile gegliedert. Teil 1 mit Namensangabe für die Abrechnung von Nebenlöhnen wird 5 Jahre aufbewahrt; Teil 2 ohne identifizierende Angaben für die Kostenrechnung wird nach Erfassung im Kostenrechner vernichtet. Werden keine Nebenlöhne berechnet, sollen die Arbeitsnachweise direkt der Kostenrechnungsstelle vorgelegt werden.
- Für Personen, die für die Kostenrechnung anschreiben, werden Pools gebildet. Sie umfassen immer mehr als drei Mitarbeiter, um eine Reidentifizierung auszuschließen. Für die Pools werden durchschnittliche Stundensätze nach bestimmten Pauschalwerten berechnet.
- Die Zuständigkeiten für die Abrechnung der Nebenlöhne und für die Kostenrechnung werden organisatorisch und personell getrennt.

6.4 Mitarbeiter- und Vorgesetztengespräch

Das Mitarbeiter- und Vorgesetztengespräch war wiederholt Berichtsgegenstand (vgl. 12. TB, 7.11; 13. TB, 7.6.1). Zuletzt hatten wir über einen grundlegenden Dissens mit dem Personalamt über die Freiwilligkeit des Gesprächs und die daraus resultierenden datenschutzrechtlichen Konsequenzen zur Aufklärung berichtet. Wir hatten dem Personalamt anheimgestellt, unsere Hinweise selbst an die beteiligten Behörden weiterzugeben oder von uns aus diese Hinweise zu versenden.

Nach weiteren Debatten kamen wir überein, daß unsere Anforderungen im Kreis der Personalentwickler dargestellt werden sollten und unsere schriftlichen Empfehlungen anschließend von diesen an die jeweiligen Behördenleitungen weiterzuleiten waren.

In den Empfehlungen haben wir ausdrücklich darauf hingewiesen, daß diese Erläuterungen zum Datenschutz allen Teilnehmern am Mitarbeiter- und Vorgesetztengespräch in Ergänzung zur Orientierungshilfe und den Vorbereitungshilfen des Personalamts in geeigneter Form zur Kenntnis zu geben sind. Nur so kann auf die eigentlich erforderliche Schriftform der Einwilligung nach § 5 HmbDSG verzichtet werden.

Nach Auskunft des Personalamts ist die Verteilung an die Personalentwickler zwischenzeitlich erfolgt.

6.5 Ärztlicher Dienst der Behörde für Inneres (BfI)

Im letzten TB haben wir ausführlich über Datenschutzdefizite beim Ärztlichen Dienst der Behörde für Inneres (BfI) berichtet (vgl. 13. TB, 7.8). Über die Umsetzung der von uns geforderten Maßnahmen wurde weiterhin intensiv diskutiert.

Als wesentliche Maßnahme zur Abschottung der einzelnen medizinischen Bereiche hatten wir uns bereits im Sommer 1994 auf den Einsatz einer Archivkraft geeinigt. Sie sollte dafür Sorge tragen, daß die verschiedenen Bereiche des Ärztlichen Dienstes auf Anforderung nur noch die sie betreffenden Aktenteile aus den umfassend geführten Krankenakten erhalten sollten. Nach verschiedenen untauglichen Versuchen konnte bis Redaktionsschluß lediglich mitgeteilt werden, daß mit der neuen Leitung des Ärztlichen Dienstes ein problemorientiertes Gespräch erfolgen soll, um den weiteren erhöhten Anforderungen gerecht zu werden und erforderlichenfalls den Rückgriff auf medizinisches Fachwissen zu gewährleisten. Hier erwarten wir jetzt den zügigen, sachgerechten Einsatz einer Archivkraft.

Darüber hinaus konnte zu den aufgeworfenen Fragen und Anforderungen weitgehend Einvernehmen erzielt werden.

Nachdem der Ärztliche Dienst zum 1. Juli 1995 erneut umstrukturiert worden ist, sind die beim verbleibenden Teil erforderlichen Baumaßnahmen eingeleitet worden. Für die Unterbringung der Krankenakten wurden jetzt Stahlschränke bestellt.

Einvernehmen besteht auch über die langfristige Aufbewahrung der archivierten Krankenakten. Da die Behörde für Inneres erklärt hat, auf die Akten nur bei Vorliegen einer Schweigepflicht-Entbindungserklärung zurückzugreifen, ist der Schutz der Betroffenen hinreichend gewährleistet.

6.6 Prüfung beim Personalrat der Justizbehörde

Schon in den Vorjahren (12. TB, 7.8; 13. TB, 7.7) hatten wir uns mit verschiedenen Rechtsfragen der Datenverarbeitung durch Personalräte befaßt. Wir hatten es für vertretbar erachtet, daß der Personalrat gewisse Grunddaten der Beschäftigten auch auf Dauer automatisiert verarbeitet. Außerdem hatten wir dem Personalamt zu der seit langem angekündigten Novellierung des Hamburgischen Personalvertretungsgesetzes (HmbPersVG) verschiedene datenschutzrechtliche Änderungsvorschläge unterbreitet, die sich im wesentlichen aus allgemeinen datenschutzrechtlichen Grundsätzen ergaben.

Auf der Grundlage dieser Ausführungen, die wir auch mit dem Personalrat der Justizbehörde erörtert hatten, haben wir im Berichtsjahr erstmals die Datenverarbeitung bei einem Personalrat geprüft. Schwerpunkte waren die Aktenführung und die automatisierte Datenverarbeitung. Die Ergebnisse werden mit dem Personalrat und der Justizbehörde, soweit sie für die Datensicherheit verantwortlich ist, erörtert.

Die Aktenführung ergab, daß oftmals Unterlagen personenbezogen zu lange gespeichert werden. Unterlagen, die der Personalrat im Rahmen von Mitbestimmungsverfahren erhält, sind zurückzugeben oder zu vernichten, wenn das Verfahren abgeschlossen ist. Sollen bestimmte Sachfragen anhand einzelner Fälle besonders dokumentiert werden, sind die Einzelfälle zu diesem Zweck zu anonymisieren und nach dem Sachthema zu verwalten. Ein Rückgriff auf personenbezogene Unterlagen ist dann nicht mehr erforderlich und daher unzulässig. Auch eigene Unterlagen des Personalrats wie Protokolle, Einladungen und sonstige Korrespondenz sind nur befristet aufzubewahren, da sie oft personenbezogene Inhalte aufweisen.

Werden Personalratsunterlagen automatisiert erstellt, ist außerdem zu beachten, daß der automatisierten Verarbeitung nur Hilfsfunktion zukommt. Soweit Daten für eine automatisierte Verarbeitung nicht mehr benötigt werden, müssen sie im System gelöscht werden (§ 19 Abs. 3 HmbDSG). Unproblematisch ist jedoch ein Rückgriff bis zur Erstellung des Rechenschaftsberichts im Rahmen von Personalversammlungen.

Bei der automatisierten Datenverarbeitung benutzen alle zugangsberechtigten Personalratsmitglieder dasselbe Paßwort. Dadurch ist z. B. die Abschottung bei der Bearbeitung aufgrund von Einzelberatungen nicht gewährleistet. Im vorliegenden Fall war ferner ein schwerwiegender Mangel, daß der alte PC des Personalrats innerhalb der Verwaltung weitergenutzt wurde, ohne daß die empfindlichen Daten des Personalrats hinreichend physikalisch gelöscht worden waren. Aufgrund der nur logischen Löschung konnten die meisten Daten wiederhergestellt und von den nun mit dem Gerät arbeitenden Mitarbeitern eingesehen werden.

Außerdem ist die Erforderlichkeit der Daten in automatisierten Dateien alle vier Jahre zu prüfen (§ 19 Abs. 6 HmbDSG). Dies gilt z. B. auch für die Protokolle.

Problematisch war auch zum Teil die räumliche und sachliche Ausstattung des Personalrats: Der einzige dem Personalrat zur Verfügung stehende Raum muß für die laufende Arbeit, Sitzungen und zum Teil parallele telefonische oder persönliche Beratungen genutzt werden. Wegen der unzureichenden Schallisolierung können Gespräche auf dem Flur und in den angrenzenden Räumen mitgehört werden. Hier halten wir bauliche Veränderungen und die Möglichkeit, andere ausreichend gesicherte Räume mitzunutzen, für erforderlich. Ebenso müssen die personenbezogenen Unterlagen beim Personalrat in Stahlschränken aufbewahrt werden, und die einzelnen Personalratsmitglieder

müssen in der Lage sein, Unterlagen des Personalrats auch an ihrem Arbeitsplatz sicher unter Verschluß halten zu können.

Wir gehen davon aus, daß die in diesem Fall festgestellten Probleme in gleicher oder ähnlicher Weise auch bei anderen Personalräten auftreten. Daher erwarten wir, daß die Personalräte gegenüber den zuständigen Dienststellen auf eine Mängelbeseitigung hinwirken, soweit sie die Probleme nicht selbst lösen können. Wir erwarten ferner, daß die Dienststellen von sich aus zu geeigneten Problemlösungen beitragen und auftretende Schwierigkeiten bei Bedarf mit ihrem Personalrat erörtern.

7. Schule und Berufsbildung

7.1 Mitteilung von Prüfungsergebnissen durch die Handelskammer Hamburg an die Ausbildungsbetriebe

Eine förmliche Beanstandung mußte ich an die Handelskammer richten; meinen datenschutzrechtlichen Bedenken hat die Handelskammer inzwischen Rechnung getragen. Bislang konnten Ausbildungsbetriebe mit dem Formular „Anmeldung zur Abschlußprüfung" beantragen, daß ihnen die Abschlußprüfungsergebnisse der Auszubildenden mitgeteilt werden. Diesen Anträgen wurde seitens der Handelskammer entsprochen, wenn sich der Betrieb verpflichtete, mitgeteilte Abschlußprüfungsergebnisse vertraulich zu behandeln. Eine Einwilligung der Auszubildenden wurde dafür bisher nicht eingeholt.

Der wesentliche Grund für dieses Verfahren war nach Auffassung der Handelskammer, daß sie zu diesem Verfahren verpflichtet sei, um dadurch den Betrieb hinsichtlich der Qualität seiner Ausbildung zu beraten. Weiche das Prüfungsergebnis deutlich von einer Beurteilung des Auszubildenden durch den Betrieb ab, werde dies von der Handelskammer als Hinweis auf Beratungsbedarf gesehen. Die einfachste Form der Beratung sei zunächst die Mitteilung der Prüfungsergebnisse.

Diese Begründung war aber offensichtlich unzutreffend. Denn wenn die Mitteilung der Abschlußprüfungsergebnisse zur Erfüllung der gesetzlichen Beratungsaufgabe der Handelskammer erforderlich wäre, dürfte sie nicht von einem Antrag des Betriebes abhängig gemacht werden. Die Mitteilung bloßer Prüfungsergebnisse kann zudem auch keine qualifizierte Beratung darstellen. Eine solche müßte vielmehr dadurch geprägt sein, daß dem Betrieb konkret mitgeteilt wird, inwiefern er die Ausbildung verbessern muß.

Im übrigen fehlt für solche Mitteilungen auch eine Rechtsgrundlage. § 45 Berufsbildungsgesetz (BBiG) regelt in Satz 1 eine allgemeine Beratungspflicht; dies stellt aber keine verfassungsgemäße Datenverarbeitungbefugnis dar. Satz 3 der Vorschrift regelt zwar eine Auskunftspflicht; diese trifft aber nur den Betrieb gegenüber der Handelskammer, nicht jedoch umgekehrt die Handelskammer gegenüber dem Betrieb. Die Handelskammer wäre auch gehindert,

solche Mitteilungen in der Prüfungsordnung zu regeln. Denn auch wenn man die Prüfungsordnung als Satzung und somit als Gesetz im materiellen Sinn auffaßt, enthält § 41 BBiG, auf den sich die Prüfungsordnung stützt, keine Ermächtigung, die Datenverarbeitung zu regeln.

Als Rechtsgrundlage für diese Datenverarbeitung verbleibt dann nur noch eine Einwilligung. Daher ist es erforderlich, daß die Ergebnisse bestandener Abschlußprüfungen nur noch mit schriftlicher Einwilligung der Auszubildenden an den Betrieb mitgeteilt werden. Dieser Auffassung ist im übrigen auch die Handwerkskammer, wo die Rechtslage für die Gesellenprüfung insoweit praktisch identisch ist. In Berlin ist es bereits eingeführte Praxis, daß die Auszubildenden bei der Anmeldung zur Abschlußprüfung um ihr Einverständnis dafür gebeten werden, die Prüfungsergebnisse dem Ausbildungsbetrieb mitzuteilen. Dabei wird ausdrücklich auf die freie Widerruflichkeit der Einwilligung hingewiesen.

Die Handelskammer hat inzwischen den Text einer solchen Einwilligungserklärung mit mir abgestimmt und will künftig entsprechend geänderte Anmeldeformulare verwenden.

7.2 Lernausgangslagenuntersuchung

Erstmalig im Mai 1995 informierte uns die Behörde für Schule, Jugend und Berufsbildung (BSJB) über ihre Absicht, eine Lernausgangslagenuntersuchung durchzuführen. Dabei sollen die Fähigkeiten der Fünftklässler im Lesen, Schreiben und Rechnen/Mathematik sowie hinsichtlich des Sachwissens, der Kreativität und der Lernmotivation festgestellt werden. Zunächst sollte im Schuljahr 1995/96 in ca. 100 fünften Klassen eine Vorstudie durchgeführt werden. Für das Schuljahr 1996/97 ist dann als Hauptstudie eine Erhebung bei sämtlichen ca. 15.000 Fünftklässlern vorgesehen. Erhebungsinstrumente sind Testverfahren und Fragebögen.

Hinsichtlich der vorgesehenen Befragungen der Schüler und ihrer Eltern bedarf es nach § 2 Hamburgisches Statistikgesetz (HmbStatG) einer Rechtsvorschrift als Grundlage. Der Senat hat daher am 8. August 1995 die „Verordnung über eine Erhebung von soziodemographischen Daten im schulischen Bereich" beschlossen. Diese Verordnung kann nach unserer Auffassung aber nur für die Vorstudie eine ausreichende Rechtsgrundlage sein. Denn nach § 2 Abs. 3 HmbStatG ist eine Rechtsverordnung nur ausnahmsweise ausreichend, wenn u. a. nur ein beschränkter Personenkreis erfaßt wird. Damit sind gemäß der amtlichen Begründung (Bürgerschaftsdrucksache 13/6831) Repräsentativerhebungen bei einem beschränkten Personenkreis gemeint. Da bei der Hauptstudie aber die Gesamtheit aller Fünftklässler erfaßt wird, bedarf es dazu eines Gesetzes der Bürgerschaft, das noch vor Beginn der Hauptstudie verabschiedet und in Kraft gesetzt werden muß; sonst wäre die Durchführung der Hauptstudie rechtswidrig.

Die Daten sollen in erster Linie klassenbezogen aufbereitet werden, aber auch schülerbezogen, um später eine Verlaufskontrollstudie durchführen zu können. Die Auswertung der Erhebung erfolgt durch externe Hilfskräfte, womit im Grundsatz sichergestellt wird, daß die Informationen aus der Studie nicht in die Bewertung der schulischen Leistungen der Schüler einfließen.

Für die Verlaufskontrollstudie hatten wir der BSJB empfohlen, ein Matchcodeverfahren zu verwenden, bei dem zwar zwei Datensätze einander zugeordnet werden können, nicht aber einem bestimmten Schüler. Das Verfahren wollte die BSJB vor Beginn der Vorstudie einvernehmlich mit uns klären. Sie hat sich über diese Zusage dann aber hinweggesetzt und die Vorstudie ohne abschließende Klärung mit uns durchgeführt. Dabei hat sie ein datenschutzrechtlich schlechteres Verfahren verwendet: Weil die Schüler mit dem Matchcode-Verfahren angeblich überfordert waren, wurden Listen verwendet, die die Schülernamen und dazugehörige Codenummern enthalten. Mit diesen Codenummern sind auch die jeweiligen Datensätze gekennzeichnet. Dadurch können die Datensätze den jeweils betroffenen Schülern so lange zugeordnet werden, wie die Listen aufbewahrt werden. Wir erwarten, daß die BSJB uns vor der Durchführung der Hauptstudie an der Klärung solcher Verfahrensfragen beteiligt.

Die erhobenen Informationen sollen auch bezogen auf die vorherigen vierten Klassen ausgewertet werden und beziehen sich somit auch auf die dortigen Lehrer. Wir haben der BSJB daher empfohlen, die zuständigen Lehrerpersonalräte vor Beginn der Studie zu beteiligen. Dieser Empfehlung ist sie allerdings nicht gefolgt.

8. Finanzen und Steuern

8.1 Zweitwohnungsteuer

Im letzten Tätigkeitsbericht (vgl. 13. TB, 10.2) hatten wir über die Prüfung des Verfahrens zur Erhebung der Zweitwohnungsteuer berichtet. Unsere Feststellungen vor Ort hatten seinerzeit ergeben, daß personenbezogene Daten, deren Kenntnis für die Aufgabenerfüllung im Bereich der Zweitwohnungsteuer nicht mehr erforderlich war, nicht den Anforderungen gemäß § 4 Abs. 2 Nr. 6 HmbDSG entsprechend gelöscht worden sind.

Seit Juli 1995 werden nunmehr in regelmäßigen Abständen automatisierte Löschungsläufe für die Speicherkonten aus dem Zweitwohnungsteuerbestand durchgeführt. Dabei werden jeweils alle vorhandenen Datensätze auf die Erfüllung einer Reihe verbindlicher Löschungskriterien untersucht. Treffen diese zu, erfolgt eine unwiderrufliche physische Entfernung aus dem Datenbestand. Diese Vorgehensweise ist datenschutzgerecht.

9. Wissenschaft, Forschung und Kultur

9.1 Überprüfung der Erfüllung von Lehrverpflichtungen

Im Januar 1995 wurden Professoren der Universitätsklinik Eppendorf (UKE) in der Presse namentlich erwähnt, weil sie ihren Lehrverpflichtungen nicht ausreichend nachgekommen sein sollen. Wir hatten daher Zweifel, ob diese Daten im UKE durch die Kommission zur Überprüfung der Erfüllung von Lehrverpflichtungen mit der erforderlichen Vertraulichkeit behandelt worden waren. Auf unsere mehrfache Nachfrage hinsichtlich der künftigen Praxis teilte uns das UKE schließlich mit, die Kommissionsmitglieder (einschließlich der Studierenden) würden zur Verschwiegenheit verpflichtet und es würden keine personenbezogenen Daten öffentlich gemacht werden.

9.2 Lebenslauf in Dissertationen

Eine Petentin berichtete uns, sie solle nach dem Willen ihres Fachbereichssprechers in die Pflichtexemplare ihrer Dissertation ihren Lebenslauf einbinden; da die Dissertation zu veröffentlichen ist, würde damit also auch ihr Lebenslauf veröffentlicht werden. Begründet wurde ihr dies zunächst unter Hinweis auf die Promotionsordnung. Nachdem sie selber dieser Vorschrift eine solche Pflicht nicht entnehmen konnte, wurde sie darauf verwiesen, der Sprecher des Fachbereichs würde die Arbeit sonst nicht anerkennen.

Ob es eine sachliche Rechtfertigung für diese Forderung gibt, erscheint zweifelhaft. Jedenfalls gibt es aber keine Rechtsgrundlage dafür. Die fragliche Promotionsordnung enthält eine derartige Verpflichtung nicht. Selbst wenn sie es täte, wäre das unbeachtlich, denn § 63 Hamburgisches Hochschulgesetz, auf den sich die Promotionsordnungen stützen, enthält keine Ermächtigung für derartige Eingriffe in das informationelle Selbstbestimmungsrecht der Doktoranden. Der Fachbereich hat inzwischen bestätigt, daß eine Dissertation auch ohne eingebundenen Lebenslauf anerkannt werden kann. Die Universität prüft, ob entsprechender Klärungsbedarf noch in anderen Fachbereichen besteht.

9.3 Einsichtnahme in Personenstandsbücher für das Projekt der KZ-Gedenkstätte Neuengamme

Im 13. TB (11.3) hatten wir darüber berichtet, daß die KZ-Gedenkstätte Neuengamme beabsichtigt, aus Anlaß des 50. Jahrestages der Befreiung vom Nationalsozialismus im Mai 1995 ein Totenbuch mit den Daten der Opfer des früheren KZ-Neuengamme und seiner Außenlager zu erstellen, und daß zur Realisierung dieses Projekts auch die beim Sonderstandesamt Arolsen beurkundeten ca. 6.000 Sterbefälle herangezogen werden sollen.

Gegen dieses Vorhaben haben wir keine datenschutzrechtlichen Bedenken erhoben. Das Regierungspräsidium Kassel als Obere Standesamtaufsicht für

das Sonderstandesamt Arolsen und das Hessische Ministerium des Innern vertraten dagegen die Auffassung, daß § 61 Personenstandsgesetz (PStG) die Einsicht in die Sterbebücher nicht zuläßt, weil die KZ-Gedenkstätte angeblich nicht die an den Behördenbegriff des § 61 Abs. 1 PStG zu knüpfenden Voraussetzungen erfüllt. Außerdem dürften die aus der Einsichtnahme gewonnenen personenbezogenen Daten nur zur Erledigung der konkreten Verwaltungsaufgabe verwendet, nicht aber, wie in dem Projekt vorgesehen, auch in einem Totenbuch veröffentlicht werden; dies würde angeblich zu einer Umgehung der bereichsspezifischen Regelung des § 61 Abs. 1 PStG führen.

Wegen der unterschiedlichen Rechtsauffassungen und der Bedeutung dieser Angelegenheit haben wir den Hessischen Datenschutzbeauftragten gebeten, die Auslegung des § 61 PStG mit dem Hessischen Ministeriums des Innern und dem Regierungspräsidium Kassel zu klären.

Entgegen der Auffassung des Regierungspräsidiums Kassel und des Hessischen Ministeriums des Innern sind sowohl der Hessische Datenschutzbeauftragte als auch das Bundesministerium des Innern übereinstimmend zu dem Ergebnis gelangt, daß es sich bei der KZ-Gedenkstätte Neuengamme um eine Einrichtung der Freien und Hansestadt Hamburg handelt, die in einer besonderen Organisationsform bestimmte, in den Zuständigkeitsbereich der Kulturbehörde fallende Aufgaben wahrnimmt. Sie erfüllt damit die für eine Einsichtnahme erforderlichen Voraussetzungen nach § 61 Abs. 1 PStG.

Auch in Hinblick auf die vorgesehene Verwendung der Daten wurden weder irgendwelche Hindernisse oder gar Umgehungen des § 61 Abs. 1 PStG erkannt, die einer Benutzung der Personenstandsbücher durch die Gedenkstätte entgegenstehen. Denn die Daten, die veröffentlicht werden sollen, sind nicht dazu geeignet, Unberechtigten rechtlich relevante Informationen zu verschaffen.

Damit wurde die von uns vertretene Auffassung in vollem Umfang bestätigt. Das Hessische Ministerium des Innern und das Regierungspräsidium Kassel haben daraufhin ihre ursprünglichen Bedenken gegen die gewünschte Einsichtnahme in die Personenstandsunterlagen des Sonderstandesamtes Arolsen zurückgestellt.

Anschließend hat das Hessische Ministerium des Innern aber erneut Bedenken gegen eine Einsichtnahme und Verwendung der Daten erhoben, die eine Realisierung des Projekts in Frage stellen könnten und daher einer Klärung bedürfen.

Diese Bedenken wurden insbesondere von dem Internationalen Suchdienst des Roten Kreuzes (ISD) vorgetragen, der dem Sonderstandesamt noch heute jährlich umfangreiche Unterlagen über ehemalige zivile Verfolgte des NS-Regimes zur Verfügung stellt. Voraussetzung für diese einseitige Überlassung ist der Abschluß von Verträgen (z. B. mit dem Staatsarchiv Warschau, Staatsarchiv Bremen), in denen sich der ISD verpflichtet, das Material ausschließlich

im Interesse des betreuten Personenkreises zwecks Geltendmachung seiner Rechte, d.h. für den humanitären Auftrag zu verwenden.

Das Hessische Ministerium des Innern hat daher seine Entscheidung zu der Einsichtnahme in die Unterlagen des Sonderstandesamts bis zu einer abschließenden Klärung zurückgestellt.

Über den Projektfortgang werden wir weiter berichten.

10. Bauwesen und Stadtentwicklung

10.1 Mietenspiegelerhebung 1995 mittels Laptop

Wie bereits im 12. TB (12.3) berichtet, hat der Senat für jede Mietenspiegelerhebung eine neue Rechtsverordnung mit einer Geltungsdauer von 3 Jahren auf der Grundlage von § 2 Abs. 3 Hamburgisches Statistikgesetz (HmbStatG) zu erlassen.

Mit der Mietenspiegelbefragungsverordnung vom 28. März 1995 (Hamburgisches Gesetz- und Verordnungsblatt Seite 67) ist eine Rechtsverordnung – ohne Auskunftspflicht – für die Erstellung der Mietenspiegel 1995 (Grunderhebung) und 1997 (Fortschreibung) geschaffen worden. Dabei soll sich die Grunderhebung auf eine repräsentative Brutto-Stichprobe von rund 22.500 Wohnungen, die Fortschreibung dagegen auf rund 6.600 Wohnungen erstrecken, wobei die Mieter oder Vermieter zu gleichen Teilen befragt werden.

Da die Mietenspiegelerhebung 1995 bei den betroffenen Mietern und Vermietern erstmalig unter Einsatz von tragbaren PC (Laptop) erfolgen sollte, wurde in § 4 der Mietenspiegelbefragungsverordnung folgende Regelung festgelegt: Die Erhebung erfolgt durch eine Interviewer-Befragung unter Verwendung eines standardisierten Fragebogens oder mit Einverständnis der zu Befragenden mittels tragbaren PC (Laptop PC) unter Verwendung eines inhaltlich gleichen Fragebogens.

Im Vorfeld war daher zu prüfen, unter welchen Voraussetzungen ein Laptop-Einsatz in Frage kommen könnte. Gegen einen Einsatz von Laptops bei Mietenspiegelerhebungen bestehen nach unserer Ansicht dann keine grundsätzlichen Bedenken, wenn unter Berücksichtigung der Sensibilität der zu verarbeitenden personenbezogenen Daten auch die entsprechenden Maßnahmen zur Gewährleistung des Schutzes der Daten erfüllt werden. Die von uns für erforderlich angesehenen Maßnahmen haben wir den beteiligten Stellen zugeleitet.

In einer abschließenden gemeinsamen Besprechung mit Vertretern der verantwortlichen Baubehörde und der mit der Erhebung und Auswertung der Mietenspiegeldaten beauftragten Unternehmen wurden dann die für die Nutzung von Laptops im Rahmen der Mietenspiegelerhebung 1995 erforderlichen tech-

nischen und organisatorischen Maßnahmen zur Datensicherung (§ 8 Hamburgisches Datenschutzgesetz) erörtert und folgende Verfahrensweise festgelegt:

1. Die Interviewer erhalten für den Erhebungszeitraum der Mietenspiegelerhebung 1995 einen bestimmten, einer Person fest zugeordneten tragbaren PC (Laptop) vom gleichen Typ. Der Einsatz von privaten Laptop ist auszuschließen.

   Auf den Rechnern dürfen sich neben dem Betriebssystem ausschließlich das Erhebungsprogramm – in compilierter Form – und folgende, für die Bearbeitung notwendige Dateien befinden:

   - eine Adreßdatei, die die Namen und Anschriften der zu befragenden Personen, eine ID-Nummer (Hilfsmerkmal für die Trennung von Befragungsergebnissen), den jeweiligen Status des Interviews (z. B. erfolgreich/erfolglos), Besuchszeiten und ggf. vereinbarte Termine enthält,
   - ein „coded answer file", in dem die codierten Ergebnisse der Befragungen unter der jeweiligen ID-Nummer abgelegt werden,
   - ein „open answer file", in dem die zu einigen Fragen möglichen wörtlichen Antworten, Begründungen und Anmerkungen unter der jeweiligen ID-Nummer gespeichert werden.

2. Die Laptops sind mit einem Festplattenschutz auszustatten, der verhindert, daß jedwede Person vom Diskettenlaufwerk aus booten kann, um von der Festplatte Daten zu lesen oder zu entnehmen, Viren aufzuspielen, Programme zu kopieren oder andere Manipulationen vorzunehmen.

   Außer dem autorisierten Fachpersonal des beauftragten Unternehmens darf es niemandem ermöglicht werden, auf die Betriebsebene zu gelangen.

3. Für die Interviewer sind immer zwei individuelle und unterschiedliche Paßworte einzurichten; eines für den Start des Rechners und ein weiteres für die Benutzung des Erhebungsprogramms. Letzteres wird über die Anwendung so gesteuert, daß eine dreimalige fehlerhafte Eingabe zum Abbruch führt, der nur durch das beauftragte Unternehmen wieder behoben werden kann.

4. Die Interviewer erhalten keinen Zugriff auf die Betriebsebene. Nach korrekter Eingabe der jeweiligen Paßworte wird übergangslos das Erhebungsprogramm gestartet. Die Benutzung erfolgt menügesteuert, d. h. die Anwender können den Fragenkatalog nur über das angebotene Menü abarbeiten. Ein Abbruch des Programms führt nicht dazu, daß Betriebssystembefehle abgesetzt werden können.

   Der nachträgliche Zugriff auf abgeschlossene Interviews durch den Interviewer ist ausgeschlossen. Wird anschließend festgestellt, daß Eingaben unvollständig oder fehlerhaft erfolgt sind, muß dieser Fall durch das beauftragte Unternehmen erneut freigegeben und das Interview ggf. wiederholt werden.

5. Die Codierung der Ergebnisdaten erfolgt auf den Laptops programmgesteuert. Sie dürfen nicht in Klarschrift lesbar sein.

   Ein Datenaustausch findet nur im Büro des beauftragten Unternehmens durch autorisiertes Fachpersonal statt. Die Übernahme der Ergebnisdaten in das dortige DV-Netzwerk erfolgt über die serielle Schnittstelle des Laptops. Die codierten Ergebnisdaten können nur durch Eingabe eines gesonderten, ausschließlich dem autorisierten Fachpersonal bekannten Paßwortes lesbar gemacht werden.

   Da keine Verschlüsselung im engeren Sinne stattfindet, erhalten die Interviewer ihren Laptop jeweils nur mit einer geringen Anzahl von Adressen für einen begrenzten Erhebungszeitraum von einer Woche. Jeder Interviewer hat mindestens einmal wöchentlich seine Ergebnisse bei dem beauftragten Unternehmen abzuliefern. Nach Übernahme der Daten sind die auf der Festplatte der Laptops gespeicherten Daten physikalisch zu löschen. Der Interviewer erhält dann neue Adreßdaten.

6. Nach Abschluß der Erhebung und Kontrolle der ordnungsgemäß durchgeführten Interviews werden die Adreß- und Ergebnisdaten bis zur Auftragserledigung auf getrennten Rechnern gespeichert.

7. Die Umgangs- und Verfahrensweise sowie die Schutzmaßnahmen beim Einsatz von Laptops sind im Interviewer-Handbuch festzulegen. Dabei ist zu beachten, daß bestimmte Programme (z. B. Software oder Maßnahmen für Verschlüsselung) nicht benannt werden.

8. In das Interviewer-Handbuch sind neben den bereits für die Mietenspiegelerhebung 1993 festgelegten Regelungen (vgl. 12. TB, 12.3) weitere Einzelheiten aufzunehmen. Dazu gehören insbesondere,

   - daß bei Ausfall des Laptop oder auf Wunsch des zu Befragenden der Fragebogen zu benutzen ist,
   - wo und wie der Laptop bei Nichtbenutzung (z. B. nachts, aber auch auf dem Transportwege zu den vorgegebenen Adressen, insbesondere bei Nutzung öffentlicher Verkehrsmittel) sicher zu verwahren ist,
   - daß die erfaßten Daten mindestens einmal wöchentlich beim beauftragten Unternehmen abzuliefern sind.

Die Einhaltung der oben beschriebenen Maßnahmen zur Gewährleistung des Schutzes der personenbezogenen Daten wurde von der verantwortlichen Baubehörde und den beauftragten Unternehmen zugesichert, so daß aus unserer Sicht keine Bedenken gegen den Einsatz von Laptops für die Mietenspiegelerhebung 1995 zu erheben waren.

Vor dem Hintergrund, daß die Feldarbeiten für die Mietenspiegelerhebung erstmalig in Hamburg unter Einsatz von Laptops durchgeführt wurden, haben wir während der Erhebungsphase eine Prüfung bei dem mit der Erhebung beauftragten Unternehmen durchgeführt. Die Prüfung hat ergeben, daß die technischen und organisatorischen Maßnahmen zur Datensicherung den Forderungen entsprachen, die in der gemeinsamen Besprechung mit Vertretern der Baubehörde und der beauftragten Unternehmen festgelegt wurden.

Die Auswertungen der Mietenspiegelbefragung 1995 haben ergeben, daß die Erhebung mittels Laptop – entgegen ursprünglichen Befürchtungen – weitestgehend von den zu Befragenden akzeptiert wurde. Dies wird dadurch bestätigt, daß sich lediglich 10 Mieter gegen eine Erhebung mittels Laptop entschieden und den Fragebogen vorgezogen haben.

Weiterhin hat sich gezeigt, daß die durchschnittlichen Verweigerungsquoten sowohl aus allgemeinen Gründen (13,8 %) als auch aus datenschutzrechtlichen Gründen (0,4 %) im Vergleich zu der Mietenspiegelerhebung 1993 nahezu konstant geblieben sind. Es ist daher davon auszugehen, daß bei der Mietenspiegelerhebung 1997 auch wieder Laptops eingesetzt werden.

10.2 Einrichtung des Flächenbezogenen Informationssystems (FIS) und Projekt Hamburgisches Automatisiertes Liegenschaftsbuch (HALB)

Die für Anfang 1996 vorgesehene Realisierung des beschreibenden Teils des Flächenbezogenen Informationssystems (Projekt HALB = Hamburgisches Automatisiertes Liegenschaftsbuch) wird sich aufgrund der Komplexität bis Mai 1996 verlängern (vgl. 13. TB, 12.1).

Ab August 1996 sind mehrmonatige Pilotverfahren (Parallelbetrieb) beim Kataster- und Vermessungsamt des Bezirksamtes Hamburg-Nord und Schulungen der Anwender vorgesehen. Mit dem flächendeckenden Einsatz von HALB soll dann im Januar 1997 begonnen werden.

Zwischenzeitlich sind auch die vorbereitenden Maßnahmen für die Erstellung einer

- Fachlichen Weisung über die Übermittlung und Nutzung von Daten des Flächenbezogenen Informationssystems (FIS) und der Landesvermessung,
- Verordnung über das automatisierte Abruf- und Zugriffsverfahren beim Flächenbezogenen Informationssystem (FIS) auf Grund von § 14 Abs. 5 und 6 Hamburgisches Gesetz über das Vermessungswesen (vgl. 12. TB, 12.1),
- Vereinbarung nach § 94 Hamburgisches Personalvertretungsgesetz (HmbPersVG) über die Einrichtung und Nutzung des FIS intensiviert worden.

Aufgrund der bisher mit uns geführten Gespräche und Stellungnahmen zur Übermittlung und Nutzung des FIS sowie zum automatisierten Abruf- und

Zugriffsverfahren wurde die in HALB integrierte Systemkomponente „HALB-Datenschutz" (vgl. 13. TB, 12.1) in ihrer Funktionalität erweitert.

Für den künftigen automatisierten Datenaustausch zwischen Vermessungs- und Grundbuchverwaltung (IuK-Vorhaben „Automation Grundbuch") konnten gemeinsam erarbeitete Lösungsmodelle bisher nicht realisiert werden (vgl. 13. TB, 12.1).

Über den Projektfortgang werden wir weiter berichten.

10.3 Projekt Bauaufsicht mit Computerunterstützung (BACom)

Das für die Bauprüfdienststellen entwickelte computerunterstützte Baugenehmigungsverfahren BACom (vgl. 13. TB, 12.2) ist systemtechnisch weitgehend fertiggestellt, fachlich jedoch noch nicht vollständig eingerichtet. Die entsprechenden Maßnahmen (z. B. Textbausteine und Prüfhilfen) erfolgen für jede Vorgangsart, z. B. für das Baugenehmigungsverfahren, separat und komplett. Bisher sind so die Vorgangsarten „Verfahren nach der Hamburgischen Bauordnung (HmbBauO)" und „Verfahren nach dem Hamburgischen Gesetz zur Erleichterung des Wohnungsbaus (HmbWoBauErlG)" eingerichtet worden. Der Abschluß „Vorbescheidsverfahren" steht kurz bevor.

Im Bereich Wandsbek (Kerngebiet) und in Rahlstedt sind seit 1. Oktober 1995 zwei Verfahren zur Pilotierung eingerichtet worden. Die Pilotierungsphasen sind bis Ende 1995 vorgesehen.

Ziel der Pilotierung ist festzustellen, ob sich BACom in der vorhandenen Version im praktischen Einsatz grundsätzlich bewährt, welche notwendigen Berichtigungen und Verbesserungen vorgenommen werden müssen und welche Fachanwenderwünsche realisiert werden können.

Wir haben gegenüber dem Senatsamt für Bezirksangelegenheiten angekündigt, daß wir das BACom-Verfahren vor dem flächendeckenden Einsatz prüfen werden.

10.4 Prüfung des Fehlbelegungsabgabe-Verfahrens

Nachdem die 1991 durchgeführte Prüfung des Fehlbelegungsabgabe-Verfahrens der Mietenausgleichszentrale (MAZ) als Abteilung der Hamburgischen Wohnungsbaukreditanstalt (WK) in 1992 abgeschlossen wurde (vgl. 11. TB, 12.2.1), ist die Gewährleistung der seinerzeit zugesagten technischen und organisatorischen Maßnahmen beim Fehlbelegungsabgabe-Verfahren erneut geprüft worden.

Dies geschah insbesondere vor dem Hintergrund, daß die MAZ ab ca. Mitte 1992 damit begonnen hat, die Akten der abgeschlossenen Fälle von leistungsfreien Wohnungsinhabern im Rahmen einer Auftragsdatenverarbeitung durch ein Fremdunternehmen verfilmen und anschließend vernichten zu lassen. Zur Umsetzung dieser Maßnahme wurde eine vertragliche Vereinbarung zwischen

der WK (Auftraggeber) und dem beauftragten Fremdunternehmen (Auftragnehmer) getroffen.

Die uns vorgelegten Vertragsunterlagen für die Mikroverfilmung und die anschließende Aktenvernichtung enthielten nur sehr allgemein gehaltene Bestimmungen zum Datenschutz und bezogen sich ausschließlich auf das Bundesdatenschutzgesetz (BDSG). Eine klare Abgrenzung zwischen den Bestimmungen des BDSG und denen des Hamburgischen Datenschutzgesetzes (HmbDSG) wurde nicht vorgenommen.

Für die Datenverarbeitung im Auftrag öffentlicher Stellen der Freien und Hansestadt Hamburg gelten aber die Vorschriften des § 3 HmbDSG. Die sich daraus ergebende Prüfkompetenz des Hamburgischen Datenschutzbeauftragten beim Auftragnehmer und die Sicherstellung, daß der Auftragnehmer insbesondere die Bestimmungen der Datensicherungsregelungen des HmbDSG befolgt, sind in dem Vertrag nicht geregelt worden. Weiterhin sind in diesem Zusammenhang auch keine konkreten technischen und organisatorischen Maßnahmen zur Datensicherung getroffen und schriftlich vereinbart worden, um die Ausführung der Vorschriften des HmbDSG zu gewährleisten. Diese Maßnahmen werden von uns angesichts der Sensibilität der in den Akten gespeicherten Daten (z. B. Einkommensnachweise von Mietern und anderen Wohnungsnutzern) für erforderlich angesehen.

Zwischenzeitlich sind zwar einige vertragliche und organisatorische Nachbesserungen zur Datensicherung erfolgt, die nach unserer Auffassung aber noch nicht ausreichen, um die Ausführung der Vorschriften des HmbDSG zu gewährleisten. Unsere Gespräche mit der WK und der MAZ waren bei Redaktionsschluß noch nicht beendet. Über das Ergebnis werden wir weiter berichten.

11. Meldewesen

11.1 Rechtsgrundlagen

11.1.1 Novellierung des Hamburgischen Meldegesetzes

Der Senat hat der Bürgerschaft im Juni 1995 den Entwurf eines Vierten Gesetzes zur Änderung des Hamburgischen Meldegesetzes (HmbMG) zugeleitet.

Die beabsichtigte Neuregelung beseitigt die bislang geltende Bindung an die örtlich jeweils zuständige Meldebehörde. Sie ermöglicht den überörtlichen Zugriff auf einen einheitlichen Einwohnerdatenbestand.

Ob damit, wie vom Senat erwartet, tatsächlich die Chance einer bürgernäheren und flexibleren Aufgabenwahrnehmung eröffnet wird (vgl. hierzu 13. TB, 13.2), bleibt abzuwarten. Über die Umsetzung der geplanten Änderungen soll dem Senat bis Ende 1996 ein Prüfbericht vorgelegt werden.

Ferner wird den Wahlberechtigten künftig ein Widerspruchsrecht gegen Auskünfte aus dem Melderegister an Parteien oder Wählervereinigungen im Zusammenhang mit Wahlen eingeräumt. Die gegenwärtige Praxis, entsprechend einem Ersuchen der Bürgerschaft generell keine Auskünfte für Zwecke der Wahlwerbung zu erteilen, sollte allerdings auch nach Einführung des Widerspruchsrechts fortgesetzt werden. Eine entsprechende Klarstellung für die Amtliche Begründung haben wir in der Sitzung des Innenausschusses der Bürgerschaft am 30. November 1995 angeregt.

Ferner haben wir uns dafür eingesetzt, die bislang schon praktizierte Speicherung von Angaben zu Art und Ausgabedatum von Untersuchungsberechtigungsscheinen nach dem Jugendarbeitsschutzgesetz auf eine normenklare meldegesetzliche Grundlage zu stellen.

Schließlich haben wir uns dafür ausgesprochen, Auskünfte aus Verzeichnissen über Personen, die in Krankenhäuser, Pflegeheime oder ähnliche Einrichtungen aufgenommen wurden, an Polizei und Feuerwehr zum Zwecke der Gefahrenabwehr allein dann zuzulassen, wenn die Gefahr nicht nur als erheblich, sondern darüber hinaus auch als gegenwärtig einzuschätzen ist. Der Bund hat im Melderechtsrahmengesetz (MRRG) bereits eine entsprechende Einschränkung der Übermittlungsbefugnis vorgenommen. Nach unserer Ansicht handelt es sich dabei um eine Vollregelung der Materie mit unmittelbar verbindlicher Wirkung für den Landesgesetzgeber.

Unsere Vorschläge werden von der Behörde für Inneres unterstützt. Wir gehen davon aus, daß auch der Innenausschuß der Bürgerschaft diesen Empfehlungen voraussichtlich folgen wird.

11.1.2 Zweite Bundesmeldedatenübermittlungsverordnung

Am 9. November 1995 ist die Zweite Bundesmeldedatenübermittlungsverordnung (2. BMeldDÜV) in Kraft getreten. Sie regelt die Durchführung regelmäßiger Datenübermittlungen der Meldebehörden an Kreiswehrersatzämter, die Bundesanstalt für Arbeit, den Postrentendienst und die Datenstelle der Rentenversicherungsträger.

Mit Unterstützung der Behörde für Inneres konnten wir erreichen, daß uns künftig Gelegenheit zur Äußerung gegeben wird, bevor Meldebehörde und Datenempfänger Vereinbarungen über Datenträger, Codes oder Datenübertragungswege treffen, die vom Datensicherheitsstandard der 2. BMeldDÜV abweichen.

11.2 Projekt Reorganisation Einwohner-Meldewesen

Im 13. TB (13.1) berichteten wir über das Projekt Reorganisation Einwohner-Meldewesen (MEWES). Die Diskussion zu diesem Projekt wurde weitergeführt, insbesondere hinsichtlich der Protokollierung von Auskunftsersuchen.

Nach dem Ergebnis unserer Analyse entspricht die Datensatzbeschreibung, abgesehen von den Angaben zu Art und Ausgabedatum der Untersuchungsberechtigungsscheine (vgl. 11.1.1), dem Umfang der melderechtlichen Speicherungsbefugnis. Eine Klarstellung zum Begründungstext des Gesetzes erwarten wir allerdings für sog. Doppelfallmerker, die gezielte Hinweise auf Meldepflichtige mit identischen Datensätzen vermitteln sollen. Wir wenden uns aber nicht gegen die Notwendigkeit dieser Speicherungen aus fachlicher Sicht, sondern sehen den Vorteil, daß mit Hilfe der Doppelfallmerker fehlerhafte Melderegisterauskünfte vermieden werden.

12. Ausländerangelegenheiten

12.1 Verordnung zur Durchführung des Gesetzes über das Ausländerzentralregister

Auf datenschutzrechtliche Probleme im Zusammenhang mit dem Gesetz über das Ausländerzentralregister (AZRG) sind wir bereits im 13. TB (15.2) ausführlich eingegangen.

Am 25. Mai 1995 ist die Durchführungsverordnung zu diesem Gesetz (AZRG - DV) in Kraft getreten. Sie regelt Einzelheiten zum Anlaß und Inhalt der Speicherung im Register, zur Datenübermittlung an und durch das Bundesverwaltungsamt als Registerbehörde, zur Auskunft an den Betroffenen sowie zur Berichtigung, Löschung und Sperrung von Daten.

Bei der Beratung der AZRG-DV haben wir uns – allerdings erfolglos – dafür eingesetzt, telefonische Ersuchen öffentlicher Stellen um Übermittlung von Daten aus dem Register stärker einzuschränken. Nicht durchgesetzt werden konnte auch unser Anliegen, die Unterrichtung der Datenschutzbeauftragten über Gruppenauskünfte, die eine Mehrzahl von Ausländern mit gemeinsamen Merkmalen (Personalien, ausländerrechtlicher Status, räumliche Zuordnung innerhalb des Bundesgebiets) betreffen, zu erweitern.

12.2 Asyl-Card

Vorschläge einer „Bund-Länder-Arbeitsgruppe zur Harmonisierung der Verwaltungsabläufe im Asylverfahren" sehen die Einführung einer sog. ASYL-CARD vor. Jeder Asylbewerber soll verpflichtet werden, diese multifunktional nutzbare Chipkarte mit Daten zu seiner Identifizierung, zum Stand des Asylverfahrens, zur Arbeitserlaubnis und zum Empfang von Unterstützungsleistungen bei sich zu führen. Überlegt wird, die ASYL-CARD nicht nur mit einem Lichtbild, sondern auch mit den biometrischen Daten des Fingerabdrucks zu versehen.

Für eine Machbarkeitsstudie zu den rechtlichen und technischen Möglichkeiten und Grenzen der ASYL-CARD haben sich bereits sieben Bundesländer ausgesprochen.

Diesem Vorhaben sind wir entschieden entgegengetreten. Die umfassende Zusammenführung und Registrierung sensibler Daten aus unterschiedlichen Lebensbereichen stellt einen schwerwiegenden Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar, dessen Erforderlichkeit für Verwaltungszwecke nicht belegt ist.

13. Verfassungsschutz

13.1 Befugnisse des Bundesnachrichtendienstes bei der Überwachung des internationalen Fernmeldeverkehrs

Im 13. TB (18.4) haben wir kritisiert, daß die Befugnisse des Bundesnachrichtendienstes (BND) zur Überwachung des internationalen nicht leitungsgebundenen Fernmeldeverkehrs durch das Verbrechensbekämpfungsgesetz vom 28. Oktober 1994 erheblich erweitert worden sind.

Auf die Verfassungsbeschwerde eines Hamburger Hochschullehrers hat das Bundesverfassungsgericht am 5. Juli 1995 durch einstweilige Anordnung die Wirkungen der sog. verdachtslosen Rasterfahndung wesentlich begrenzt. Künftig dürfen personenbezogene Daten, die durch eine derartige Überwachungsmaßnahme gewonnen wurden, vom BND nur noch dann ausgewertet und an Strafverfolgungsbehörden übermittelt werden, wenn bestimmte Tatsachen den Verdacht begründen, daß jemand eine der im Gesetz genannten Straftaten plant, begeht oder begangen hat.

Nach dieser vorläufigen Entscheidung ist zu erwarten, daß das Bundesverfassungsgericht auch im Hauptsacheverfahren die besondere Bedeutung der Kommunikationsfreiheit betonen und die Überwachung einer Vielzahl unverdächtiger Bürgerinnen und Bürger begrenzen wird.

13.2 Hamburgisches Verfassungsschutzgesetz

Das Hamburgische Verfassungsschutzgesetz (HmbVerfSchG), dessen Beratung in der Bürgerschaft wir bereits im 13. TB (18.1) behandelt haben, ist am 14. März 1995 in Kraft getreten.

Wir konnten eine Absicherung des sog. Trennungsgebots bei Datenübermittlungen zwischen dem Landesamt für Verfassungsschutz und den Strafverfolgungsbehörden erreichen. So darf das Landesamt für Verfassungsschutz personenbezogene Daten, die es selbst mit nachrichtendienstlichen Mitteln erhoben hat, nur dann an Staatsanwaltschaft oder Polizei übermitteln, wenn bei diesen Behörden ihrerseits die Befugnisse zur verdeckten Datenerhebung vorgelegen hätten.

13.3 Querschnittsprüfung des Landesamtes für Verfassungsschutz

Das Landesamt für Verfassungsschutz hat zu den Ergebnissen unserer im Jahre 1994 durchgeführten Querschnittsprüfung (vgl. 13. TB, 18.3) zwischenzeitlich Stellung genommen.

Die neue automatisierte Referatsarbeitskartei (RAK) wurde installiert. Ein Abgleich der personenbezogenen Daten zwischen der RAK und den an Organisationen oder Ereignissen orientierten Indices ist erfolgt.

Das Landesamt für Verfassungsschutz vertritt den Standpunkt, daß Übermittlungen personenbezogener Informationen zwischen den Verfassungsschutzbehörden nur dann nicht erforderlich sind, wenn erkennbar ist, daß diese Informationen für die Aufgabenerfüllung nicht relevant sind oder sein können. In der weiteren Diskussion wird zu klären sein, ob nicht der Auswertung durch den Datenempfänger verstärkt eine Erforderlichkeitsprüfung der übermittelnden Verfassungsschutzbehörde entsprechend den dortigen Erkenntnissen vorgeschaltet werden muß.

14. Verkehrswesen

14.1 Prüfung bei der Führerscheinstelle der Landesverkehrsverwaltung

1995 haben wir die Datenverarbeitung bei der Führerscheinstelle der Landesverkehrsverwaltung querschnittsmäßig geprüft.

Hierbei ging es zum einen um Probleme der Erhebung und Übermittlung von Daten bei der Erteilung und dem Entzug von Fahrerlaubnissen, auf die hier nicht näher eingegangen werden soll. Im Vordergrund des Interesses standen daneben die Maßnahmen zur Datensicherung und die inhaltliche Verarbeitung von Daten im neuen automatisierten Bildschirmdialogverfahren der Führerscheinstelle (14.1.1) sowie die Speicherung von Daten in Karteien (14.1.2) und Akten (14.1.3), die im folgenden dargestellt werden.

Eine Stellungnahme der Behörde für Inneres zu unserem Prüfbericht vom April 1995 lag bei Redaktionsschluß dieses TB noch nicht vor.

14.1.1 Neues automatisiertes Verfahren der Führerscheinstelle

Seit April 1994 werden die Daten aller Führerscheininhaber, die erstmals eine Fahrerlaubnis in Hamburg beantragen, in einer zentralen automatisierten Datei gespeichert. Je nach Wohnsitz des Führerscheininhabers erfolgt die Erfassung in den drei Führerscheinstellen Ausschläger Weg, Bezirksamt Bergedorf oder Bezirksamt Harburg.

Alle Sachbearbeiter der drei Hamburger Führerscheinstellen haben lesenden Zugriff auf die Daten aller in Hamburg automatisiert erfaßter Führerscheininhaber. Eine regionale Differenzierung von Zugriffsbefugnissen zwischen den einzelnen Führerscheinstellen besteht nur insoweit, als ändernde und bearbeitende Zugriffe auf Datensätze im Zuständigkeitsbereich der jeweils anderen Dienststellen gesperrt sind.

Wir halten diese überregionalen Zugriffsbefugnisse nicht für zulässig. Im Rahmen der Zugriffskontrolle nach § 8 Abs. 2 Nr. 5 HmbDSG ist zu gewährleisten,

daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Bearbeitungszuständigkeit unterliegenden Daten zugreifen können.

Die einzelnen Dienststellen benötigen für ihre eigenen Aufgaben nur die Daten derjenigen Fahrerlaubnisinhaber, die ihrer regionalen – und persönlichen – Zuständigkeit unterliegen. Eine Begrenzung der Zugriffsmöglichkeit ist auch im Interesse der Mitarbeiter geboten. Wenn z. B. die Behauptung aufgestellt wird, aus dem Verfahren seien Daten unzulässigerweise anderen Stellen oder Privatpersonen übermittelt worden, fällt der Verdacht in erster Linie auf den zuständigen Mitarbeiter. Wegen des unbegrenzten Zugriffs können jedoch alle anderen Mitarbeiter der drei Dienststellen für die unzulässige Weitergabe verantwortlich sein. Wir haben daher gefordert, den Lesezugriff auf Daten anderer Dienststellen nach § 8 Abs. 2 Nr. 5 HmbDSG durch geeignete Sicherungsmaßnahmen im System zu unterbinden.

Innerhalb der Dienststelle haben alle Sachbearbeiter lesenden und ändernden Zugriff auf den Datenbestand des automatisierten Führerscheinwesens im regionalen Zuständigkeitsbereich. Obwohl die sachliche Zuständigkeit der einzelnen Sachbearbeiter – mit Ausnahme von übergreifenden Aufgaben wie der Erteilung von Berechtigungen zur Fahrgastbeförderung – nach Buchstaben der Nachnamen von Führerscheininhabern alphabetisch abgegrenzt ist, wird diese Zugriffsbeschränkung im EDV-System nicht nachvollzogen. Für einzelne Sachbearbeiter sind lediglich bestimmte Funktionen aus dem Bearbeitungsmenü gesperrt.

Ändernde Zugriffe auf Daten von Führerscheininhabern, die nicht der eigenen Bearbeitungszuständigkeit unterliegen, sind nicht erforderlich und damit durch geeignete Sicherungsmaßnahmen im System der EDV zu unterbinden. Dienststellenintern könnte allenfalls ein übergreifender lesender Zugriff auf eng begrenzte Datensatzinhalte, deren Kenntnis zwingend erforderlich ist, in Frage kommen.

Die Kriterien für das Auffinden von Datensätzen im automatisierten Verfahren sind diesen Anforderungen entsprechend anzupassen. Es existiert zur Zeit keine Festlegung, welche Suchkriterien mindestens am Bildschirm eingegeben werden müssen, um eine Abfrage erfolgreich abzuschließen. Bislang kann sich z. B. jeder Sachbearbeiter alle Datensätze von Führerscheininhabern anzeigen lassen, indem er etwa nur den ersten Buchstaben des Namens oder des Vornamens eingibt. Ebenso ist es bislang möglich, Datensätze über Teile einer Vorgangsnummer zu suchen.

Das Auffinden von Datensätzen sollte dagegen nur über eine gleichzeitig einzugebende Kombination aus Buchstaben des Vor- und Nachnamens sowie Zahlen des Geburtsdatums ermöglicht werden, um rechtlich problematische und verwechslungsträchtige „Gesamtauswertungen" zu vermeiden.

Ferner sind Freitextfelder über „Bemerkungen und Hinweise" problematisch. So fanden wir in einem Bemerkungsfeld die zum Zeitpunkt der Prüfung wahrscheinlich längst überholte Angabe vor: „Hält sich seit zwei Monaten auf Sylt auf laut Arbeitgeber." Wir haben gefordert, die Eintragungsmöglichkeiten in diesen Bemerkungs- und Hinweisfeldern auf Verweise zu begrenzen, die zum Auffinden von Akten erforderlich sind und den Ablauf einer Sperrfrist kennzeichnen.

Schließlich war zu kritisieren, daß das automatisierte Verfahren keine Löschfunktionen nach bestimmten Fristen vorsieht. Vielmehr können die Sachbearbeiter nur menügesteuert eine „Löschung" auslösen. Dies führt allerdings nicht zur Löschung in der Datenbank, sondern nur zu einer besonderen Kennzeichnung des Datensatzes. Der Datensatz wird damit zwar dem Zugriff der Mitarbeiter entzogen, ist jedoch für die fachliche Leitstelle und die Systemadministration weiterhin lesbar.

14.1.2 Kartei der Altfälle

Die ca. 1,5 Millionen Altfälle aus der Zeit vor Einführung des neuen automatisierten Verfahrens sind weiter auf Karteikarten erfaßt. Diese Altkarteien sind seit Einführung des neuen automatisierten Verfahrens insgesamt problematisch. Nach den bisherigen Regelungen werden die Karteikarten bis zum 85. Lebensjahr des Führerscheininhabers aufbewahrt. Eine regelmäßige Kontrolle der Kartei im Hinblick auf das Erreichen der Speicherungsfrist erfolgt nicht.

Erst im Zusammenhang mit der für 1996/97 geplanten Einführung des einheitlichen Führerscheins der Europäischen Union ist eine komplette Karteivernichtung nach dem Abschluß der Nacherfassung geplant.

Wir haben dagegen deutlich gemacht, daß die weitere Speicherung der Altfälle, die bereits im automatisierten Verfahren erfaßt sind, nicht gemäß § 19 Abs. 3 Nr. 2 HmbDSG erforderlich ist. Nach einer Kontrolle zum Zeitpunkt der Nacherfassung sind die Karteikarten daher ohne weitere Aufbewahrungsfrist zu vernichten.

14.1.3 Speicherung in Akten

Über Führerscheininhaber, denen die Fahrerlaubnis durch gerichtliche oder behördliche Entscheidung entzogen wurde, führt die Führerscheinstelle sogenannte persönliche Akten, in denen alle mit Fragen der Entziehung und der Neuerteilung zusammenhängenden Vorgänge enthalten sind. Zur Zeit existieren in der Führerscheinstelle der Landesverkehrsverwaltung ca. 70.000 persönliche Akten.

Ihr Inhalt besteht hauptsächlich aus Gerichtsurteilen, Auszügen aus dem Bundeszentral- oder Verkehrszentralregister, ärztlichen Gutachten (Facharzt, Medizinisch-psychologische Untersuchungsstellen), Nachschulungsberichten

sowie aus dem Schriftwechsel der Führerscheinstelle mit dem Führerscheininhaber und den untersuchenden Stellen.

In überprüften Akten haben wir zum Beispiel längst veraltete Auszüge aus dem Verkehrszentralregister bzw. Führungszeugnisse aus dem Bundeszentralregister vorgefunden. Obwohl die Mitarbeiter erkannt hatten, daß sie unverwertbar waren und daher aktuelle Auszüge angefordert haben, wurden die alten nicht entfernt.

Der lediglich anlaßbezogenen Löschung ist eine fristgerechte Aussonderung der zu vernichtenden Eintragungen vorzuziehen. Nach der Einführung des automatisierten Verfahrens kann dies geschehen, indem Wiedervorlagefristen im Verfahren notiert werden, die die Sachberarbeiter zur Vernichtung der veralteten Eintragungen veranlassen.

Eine Pflicht zur Vernichtung besteht insbesondere auch dann, wenn Erkenntnisse nicht einmal auf zulässigen Registeranfragen beruhen, sondern auf unzulässigen Mitteilungen aus dem polizeilichen Informationssystem (vgl. den im 12. TB, 16.1 geschilderten Fall).

14.2 Neues Fahrerlaubnisrecht

14.2.1 Entwurf einer Fahrerlaubnisverordnung

Die bei der Prüfung der Führerscheinstelle (14.1) aufgetretenen Probleme haben auch deutlich gemacht, daß wesentliche Fragen der Datenverarbeitung im Zusammenhang mit Fahrerlaubnissen nicht geregelt sind.

Daher ist es grundsätzlich zu begrüßen, daß die Bundesregierung eine Neufassung des Fahrerlaubnisrechts plant. Die in der Straßenverkehrszulassungsordnung (StVZO) nur ansatzweise enthaltenen Regelungen sollen konkretisiert und in eine neue Fahrerlaubnisverordnung (FeV) eingearbeitet werden. Der bisher bekanntgewordene Entwurf der Verordnung leistet die beabsichtigte und auch mögliche klare Regelung der Voraussetzungen und des Umfangs der Datenverarbeitung bei der Erteilung und dem Entzug von Fahrerlaubnissen jedoch nur unzureichend. Zu bemängeln sind insbesondere Unklarheiten und nachteilige Regelungen bei

- der Feststellung von Bedenken an der Eignung, ein Fahrzeug zu führen;
- dem Verfahren zur Prüfung der Eignung insbesondere durch die medizinisch-psychologische Untersuchung (MPU);
- den Speicherungsfristen in Dateien und Akten;
- der Harmonisierung zwischen den Tilgungsfristen im Bundes- und Verkehrszentralregister und den Löschungsverpflichtungen für entsprechende Informationen in Akten.

Wir haben die Behörde für Inneres in einer Stellungnahme aufgefordert, sich in den weiteren Beratungen für Verbesserungen einzusetzen.

14.2.2 Zentrales Fahrerlaubnisregister

Neben den Regelungen über das Verfahren bei der Erteilung von Fahrerlaubnissen ist im Zuge der Neuregelung des Straßenverkehrsrechts geplant, ein zentrales Register beim Kraftfahrt-Bundesamt in Flensburg zu schaffen, in dem sämtliche Fahrerlaubnisse erfaßt werden. Dieses zentrale Fahrerlaubnisregister wäre eine der größten personenbezogenen Datensammlungen in Deutschland mit Angaben über fast 50 Millionen Einwohner.

Die Bundesregierung begründet die Einführung dieser zentralen Führerscheindatei mit der Umsetzung der Zweiten EG-Führerscheinrichtlinie von 1991 und dem Erfordernis eines schnellen Informationsaustauschs zwischen den Partnern der Europäischen Union.

Bereits im Jahr 1993, als diese Pläne erstmalig bekannt wurden, haben wir uns gegen die Einrichtung dieses Registers gewandt, weil es für die zentrale Registrierung der großen Mehrheit der Bevölkerung keine überwiegenden Interessen der Allgemeinheit gibt. Angaben über Verkehrsverstöße und entzogene Führerscheine stehen bereits heute zentral für den Abruf der Verkehrsbehörden und Polizeidienststellen im Verkehrszentralregister zur Verfügung. Wenn ein Führerschein aus einem anderen Land der EU Unklarheiten aufweist, schreibt die EG-Richtlinie die Beteiligung der örtlich zuständigen Führerscheinbehörden in Art. 8 Abs. 5 ausdrücklich vor. Demnach macht ein zentrales Register Anfragen bei den örtlichen Stellen nicht entbehrlich und ist deshalb auch nicht im Sinne der Verwaltungsvereinfachung und eines reibungslosen Informationsaustauschs erforderlich.

Fälle, in denen Führerscheine nach dem Entzug der Fahrerlaubnis gefälscht oder unberechtigterweise Zweitausfertigungen benutzt werden, sind bei Verkehrskontrollen durch Abfragen im Verkehrszentralregister erkennbar. Nur solche Fälle, in denen jemand noch nie eine Fahrerlaubnis hatte, aber einen Führerschein benutzt, könnten mit Anfragen an das zentrale Führerscheinregister aufgedeckt werden. Voraussetzung wäre jedoch, daß zukünftig bei allen Kontrollen auch ohne Anhaltspunkte für Mißbrauch routinemäßig das Führerscheinregister abgefragt wird. Damit ist schon wegen des Zeitaufwands nicht zu rechnen.

Im übrigen bestünde das Risiko, daß jemand, der in Wahrheit eine ordnungsgemäße Fahrerlaubnis besitzt, aber im zentralen Register fälschlicherweise nicht eingetragen ist, erhebliche Schwierigkeiten bekommt und an der Weiterfahrt gehindert wird. Ein absolutes Vertrauen darauf, daß bei einem „Schweigen" des Registers auch keine Fahrerlaubnis erteilt worden ist, kann es nicht geben. Die Erfahrungen mit der Registrierung von Fahrzeugen und Haltern im zentralen Fahrzeugregister haben deutlich gemacht, daß erhebliche Diskrepanzen zwischen zentralen und örtlichen Beständen vorkommen, die immer wieder zu Fehlern führen.

Wegen des enormen Aufwandes und der massiven Zweifel am Sinn der Einrichtung eines zentralen Führerscheinregisters sind die Pläne 1993 vorerst aufgegeben worden. Neue Argumente sind seitdem nicht bekannt geworden. Gleichwohl soll das Vorhaben mit der alten Begründung nunmehr im Zuge einer Änderung des Straßenverkehrsgesetzes umgesetzt werden.

14.3 Automation in der Bußgeldstelle

Im 13.TB (16.1) hatten wir berichtet, daß ab Oktober 1994 das neue automatisierte Verfahren „OPAL" in der Bußgeldstelle des Einwohnerzentralamts eingerichtet würde. Diese Darstellung beruhte auf den Informationen, die wir unmittelbar vor dem geplanten Einführungstermin bei einer Prüfung erhalten hatten.

Als wir dann im Frühjahr 1995 noch Fragen der Datensicherheit prüfen wollten, erfuhren wir, daß das neue Verfahren noch nicht eingeführt worden ist. Es hatten sich vielmehr eine Reihe von technischen Problemen bei der Datenerfassung und der Übernahme von Daten aus anderen Beständen ergeben, die zu einer erheblichen Verzögerung führten. Bei Redaktionsschluß wurde Anfang 1996 als neuer Einführungstermin genannt.

14.4 Zugriff auf das Personalausweisregister im Bußgeldverfahren

Im 11.TB (16.1) waren die Voraussetzungen geschildert worden, unter denen die Polizei zur Feststellung des Verantwortlichen für eine Verkehrsordnungswidrigkeit Lichtbilder aus dem Personalausweis- oder Paßregister anfordern konnte. Danach war die Heranziehung der Lichtbilder nur dann möglich, wenn es sich um eine Ordnungswidrigkeit handelte, die mit einem Bußgeld von mindestens 80 DM und einer Eintragung im Verkehrszentralregister geahndet werden konnte.

Im Oktober 1994 hat der Bund-Länder-Fachausschuß für Straßenverkehrsordnungswidrigkeiten jedoch beschlossen, diese bisherige Grenze fallen zu lassen. Auch bei geringfügigen Verstößen, die nicht zur Eintragung im Verkehrszentralregister führen, soll der Lichtbildvergleich mit Hilfe des Paßfotos aus den amtlichen Registern zugelassen werden. Hamburg will sich dieser Verfahrensweise anschließen.

Wir haben uns gegen diese Entscheidung gewandt, weil die bisherige Grenze dem Grundsatz der Verhältnismäßigkeit entsprach. Dem ist die Behörde für Inneres nicht gefolgt. Da die gesetzlichen Vorschriften im Personalausweis- und Paßgesetz die genannten engeren Voraussetzungen nicht ausdrücklich vorschreiben, sehen wir keine Möglichkeit, die Absenkung der Grenze für den Zugriff auf die Daten des Paß- und Personalausweisregisters zu verhindern. Allenfalls die Gerichte könnten in einzelnen Verfahren die Beweiserhebung

wegen Verstoßes gegen den Verhältnismäßigkeitsgrundsatz für unzulässig erklären.

Falls es nicht zu derartigen Gerichtsurteilen kommt und die weitere Entwicklung zeigt, daß der Lichtbildvergleich in erheblichem Umfang bei geringen Verkehrsverstößen erfolgt, wird eine Gesetzesänderung zur Beachtung des Verhältnismäßigkeitsgrundsatzes zu prüfen sein.

15. Polizei

15.1 Parlamentarischer Untersuchungsausschuß „Hamburger Polizei"

15.1.1 Zentrale Forderungen des Datenschutzes

Bereits im 13. TB (17.8) haben wir die Forderung nach wirksamen Vorkehrungen zum Schutz des Persönlichkeitsrechts bei Aktenvorlage an den Parlamentarischen Untersuchungsausschuß (PUA) unterstrichen.

Dieser Vorkehrungen bedarf es insbesondere deshalb, weil angesichts der Vielzahl der vom Untersuchungsauftrag erfaßten Sachverhalte nicht in jedem Einzelfall die Einwilligung der Betroffenen hinsichtlich ihrer Daten eingeholt werden kann.

Durch namentliche Erwähnung in Akten sind häufig auch unbeteiligte Personen betroffen, die in keiner Weise Anlaß zu einer Untersuchung gegeben haben, sowie Polizeibeamte, die sich Vorwürfen ohne hinreichende tatsächliche Anhaltspunkte ausgesetzt sehen.

Die Bürgerschaft steht in der Verantwortung, durch ein Untersuchungsausschußgesetz und eine Datenschutzordnung klare Rahmenbedingungen zu schaffen, um Gefährdungen des Persönlichkeitsrechts entgegenzuwirken. Dazu zählen insbesondere Regelungen, die eine vom Untersuchungsauftrag her nicht gebotene Erörterung in öffentlicher Sitzung vermeiden.

Zunächst obliegt allerdings dem Senat die Prüfung, inwieweit eine personenbezogene Übermittlung von Unterlagen an den PUA überhaupt erforderlich ist, damit dieser seine verfassungsrechtlichen Aufgaben wahrnehmen kann. Soweit für den Untersuchungszweck eine anonymisierte Aufbereitung der Unterlagen ausreicht, kann eine Befugnis des Senats, die Akten dem PUA gleichwohl personenbezogen zugänglich zu machen, auch nicht bei hinreichenden datenschutzrechtlichen Geheimhaltungsvorkehrungen des Parlaments begründet werden.

15.1.2 Position des Senats

Diesen von uns frühzeitig eingebrachten und durch konkrete Verfahrensvorschläge begleiteten Überlegungen ist der Senat nur teilweise gefolgt.

Daten von Personen, die lediglich als Zeugen in Betracht kommen, hat er generell für weniger schutzwürdig gehalten; demzufolge hat er eine öffentliche Ausschußverhandlung für diesen Personenkreis als zumutbar betrachtet.

Hinsichtlich der personenbezogenen Daten von Polizeibeamten, gegen die sich Vorwürfe richten, sowie von Geschädigten und Beschwerdeführern hat der Senat eine Vorlagepflicht grundsätzlich bejaht; er hat die Vorlage allerdings mit der Auflage verbunden, daß über personenbezogene Akteninhalte vom PUA ausschließlich in nichtöffentlicher Sitzung und unter Wahrung der Vertraulichkeit verhandelt werde.

15.1.3 Rechtsstreit Senat – PUA über den Umfang der Vorlagepflicht

Die Auflage des Senats für die weitere Verfahrensgestaltung durch den PUA führte zu gerichtlichen Auseinandersetzungen.

Der auf uneingeschränkte Herausgabe der Akten durch den Senat gerichtete Beschlagnahmeantrag des PUA hatte vor dem Amtsgericht und Landgericht Hamburg zwar zunächst Erfolg. Auf Antrag des Senats erließ das Hamburgische Verfassungsgericht jedoch am 1. März 1995 eine einstweilige Anordnung, die als vorläufige Regelung eine Übergabe der Akten an den PUA nur zur nichtöffentlichen und vertraulichen Verhandlung personenbezogener Daten zuließ.

Das Hauptsacheverfahren vor dem Hamburgischen Verfassungsgericht wurde durch Urteil vom 19. Juli 1995 – HVerfG 1/95 – entschieden.

Dieses Urteil enthält grundsätzlich bedeutsame Aussagen zu den verfassungsrechtlichen Grundlagen parlamentarischer Aktenherausgabeansprüche, zur Abwägung von Untersuchungsauftrag und Persönlichkeitsrecht sowie zu den Anforderungen an eine Daten- oder Geheimschutzordnung der Bürgerschaft. Das Hamburgische Verfassungsgericht hebt die hohe Sensibilität des Grundrechts auf informationelle Selbstbestimmung und die hierauf ausgerichteten Schutzpflichten des Staates hervor. Für das Parlament verlangt es einen durch Normen sicherzustellenden Datenschutzstandard entsprechend den Vorschriften des Grundgesetzes.

Das Hamburgische Verfassungsgericht geht in seinem Urteil zwar auch auf den Gesichtspunkt der Amtshilfe gegenüber dem PUA ein. Insgesamt bestätigen die Aussagen des Urteils zur Normenklarheit und Verhältnismäßigkeit aber, daß auch weiterhin die Anforderungen des Bundesverfassungsgerichts an einen – amtshilfefesten – Schutz des Grundrechts auf informationelle Selbstbestimmung maßgebend sind.

Die zentralen Aussagen des Gerichts zur Aktenvorlage lassen sich wie folgt zusammenfassen:

Solange die Bürgerschaft eine Datenschutzordnung, die formell und inhaltlich den verfassungsrechtlichen Vorgaben entspricht, nicht beschlossen hat, trägt der Senat eine Mitverantwortung für den Schutz der personenbezogenen Daten. Soweit er angeforderte Akten dem PUA noch nicht vorgelegt hat, obliegt es dem Senat, dem PUA die wesentlichen Gründe für seine Forderung nach nichtöffentlicher Verhandlung personenbezogener Akteninhalte darzulegen. Umgekehrt trifft den PUA für die an ihn bereits herausgegebenen und vom Senat als nichtöffentlich verhandelbar bezeichneten Akten die Darlegungslast, daß eine Erörterung in öffentlicher Sitzung geboten sei. Kommt eine Einigung darüber, wie einzelne Akten einzustufen sind, nicht zustande, können Senat und Bürgerschaft das Hamburgische Verfassungsgericht anrufen.

Für die Zeit nach Erlaß verfassungsmäßiger Normen über den parlamentarischen Datenschutz geht das Hamburgische Verfassungsgericht von einer unbeschränkten Vorlagepflicht des Senats gegenüber der Bürgerschaft und ihren Ausschüssen aus. Dazu stellt das Gericht allerdings fest, daß es in den meisten Fällen für die Bürgerschaft und für die Öffentlichkeit nicht darauf ankomme, die Namen der in den Akten behandelten Personen kennenzulernen.

15.1.4 Ausblick

Nach dem Urteil des Hamburgischen Verfassungsgerichts ist nun die Neuregelung des Rechts der Untersuchungsausschüsse im Zuge der geplanten Verfassungsreform abzuwarten.

Im übrigen schließt das Urteil Regelungen nicht aus, die eine Vorklärung der Schutzwürdigkeit personenbezogener Daten im Einzelfall einem kleineren Kreis von Ausschußmitgliedern übertragen. Derartige Regelungen, die auch das Bundesverfassungsgericht als geeignete Verfahrensweise anerkannt hat, wahren die Stellung des PUA als „Herr des Untersuchungsverfahrens", beschränken jedoch zugleich die Bekanntgabe personenbezogener Daten auf den erforderlichen Umfang.

Zu diesem Zweck sind die Artikel in der Hamburgischen Verfassung über Aktenvorlage und über Untersuchungsausschüsse weiterzuentwickeln und durch gesetzliche Vorschriften insbesondere in einem Untersuchungsausschußgesetz zu konkretisieren.

15.2 Datenschutzrechtliche Probleme infolge des sogenannten „Polizeiskandals"

Die gegen Polizeibeamte erhobenen Vorwürfe, es seien Übergriffe und Mißhandlungen erfolgt, sind Gegenstand des Parlamentarischen Untersuchungsausschusses „Hamburger Polizei" (siehe oben 15.1) und von Strafermittlungsverfahren. Ob das in diesem Zusammenhang gebrauchte Stichwort „Polizeiskandal" zutrifft, unterliegt nicht unserer Beurteilung. Im folgenden wird es daher nur verwendet, um den Zusammenhang deutlich zu machen.

Die unter 15.2.1 bis 15.2.4 geschilderten Probleme machen deutlich, daß der Datenschutz für Polizisten ebenso gilt, wie für alle anderen Bürger. Wenn insbesondere von Polizeibeamten stets gefordert werden muß, daß sie die Rechte anderer wahren, haben sie Anspruch darauf, daß auch ihre Rechte nicht geringer veranschlagt werden. Die hier dargestellten Konflikte zwischen dem Schutz personenbezogener Daten und den Interessen zur Verfolgung von Straftaten, zur Wahrung der Gesetzmäßigkeit der Verwaltung und zur öffentlichen Berichterstattung sind aktuell im Bereich der Polizei aufgetreten. Sie können jederzeit in vergleichbarer Form auch andere Bürger innerhalb und außerhalb der Verwaltung betreffen.

15.2.1 Ermittlungen gegen Polizeibeamte

Ende 1994 erfuhren wir, daß die bei der Staatsanwaltschaft eingerichtete Ermittlungsgruppe zur Klärung strafrechtlicher Vorwürfe gegen Polizeibeamte die Personalakten einer ganzen Gruppe von insgesamt 47 Polizeibeamten angefordert hatte.

Bei einer Prüfung stellten wir den Grund für die Heranziehung der Akten fest: Die Ermittlungsgruppe der Staatsanwaltschaft wollte Informationen über den dienstlichen Werdegang, berufliche Vorkenntnisse, weitere Ermittlungsvorgänge usw. erlangen. Allerdings hatte sich bald herausgestellt, daß die Akten hierzu wenig weiterführende Informationen enthielten. Sie sind nach der Auswertung zurückgegeben worden.

Aufgrund der Akten sind sog. „Personalbögen" erstellt worden, die zur Vorbereitung der Anhörungen der Betroffenen angelegt worden sind. Nach Durchführung der jeweiligen Anhörungen sind die „Personalbögen" vernichtet worden.

Zur rechtlichen Zulässigkeit der Übersendung der Personalakten haben die Behörde für Inneres und die Justizbehörde Stellung genommen. Beide sind übereinstimmend zur Auffassung gelangt, daß die Aktenübersendung zur Durchführung des Strafermittlungsverfahrens nicht zulässig war, da die Vorlage an die Staatsanwaltschaft zu strafprozessualen Ermittlungen ohne Einwilligung des Betroffenen in § 96e Abs. 1 des Hamburgischen Beamtengesetzes (HmbBG) nicht vorgesehen ist. Dieser Auffassung haben wir uns angeschlossen.

Nach Auffassung der Justizbehörde wäre gemäß § 96e Abs. 2 und 3 HmbBG lediglich eine Erteilung von Auskünften im erforderlichen Umfang möglich gewesen. Diese Differenzierung zwischen Übersendung von und Auskunftserteilung aus Personalakten ist an sich zutreffend. Wesentlich ist allerdings die Frage, um welche Sachverhalte es bei den Auskünften aus Personalakten überhaupt geht.

In diesem Fall waren nur die Angaben, die in den von der Staatsanwaltschaft erstellten Personalbögen enthalten waren, z. B. über den bisherigen beruflichen Werdegang, von Interesse. Nach § 96e Abs. 2 HmbBG sind Auskünfte aus Personalakten dann ohne Einwilligung zulässig, wenn sie zur Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder zum Schutz berechtigter höherrangiger Interessen des Empfängers zwingend erforderlich sind. Zwingend erforderlich ist eine Auskunft aus der Personalakte nur dann, wenn sie nicht hinweggedacht werden kann, ohne daß der Erfolg (hier die Durchführung des Strafverfahrens) vereitelt würde.

Dies dürfte auf Unterlagen und Informationen zutreffen, denen im Zusammenhang mit dem konkreten strafrechtlichen Vorwurf Beweiskraft zukommt. Die in die Personalbögen aufgenommenen Angaben haben aber gerade nichts mit den konkreten Tatvorwürfen zu tun, sondern beinhalten ausschließlich allgemeine Angaben zur Person. Demgemäß wurden sie auch in erster Linie zur Vorbereitung der persönlichen Anhörung genutzt. Es reicht nach § 96e Abs. 2 HmbBG nicht aus, wenn die Angaben für den verfolgten Zweck lediglich hilfreich sind. Die Übermittlung dieser allgemeinen Daten der Betroffenen kam im Wege der Auskunft aus der Personalakte daher nach § 96 e Abs. 2 HmbBG nur mit vorheriger schriftlicher Einwilligung der Betroffenen in Betracht. Ohne Einwilligung wäre auch die Auskunftserteilung unzulässig gewesen.

Die Übersendung der Akten hat zu keinen weiteren Nachteilen für die Betroffenen geführt, insbesondere ist keine dauerhafte Speicherung von Personalaktendaten bei der Staatsanwaltschaft erfolgt.

15.2.2 Veröffentlichung von Daten über Betroffene

Im Februar 1995 wurden in der Presse Vornamen, die ersten Buchstaben der Nachnamen und Dienstgrade von Polizeibeamten veröffentlicht, gegen die angeblich Anklage wegen Körperverletzung im Amt erhoben würde.

Bei diesen veröffentlichten Angaben war es für Leser mit einigen Vorkenntnissen, insbesondere aber für Kollegen unschwer erkennbar, um welche Personen es sich handelte. Daher war eine erhebliche Gefährdung der beruflichen Interessen der Betroffenen zu befürchten.

Wir haben gegenüber der Behörde für Inneres darauf hingewiesen, daß es außer zur Öffentlichkeitsfahndung und bei Personen der Zeitgeschichte keine Befugnis zur öffentlichen Bekanntmachung von Verdächtigen während laufender Ermittlungen gibt. Die Unschuldsvermutung und das Persönlichkeitsrecht der Betroffenen haben Vorrang vor dem Interesse an einer Berichterstattung in den Medien. Dies gilt für Polizeibeamte ebenso wie für alle anderen Personen, die einer Straftat verdächtigt werden. Wir haben daher gefordert, daß bei Pressemitteilungen über laufende Ermittlungsverfahren immer dann, wenn eine Identifizierung anhand der Angaben (z. B. Namensteile, Dienstbezeichnungen) möglich ist, auf derartige Hinweise verzichtet wird.

Die Behörde für Inneres hat uns mitgeteilt, daß die Veröffentlichung nicht auf eine Mitteilung der Polizei zurückzuführen sei. Im übrigen teile sie unsere Auffassung.

Als Quelle für die veröffentlichten Angaben war zu vermuten, daß die Personalien aus einem Durchsuchungsbeschluß stammten, mit dem bei einem Presseunternehmen Bildmaterial beschlagnahmt worden war. Derartige Beschlüsse enthalten die Daten der Beschuldigten.

15.2.3 Datenverarbeitung bei der zentralen Beschwerdestelle

Bei der Polizei eingehende Beschwerden von Bürgern über Polizeibeamte sollen in Zukunft nicht mehr abschließend von den jeweiligen unmittelbaren Dienstvorgesetzten (z. B. Revierführer, Leiter einer Polizeidirektion) beantwortet werden, sondern grundsätzlich von einer zentralen Beschwerdestelle beim Polizeipräsidenten. Nur wenn die Beschwerden strafrechtliche Vorwürfe gegen Mitarbeiter der Polizei zum Gegenstand haben, werden sie an das Dezernat für interne Ermittlungen (DIE) abgegeben.

Bei der Einrichtung dieser neuen zentralen Beschwerdestelle sind Überlegungen angestellt worden, ob und in welchem Rahmen eine Unterstützung der Beschwerdestelle durch eine Datei zur Verwaltung und Auswertung von Beschwerden zweckmäßig und möglich ist. Insbesondere wird erwogen, ob eine Datei so ausgestaltet werden kann, daß sie Auswertungen über besondere Fälle ermöglicht, deren Relevanz im Einzelfall nicht erkannt worden ist, aber z. B. bei Häufung von Beschwerden gegen bestimmte Beamte neu betrachtet werden muß. Diese Überlegungen sind polizeiintern noch nicht abgeschlossen.

Hierbei stellen sich schwierige Fragen zur fachlichen Erforderlichkeit einer auswertbaren Datei über Beschwerden, die nicht strafrechtlich relevant sind, und zur Zulässigkeit nach dem Personalaktenrecht.

Es muß auch berücksichtigt werden, daß sich eine derartige Datei mit präventiver Zielsetzung stark der Datenverarbeitung annähert, die die Polizei bei ihren Aufgaben der Strafverfolgung und Gefahrenabwehr benutzt. Für diese präventivpolizeilichen Dateien gelten besondere Voraussetzungen:

Die Speicherung von Daten mit der Zielsetzung der Verhütung und vorbeugenden Bekämpfung zukünftiger Straftaten setzt voraus, daß gegen eine Person bereits wegen einer Straftat ermittelt worden ist. Nur in Ausnahmefällen können Speicherungen über Personen erfolgen, gegen die bisher kein Verdacht auf eine Straftat vorlag. In diesen Ausnahmefällen müssen aber tatsächliche Anhaltspunkte dafür vorliegen, daß Straftaten von erheblicher Bedeutung begangen werden sollen. Somit stellt sich für eine etwaige Datei mit präventiver Zielsetzung, in der Beschwerden gegen Polizeibeamte ohne strafrechtliche Relevanz erfaßt werden, die Frage, ob von diesen Grundsätzen wegen der

Erforderlichkeit einer gesteigerten Dienstaufsicht über Polizeibeamte abgewichen werden kann.

Wir werden an der Planung der Datei beteiligt, falls sie nach den weiteren behördeninternen Überlegungen eingeführt werden soll. Bei Redaktionsschluß dieses Tätigkeitsberichts waren diese vorbereitenden Überlegungen noch nicht abgeschlossen.

15.2.4 Überlegungen zur Einrichtung eines Polizeibeauftragten

In Reaktion auf den „Polizeiskandal" ist vorgeschlagen worden, das Amt eines Polizeibeauftragten zu schaffen. Die Bürgerschaft hat daher den Senat ersucht, zu prüfen, ob die Einrichtung eines unabhängigen Polizeibeauftragten der Hamburgischen Bürgerschaft vergleichbar mit dem Wehrbeauftragten des Deutschen Bundestages sinnvoll erscheint.

Wir haben gegenüber der Behörde für Inneres zur Vorbereitung einer behördeninternen Anhörung zu datenschutzrechtlichen Problemen Stellung genommen, die sich bei der Einrichtung eines Polizeibeauftragten ergeben könnten. Im Vordergrund standen dabei die möglichen Befugnisse des Polizeibeauftragten zur Erhebung und Verwendung personenbezogener Daten, das Erfordernis seiner umfassenden rechtlichen und tatsächlichen Unabhängigkeit und Probleme im Zusammenhang mit dem Zeugnisverweigerungsrecht.

15.3. Problematik der Einwilligung bei der Polizei

15.3.1 Anforderung von Selbstauskünften aus polizeilichen Dateien

In letzter Zeit ist uns bekannt geworden, daß private Arbeitgeber in einzelnen Fällen zu folgender Praxis übergehen: Mitarbeiter und insbesondere Bewerber um eine freie Stelle werden aufgefordert, im Wege einer datenschutzrechtlichen Auskunft nach § 18 des Hamburgischen Datenschutzgesetzes (HmbDSG) oder entsprechender Vorschriften anderer Datenschutzgesetze selbst festzustellen, ob Eintragungen über sie in polizeilichen Dateien vorliegen. Durch die Polizei erteilte Auskünfte sollen dann dem Arbeitgeber vorgelegt werden. Insbesondere von privaten Sicherheitsdiensten wurden derartige Selbstauskünfte verlangt.

Wir haben die zuständigen Dienststellen in Hamburg, die anfragenden Sicherheitsdienste und Petenten, die aus diesem Grund Auskunftsersuchen gestellt haben, von unserer Rechtsauffassung zu dieser Praxis informiert. Unsere Stellungnahme ist in der Zeitschrift „Datenschutz und Datensicherheit" (DuD) 1995, S. 638 unter der Rubrik „Datenschutzbehörden" veröffentlicht. Auf diesen Beitrag wird verwiesen.

15.3.2 Verwendung von Einwilligungsformularen in polizeilichen Ermittlungen

Einzelne Länderpolizeien benutzen in strafrechtlichen Ermittlungsverfahren Formulare, in denen die Beschuldigten ihre „Einwilligung" zur Datenerhebung der Polizei bei anderen Behörden oder auch privaten Stellen erklären sollen. Solche Formulare enthalten z. B. folgende Formulierungen:

„Ich willige ein, daß meine als Sozial- oder Datengeheimnis zu wahrenden persönlichen und sachlichen Verhältnisse (personenbezogenen Daten), insbesondere meine Arbeits-, Krankheits- und Einkommensverhältnisse sowie der etwaige Bezug von Sozialleistungen der Polizei für das genannte Ermittlungsverfahren offenbart werden. Meine Einwilligung schließt die Offenbarung der von einem Arzt oder einer anderen in § 203 Abs. 1 des Strafgesetzbuches genannten Person den Leistungsträgern zugänglich gemachten personenbezogenen Daten mit ein. Insoweit entbinde ich diese Personen von der ihnen obliegenden Schweigepflicht."

Teilweise werden pauschale Einwilligungsformulierungen noch mit Listen von A bis Z ergänzt, die man der Einfachheit halber ankreuzen kann: „Arbeitsamt, Arzt, Finanzamt, Geldinstitut mit Angaben zum Konto, Jugendamt, Krankenhaus, Krankenkasse, Postamt, Rentenversicherungsträger, Schule, Sozialamt, Versicherungsgesellschaft, Zolldienststelle."

Im Bereich der Polizei Hamburg sind uns derartige Formulare bisher nicht bekannt geworden. Sie wären auch gleichermaßen unzulässig wie überflüssig.

Die andernorts verwendeten Formulierungen sind so pauschal, daß sie die erforderliche Aufklärung über den Gegenstand, Inhalt und Umfang der beabsichtigten Datenverarbeitung nicht leisten. Sie weisen auch nicht immer unter Darstellung der Rechtsfolgen darauf hin, daß die „Einwilligung" verweigert werden kann. Sie genügen daher schon formal nicht den allgemeinen Anforderungen an rechtswirksame Einwilligungen, wie sie z. B. in § 5 Abs. 2 HmbDSG beschrieben sind.

Die Praxis der Verwendung der Formulare vernachlässigt außerdem, daß Beschuldigte im Strafermittlungsverfahren gerade nicht frei über die Erhebung und Verwendung ihrer Daten bestimmen können, sondern sich einem – grundsätzlich zulässigen – rechtlichen wie faktischen Zwang ausgesetzt sehen. Das Strafermittlungsverfahren ist dadurch gekennzeichnet, daß ohne und gegen den Willen des Beschuldigten Beweise erhoben werden können. Insofern vermitteln die Formulare einen Eindruck von Entscheidungsfreiheit, die die Beschuldigten gar nicht haben.

Auch die Stellen, bei denen die Angaben aufgrund der „Einwilligungen" erhoben werden sollen, bekommen leicht eine falsche Vorstellung von den rechtlichen Voraussetzungen. Wenn sie derartige Formulare vorgelegt bekommen,

kann der Eindruck entstehen, der Beschuldigte sei mit allem einverstanden, die Erhebung liege womöglich sogar in seinem Interesse, obwohl sie ihn tatsächlich belastet.

Die Verwendung der Formulare ist auch überflüssig. Denn wenn man den Beschuldigten die angebliche Freiheit zu Einwilligungserklärungen zubilligt, kann man sie auch selbst fragen oder sie zur Vorlage von einzelnen Unterlagen bitten und sich so den Weg über die Datenerhebung bei anderen Stellen sparen. Es ist jedoch davon auszugehen, daß die Beschuldigten nicht immer derartige Angaben machen, sondern ihr Recht wahrnehmen, sich nicht zu äußern. Dann sind die Strafermittlungsbehörden gesetzlich berechtigt, die Daten auch ohne Einwilligung bei Dritten zu erheben. Dies gilt generell bei allen privaten Stellen (z. B. Arbeitgeber, Banken, Versicherungen), die auf Fragen der Staatsanwaltschaft sogar antworten müssen, wenn sie keine Zeugnisverweigerungsrechte haben, wie z. B. Ärzte. Auch öffentliche Stellen sind ohne Einwilligung der Betroffenen zu Auskünften im Strafermittlungsverfahren verpflichtet, es sei denn, es liegen besondere gesetzliche Geheimhaltungspflichten vor. Wenn dies der Fall ist, z. B. bei Sozialleistungsträgern und Finanzbehörden, ist im Einzelfall zu prüfen, ob die gesetzlichen Übermittlungsvoraussetzungen vorliegen oder besondere Verfahren einzuhalten sind (z. B. die richterliche Anordnung nach § 73 Abs. 3 SGB-X).

Im Strafverfahren als klassischer Eingriffsverwaltung gilt somit der Grundsatz des Gesetzesvorrangs, der nicht durch pauschale „Einwilligungen" umgangen werden kann (vgl. 1.2.2). Soweit die besonderen gesetzlichen Verwendungsregeln ihrerseits die Datenverarbeitung aufgrund einer Einwilligung erlauben (z. B. § 67b SGB-X), ist es Sache der Sozialleistungsträger, die Einwilligung vom Betroffenen einzuholen. Sie können sich jedoch nicht mit pauschalen „Einwilligungsformularen", die ihnen von anderen Behörden präsentiert werden, zufrieden geben.

Sofern im Strafermittlungsverfahren Einwilligungen von Zeugen für Datenerhebungen bei anderen Stellen eingeholt werden sollen, um den Zeugen zusätzlichen Aufwand zu ersparen, sind die beschriebenen Formulare ebenfalls ungeeignet. In diesen Fällen bedarf es insbesondere einer genauen Aufklärung über den Gegenstand der Erhebung und den Verwendungszweck, wobei die bestehenden gesetzlichen Zeugenpflichten unmißverständlich klarzustellen sind. Dies leisten Formulare nicht, da sie nicht für die jeweils unterschiedlichen Sachverhalte vorformuliert werden können.

15.3.3 Einwilligung bei verdeckten Datenerhebungen?

Ein besonderes Problem für die Anwendbarkeit der Rechtsfigur „Einwilligung" sind verdeckte Datenerhebungen. Wesentliches Merkmal einer verdeckten Datenerhebung ist, daß der Betroffene mit Absicht darüber im Unklaren gelassen oder sogar darüber getäuscht wird, daß es sich um Erhebungen von

öffentlichen Stellen, insbesondere der Polizei handelt. Eine wirksame Einwilligung erfordert dagegen die umfassende Aufklärung über Gegenstand, Inhalt und Umfang der erlaubten Verarbeitung. Der Konflikt zwischen verdeckter Erhebung und den Voraussetzungen für eine wirksame Einwilligung ist daher offenkundig.

Gleichwohl werden gerade im Zusammenhang mit verdeckten Erhebungen immer wieder Einwilligungsfiktionen verwendet. Z. B. heißt es in § 110c Strafprozeßordnung (StPO): „Verdeckte Ermittler dürfen unter Verwendung ihrer Legende eine Wohnung mit dem Einverständnis des Berechtigten betreten. Das Einverständnis darf nicht durch ein über die Nutzung der Legende hinausgehendes Vortäuschen eines Zutrittsrechts herbeigeführt werden." Demnach unterstellt die Regelung ein Einverständnis, obwohl der Berechtigte darüber getäuscht wird, wer tatsächlich zu welchem Zweck die Wohnung betritt. Für den Betroffenen ist es nicht unerheblich, ob es sich bei einer Person, die Einlaß begehrt, z. B. um einen Klempner oder einen Polizeibeamten handelt, der Ermittlungen gegen den Wohnungsberechtigten führt. Von einer wirksamen Einwilligung, die zur Annahme führen könnte, es handele sich nicht um einen Eingriff in den Schutzbereich von Art. 13 Grundgesetz (GG), kann daher nicht die Rede sein.

Ein anderes Beispiel sind sogenannte Hörfallen: Die Polizei veranlaßt eine Privatperson zu einem Telefonat mit dem Beschuldigten in einem Strafermittlungsverfahren. Dieses „Privatgespräch" wird von einem Polizeibeamten mitgehört. Wenn sich der Beschuldigte in dem „Privatgespräch" offenbart und Angaben macht, die ihn belasten, schnappt die Hörfalle zu: Der 2. Strafsenat des Bundesgerichtshofes (Computer und Recht 1994 S. 765 ff.) hat die auf diese Weise erlangten Erkenntnisse für gerichtlich verwertbar gehalten, da die Polizei nicht in ein Ferngespräch eindringe, sondern lediglich mit Einwilligung des Gesprächspartners hieran partizipiere.

Diese Prämisse des Gerichts, wonach die Einwilligung eines der Gesprächspartner ausreiche, ist fragwürdig. Hierbei wird verkannt, daß sich der andere Teilnehmer nur einer bestimmten, von ihm für vertrauenswürdig gehaltenen Person offenbart hatte und die Annahme lebensfremd ist, ihm sei es gleichgültig gewesen, wer noch mithört.

Gegen die weitere Annahme, die in einem „Privatgespräch" freiwillig offenbarten Angaben könnten von den mithörenden Strafverfolgungsbehörden und vom Gericht grundsätzlich verwendet werden, hat sich nunmehr der 5. Strafsenat des Bundesgerichtshofes ausgesprochen. In einem Beschluß vom 22. März 1995 (Strafverteidiger 1995 S. 283 ff.) äußert der Senat gewichtige Zweifel an der These, die Offenbarung in dem polizeilich mitgehörten Telefonat sei freiwillig unter Privatleuten erfolgt. Der 5. Senat hält daher die durch eine Hörfalle erlangten Erkenntnisse im weiteren Strafverfahren nicht für verwertbar.

Wenn das Telefonat zwischen den Privatpersonen dem Zweck diene, ein Beweismittel zur Überführung des Beschuldigten zu beschaffen, würden die gesetzlichen Pflichten zur Belehrung, daß es dem Beschuldigten freisteht, sich zu der Beschuldigung zu äußern oder nicht zur Sache auszusagen (§ 136 Abs.1 Satz 2, § 163a Abs. 4 StPO), umgangen. Das polizeilich mit dem Zweck der Beweisführung veranlaßte und mitgehörte Privatgespräch stehe einer förmlichen Vernehmung gleich, die dann unverwertbar ist, wenn sie ohne Belehrung erfolgt.

Die Äußerung des Beschuldigten in einem solchen polizeilich veranlaßten Gespräch erfolge insbesondere auch nicht freiwillig. Vielmehr könne der von der Polizei eingesetzte Gesprächspartner (z. B. eine V-Person) mit Informationen ausgestattet werden, die das gezielte Aushorchen des anderen Teilnehmers ermöglichen oder fördern.

Diese Ausführungen des 5. Strafsenats sind zu begrüßen. Sie betonen im Bereich des hoheitlichen Handelns den Vorrang der gesetzlich vorgesehenen Verfahrensweise und ihrer besonderen Bindungen hier der Belehrungspflichten (vgl. 1.2.2). Sie machen ferner deutlich, daß nur dann von freiwilligen Äußerungen ausgegangen werden kann, wenn kein informatorisches Ungleichgewicht zwischen den Gesprächspartnern besteht (vgl. 1.2.1.).

Da der 5. Strafsenat von der Rechtsprechung des 2. Strafsenats abweichen will, ist eine Entscheidung des Großen Senats für Strafsachen beim Bundesgerichtshof zu erwarten, wenn der 2. Senat seine Auffassung nicht revidiert. Bei Redaktionsschluß stand noch nicht fest, welchen Ausgang das Verfahren nimmt.

15.4 Entwurf eines Gesetzes über das Bundeskriminalamt

Die Bundesregierung hat Anfang 1995 den Entwurf für ein Gesetz über das Bundeskriminalamt (BKA-Gesetz) verabschiedet und in die parlamentarischen Beratungen eingebracht. Die vorangegangenen Überlegungen hatten wir im 13. TB (17.1) dargestellt. In unseren Stellungnahmen und einer Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben wir deutlich gemacht, daß der Gesetzentwurf trotz einiger positiver Regelungen nach wie vor gewichtigen Bedenken begegnet, da er tiefe Eingriffe in die Rechte von Betroffenen ermöglicht. Deren Voraussetzungen und Reichweite sind unklar oder sie sind nicht durch überwiegende Interessen der Allgemeinheit gerechtfertigt. Dies gilt insbesondere für

- die Verwendung des Begriffs der Straftaten von erheblicher Bedeutung ohne Definition, um welche Tatbestände es sich handelt, weil damit nicht mehr voraussehbar ist, wann die an diesen Begriff anknüpfenden Eingriffsbefugnisse zur Datenverarbeitung eröffnet sind;

- die Befugnisse der Zentralstelle zu selbständigen Datenerhebungen und Übermittlungen bis hin zum automatisierten Datenverbund mit ausländischen und zwischenstaatlichen Stellen ohne Einvernehmen mit den jeweils verantwortlichen Länderpolizeien;

- die unklare Abgrenzung der Datenverarbeitungsbefugnisse im Hinblick auf die unterschiedlichen Aufgaben zur Strafverfolgung, Gefahrenabwehr, Verhütung von Straftaten und Vorsorge für künftige Strafverfolgung sowie die fehlende klare Zweckbindungs- und Zweckänderungsregelung;

- die Befugnis zur verdeckten Datenerhebung aus Wohnungen ohne eindeutige Begrenzung auf den Schutz gefährdeter Ermittler.

Der Bundesrat hat in seiner Stellungnahme verschiedene Verbesserungen insbesondere bei den Regelungen zur datenschutzrechtlichen Kontrolle des INPOL-Systems verlangt und ist damit insoweit unseren Vorschlägen gefolgt. In anderen Punkten, z. B. der Speicherung von Zeugen und Opfern, sieht die Stellungnahme des Bundesrates jedoch erhebliche Verschlechterungen des Gesetzentwurfs vor. Bei Redaktionsschluß war zwar die erste Lesung des Gesetzentwurfs im Bundestag erfolgt. Die eingehende Beratung in den Ausschüssen war jedoch noch nicht absehbar.

15.5 INPOL-Neukonzeption

Nachdem im Jahr 1993 ein fachliches Grobkonzept für die INPOL-Neukonzeption vorgelegt worden war (12.TB, 17.1.3), wurde im Frühjahr 1995 auf dieser Grundlage ein technisches Grobkonzept entwickelt. Eine detaillierte datenschutzrechtliche Bewertung dieses Konzepts war noch nicht möglich, da zu viele Fragen der künftigen Datensicherung für das neue INPOL-System offen blieben.

Zu begrüßen ist grundsätzlich der Ansatz, daß die notwendigen Sicherungsmaßnahmen bereits auf der Ebene der zu schaffenden technischen Infrastruktur verwirklicht werden sollen und nicht erst auf der Ebene der einzelnen Anwendungen. Die von der Konferenz der Datenschutzbeauftragten beschlossenen Anforderungen für die Gewährleistung bei elektronischen Mitteilungssystemen (siehe 3.3) müssen jedenfalls erfüllt werden.

Die Erarbeitung von fachlichen und technischen Feinkonzepten durch die beim Bundeskriminalamt angesiedelte Projektgruppe für die INPOL-Neukonzeption ist ab 1996 vorgesehen. Diese Feinkonzepte werden eine Beurteilung im Detail ermöglichen. Die Datenschutzbeauftragten des Bundes und der Länder beabsichtigen, das Projekt zur INPOL-Neukonzeption durch eine kontiniuierliche Arbeitsgruppe zu begleiten.

15.6 Entwurf eines Übereinkommens für ein europäisches Polizeiamt (Europol)

Der Rat der Europäischen Union hat im Juni 1995 den Entwurf eines Übereinkommens über die Errichtung eines Europäischen Polizeiamtes (Europol-Übereinkommen) beschlossen. Den im 13. TB (17.2) beschriebenen datenschutzrechtlichen Anforderungen wird dieser Entwurf in wesentlichen Punkten nicht gerecht:

Das Europol-Übereinkommen betrachtet die Informationsbeziehungen zwischen den Polizeibehörden nur aus Sicht der Europol-Zentrale und der nationalen Zentralstellen. Dies vernachlässigt die fachlichen Zuständigkeiten der dezentralen Polizeibehörden, insbesondere der deutschen Länderpolizeien. Dadurch entstehen erhebliche Gefahren für die Rechte der Betroffenen. Die zuständigen Polizeibehörden können nicht selbst entscheiden, welche Speicherungen im Europol-Informationssystem sie vornehmen. Den Zentralstellen und Europol fehlen die Hintergrundkenntnisse, um die Zulässigkeit und Richtigkeit der Speicherungen beurteilen zu können. Damit wird die datenschutzrechtliche Verantwortlichkeit für das Europol-Informationssystem aufgehoben. Zugleich wird eine wirksame Datenschutzkontrolle beeinträchtigt. Dies gilt insbesondere für die Analyse-Dateien mit höchst sensiblen Angaben über unverdächtige Personen bis hin zu Angaben über die sogenannte rassische Herkunft, politische Anschauungen, religiöse Überzeugungen, zur Gesundheit und zum Sexualleben.

Als Alternative kommt nach dem Vorbild des Schengener Informationssystems in Betracht, daß Speicherungen bei Europol nur von den zuständigen Länderpolizeien in eigener Verantwortung nach Maßgabe der Europol-Konvention – unter Verzicht auf die genannten hochsensiblen Angaben der Analysedateien – veranlaßt werden. Dies könnte durch besondere innerstaatliche Vorkehrungen und Verfahrensweisen realisiert werden. Bei der Umsetzung des Übereinkommensentwurfes in innerstaatliches Recht, die im Zustimmungsgesetz erfolgt, wird es daher darauf ankommen, den Grundsatz der datenschutzrechtlichen Verantwortung (siehe auch 13. TB, 1.3) zu sichern. Diese Einschätzung wird auch vom Senat geteilt (Bürgerschaftsdrucksache 15/4078).

15.7 Rechtstatsachensammlung

Die Vorschläge der Datenschutzbeauftragten für eine umfassende Rechtstatsachensammlung über die Anzahl besonderer Erhebungsmethoden, den Erfolg dieser Maßnahmen und Durchführungsschwierigkeiten (13.TB, 17.4.1) sind bisher von der Mehrzahl der Länderpolizeien bei der Vorlage des Schlußberichts in der AG Kripo am 7./8. Dezember 1994 abgelehnt worden. Stattdessen soll eine Bund/Länder-Fallsammlung eingerichtet werden, in der nur ausgewählte Fälle erfaßt werden sollen, die insbesondere zur Untermauerung rechtspolitischer Forderungen nach der Ausweitung polizeilicher Befugnisse geeignet sind.

Die Datenschutzbeauftragten des Bundes und der Länder haben mich als Vorsitzenden des Arbeitskreises Sicherheit deshalb beauftragt, gegenüber der Innenministerkonferenz die Bedeutung einer Überprüfung der Erforderlichkeit polizeilicher Befugnisse und der Auswirkungen für die Rechte der Betroffenen erneut zu verdeutlichen. Ich habe dem Vorsitzenden der Innenministerkonferenz mitgeteilt, daß die Einrichtung einer Rechtstatsachensammlung als objektives Instrument zur Bewertung polizeilicher Eingriffsbefugnisse auch aus datenschutzrechtlicher Sicht zu begrüßen wäre. Diese Sammlung darf jedoch nicht einseitig den Zweck verfolgen, Forderungen der Polizei zur Einführung zusätzlicher Befugnisse argumentativ zu unterstützen.

Die Datenschutzbeauftragten halten daher ihren Vorschlag einer ergebnisoffenen Überprüfung der bestehenden Befugnisse aufrecht. Sie erwarten, daß sich die Polizeien der Diskussion über die Erforderlichkeit und Angemessenheit weitreichender Befugnisse zu Eingriffen in das Persönlichkeitsrecht nicht entziehen werden. In Betracht kommt auch eine unabhängige Überprüfung der bestehenden polizeilichen Eingriffsbefugnisse durch das kriminalistische Institut beim Bundeskriminalamt in enger Kooperation mit einem fachlich qualifizierten unabhängigen Forschungsinstitut.

Die Ablehnung einer umfassenden Rechtstatsachensammlung durch die Länder ist auch bei den Vertretern aller Fraktionen im Innenausschuß des Deutschen Bundestages kritisiert worden.

Die Behörde für Inneres hat mitgeteilt, daß im ersten Halbjahr 1995 von Hamburg keine Fälle an die Bund/Länder-Fallsammlung gemeldet worden sind, weil es keine Sachverhalte gegeben hat, die dem vorgesehenen Themenraster entsprachen.

15.8 Überprüfung der Erforderlichkeit von Dateien

§ 26 Abs. 3 des Gesetzes über die Datenverarbeitung der Polizei schreibt vor, daß die Polizei alle vier Jahre die Notwendigkeit der Weiterführung oder Änderung ihrer Dateien überprüft. Für mehrere Dateien ist 1995 diese Überprüfung durchgeführt worden. Die Diskussion über die Ergebnisse war bei Redaktionsschluß dieses TB noch nicht abgeschlossen.

15.9 Arbeitsdatei PIOS „Innere Sicherheit" (APIS)

Im 10. TB (16.9) und 12. TB (17.7) hatten wir über unseren Vorschlag berichtet, daß auch die hamburgische Polizei die in Schleswig-Holstein praktizierte Regelung übernimmt. Danach werden in APIS nur solche Straftaten erfaßt, die nach ihrer Schwere und der Gefahr für die freiheitliche demokratische Grundordnung mit den eigentlichen Staatsschutzdelikten vergleichbar sind. Indizien

für die Schwere sind aktive Gewaltanwendung gegen Personen, deren Androhung oder gewaltverursachte Sachbeschädigung über 1 000 DM.

Aufgrund eines Ersuchens der Bürgerschaft hat die Polizei die Übernahme dieser Regelungen erprobt. Nach Abschluß des Erprobungszeitraums ist im Oktober 1995 entscheiden worden, daß personenbezogene Daten in APIS nur dann erfaßt werden sollen, wenn sie den genannten Kriterien entsprechen.

Diese Entscheidung ist sehr zu begrüßen. Wir hoffen, daß die Anwendung der ergänzenden Regelungen den Zweck der Datei, relevante Angaben zu Personen von unbedeutenden Hinweisen zu unterscheiden, besser als bisher gewährleistet.

15.10 Errichtungsanordnung für das automatisierte Fingerabdruck-Identifizierungssystem (AFIS)

Bereits im 13.TB (17.6.3) hatten wir kritisiert, daß für AFIS eine Errichtungsanordnung fehlt. Hieran hat sich auch 1995 nichts geändert. Damit wird eine der wichtigsten polizeilichen Dateien bisher gleichsam ohne „Zulassung" betrieben.

Unklar ist nach wie vor, wie vom Bundeskriminalamt als Betreiber von AFIS die notwendige Überprüfung gewährleistet wird. Es muß überprüft werden können, ob polizeiliche Recherchen im Bestand von Fingerabdrücken über Asylbewerber stattgefunden haben, die von besonderen gesetzlichen Voraussetzungen abhängen.

Der Bundesbeauftragte für den Datenschutz hat inzwischen den Bundesminister des Innern zu einer umgehenden Stellungnahme über den aktuellen Sachstand hinsichtlich der Errichtungsanordnung für AFIS aufgefordert.

15.11 Datei über die Drogenszene in St. Georg

Im 12. TB (17.4) hatten wir die damaligen Pläne für eine Kartei über Platzverweise zur Bekämpfung der offenen Rauschgiftszene in St. Georg und unsere Kritik an einer derartigen Kartei beschrieben. Inzwischen hat die Polizei das Konzept zur Verdrängung der offenen Rauschgiftszene in diesem Gebiet verstärkt und erneut die Erforderlichkeit einer auf einem PC geführten Datei zur Unterstützung der polizeilichen Maßnahmen betont.

Wir haben im Ergebnis keine Bedenken gegen die Einführung einer derartigen automatisierten Datei mehr vorgebracht. Zwar besteht nach wie vor das im 12. TB geschilderte Problem, daß diese Datei vor allem mit Informationen aufgrund von Maßnahmen nach dem Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung (SOG) gespeist wird, während Informationen über eingeleitete Strafermittlungsverfahren gegen Dealer in der Minderzahl bleiben. Maßgeblich für unseren Meinungswandel war letztlich, daß die Gerichte bei ihren Entscheidungen über die Zulässigkeit von polizeilichen Maßnahmen insbesondere auch Angaben darüber verlangen, welche Maßnahmen gegen die Betroffenen bereits zuvor ergriffen worden waren.

Die auch zwischen einzelnen zuständigen Richtern am Amtsgericht Hamburg unterschiedlich bewertete Streitfrage, ob die Platzverweise, Ingewahrsamnahmen und Aufenthaltsverbote in diesem Zusammenhang überhaupt nach dem SOG zulässig und zur Bekämpfung der offenen Rauschgiftszene geeignet sind, ist dagegen nicht datenschutzrechtlich zu entscheiden. Wenn in obergerichtlichen Entscheidungen festgestellt würde, daß die polizeilichen Maßnahmen nicht zulässig sind, würde der Datei die Grundlage entzogen. Solange es derartige Entscheidungen jedoch nicht gibt, rechtfertigen die richterlichen Entscheidungen, die Informationen über frühere polizeiliche Maßnahmen zugrunde legen, die Dateiführung.

Dauerhaft gespeichert mit einer Frist von drei Monaten werden in der Datei Personen, gegen die ein Platzverweis ausgesprochen wurde oder die in Gewahrsam genommen worden sind. In Gewahrsam genommene Personen, die mindestens sechsmal in der Rauschgiftszene mit mindestens einem beweisbaren Drogenhandel auffällig geworden sind, oder die mit drei beweisbaren Rauschgiftverstößen festgestellt worden sind (sogenannte Intensivdealer), werden bis zu sechs Monaten gespeichert. Das polizeiliche Konzept sieht ferner vor, daß gegen diese sogenannten Intensivdealer Aufenthaltsverbote verhängt werden können. In diesen Fällen beginnt die Speicherungsfrist erst mit Ablauf des Aufenthaltsverbots, in allen anderen Fällen jeweils mit dem Ereignis. Bei reinen Personalienfeststellungen ohne weitere Maßnahmen findet keine dauerhafte Dateispeicherung statt. Vielmehr dient der PC nur zur Erstellung der Listen über festgestellte Personalien, die zur Dokumentation polizeilichen Handelns erforderlich sind. Diese Daten werden nach Ausdruck der Liste im 24 Stunden-Rhythmus gelöscht. Die Listen werden drei Monate aufbewahrt.

Da die Datei automatisiert auf einem PC geführt wird, ist aufgrund der technischen Vorkehrungen im Unterschied zur früheren manuellen Kartei damit zu rechnen, daß die Speicherfristen eingehalten werden.

16. Staatsanwaltschaft

16.1 Probleme der Telefonüberwachung (TÜ)

Im Jahr 1995 haben wir im Bereich der Staatsanwaltschaft schwerpunktmäßig datenschutzrechtliche Fragen im Zusammenhang mit der Telefonüberwachung (TÜ) zur Verfolgung von Straftaten nach §§ 100a, b Strafprozeßordnung (StPO) geprüft. Die Prüfungen bezogen sich nicht darauf, ob Telefonüberwachungen zu Recht angeordnet worden sind; dies ist vielmehr gemäß § 100b Abs. 1 StPO Sache des zuständigen Richters. Vielmehr ging es anläßlich eines Einzelfalls (16.1.1) um die Frage, ob und unter welchen Voraussetzungen Unterlagen, die aus Telefonüberwachungen stammen, an andere Stellen weiter-

gegeben werden dürfen. Darüber hinaus haben wir querschnittsmäßig die Praxis bei der Einhaltung der gesetzlichen Vorschriften zur Löschung von Unterlagen und der Benachrichtigung von Betroffenen überprüft (16.1.2).

16.1.1 Weitergabe von TÜ-Unterlagen

Zu Beginn des Jahres wurden wir durch eine Eingabe mit einem Fall befaßt, in dem eine ganze Akte mit Unterlagen aus einer Telefonüberwachung von der zuständigen Staatsanwaltschaft an das Strafvollzugsamt weitergegeben worden war.

Bei unserer Überprüfung des Ablaufs haben wir das Fazit gezogen, daß die Übersendung der Unterlagen aus der Telefonüberwachung an das Strafvollzugsamt nach sämtlichen in Betracht kommenden rechtlichen Gesichtspunkten unzulässig gewesen ist. In einem ausführlichen Prüfbericht haben wir diese Schlußfolgerung damit begründet, daß es keine Rechtsgrundlage für die Übersendung gegeben habe, sondern das durch Art. 10 Grundgesetz geschützte Fernmeldegeheimnis eine derartige Verwertung von Erkenntnissen aus einer Telefonüberwachung verbiete.

Die vollständig übersandten Unterlagen enthielten eine große Anzahl von Aufzeichnungen über Gespräche, die für das Strafvollzugsamt keinerlei Relevanz hatten. Sie dienten vielmehr nur der Strafverfolgung. Sie hätten durch die Staatsanwaltschaft auf ihre Bedeutung für Zwecke der Strafverfolgung geprüft werden müssen. Nicht erforderliche Unterlagen wären zu vernichten gewesen. Sicherheitsbelange des Strafvollzugs hätten auch ohne Übersendung der TÜ-Unterlagen auf andere Weise gewahrt werden können.

Die Justizbehörde hat dagegen die Auffassung vertreten, daß der sogenannte Übergangsbonus im Hinblick auf die im Entwurf für ein Strafverfahrensänderungsgesetz von 1994 vorgesehene Regelung die Übersendung der Unterlagen gerechtfertigt habe. Da die Staatsanwaltschaft die Relevanz für die Sicherheit im Strafvollzug nicht selbst habe beurteilen können, sei eine Auswertung der vollständigen Unterlagen durch das Strafvollzugsamt erforderlich gewesen.

Die Angelegenheit ist ausführlich im Rechtsausschuß der Bürgerschaft behandelt worden. Der Bericht des Rechtsausschusses in Bürgerschaftsdrucksache 15/4067 vom 29. September 1995 enthält als Anlage 1 unseren Prüfbericht, als Anlage 2 die Stellungnahme der Justizbehörde. Auf diese Darstellungen wird wegen weiterer Einzelheiten verwiesen.

Aus Anlaß dieser Kontroverse ist vom damaligen Präses der Justizbehörde eine aus Vertretern des Justizamtes und der Staatsanwaltschaft bestehende Arbeitsgruppe gebildet worden, an der wir beteiligt worden sind. Diese Arbeitsgruppe hat die rechtlichen und tatsächlichen Probleme bei der Weitergabe von Erkenntnissen aus Telefonüberwachungsmaßnahmen in strafrechtlichen Ermittlungsakten durch die Staatsanwaltschaft an öffentliche Stellen zu Zwecken der Gefahrenabwehr eingehend beraten.

Als Ergebnis ist ein sogenannter „Basis-Konsens" erarbeitet worden, der in der Bürgschaftsdrucksache 15/4067 als Anlage 4 veröffentlicht worden ist. Das wesentliche Kriterium für die Weitergabe von Informationen aus einer Telefonüberwachung ist danach, ob diese Erkenntnisse erforderlich sind zur Abwehr von gegenwärtigen konkreten Gefahren für Leib oder Leben einer Person oder zur Verhütung von Straftaten, die im Katalog von § 100a StPO genannt werden. Aus unserer Sicht ist mit diesem Kriterium die Grenze der zulässigen Weitergabe von Erkenntnissen, die auf einem Eingriff in das Fernmeldegeheimnis beruhen, gekennzeichnet.

Nicht zugestimmt haben wir daher der weitergehenden Auffassung der Justizbehörde, wonach jedenfalls de lege ferenda ein Eingriff in das Fernmeldegeheimnis durch Weitergabe von Erkenntnissen aus Telefonüberwachungsmaßnahmen in strafrechtlichen Ermittlungsverfahren durch die Staatsanwaltschaft zum Zwecke der Gefahrenabwehr auch zur Abwehr anderer erheblicher Gefahren anzustreben und von Verfassungs wegen zulässig sei.

16.1.2 Praxis bei der Löschung von TÜ-Unterlagen und der Benachrichtigung von Betroffenen

§ 100b Abs. 6 Strafprozeßordnung (StPO) schreibt vor, daß aus Telefonüberwachungen stammende Unterlagen, die zur Strafverfolgung nicht mehr erforderlich sind, unverzüglich unter Aufsicht der Staatsanwaltschaft zu vernichten sind. Nach § 101 StPO sind von Maßnahmen zur Telefonüberwachung die Beteiligten zu unterrichten, sofern diese Unterrichtung nicht die im Gesetz näher beschriebenen Gefahren hervorruft. Mit diesen Regelungen hat der Gesetzgeber dem Verfassungsgebot Rechnung getragen, wonach zulässige Eingriffe in ein Grundrecht – hier das Fernmeldegeheimnis nach Art. 10 Grundgesetz – auf das unumgängliche Maß zu begrenzen sind. Es müssen Vorkehrungen getroffen werden, um Rechtsverletzungen zu vermeiden, und zumindest nachträglich muß gewährleistet sein, daß die Betroffenen von Grundrechtseingriffen erfahren.

Ziel der Prüfung war es, Erkenntnisse darüber zu erlangen, ob diese grundrechtlichen Schutzpflichten in der Praxis beachtet werden.

- Mängel bei der Löschung

Aufgrund des Verzeichnisses über TÜ-Aufzeichnungsbänder, die bei der Polizei noch vorliegen, haben wir in mehreren Verfahren aus Jahren 1980 bis 1987 die Akten daraufhin überprüft, warum die Löschungen noch nicht stattgefunden haben. Teilweise lag dies daran, daß die Verfahren noch nicht abgeschlossen waren. Wir haben in diesen Fällen nicht weiter geprüft, ob die TÜ-Unterlagen noch erforderlich waren. Teilweise waren die Akten nicht greifbar, so daß

keine nähere Prüfung möglich war. Bei den geprüften Akten haben wir allerdings Abläufe festgestellt, die erschreckend waren:

Zum Beispiel waren bei einer TÜ-Maßnahme 1984 mehrere Anschlüsse von Beschuldigten und dritten Anschlußinhabern abgehört worden. Insgesamt waren über 50 Überwachungsbänder mit abgehörten Gesprächen und 4 Ordner mit protokollierten Unterlagen entstanden. Das Verfahren war im Jahr 1985 mit rechtskräftigem Urteil abgeschlossen worden.

Danach waren in der Akte folgende Abläufe feststellbar:

- Einem Verteidiger wurden Fotokopien von TÜ-Unterlagen ausgehändigt.
- Die Akte wurde mit TÜ-Unterlagen zweimal an auswärtige Staatsanwaltschaften übersandt.
- Die Polizei bat die Staatsanwaltschaft ergebnislos um Hergabe einer Löschungsverfügung.
- Eine staatsanwaltschaftliche Verfügung zur Löschung der Unterlagen von 1994 wurde nicht ausgeführt.
- Schließlich wanderte die Akte 1995 unbesehen ins Archiv.

Wir haben die Staatsanwaltschaft daran erinnert, daß in § 100b Abs. 6 StPO gesetzlich vorgeschrieben ist, daß die nicht mehr erforderlichen Unterlagen „unverzüglich" zu vernichten sind und das „unverzüglich" in der Praxis nur schwerlich mit „10 Jahre und länger" übersetzt werden kann.

Dies war nur der krasseste Fall. Auch in anderen Akten aus den achtziger Jahren gab es entweder gar keine Verfügungen in Bezug auf die Löschung oder höchstens die formelhafte Begründung, die Unterlagen würden für ein etwaiges Wiederaufnahmeverfahren weiter aufbewahrt. Angaben dazu, ob und wenn ja, welche Unterlagen aus der Telefonüberwachung für ein etwaiges Wiederaufnahmeverfahren von Bedeutung sein könnten, gab es nicht.

Aus den festgestellten Abläufen wurde deutlich, daß lediglich bei konkreten Nachfragen der Polizei zur Frage der Löschung Verfügungen getroffen wurden, allerdings mit dem Ergebnis der weiteren Aufbewahrung. Diese Verfügungen erfolgten dann jedoch nur formelhaft und undifferenziert, ohne Auseinandersetzung mit der Frage, was tatsächlich noch zur Strafverfolgung im Sinne von § 100b Abs. 6 StPO erforderlich ist. Eigene Initiativen der Staatsanwaltschaft zur Wahrung der Schutzpflichten waren nicht erkennbar, selbst dann nicht, wenn die Akten aus anderen Anlässen wiedervorgelegt oder sogar an andere Stellen übersandt wurden.

- Mitteilungen an die Beteiligten

Besondere Mitteilungen an die Beteiligten nach § 101 StPO waren aus keiner der geprüften Akten ersichtlich.

In einzelnen Verfahren, in denen die TÜ zum Gegenstand der Hauptverhandlung gemacht worden war, hat der Angeklagte spätestens durch die Verlesung in der Hauptverhandlung Kenntnis von der TÜ erhalten, so daß keine gesonderte Mitteilung gegenüber dem Angeklagten mehr erforderlich war.

Ob dies gegenüber allen Beteiligten, insbesondere dritten Anschlußinhabern und Gesprächspartnern, deren Gespräche weiter verwendet wurden, ebenso gilt, war dagegen zweifelhaft. Insbesondere in Verfahren, in denen die TÜ für die Überführung der Täter keine Rolle gespielt hat, kann nicht ohne weiteres davon ausgegangen werden, daß sich die Mitteilung durch die Akteneinsicht von Verteidigern erledigt habe. Die Staatsanwaltschaft genügt ihrer Mitteilungspflicht nicht, wenn sie darauf vertraut, daß die Verteidiger ihren Mandanten irgendwie berichten werden, daß auch eine TÜ stattgefunden hat, wenn sich selbst in der Anklageschrift keine Hinweise auf die TÜ befinden.

Die Verteidiger sind auch nicht berechtigt, dritten Anschlußinhabern und Gesprächspartnern mitzuteilen, daß eine TÜ gegen ihre Mandanten stattgefunden hat, wenn es hierauf für Verteidigungszwecke nicht ankommt.

- Maßnahmen zur Vermeidung der Mängel

Bei den weiteren Erörterungen mit der Staatsanwaltschaft bestand weitgehend Einvernehmen darüber, daß Abläufe wie in den geschilderten Fällen vermieden werden müssen. Zu diesem Zweck dienen seit 1989 sogenannte „TÜ-Listen", in denen Angaben zu Verfahren mit Telefonüberwachungen und auch die Löschungszeitpunkte erfaßt werden. Diese Listen werden monatlich von den Abteilungsleitern und vierteljährlich von den Hauptabteilungsleitern der Staatsanwaltschaft überprüft. Die festgestellten Mängel waren anscheinend darauf zurückzuführen, daß es sich um Fälle aus der Zeit vor Einführung der „TÜ-Listen" handelte. Aktuellen Listen aus der Hauptabteilung, die die meisten Telefonüberwachungen durchführt, war zu entnehmen, daß keine vergleichbar alten Unterlagen mehr vorlagen.

Aufgrund der gemeinsamen Erörterungen sollen bestimmte Anlässe festgelegt werden, bei denen eine zwingende Überprüfung der weiteren Erforderlichkeit von Unterlagen aus Telefonüberwachungen erfolgt. Insbesondere wenn Verfahren eingestellt werden, weil die Telefonüberwachung unergiebig war, Anklage erhoben wird ohne Bezugnahme auf die TÜ und die Akten nach Verfahrensabschluß vom Gericht zurückkommen, soll in den „TÜ-Listen" konkret begründet werden, warum die Unterlagen noch nicht vernichtet sind. Auch der Zeitpunkt der Benachrichtigung der Beteiligten soll in den Listen festgehalten werden. Die Löschungstermine sollen nicht wie bisher nur zwei bis dreimal im Jahr, sondern im Abstand von zwei Monaten nach einem festgelegten Turnus stattfinden. Diese Neuregelungen sollen in eine überarbeitete Rundverfügung der Staatsanwaltschaft zur Telefonüberwachung aufgenommen werden.

Danach ist zu hoffen, daß sich die festgestellten Mängel nicht wiederholen und die Praxis besser dem gesetzlichen Gebot zur unverzüglichen Löschung entspricht.

16.2 Zentrales staatsanwaltschaftliches Verfahrensregister

Nachdem im Dezember 1994 die Vorschriften über das zentrale staatsanwaltschaftliche Verfahrensregister (§§ 473 bis 477 der Strafprozeßordnung) in Kraft getreten sind (13. TB, 19.1.1), hat der Bundesrat im Juli 1995 der Errichtungsanordnung des Bundesministeriums der Justiz für das Verfahrensregister zugestimmt. Die Eile bei der Schaffung der Rechtsgrundlagen für dieses Register ist bemerkenswert, weil noch lange nicht absehbar ist, wann das Register tatsächlich seinen Betrieb aufnehmen kann. Wir haben in unserer Stellungnahme zum Entwurf geltend gemacht, daß die Errichtungsanordnung den gesetzlichen Auftrag in wesentlichen Fragen nicht erfüllt.

In § 476 Abs. 5 StPO ist vorgeschrieben, daß in der Errichtungsanordnung nähere Einzelheiten insbesondere zu den erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung getroffen werden müssen. Die Errichtungsanordnung enthält jedoch hierzu lediglich die Aussage, daß die Daten besonders sensibel sind. Daher seien besondere Maßnahmen erforderlich, um die Verfügbarkeit, Integrität und Vertraulichkeit der Daten zu sichern. Zur Feststellung dieser allgemein bekannten Tatsache benötigt man keine Rechtsvorschriften. Von Interesse wäre vielmehr gewesen, welche konkreten Maßnahmen denn verbindlich vorgeschrieben werden. Hierzu enthält die Errichtungsanordnung nichts.

Der Grund für dieses Defizit ist darin zu sehen, daß bisher niemand weiß, wie die Daten von den einzelnen Staatsanwaltschaften in das Register gelangen sollen, und welche Infrastruktur für Anfragen und Übermittlungen aus dem Register geschaffen werden soll. Somit fehlt die Grundlage für die Beurteilung der erforderlichen Maßnahmen zur Datensicherung. Der Bundesrat hat darauf hingewiesen, daß für die Steuerverwaltungen in steuerstrafrechtlichen Angelegenheiten eine Direkteingabe in das Register derzeit nicht möglich und auch nicht absehbar ist. Dasselbe hätte eigentlich für die Staatsanwaltschaften festgestellt werden müssen, mit der Folge, daß die Errichtungsanordnung noch nicht verabschiedungsreif gewesen wäre. Auch die Justizbehörde hatte diese Bedenken gegenüber dem Bund vorgetragen. Sie sind jedoch übergangen worden.

16.3 Entwurf für ein Strafverfahrensänderungsgesetz

Der im 13. TB (19.1.2) kritisch gewürdigte Entwurf des Bundesrates für ein Strafverfahrensänderungsgesetz ist im Bundestag bisher nicht weiter behandelt worden. Die Bundesregierung hat lediglich die Vorlage eines eigenen Entwurfs angekündigt, über den jedoch nichts bekannt geworden ist.

Die Justizbehörde legt den Bundesrats-Entwurf gleichwohl bei ihren Überlegungen insbesondere zur Frage des Umgangs mit staatsanwaltschaftlichen Ermittlungsakten zugrunde. Eine Rundverfügung der Staatsanwaltschaft zur Akteneinsicht vom August 1995, die die bisherigen Regelungen zur Akteneinsicht in den Richtlinien für das Straf- und Bußgeldverfahren ersetzen soll, hat sich an dem Gesetzentwurf orientiert. Die neue Rundverfügung ist demnach zwar umfangreicher als die bisherige Ziffer der Richtlinien, besagt in der Sache jedoch kaum etwas anderes.

Bis auf wenige Detailfragen war die Justizbehörde nicht bereit, den von uns im 13. TB (19.1.2) skizzierten Anforderungen an die Einsichtnahmen anderer Behörden oder Privatpersonen in staatsanwaltschaftliche Akten oder an Auskünfte aus den Akten zu folgen. Sie begründet dies mit angeblich unvertretbarem Aufwand. Vernachlässigt wird dabei, daß inzwischen auch die Gerichte bei Entscheidungen über die Zulässigkeit von Akteneinsichtnahmen sorgfältig differenzieren, um welche Inhalte es sich handelt und bei welchen Sachverhalten überwiegende schutzwürdige Interessen entgegenstehen.

Unverständlich ist auch, daß die Justizbehörde nach wie vor daran festhält, daß sogenannte berechtigte Interessen von Privatpersonen für die Einsichtnahme in staatsanwaltschaftliche Akten und Auskünfte aus ihnen ausreichen sollen. Bei Sachverhalten, die regelmäßig viel weniger sensibel sind, werden hingegen gesetzlich jeweils rechtliche Interessen gefordert (z. B. § 299 Abs. 2 Zivilprozeßordnung für Akten der Zivilgerichte, § 61 Personenstandsgesetz für Personenstandbücher und § 16 Abs. 1 Nr. 3 Hamburgisches Datenschutzgesetz für Daten der allgemeinen Verwaltung).

16.4 Automation bei der Staatsanwaltschaft

Das im 13.TB (19.2.1) beschriebene Konzept zur Einführung des Verfahrens „GEORG" (Geschäftstellenorganisation) bei der Staatsanwaltschaft ist nicht weiter verfolgt worden. Grund hierfür war zum einen, daß die Programmierung für das Datenbanksystem der neuen Zentralkartei als Grundlage für die weitere Automation in den Geschäftstellen nicht fristgerecht fehlerfrei erstellt werden konnte und der Vertrag mit dem Auftragnehmer gekündigt worden ist. Die Untersuchung eines externen Beratungsunternehmens zur Erstellung einer umfassenden EDV-Strategie für die Staatsanwaltschaft kam ferner im Juli 1995 zu dem Ergebnis, daß das Verfahren „GEORG" für die Erfordernisse der Staatsanwaltschaft ungeeignet sei. Die von uns im 13. TB (19.2.1) geäußerten Zweifel wurden damit bestätigt.

Nunmehr ist vorgesehen, eine neue Grundsatzentscheidung über die in der Staatsanwaltschaft einzusetzende IuK-Technik zur Vorgangsbearbeitung zu treffen. An der neu eingesetzten Lenkungsgruppe sind wir wie bisher beteiligt. Bei Redaktionsschluß war noch keine Entscheidung für ein neues Verfahren getroffen worden.

16.5 Zentralkartei der Staatsanwaltschaft

Aufgrund unserer Kritik an den massiven Rückständen bei der Eintragung von Verfahrensergebnissen in der Zentralkartei im 13. TB (19.2.2) hatte die Justizbehörde seit Beginn des Jahres 1995 zusätzliche Kräfte eingestellt, um die Rückstände abzubauen. Bis zum Mai war mehr als die Hälfte der unerledigten Mitteilungen über Verfahrensergebnisse (sogenannte „Gelbe Zettel") abgearbeitet. Dann brach jedoch für mehr als eine Woche das technische System der Zentralkartei vollständig zusammen. Somit entstand zusätzlich vorübergehend ein erheblicher Rückstand bei der erstmaligen Eintragung von Verfahren, der vorrangig abgebaut wurde. Dadurch erhöhte sich der Rückstand bei den Verfahrensergebnissen erneut rapide. Bis Ende Oktober 1995 konnte dieser Rückstand bei den „Gelben Zetteln" dann aber vollständig abgebaut werden.

Ein Dauerproblem stellen die Eintragungen in der Zentralkartei dar, die aus der alten – bis 1985 auf Karten geführten – manuellen Kartei stammen. Diese Eintragungen enthalten keine Angaben zum Verfahrensergebnis, so daß der Anknüpfungspunkt für die Löschungen entsprechend den Aufbewahrungsfristen der dazugehörigen Akten fehlt. Bei der Überprüfung von Einzelfällen haben wir regelmäßig derartige Eintragungen aus dem Altbestand festgestellt, bei denen die Akten vernichtet waren. Die Daten in der Zentralkartei waren somit nicht mehr zum Aktennachweis erforderlich und zu löschen. Wir haben gefordert, daß bei der Einführung eines neuen automatisierten Verfahrens die generelle Löschung dieses mindestens zehn Jahre alten Bestandes ohne Verfahrensergebnisse erfolgt. Diese Forderung ist auch von der Projekt- und Lenkungsgruppe für die Automation der Zentralkartei unterstützt worden. Eine endgültige Entscheidung hierzu ist noch nicht getroffen worden.

16.6 Speicherungen von Mitteilungen nach dem Geldwäschegesetz

Über die im 13. TB (19.2.3) kritisierte Speicherung von Mitteilungen nach dem Geldwäschegesetz (GwG) durch die Staatsanwaltschaft ist 1995 eine pragmatische Einigung erzielt worden. Zwar vertritt die Staatsanwaltschaft nach wie vor die Auffassung, daß sie aufgrund des Geldwäschegesetzes befugt sei, personenbezogene Speicherungen zum Zwecke der Vorsorge für künftige Strafverfolgung vorzunehmen. Wir sind dagegen der Auffassung, daß der Gesetzgeber mit dem Gesetz über die Datenverarbeitung der Polizei (HmbPolDVG) allein der Polizei diese Aufgabe und die entsprechende Datenverarbeitungsbefugnis zugewiesen hat und die damit verbundenen Eingriffe nicht zusätzlich von der Staatsanwaltschaft vorgenommen werden können.

Die Staatsanwaltschaft hat jedoch akzeptiert, daß sie nicht sämtliche Mitteilungen speichern kann, sondern nur solche, bei denen tatsächliche Anhaltspunkte dafür sprechen, daß die im Geldwäschetatbestand nach § 261 StGB genannten Straftaten begangen werden. Ferner sollen im Unterschied zur bisherigen Praxis Angaben über Personen, die nicht als Beschuldigte gelten,

maximal drei Jahre gespeichert werden und die Daten über die als Beschuldigte angesehenen Personen 5 Jahre. Damit werden die im HmbPolDVG vorgesehenen Einschränkungen entsprechend unserer Forderung vom Grundsatz her eingehalten. Allerdings ist die Erarbeitung einer völlig neuen Dateistruktur erforderlich, um die Speicherungsfristen auch technisch zu gewährleisten. Wir haben der Staatsanwaltschaft vorgeschlagen, bei der Erstellung der neuen Datenbank mit der Polizei zusammenzuarbeiten.

17. Justiz

17.1 Gesetz zur Änderung des AGB-Gesetzes

Der Rat der Europäischen Union hat am 5. April 1993 eine Richtlinie über mißbräuchliche Klauseln in Verbraucherverträgen verabschiedet. Durch diese Richtlinie sollen die Rechtsvorschriften der Mitgliedstaaten über vorformulierte Bestimmungen in Verbraucherverträgen angeglichen werden.

Der Begriff des „Verbrauchervertrages" umfaßt nicht nur die für eine Vielzahl von Verträgen vorformulierten Allgemeinen Geschäftsbedingungen (AGB), sondern auch Klauseln, die der Unternehmer nur zur einmaligen Verwendung diktiert. Auch die letztgenannten Klauseln müssen einer wirksamen richterlichen Inhaltskontrolle unterworfen werden, um den Verbraucher vor unangemessenen Benachteiligungen zu schützen.

Nach unserer Auffassung liegt eine unangemessene Benachteiligung auch dann vor, wenn der Unternehmer vor Beginn der Vertragsverhandlungen Daten über den Verbraucher wider Treu und Glauben oder in rechtswidriger Weise erhoben hat, um sie bei der Vertragsgestaltung zum Nachteil des Verbrauchers auswerten zu können. Diese Gefahr droht gerade bei einseitiger Festlegung von Klauseln, die individuell auf die Rechte und Pflichten eines bestimmten Vertragspartners ausgerichtet sind.

Wir haben uns deshalb für eine verbraucherfreundliche Regelung des Problems im Gesetz zur Änderung des AGB-Gesetzes ausgesprochen, das die genannte EG-Richtlinie umsetzen soll. Justiz- und Wirtschaftsbehörde haben diese Anregung bei den Beratungen des Gesetzentwurfs im Bundesrat leider nicht aufgegriffen.

17.2 Drittes Gesetz zur Änderung der Bundesnotarordnung und anderer Gesetze

Bei der anstehenden Novellierung der Bundesnotarordnung (BNotO) sollten bereichsspezifische datenschutzrechtliche Regelungen für das Notariat geschaffen werden. Wichtig ist in diesem Zusammenhang, daß die Prüfung der ordnungsgemäßen Amtsführung durch die Aufsichtsbehörden auch Vorgänge automatisierter Datenverarbeitung einbezieht. Entsprechende Vorschläge haben wir unterbreitet.

17.3 2. Zwangsvollstreckungsnovelle

Die Pfändung und Zwangsversteigerung von EDV-Anlagen erfordern wirksame Schutzvorkehrungen für personenbezogene Daten des Schuldners oder anderer Personen, die auf den Datenträgern der Anlage gespeichert sind. Die geltenden gesetzlichen Pfändungsverbote und -beschränkungen, die vorrangig der wirtschaftlichen und beruflichen Sicherung des Schuldners dienen, werden diesem Problem nicht gerecht.

Aufgrund verschiedener Eingaben sind wir davon überzeugt, daß der Datenschutz in der Vollstreckungspraxis wachsende Bedeutung gewinnt.

Die nach dem Volkszählungsurteil des Bundesverfassungsgerichts erforderlichen technischen und organisatorischen Schutzmaßnahmen hat der Gesetzgeber zu treffen. Interne Geschäftsanweisungen für Gerichtsvollzieher oder gemeinsame Regelungen der Justizministerien reichen nicht aus.

Wir treten deshalb dafür ein, daß die datenschutzrechtliche Verantwortung der Gerichtsvollzieher im Rahmen der geplanten 2. Zwangsvollstreckungsnovelle bereichsspezifisch abgesichert und konkretisiert wird.

17.4 Prüfung Registratur Justizbehörde

Im April 1995 führten wir eine umfassende Prüfung in der Registratur der Justizbehörde durch.

Die Aufbewahrung verschiedener Akten, insbesondere über dienstrechtliche Verhältnisse der Beamten und Richter, entsprach bei der Prüfung bereits dem erforderlichen hohen Sicherheitsstandard. In anderen Bereichen ergab die Prüfung hingegen dringenden Handlungsbedarf.

Anzuerkennen ist, daß die Justizbehörde diesen Handlungsbedarf mit erheblichem Kostenaufwand durch Anschaffung von Roll- und Stahlschränken rasch und konsequent umgesetzt hat.

17.5 Verwahrung gesammelter arbeitsrechtlicher Urteile

Im September 1995 beschäftigten wir uns aus Anlaß eines konkreten Vorkommnisses in der Bibliothek des Landesarbeits- und Arbeitsgerichts mit der Frage, welche Anforderungen an die Anonymisierung von Urteilen zu stellen sind, die gerichtsintern gesammelt und für eine Rechtsprechungskartei aufbereitet werden. Da Urteile häufig sensible Daten über Prozeßbeteiligte, Zeugen und andere Betroffene enthalten, sehen wir in der vollständigen und technisch einwandfreien Anonymisierung ein wesentliches datenschutzrechtliches Anliegen.

Dank der sehr konstruktiven Haltung der beteiligten Gerichtspräsidenten gelang es, kurzfristig und einvernehmlich ein tragfähiges Gesamtkonzept zur

Datensicherheit im Bereich der Arbeitsgerichtsbarkeit zu entwickeln. In dieses Konzept wurde auch die Geschäftsstellenverwaltung einbezogen.

17.6 Automation Bußgeldfonds

Das automatisierte Verfahren zur Bearbeitung von Bußgeldzahlungen im Rahmen von Strafverfahren wurde von uns im September 1995 geprüft.

Wir kamen zu dem Ergebnis, daß die automatisierte Speicherung der Namen von Bußgeldpflichtigen zeitlich begrenzt werden muß. Als Alternative zur regelmäßigen Unterrichtung der Sachbearbeiter durch Gerichte und Staatsanwaltschaften über die Erledigung der Zahlungspflicht hat die Justizbehörde vorgeschlagen, die Namen grundsätzlich nach neun Monaten zu löschen.

Diesen Weg halten auch wir für sachgerecht. Der genannte Zeitraum entspricht der Frist, die für eine Erfüllung von Auflagen und Weisungen als Voraussetzung einer strafprozessualen Verfahrenseinstellung von der Staatsanwaltschaft oder dem Gericht selbst im Falle der Verlängerung höchstens eingeräumt werden darf.

Einvernehmen mit der Justizbehörde konnte ferner darüber erzielt werden, daß Namen Dritter, die anstelle des Bußgeldpflichtigen Zahlungen leisten, künftig nicht mehr automatisiert gespeichert werden.

17.7 Automation Grundbuchverfahren

Das maschinell geführte Grundbuch mit der Möglichkeit des automatisierten Abrufs wirft eine Reihe datenschutzrechtlicher Probleme auf.

In den fachlich zuständigen Gremien haben wir konkrete Vorschläge zur Begrenzung der Risiken und zur Ahndung von Mißbräuchen unterbreitet, die beim automatisierten Abruf von Grundbuchdaten drohen. Weiterhin werden wir uns für differenzierte Zugriffsberechtigungen der Teilnehmer einsetzen, die Abrufe auf den erforderlichen Umfang beschränken.

18. Strafvollzug

18.1 Einwilligung im Strafvollzug

Der Strafvollzug zeichnet sich in besonderem Maße durch Ausübung staatlicher Hoheitsgewalt aus, die zwangsweise persönliche Freiheitsräume der Betroffenen erheblich einschränkt. Das Strafvollzugsgesetz (StVollzG) gewährt in einer Reihe von Vorschriften Befugnisse zu Eingriffen in das Grundrecht auf informationelle Selbstbestimmung ohne Einwilligung der Betroffenen, insbesondere für die Überwachung von Besuchen (§ 24 Abs. 3, § 27), die Briefkontrolle (§ 29) und erkennungsdienstliche Maßnahmen (§ 86).

Die Bedeutung der Einwilligung für den Strafvollzug ist gleichwohl hoch einzuschätzen. Sie zeigt sich zum einen in Fällen der Datenverarbeitung für andere

als Vollzugszwecke, insbesondere bei Forschungsvorhaben, die unter Einbeziehung von Gefangenenpersonalakten oder Auskünften der Anstaltsinsassen durchgeführt werden sollen (18.1.1).

Daneben muß der Strafvollzug in bestimmtem Umfang auf personenbezogene Daten von Besuchern zurückgreifen (18.1.2).

18.1.1 Einsicht in Gefangenenpersonalakten für Forschungszwecke

Die Notwendigkeit kriminologischer Forschung im Strafvollzug ist unbestritten und vom Gesetzgeber ausdrücklich anerkannt (§ 166 StVollzG).

Datenverarbeitung für Forschungsprojekte ist zulässig, soweit der Betroffene nach umfassender Aufklärung über das Vorhaben eingewilligt hat (§ 5 HmbDSG). Der Betroffene ist darüber zu unterrichten, daß seine Teilnahme freiwillig ist, welchem Zweck das Forschungsprojekt dient und in welcher Weise die Datenverarbeitung durchgeführt, insbesondere die möglichst frühzeitige Anonymisierung der Daten gewährleistet werden soll. Ferner ist der Betroffene über den Träger bzw. Auftraggeber des Vorhabens und die Person des wissenschaftlichen Projektleiters zu informieren. Schließlich muß dem Betroffenen verdeutlicht werden, daß er seine Einwilligung auf bestimmte Daten beschränken oder die Verarbeitung für einzelne Daten untersagen kann, z. B. für besonders sensible medizinische Sachverhalte.

Die Einwilligung ist verzichtbar, soweit schutzwürdige Interessen des Betroffenen nicht beeinträchtigt werden oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens erheblich überwiegt und der Zweck der Forschung ohne personenbezogene Daten nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann (§ 27 HmbDSG).

Der hohe Rang des Grundrechts auf informationelle Selbstbestimmung verlangt, an den Begriff des „erheblich überwiegenden öffentlichen Interesses" strenge Anforderungen zu stellen. Dies gilt insbesondere für Diplomarbeiten und Dissertationen, deren Ergebnisse nicht unmittelbar für den Strafvollzug ausgewertet werden sollen. Gesetzliche Vorschriften zum Schutze besonderer persönlicher Verhältnisse (z. B. Adoptionsgeheimnis) sind zu beachten.

Hat der Forscher sich vergeblich um die Einwilligung des Betroffenen bemüht, so ist dessen Weigerung, an dem Vorhaben mitzuwirken, zu respektieren. Der Forscher kann in diesem Falle nicht nachträglich auf die „Forschungsklausel" des § 27 HmbDSG zurückgreifen. „Freiwilligkeit" ist nämlich nur dann gewährleistet, wenn der Betroffene darauf vertrauen kann, daß er selbst abschließend über die Zulässigkeit der Datenverarbeitung bestimmt.

Als Erkenntnisquelle für Forschung im Strafvollzug kommt neben dem persönlichen Gespräch insbesondere die Gefangenenpersonalakte in Betracht. Die besondere Sensibilität dieser Akte haben wir bereits im 13. TB (20.2) unterstrichen. Akteneinsicht für Forschungszwecke darf grundsätzlich nur innerhalb der Justizvollzugsanstalt (JVA) und allein solchen Personen gewährt werden, die zur Geheimhaltung verpflichtet sind. Die Akteneinsicht ist auf den für das konkrete Forschungsprojekt erforderlichen Umfang zu beschränken, und zwar auch dann, wenn der Betroffene eingewilligt hat.

Kommt es für die weitere Nutzung der Daten auf den Personenbezug nicht an, so sind die Daten anonymisiert zu erheben. Die Anfertigung von Notizen oder Ablichtungen aus der Akte, die auch später noch einen Personenbezug herstellen könnten, ist in diesem Falle unzulässig.

18.1.2 Ausweiskopien von Besuchern einer Justizvollzugsanstalt

Durch verschiedene Eingaben wurden wir auf die mit Beginn des Jahres 1995 eingeführte Praxis einer JVA aufmerksam, Gefangenen bei erstmaliger Antragstellung eine Kopie des Personalausweises oder Reisepasses des gewünschten Besuchers abzuverlangen bzw. Besucher zur direkten Übersendung der Kopie an die JVA zu veranlassen.

Das Strafvollzugsamt hat diese Praxis unter Hinweis auf das hohe Besucheraufkommen und den erheblichen Ausländeranteil der JVA gerechtfertigt. Die zweifelsfreie Identifizierung sei Grundlage für eine korrekte Eingabe der Besucherdaten in die hierfür vorgesehene automatisierte Datei der JVA, das Gefangenen- und Besucher-Informationssystem (GEBIS). Ohne eine zuverlässige Datenerfassung könne der Besucherverkehr nicht zügig und reibungslos abgewickelt werden.

Nach intensiver Diskussion setzten sich unsere Bedenken gegen das beschriebene Verfahren durch. Die JVA hob die entsprechende Verfügung im September 1995 auf. Unsere Bedenken stützten sich insbesondere darauf, daß die Vorlage von Ausweiskopien bereits im Zeitpunkt erstmaliger Antragstellung nicht erforderlich ist, um die spätere – zulässige – Ausweiskontrolle beim Betreten und Verlassen der JVA ohne Verzögerungen sicherzustellen.

Noch nicht abgeschlossen ist unsere Diskussion mit dem Strafvollzugsamt in einem weiteren Punkt: Wir setzen uns dafür ein, daß die Besucher selbst darüber entscheiden können, ob und wie lange ihre personenbezogenen Daten in der Besucherdatei gespeichert werden. Da Besuche nur stattfinden können, wenn und solange alle Beteiligten dies wünschen, reicht es nach unserer Ansicht nicht aus, daß die JVA Besucherdaten erst bei Entlassung bzw. Verlegung oder auf besonderen Antrag des Gefangenen löscht.

18.2 Mitwirkung von Praktikanten bei der Vollzugsgestaltung

Aus Anlaß einer Eingabe haben wir uns grundsätzlich mit der Frage auseinandergesetzt, welche Grenzen der Mitwirkung von Praktikanten im Strafvollzug an der Briefkontrolle (§ 29 StVollzG) gezogen sind.

Praktikanten müssen sich zu Beginn ihrer Ausbildung schriftlich zur Verschwiegenheit verpflichten. Daneben werden sie vom Anstaltsleiter noch gesondert über die Vertraulichkeit der ihnen zugänglichen Erkenntnisse belehrt.

Der Ausbildungszweck erfordert zwar unstreitig eine praxisnahe Einführung der Praktikanten in Vollzugsabläufe. Wir meinen allerdings, daß dieser Grundsatz für die Überwachung des Schriftverkehrs nur mit Einschränkungen gelten kann.

Nach Ansicht des Bundesverfassungsgerichts, die wir teilen, verlieren Mitteilungen von oder gegenüber Gefangenen infolge der Kontrolle nach § 29 StVollzG nicht ihren privaten und vertraulichen Charakter. Praktikanten können, anders als Vollzugsbedienstete im Beamtenverhältnis, bei Verletzung ihrer Verschwiegenheitspflicht nicht disziplinarrechtlich zur Verantwortung gezogen werden. Auch ein lückenloser strafrechtlicher Schutz des Briefgeheimnisses ist bei Überwachung durch Praktikanten nicht gewährleistet.

Das Strafvollzugsamt sieht bislang keine Veranlassung, von der gegenwärtigen Ausbildungspraxis abzuweichen. Es hält die schriftliche Verpflichtung und gesonderte Belehrung der Praktikanten für ausreichend. Wir werden uns weiterhin für sachgerechte Einschränkungen bei der Teilnahme von Praktikanten an der Briefkontrolle einsetzen, die auch dem Ausbildungszweck Rechnung tragen.

19. Gesundheitswesen

19.1 Chipkarten im Gesundheitswesen

19.1.1 Stand der Entwicklung

Seit Anfang 1995 ersetzt in ganz Deutschland die Krankenversicherungskarte den bisherigen Krankenschein. Ihre technische Ausgestaltung mit einem Chip und die notwendige Infrastruktur mit Lesegeräten in jeder Arztpraxis wiesen den Weg zu den sog. freiwilligen Gesundheits-Chipkarten:

In einer Reihe von Pilot- und Modellprojekten werden Karten erprobt, deren Chip nicht nur Verwaltungs- und Identitätsdaten des Versicherten verarbeiten, sondern auch sensible Gesundheitsdaten wie Anamnesen, Risikofaktoren, Befunde, Diagnosen, Behandlungsdokumentationen, Medikationen, Notfall- und Rehabilitationsdaten. Dabei dienen einzelne Systeme wie die geplante A-Card der Apotheken, die Vital-Card der AOK Leipzig und die „persönliche Patientenkarte" Neuwied der Kommunikation zwischen vielen im voraus nicht festgelegten Institutionen des Gesundheitswesens. Andere Systeme wie die Dialyse-Card, die Deficard und die Diab-Card bilden ein krankheitsspezifisches Informationsmedium nur für die an der Behandlung der Krankheit beteiligten Stellen.

Ziel aller dieser Projekte ist es, die für die medizinische Versorgung der Patienten erforderlichen Daten zuverlässig, vollständig und schnell zur Verfügung zu stellen. Der Zugriff auf die im Chip gespeicherten medizinischen Daten ersetzt die oft lückenhaften Anamneseangaben des Patienten und die langwierige Versendung von Arztbriefen und Patientenakten.

Fortentwicklungen der Technik zum komplexen Prozessor-Chip erlauben bei den neuen Gesundheitskarten ungleich differenziertere Datenverarbeitungen als bei den „dummen" Speicher-Chipkarten wie der Krankenversicherungskarte. So können auf dem Chip unterschiedliche Speichersegmente angelegt und der Zugriff je nach Nutzer auf einzelne Datengruppen beschränkt werden. Auch ausgefeilte elektronische Nachweise der Zugriffsberechtigung und eine Verschlüsselung der Daten kann mit Hilfe zusätzlicher sog. „Krypto-Controller" realisiert werden.

Den technischen Möglichkeiten zur Verwirklichung von Datenschutz und Datensicherheit stehen andererseits die Anforderungen der Wirtschaftlichkeit, der Praktikabilität und der Akzeptanz sowohl bei Patienten als auch bei Ärzten gegenüber. Eine bundesweite Arbeitsgemeinschaft „Karten im Gesundheitswesen" versucht von der Arztseite aus, hersteller- und projektunabhängig technische Harmonisierungen und Standards, aber auch Richtlinien für die Umsetzung des Datenschutzes zu schaffen. Wieweit die Projektträger und EDV-Unternehmen diese umsetzen, ist allerdings noch offen.

Während die genannten krankheitsspezifischen Kartensysteme sich zum Teil schon seit längerem in der Praxis bewährt haben, befinden sich die Systeme „allgemeiner" Gesundheitskarten noch in der Planungs- bzw. Erprobungsphase. Zwar hat gegenwärtig keines der Projekte seinen Sitz in Hamburg. Lokale krankheitsspezifische Kartenprojekte können jedoch jederzeit von einzelnen Hamburger Krankenhäusern übernommen werden. Überregional konzipierte Projekte wie die A-Card werden bald auch Hamburger Bürgerinnen und Bürger vor die Abwägung von Nutzen und Risiken solcher Gesundheits-Chipkarten stellen.

19.1.2 Probleme der Einwilligung

Im Gegensatz zur gesetzlich vorgeschriebenen Krankenversicherungskarte bieten die Krankenkassen oder andere Projektträger die Gesundheits- oder Patientenchipkarten den Versicherten bzw. Patienten lediglich an. Die Annahme dieses Angebots ist freiwillig. Auch die Datenverarbeitung zur Vorbereitung eines Vertrages über die Teilnahme an einem Chipkarten-Verfahren bedarf der freien Einwilligung des Betroffenen.

Da § 28 BDSG die Verarbeitung und Nutzung personenbezogener Daten „im Rahmen der Zweckbestimmung eines Vertragsverhältnisses" erlaubt, kann bereits die Vertragsannahme erhebliche Folgen für die zukünftige Preisgabe

sensibelster personenbezogener Daten haben. Deswegen sind an die notwendige Aufklärung des Betroffenen i.S.d. § 4 BDSG – vor Vertragsschluß – hohe Anforderungen zu stellen. Eine übertrieben werbende, einseitig die Vorzüge der Chipkarte herausstellende Verfahrensbeschreibung ist hier nicht ausreichend; geboten ist vielmehr eine umfassende und objektive, Chancen und Risiken aufzeigende Information des Versicherten bzw. Patienten. Je mehr Institutionen und Personen an der Chipkarten-Kommunikation teilnehmen sollen, desto schwerer wird es für den Betroffenen, die Übersicht über die durch die Chipkarte ermöglichte Verarbeitung und Nutzung seiner Daten zu bekommen und in seinen Willen aufzunehmen.

Die im allgemeinen Kapitel über die datenschutzrechtliche Einwilligung (oben 1.2) beschriebenen Fragen der Freiwilligkeit und des sozialen Zwangs stellen sich bei der Chipkarte im Gesundheitswesen besonders deutlich. So erscheint vielfach zweifelhaft, ob die Einwilligung in die Speicherung von medizinischen Daten auf der Chipkarte und in den Zugriff Dritter auf diese Daten wirklich freiwillig erfolgt: Im Verhältnis zur Krankenversicherung und erst recht im Verhältnis zum Arzt fühlt man sich selten als gleichberechtigter Partner, sondern häufig – wenn nicht regelmäßig – unterlegen und vom Wohlwollen des anderen abhängig. Wer wird seinem Arzt, in dessen Händen die eigene Gesundheit liegt, den gewünschten Zugriff auf heikle, aber für die gegenwärtige Behandlung irrelevante Daten – z. B. des Psychiaters oder des Gynäkologen – verweigern, wenn dadurch voraussehbar das Vertrauensverhältnis zwischen Arzt und Patient zerstört wird?

Neben dieser besonderen psychologischen Abhängigkeit im Arzt-Patienten-Verhältnis ist jeder Chipkarten-Inhaber auch einem sozialen Druck ausgesetzt: Je mehr sich allgemeine Gesundheits-Chipkarten durchsetzen, je mehr also Versicherungen und Ärzte davon ausgehen, daß die Patienten über eine solche Karte verfügen, desto schwerer wird es fallen, sich dieser gesellschaftlichen „Normalität" zu entziehen. Selbst in einem begründeten Einzelfall müßte man erst einmal die Vorlage der Karte verweigern – etwa, um vor einer Operation eine unbeeinflußte zweite Meinung eines anderen Facharztes einzuholen. Informationelle Selbstbestimmung wird dann zur rechtfertigungsbedürftigen Ausnahme.

Besonders prekär wird es, wenn ein Arbeitgeber bei einer Bewerbung oder ein Versicherungsunternehmen für den Abschluß einer Lebensversicherung Zugriff auf die Chipkarten-Daten wünscht. Die faktische Unterlegenheit des Arbeitsplatzsuchenden oder des Versicherungskunden wird eine freiwillige Entscheidung kaum zulassen. Die Weigerung, die Karte vorzulegen, möglicherweise sogar die Behauptung, eine Chipkarte – entgegen der gesellschaftlichen Normalität – gar nicht zu besitzen, wird den gewünschten Vertragsabschluß gefährden.

19.1.3 Stellungnahme der Datenschutzbeauftragten

Schon im März 1994 hatten die Datenschutzbeauftragten des Bundes und der Länder einen gemeinsamen Beschluß gefaßt, der die Risiken der Gesundheits-Chipkarten aufzeigt und datenschutzrechtliche Anforderungen aufstellt.

In ihrer Konferenz am 9./10. November 1995 ergänzten und vertieften die Datenschutzbeauftragten ihre Positionen vor dem Hintergrund der ersten Erfahrungen mit Modellprojekten. Oberstes Ziel bleibt die Erhaltung der Entscheidungsfreiheit des Betroffenen im Einzelfall, der Qualität des therapeutischen Arzt-Patienten-Verhältnisses und der Sicherheit der medizinischen Daten. In der gemeinsamen Entschließung heißt es:

„Die freie Entscheidung der Betroffenen (Patienten/Versicherten), eine Chipkarte zu verwenden, muß gewährleistet sein. Dies umfaßt die Entscheidung,

- ob Daten auf einer Chipkarte gespeichert werden,
- welche der Gesundheitsdaten auf die Karte aufgenommen werden,
- welche Daten auf der Karte wieder gelöscht werden,
- ob die Karte bei einem Arztbesuch bzw. einem Apothekenbesuch vorgelegt wird und
- welche Daten im Einzelfall zugänglich gemacht werden.

. . . Eine wirksame Entscheidung für oder gegen die Verwendung einer Chipkarte setzt eine schriftliche, objektive, vollständige und nachvollziehbare Aufklärung über Zweck, Art, Umfang und Beteiligte der Chipkarten-Kommunikation voraus . . ."

Die in der Entschließung formulierten Anforderungen an Gesundheits-Chipkarten verstehen die Datenschutzbeauftragten zum einen als Prüfungsmaßstab für die Beurteilung der ihrer Kontrolle unterliegenden Projekte. Zum anderen wenden sich die Datenschutzbeauftragten ausdrücklich an den Gesetzgeber. Es ist seine Aufgabe, in Rechtsbeziehungen mit typischerweise ungleichen Partnern den unterlegenen Teil zu schützen. Die Entschließung fordert:

„Insbesondere muß der Gesetzgeber sicherstellen, daß die auf der beim Patienten befindlichen Chipkarte gespeicherten medizinischen Daten ebenso gegen Beschlagnahme und unbefugte Kenntnisnahme geschützt sind wie die beim Arzt gespeicherten Daten. Eine Kommunikation unter Vorlage der Karte mit Personen oder Stellen außerhalb des Arzt-Patienten-Verhältnisses, z. B. Arbeitgebern oder Versicherungen, muß vom Gesetzgeber untersagt werden . . .

Der Gesetzgeber muß die Patienten vor ‚billigen Gesundheitskarten' ohne ausreichende Sicherung vor einer Nutzung durch Dritte schützen. Es darf keine ‚Einwilligung' in Chipkarten und Chipkartensysteme mit verminderter Datensicherheit geben."

19.1.4 Informationsblatt

Über die Teilnahme an einem Chipkarten-Projekt müssen die Versicherten jeweils selbst entscheiden. Der Hamburgische Datenschutzbeauftragte hält deswegen die direkte Aufklärung über Gefahren und Risiken der Chipkarten-Kommunikation für besonders wichtig.

Aus diesem Grunde griff der Hamburgische Datenschutzbeauftragte die Initiative der Verbraucher-Zentrale Hamburg zu einem gemeinsamen Informationsblatt gerne auf. Das im September 1995 veröffentlichte Faltblatt „Die Gesundheits-Chipkarte: Alles auf eine Karte setzen?" stellt den behaupteten Vorteilen der Chipkarte Fragen und Hinweise auf mögliche Datenschutzgefahren gegenüber. Die Leser werden direkt angesprochen und zur Abwägung der Vorteile mit den zum Teil erst in der Zukunft entstehenden Risiken ermuntert.

Da die Chipkarten-Kommunikation auch die ärztliche Schweigepflicht berührt, bat der Hamburgische Datenschutzbeauftragte die Ärztekammer Hamburg, die Kassenärztliche Vereinigung Hamburg und die oben (19.1.1) erwähnte bundesweite Arbeitsgemeinschaft „Karten im Gesundheitswesen" um eine Stellungnahme zu den im Faltblatt aufgeworfenen Fragen und Datenschutzproblemen. Zum Schutz des Arztgeheimnisses ist eine technische Lösung denkbar, die einen Datenzugriff nur über eine ausdrückliche Freigabe durch den Arzt zuläßt, der die Daten – mit Einwilligung des Patienten – auf der Karte gespeichert hat.

Insgesamt geht es dem Hamburgischen Datenschutzbeauftragten nicht um den Boykott der Chipkarten-Technologie, sondern um einen bewußten und überlegten Umgang mit ihr. Mit dem Faltblatt versucht er, ein Gegengewicht zu bilden zu den in erster Linie werbenden Angeboten der Projektträger.

19.2 Patientenaufnahme-System SAP im Allgemeinen Krankenhaus St. Georg

19.2.1 SAP IS-H in den Landesbetrieb-Krankenhäusern

Nach der Einführung betriebswirtschaftlicher Module von SAP in den Krankenhäusern des Landesbetriebs (LBK) steht nun die Übernahme des Patientenverwaltungssystems IS-H von SAP in den Krankenhäusern an. Vorreiter dabei ist das Allgemeine Krankenhaus (AK) St. Georg, wo das System schon im Echtbetrieb läuft. Alle anderen LBK-Häuser werden diesem Beispiel folgen: AK Heidberg, Wandsbek, Bergedorf und möglicherweise Eilbek bereits zum 1. Januar 1996, das AK Ochensenzoll zum 1. Januar 1997.

Die AK Barmbek, Harburg, Hafen und Altona haben sich zu einem Pilotprojekt zusammengetan, um ein gemeinsames Rechenzentrum zu nutzen. Hier wird die Einführung von IS-H für den 1. Oktober 1996 oder den 1. Januar 1997 geplant. Das Netzkonzept wurde uns im November 1995 zur Stellungnahme übergeben.

Inzwischen hat sich auch das Universitätskrankenhaus Eppendorf für einen Einsatz von IS-H entschieden.

Bereits im Januar 1995 wiesen wir nach Durchsicht der umfangreichen SAP-Unterlagen das AK St. Georg auf grundsätzliche Probleme von IS-H hin. Sie ergaben sich aus einem Vergleich der LBK-Richtlinien zum Datenschutz und des Hamburgischen Krankenhausgesetzes einerseits mit der Standard-Konfiguration von IS-H andererseits. Es ging darum, die Standard-Software im Wege des sog. Customizing (Anpassen und Einstellen) auf die datenschutzrechtlich zulässigen Datenerfassungen und -verarbeitungen zu beschränken. Bei einzelnen Anforderungen wie z. B. der von § 14 Hamburgisches Krankenhausgesetz vorgeschriebenen Möglichkeit, Daten zu löschen, wurden die Grenzen der technischen Möglichkeiten von IS-H erreicht.

Im Mai 1995 prüften wir den Stand der Systemeinführung im AK St. Georg. Dabei stellten wir fest, daß die gebotene Anpassung der IS-H-Software an die konkreten Bedürfnisse des AK St. Georg praktisch nicht erfolgt war. Vielmehr wurden insbesondere die Aufnahmemasken ohne eine Prüfung der Erforderlichkeit der von IS-H vorgesehenen Angaben übernommen. Bei der Notaufnahme von Patienten durch das medizinische Personal einzelner Kliniken stellten sich die strukturellen Probleme des Berechtigungskonzepts von SAP, wie sie oben (3.2) dargestellt sind.

Zu unserem Prüfbericht vom 11. September 1995 ging erst unmittelbar nach Redaktionsschluß eine Stellungnahme des AK St. Georg ein.

Das AK Wandsbek lud uns im November 1995 zu einer Sitzung der Projektgruppe zur Einführung von SAP IS-H ein. Wir stellten ihr unsere derzeitigen Erkenntnisse zu Datenschutzproblemen bei der Einführung des SAP Patientenverwaltungssystems vor.

19.2.2 Aufnahme- und Abrechnungsmasken

Bei der Prüfung im AK St. Georg interessierten wir uns besonders dafür, welche Angaben IS-H für die stationäre Aufnahme eines Patienten vorsieht und wie das AK St. Georg dieses „Angebot" an Datenfeldern nutzt.

Eine Reihe von Angaben sind für die Patientenaufnahme nicht erforderlich: So wird neben dem Namen nach einem „Pseudonym" gefragt, das aber nicht in die Suchfunktion aufgenommen ist. Auch die Angabe „VIP" (very important person) ist weder für die Aufnahme noch für die Abrechnung von Bedeutung, eröffnet aber möglicherweise Ansätze für einen Mißbrauch. Etwas ähnliches gilt für die Frage „Organspender?".

Bei anderen von IS-H vorgesehenen Angaben bedarf es des Hinweises, daß der Patient diese Frage nicht zu beantworten braucht. Dies betrifft die Konfession und die Angabe von Angehörigen-Personalien zur Benachrichtigung im

Notfalle. Die Frage nach dem Arbeitgeber ist ferner nur bei Unfällen erforderlich. Es ist deswegen zunächst nach einem möglichen Unfall zu fragen.

Datenschutzrechtlich problematisch ist schließlich, daß SAP an verschiedenen Stellen der Aufnahmemasken ein Freitext-Feld „Bemerkungen" vorsieht. Da über die Aufnahmedaten auch die Abrechnung mit den Krankenkassen gesteuert wird, die hierfür zugelassenen Daten aber abschließend in § 301 Sozialgesetzbuch V genannt sind, dürfen diese „Bemerkungsfelder" nicht zu einer Ausweitung des Datenumfangs führen. Sie sollten ganz entfallen oder zu „Storno-Feldern" für den Fall einer versehentlichen Falscheingabe umfunktioniert werden.

In seiner Stellungnahme sagte das AK St. Georg nun zu, bis zum Jahresende 1995 jedenfalls den größten Teil unserer Anregungen umzusetzen. Einzelheiten bedürfen jedoch noch der Diskussion.

Dem Hamburgischen Datenschutzbeauftragten geht es insgesamt darum zu verhindern, daß der mit dem LBK vereinbarte Datensatz für die Patientenaufnahme (vgl. 13. TB, 21.10) durch die Nutzung zusätzlicher Angebote von SAP IS-H ausgeweitet wird. Die Beschränkung auch der technischen Möglichkeit der Datenerfassung auf das erforderliche Maß wird bei der datenschutzrechtlichen Beratung der anderen Krankenhäuser ebenfalls angestrebt werden.

19.3 Prüfung des Medizinischen Dienstes zur Pflegeversicherung

Im September 1995 prüfte der Hamburgische Datenschutzbeauftragte das Verfahren, mit dem der Medizinische Dienst der Krankenversicherung (MDK) im Auftrag der Pflegekassen die Pflegebedürftigkeit von Versicherten feststellt. Der Prüfungsbericht enthält folgende Maßnahmen zur Verbesserung des Datenschutzes:

- Der MDK soll eine Schweigepflicht-Entbindungserklärung mit den vom Sozialgesetzbuch geforderten Hinweisen für die Versicherten formulieren.
- Der MDK soll eine Vereinbarung mit der Kassenärztlichen Vereinigung Hamburg (KVH) kündigen, nach der der MDK Vertragsärzte mit der Begutachtung von Versicherten beauftragte und dazu Listen der Patienten an die KVH weitergab.
- Der MDK soll einen Gutachter-Rahmenvertrag ändern, um insbesondere die Aufbewahrung der Patientenunterlagen beim Gutachter auf die unbedingt erforderliche Dauer zu beschränken.
- Der MDK soll sein EDV-System zur Verfahrensunterstützung so ändern, daß die festgestellte Pflegestufe nicht gespeichert wird und die gesetzliche Löschungsfrist für personenbezogene Daten eingehalten wird.
- Der MDK soll den betroffenen Versicherten selbst Akteneinsicht gewähren und nicht an die Pflegekasse verweisen.

- Der MDK soll den Zugang unbefugter Dritter zu den Arbeitsplätzen der Sachbearbeiterinnen wirksamer unterbinden und die Versichertenunterlagen besser schützen.

Eine Stellungnahme des MDK zu diesen Forderungen liegt noch nicht vor.

19.4 Abrechnung von Krankenhäusern mit Sozialämtern

Wenn sich bei der Bezahlung von Krankenhauskosten eine Verzögerung ergibt, halten es die meisten staatlichen Krankenhäuser in Hamburg nach unseren Feststellungen immer noch für richtig, Behandlungskosten „vorsorglich" beim Sozialamt anzumelden, auch wenn gar kein Anhaltspunkt dafür besteht, daß der Patient sozialhilfebedürftig ist. Dies hatten wir für die Fälle beihilfeberechtigter Beamter bereits vor drei Jahren kritisiert (11. TB, 21.7).

Wir haben die Krankenhäuser nachdrücklich gebeten, eine Abrechnung mit dem zuständigen Sozialamt nur vorzunehmen, wenn hinreichende Anhaltspunkte für eine Sozialhilfebedürftigkeit vorliegen, denn sonst ist die Übermittlung der Patientendaten an das Sozialamt nach § 11 Abs.1 Nr. 5 Hamburgisches Krankenhausgesetz unzulässig. Im übrigen haben wir den Landesbetrieb Krankenhäuser aufgefordert, die Voraussetzungen für eine Abrechnung mit dem Sozialamt einheitlich zu regeln.

19.5 Neue Rechtsvorschriften

Im Bereich des Gesundheitswesens war der Hamburgische Datenschutzbeauftragte an folgenden im letzten Jahr beschlossenen Rechtsvorschriften beteiligt:

- Gesetz zur Neuregelung des Hamburgischen Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (HmbPsychKG): Es enthält erstmals differenzierte Datenschutzregelungen für die verschiedenen Datenverarbeitungsformen und die verschiedenen Aufgabengebiete.
- Gesetz zur Änderung des Hamburgischen Ärztegesetzes und des Hamburgischen Zahnärztegesetzes: Mit den §§ 15a – 15g wurden in das Ärztegesetz Regelungen für eine Ethik-Kommission aufgenommen, deren Aufgaben auch datenschutzrechtliche Fragen umfassen.
- Berufsordnung der Hamburger Ärzte/Ärztinnen: Aus Datenschutzgründen versagte der Senat die Genehmigung zu § 11 Abs.4, der die Verwahrung von Patientenunterlagen bei Praxisaufgabe regelte (vgl. 13.TB, 21.1).

Der angekündigte Gesetzentwurf zum öffentlichen Gesundheitsdienst wurde dem Hamburgischen Datenschutzbeauftragten bisher nicht vorgelegt.

19.6 Prüfung des Gesundheitsamts Nord

Im 13.TB (21.6) berichteten wir von der Prüfung des Gesundheitsamts Nord im Juli 1994. Inzwischen ist die Aufarbeitung der festgestellten Mängel abgeschlossen.

Folgende datenschutzrechtliche Verbesserungen konnten erreicht werden:

- Das Gesundheitsamt gibt die Personalien von Bürgern, die an verdorbenen Lebensmitteln erkrankten, in der Regel nicht mehr an das Wirtschafts- und Ordnungsamt weiter.
- Die Erklärung, mit der die zu begutachtende Person ihre Ärzte von der Schweigepflicht entbindet, wird datenschutzfreundlich konkretisiert.
- Gesundheitliche Risikofaktoren von Bewerbern für den öffentlichen Dienst teilt das Gesundheitsamt der Anstellungsbehörde nur noch mit, wenn sie Zweifel an der Eignung rechtfertigen.
- Amtsärztliche Gutachten für die Führerscheinstelle werden vor der Versendung mit der untersuchten Person besprochen.
- Der Schulzahnarzt teilt dem Klassenlehrer nicht mehr die Namen der Schüler mit, bei denen eine Behandlungsbedürftigkeit festgestellt wurde.
- Bei der Datenerhebung für die schulärztliche Untersuchung wird in Zukunft ausdrücklich darauf hingewiesen, das die Angabe des Berufs der Eltern freiwillig ist.

Nicht durchgesetzt wurde, daß das Gesundheitsamt die Betroffenen fragt, ob es frühere Vorgänge – ggf. anderer Abteilungen – heranziehen darf. Geprüft wird allerdings, ob die Aufbewahrungsfristen alter Vorgänge nicht inzwischen abgelaufen sind.

19.7 Fernwartung der Patientenüberwachungsanlage im Universitätskrankenhaus Eppendorf (UKE)

Mit der im Frühjahr 1994 auf der Intensivstation der Anästhesiologie im UKE eingeführten Patientenüberwachungsanlage beschäftigen wir uns schon seit einigen Jahren (11. TB, 3.3; 13. TB, 21.7). Auch in diesem Tätigkeitsbericht kann über das Thema Fernwartung sowie die Sicherheitsmaßnahmen noch nicht abschließend berichtet werden.

Nachdem ich Ende letzten Jahres eine datenschutzrechtliche Beanstandung ausgesprochen hatte, gab das UKE zunächst ein Datenschutzgutachten bei der Universität Hamburg in Auftrag. Nicht zuletzt aufgrund des Gutachtens hatte sich das UKE anschließend bereit erklärt, einen Teil unserer Anforderungen umzusetzen. Um zumindest eine nachträgliche Datenschutzkontrolle zu ermöglichen, sollte ein Programm zur Auswertung der Protokolldatensätze erstellt werden. Bisher werden sämtliche im Rahmen der Fernwartung übertragenen TCP/IP-Datenpakte lediglich sequentiell ohne entsprechende Auswertung abgespeichert. Abgelehnt wurde vom UKE jedoch weiterhin, einen Teil der Systemverwaltung selbst durchzuführen. Auch war das UKE nicht in der Lage, gegenüber dem Hersteller unsere Forderung nach abgestuften Zugriffsrechten für den Wartungstechniker durchsetzen.

Nunmehr ist jedoch auch die Erstellung der Auswertungssoftware nicht mehr zu erwarten. Zwar wurden vom UKE detaillierte Anforderungen an die Auswertungssoftware formuliert. Ein halbes Jahr nach Fertigstellung der Anforderungsdefinition hat uns das UKE jedoch mitgeteilt, daß kein Entwickler zu deren softwaretechnischer Umsetzung gefunden werden konnte.

Das UKE greift stattdessen einen Vorschlag wieder auf, den wir bereits im 11.TB (3.3) erwähnt haben: Um die Datenschutzproblematik bei Fernwartung zu entschärfen, sollen Namen und weitere, den Patienten unmittelbar identifizierende Daten von medizinischen Daten getrennt werden. Während der Fernwartungstechniker lediglich Zugriff auf die restlichen Daten hat, ist die Verknüpfung der Dateien für medizinische Anwendungen nur dem berechtigten Fachpersonal erlaubt. Die Umsetzung dieser Maßnahme ist angesichts der geplanten Einführung einer UKE-weiten Patientennummer wieder aktuell.

Grundsätzlich begrüßen wir den neuen Vorschlag des UKE, da er im Gegensatz zu der geplanten Auswertungssoftware die Datenschutzprobleme bei der Fernwartung grundsätzlich zu lösen in der Lage ist. Angesichts der bisherigen Verzögerungen bei der Umsetzung geplanter Datenschutzmaßnahmen sind wir jedoch skeptisch, ob es gelingt, die angestrebte Aufhebung des Personenbezugs bald zu realisieren. Um dies besser beurteilen zu können, haben wir das UKE aufgefordert, einen detaillierten Zeitplan hierüber vorzulegen.

Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich

20. Schufa

20.1 Überprüfung des berechtigten Interesses

Die Schufa hat einem Kompromißvorschlag der Aufsichtsbehörden zur stichprobenweisen Überprüfung des berechtigten Interesses bei Schufa-Anfragen zugestimmt, wonach die Zahl der monatlichen Stichproben nach einer Staffelung zu bemessen ist (vgl. 12. TB, 23.2; 13. TB, 22.2). Die Schufa wendet die Staffelregelung seit dem 1. Oktober 1995 an. Dabei sollen die von den einzelnen Geschäftsstellen manuell erteilten Auskünfte der jeweiligen Geschäftsstelle zur Errechnung der Stichprobenzahl zugerechnet werden, während die automatisierten Auskünfte jeweils der Hauptstelle zugerechnet werden.

20.2 Adressierung von Bestätigungsschreiben

Die Aufsichtsbehörden halten die Praxis, mehrere Bestätigungsschreiben über telefonische Auskünfte in einem Umschlag und ohne Zustellvermerk zu versenden, für verbesserungsbedürftig. Sie haben angeregt, diese Schreiben einem bestimmten Empfänger (Revision, Datenschutzbeauftragten) zuzustellen (vgl. 12. TB, 23.3). Die Schufa ist der Auffassung, daß diese Problematik die grundsätzliche Organisation eines Unternehmens betreffe und sie nicht in die Organisationszuständigkeit ihrer Vertragspartner eingreifen könne.

21. Private bundesweite Schuldnerverzeichnisse

Die Frage nach der Zulässigkeit privater bundesweiter Schuldnerverzeichnisse ist durch die Neufassung der §§ 915 ff. ZPO geklärt (vgl. 11. TB, 24.1). Nach § 915e Abs. 1 ZPO erhalten Antragsteller, die Abdrucke zur Errichtung und Führung zentraler bundesweiter oder regionaler Schuldnerverzeichnisse verwenden, Abdrucke aus den Schuldnerverzeichnissen, so daß für die Verbreitung von Informationen nun eine Rechtsgrundlage vorhanden ist.

22. Versicherungswirtschaft

22.1 Automationsentwicklung

Das phonetische Strukturcode-Verfahren UNIWAGNIS (vgl.13.TB, 23.1) wurde im Berichtszeitraum für das Hinweissystem der Lebensversicherer eingeführt; bei dem Informationssystem der Sachversicherer haben sich weitere Verzögerungen ergeben. Darüber hinaus soll das Hinweissystem der Transportversicherer auf UNIWAGNIS umgestellt und ein entsprechendes Hinweissystem in der Allgemeinen Haftpflichtversicherung eingeführt werden.

Die Obersten Aufsichtsbehörden werden die daraus entstehenden Probleme noch eingehend mit der Versicherungswirtschaft erörtern.

22.2 Projektgruppe Datenschutz des Europarates

Die Beratungen der Arbeitsgruppe 14 „Versicherungswesen" der Projektgruppe Datenschutz des Europarates (vgl. 13. TB, 23.3) zur Erarbeitung einer Empfehlung zum Schutz personenbezogener Daten, die zu Versicherungszwecken erhoben und verarbeitet werden, wurden fortgeführt.

22.3 Registrierung von Versicherungsvermittlern

Im Berichtszeitraum wurden unter Bezugnahme auf die EG-Empfehlung vom 18. Dezember 1991 (vgl. zuletzt 13.TB, 23.7) mehrere Vermittlerregister gegründet. Der Hinweis auf die EG-Empfehlung durch private Stellen ist jedoch in jedem Falle als irreführend anzusehen. Die Bundesregierung, zuständig für die Benennung der registerführenden Stelle, hat es zuletzt im Mai 1995 abgelehnt, ein auf der EG-Empfehlung basierendes Vermittlerregister vorzusehen.

Aus diesem Grunde sind die Register ausschließlich an den Zulässigkeitskriterien des Bundesdatenschutzgesetzes zu messen.

Derzeit befaßt sich die Arbeitsgruppe Versicherungswirtschaft des Düsseldorfer Kreises mit einem im September 1995 gegründeten Zentralregister für Versicherungsvermittler in Deutschland, das seinen Sitz in Hamburg hat. Zwar hat die Versicherungswirtschaft erklärt, daß das Register seine Tätigkeit erst aufnehmen wird, wenn die gesetzlichen Voraussetzungen für eine zentrale Registrierung der Versicherungsvermittler vorliegen. Die den Obersten Aufsichtsbehörden bisher bekannten Unterlagen lassen jedoch eine Vielzahl noch zu erörternder Probleme erkennen.

Gründungsmitglieder des als eingetragener Verein organisierten Zentralregisters für Versicherungsvermittler sind in erster Linie der Gesamtverband der Deutschen Versicherungswirtschaft und die großen Verbände der Versicherungsvermittler, in denen die meisten der bedeutenden Unternehmen bzw. Vermittler organisiert sind.

In der Entwurfsfassung der Richtlinien wird zwar kurz dargestellt, daß es sich bei dem Register um eine Selbsthilfeeinrichtung der Versicherungswirtschaft handelt. Anschließend erfolgt jedoch eine deutliche Bezugnahme auf die Empfehlung der EG-Kommission, die aber – wie bereits dargestellt – nicht auf rein private Stellen anzuwenden ist. Darüber hinaus wird irreführenderweise behauptet, daß es sich um ein „Öffentliches Register" handelt.

Bevor Personen ihre Tätigkeit als hauptberufliche Versicherungsvermittler beginnen, sollen dem Register eine Reihe von Angaben zur Person gemacht werden. Diese Angaben sind auch zu erteilen, wenn die Tätigkeit für eine juristische Person erfolgt. Angesichts der Tatsache, daß die Eintragung als Tätigkeitsvoraussetzung bezeichnet wird und es sich um ein „Öffentliches Register" handeln soll, wird der faktische Zwang zur Angabe von Wohnort, Geburtsdatum oder -ort als sehr problematisch angesehen.

Nach der rechtlichen Konstruktion ist vorgesehen, daß der Vermittler das Zentralregister beauftragt, seine Daten weiterzugeben.

Dieser Vertrag vermittelt äußerlich den Eindruck, als habe es der Vermittler selbst in der Hand, den Auftrag zu erteilen. Rechtlich muß er selbst als „speichernde Stelle" im Sinne des Bundesdatenschutzgesetzes angesehen werden, so daß sich die Frage, ob eine gesetzliche Grundlage oder Einwilligung des Betroffenen vorliegt, formal nicht mehr stellt (siehe 1.2.2).

Die Versicherungswirtschaft gibt zwar an, niemanden zur Teilnahme an dem Register zwingen zu wollen. Eine Tätigkeit für die den Verbänden angeschlossenen Unternehmen sei gleichwohl nicht ausgeschlossen. Dies läßt sich jedoch den vorliegenden Unterlagen keineswegs entnehmen. Daher ist davon

auszugehen, daß die Eintragung in das Register – zumindest nach Ablauf einer gewissen Zeit – zur Tätigkeitsvoraussetzung wird.

Im übrigen enthält der dem Auftrag zugrunde liegende Vertrag Mängel, von deren Aufzählung an dieser Stelle abgesehen wird.

Die Gespräche mit der Versicherungswirtschaft werden fortgeführt.

22.4 Zugriff auf Versichertendaten

Parallel zu der Problematik der Zugriffsrechte der Schufa-Geschäftsstellen (vgl. 13. TB, 22.3) und der Beschränkung des Zugriffs auf Kontoinformationen (vgl. 13. TB, 26.1; s. unten 25.2) wird auch im Bereich der Versicherungswirtschaft darauf hingewirkt, den Zugriff auf Versichertendaten zu beschränken. Der einzelne Versicherungsnehmer soll frei entscheiden können, ob die Befugnis innerhalb eines Unternehmens eingeschränkt wird, seine personenbezogenen Daten aufzurufen. In Betracht kommt eine Differenzierung sowohl nach Geschäftsstellen als auch nach der Art der Daten.

Die Versicherungswirtschaft hat sich zu diesem Thema bisher nicht geäußert.

22.5 Sonstiges

Im Bereich der Versicherungswirtschaft wurden über die angesprochenen Punkte hinaus etliche Probleme erörtert, von denen lediglich einige Beispiele aufgezeigt werden sollen:

- Einführung der neuen Einwilligungs-Erklärung, insbesondere die Behandlung von Altverträgen
- Private Krankenversicherung mit dem zentralen Problem der Chipkarte im Gesundheitswesen (vgl. 19.1)
- Umstellung des Verfahrens bei der Versichererwechselbescheinigung.

23. Handels- und Wirtschaftsauskunfteien

23.1 Telefonisches Auskunftsverfahren

Der Verband der Handelsauskunfteien teilte mit, daß in den Auskunftsprotokollen der drei großen Auskunfteien der Name des telefonisch Anfragenden erfaßt wird. Bei einer Auskunftei sei es auch möglich, Kennwörter für die Identifizierung von telefonisch Anfragenden zu vergeben. Mögliche Mißbräuche können mit der so praktizierten Verfahrensweise aufgedeckt werden (vgl. zuletzt 12. TB, 25.1.4).

23.2 Nachmeldungen

Unsere Zweifel an der Zulässigkeit des Verfahrens, bei dem Negativdaten von den Handelsauskunfteien ohne weitere konkrete Anfrage 6 Monate nach der

ersten Auskunft nachgemeldet werden (vgl. 12. TB, 25.2.5; 13. TB, 24.4), bestehen weiter. Die Erörterung mit dem Verband der Handelsauskunfteien ist noch nicht abgeschlossen.

24. Versandhandel

24.1 Warndatei

Wie berichtet (13. TB, 25.1), führt ein Versandhandelsunternehmen in Hamburg eine firmenübergreifende Warndatei, in der negative Daten über Kaufinteressenten und Kunden vorgehalten werden. Der vorgesehene Abstimmungsprozeß im Kreis der Obersten Aufsichtsbehörden für den Datenschutz über die rechtliche Einordnung der Angelegenheit erfolgte im Oktober 1995.

Die Arbeitsgruppe Versandhandel des Düsseldorfer Kreises kam dabei zu dem Ergebnis, daß die Tätigkeit des Versandhauses als geschäftsmäßiges Speichern zum Zwecke der Übermittlung anzusehen ist. Die Zulässigkeit einer solchen Datenverarbeitung richtet sich nach § 29 BDSG. Überdies hat das Unternehmen die Meldepflicht nach § 32 Abs. 1 Nr. 1 BDSG zu beachten. Weil die angeschlossenen Versandhäuser im Online-Verfahren auf die Datei zugreifen können, haben die beteiligten Stellen besondere Festlegungen nach § 10 BDSG zu treffen. Die Aufsichtsbehörde wird auf dieser Grundlage die Gespräche mit dem dateiführenden Versandhaus in Hamburg wieder aufnehmen und dabei die rechtlichen Möglichkeiten wahrnehmen.

Das Unternehmen vertritt dagegen weiterhin die Auffassung, daß nicht § 29 BDSG, sondern § 28 BDSG für die Datenübermittlung an die im Konzern verbundenen Unternehmen maßgeblich ist. Diese Auffassung trifft jedoch nicht zu, weil das BDSG keine Konzernklausel kennt, sondern formalrechtlich von der Selbständigkeit der einzelnen Unternehmen ausgeht; dies ist in Rechtsprechung und Literatur unstreitig.

Darüber hinaus müssen die Betroffenen rechtzeitig in geeigneter Weise über die Existenz der Warndatei unterrichtet werden. Die Information soll aus Gründen der Transparenz so rechtzeitig erfolgen, daß der einzelne Kunde vor der Abgabe einer Bestellung entscheiden kann, ob er lieber per Nachnahme bestellt, um damit einer Aufnahme in die Warndatei zu entgehen. Das Versandhandelsunternehmen hält es dagegen bisher für ausreichend, den Kunden zu unterrichten, sofern dessen Bestellung nicht angenommen wird.

Erkenntnisse über die Existenz solcher firmenübergreifender Warndateien im Versandhandel liegen im übrigen bei anderen Aufsichtsbehörden noch nicht vor. Insoweit werden die Ergebnisse unserer Verhandlungen auch bundesweit Beachtung finden. Über den Fortgang des Verfahrens werden wir uns im nächsten Tätigkeitsbericht äußern.

25. Kreditwirtschaft

25.1 Kartengestützte Zahlungsverfahren

Im November 1995 hat der Zentrale Kreditausschuß (ZKA) bei einer Informationsveranstaltung den Obersten Aufsichtsbehörden das Vorhaben „elektronische Geldbörse" vorgestellt (vgl. 13. TB, 26.2.1). Die elektronische Geldbörse auf der EC-Karte ist als vorausbezahlte Börse konzipiert. Der maximale Ladebetrag der Geldbörse beträgt 400 DM. Bezahlt werden soll damit in möglichst vielen Lebensbereichen. An dem Pilotprojekt, das ab Januar 1996 im Raum Ravensburg geplant ist, sollen neben 500 Händlern auch Parkhäuser und die Regionalbahn teilnehmen.

Beim Kauf mit der elektronischen Geldbörse wird im Händlerterminal ein Datensatz gespeichert, der Kaufdatum und Betrag enthält sowie ein weiteres Datum, aus dem sich die Kartennummer der Käuferkarte und die Nummer der Händlerkarte erzeugen läßt. Zur Abwicklung des Zahlungsverkehrs werden die Einzeltransaktionsdatensätze von den Händlern gesammelt und an die jeweils zuständige Evidenzstelle weitergegeben. Die Evidenzstelle kontrolliert und aggregiert die entgegengenommenen Beträge und leitet sie über Verrechnungsbanken an die zuständigen Kunden- und Händlerbanken weiter.

Die bei den Evidenzstellen entgegengenommenen Einzeltransaktionsdatensätze werden dort auf Magnetbänder gespeichert. Zusammen mit der Kundenbank ist die Evidenzstelle in der Lage, den Personenbezug der Transaktionsdaten herzustellen. In Reklamationsfällen ist so grundsätzlich eine eindeutige Klärung und gegebenenfalls Erstattung von Beträgen möglich.

Die Datenverarbeitung bei der Zahlungsabwicklung ist nach dem BDSG zu beurteilen. Gemäß den Angaben des ZKA können die von den Börsenevidenzzentralen verarbeiteten anonymisierten Daten nur mit erheblichem Aufwand einem bestimmten Kunden zugeordnet werden. Nach seiner Auffassung sind die Daten während des Übermittlungsvorganges von der Händlerstation bis zum Kreditinstitut nicht personenbezogen. Bei der gebotenen Gesamtbetrachtung des Systems sind und bleiben die bei der Zahlung anfallenden Transaktionsdaten aber personenbezogene Daten gem. § 3 Abs.1 i.V.m. Abs. 7 BDSG. Eine Zuordnung der Daten zu einer bestimmten natürlichen Person ist bei Zusammenwirken der Evidenzstellen, Verrechnungsbanken und Kundenbanken ohne großen Aufwand möglich und für Reklamations- und Verlustfälle auch vorgesehen. Die Datenverarbeitung bei der Zahlungsabwicklung kann allerdings nach § 28 Abs.1 Satz 1 Nummer 1 BDSG nicht als unzulässig angesehen werden.

Das Verfahren ist jedoch datenschutzrechtlich problematisch. Die Zahlungsabwicklung erfolgt insgesamt nicht anonym. Bei den Börsenevidenzstellen werden personenbezogene Daten in sogenannten Schattenkonten gespeichert, die transaktionsbezogen Auskunft über sämtliche Umsätze geben. Damit entstehen umfangreiche Datensammlungen über den Kauf von kleineren Konsumgütern, die zu Kundenprofilen verdichtet werden können und für die werbende Wirtschaft von Interesse sind. Auch Bewegungsprofile können erstellt werden. Der datenfreie Raum, in dem sich der Bürger ohne Hinterlassen von elektronischen Spuren unbeobachtet verhalten und bewegen kann, wird immer kleiner.

Die Datenschutzbeauftragten des Bundes und der Länder haber daher in ihrer Entschließung vom 13. Oktober 1995 zum Datenschutz bei elektronischen Geldbörsen den Einsatz von kartengestützten Zahlungsverfahren gefordert, die ohne personenbezogene Daten auskommen und daher datenschutzfreundlicher sind. In Betracht kommen sogenannte White-Cards, bei denen das Zahlungsverfahren anonym abgewickelt wird. Es handelt sich dabei um kontounabhängige Börsenkarten, die nach den Vorstellungen des ZKA aber nur für bestimmte Zielgruppen ohne Konto, z. B. Jugendliche oder Touristen, angeboten werden sollen. Aus Datenschutzgründen sollten White-Cards jedoch als echte Alternative zur geplanten Geldbörse ohne Beschränkung auf einen bestimmten Personenkreis und ohne zusätzliche Gebühren eingeführt werden.

Der Hamburgische Datenschutzbeauftragte wird sich auch künftig dafür einsetzen, daß wirklich anonyme kartengestützte Zahlungsverfahren zumindest als Alternative zu den personenbezogenen Zahlungsverfahren entwickelt und eingesetzt werden.

25.2 Beschränkung des Zugriffs auf Kontoinformationen

Zur Frage der Beschränkung des bankinternen Zugriffs auf bestimmte Zweigstellen bei entsprechendem Kundenwunsch (vgl. 13. TB, 26.1) erklärten sich Vertreter der Kreditwirtschaft bereit, die Anregung der Obersten Aufsichtsbehörden zu überprüfen. Die Diskussion hierüber wird fortgeführt werden.

26. Die neue BahnCard

In Zusammenarbeit mit der Citi Bank führte die Deutsche Bahn AG die neue BahnCard mit Kreditkartenfunktion zum 1. Juli 1995 ein. Durch die an die Kunden der Bahn ausgegebenen Antragsformulare wurde die Aufsichtsbehörde Hamburg auf gravierende datenschutzrechtliche Probleme aufmerksam.

In dem Antragsformular wurden den Kunden zahlreiche Informationen über ihr Privatleben unabhängig davon abverlangt, ob sie die BahnCard mit einer Kreditkarte oder mit einer Guthabenkarte (sog. Electronkarte) oder eine BahnCard ohne diese Zusatzfunktion haben wollten. Das Formular enthielt zahlreiche Fragen nach den Familienverhältnissen (bis hin zur Zahl der unterhaltsberechtigten Kinder), den Wohnverhältnissen (Miete, Eigentum oder „wohnhaft bei

den Eltern"), dem Monatseinkommen (je 1 000,– DM gestaffelt) und dem Beruf (einschließlich Angabe der früheren Beschäftigungsdauer).

Nach § 28 Abs. 1 Satz 1 Nummer 1 BDSG ist das Speichern oder Nutzen personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke im Rahmen der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen zulässig. Nach § 28 Abs. 1 Satz 2 BDSG müssen die Daten aber nach Treu und Glauben und auf rechtmäßige Weise erhoben werden. Aus diesen Vorschriften geht hervor, daß personenbezogene Daten nur insoweit erhoben und gespeichert werden dürfen, als sie zur Vertragseingehung und -erfüllung notwendig sind. Für die Ausstellung der BahnCard ohne Kreditkartenfunktion reicht die Angabe von Namen und Anschrift. Die Erhebung und Bearbeitung von weiteren personenbezogenen Daten ist in diesem Fall nach § 28 BDSG unzulässig.

Zur Abwicklung eines Kreditkarten-Vertrags sind mehr Angaben des Kunden als bei der reinen BahnCard erforderlich, da dem Kartenherausgeber eine Bonitätsprüfung des Antragsstellers möglich sein muß. Fragen nach den Familienverhältnissen, den Wohnverhältnissen und der früheren Beschäftigungsdauer sind aber auch in Kreditkarten-Anträgen unzulässig, da sie keine Rückschlüsse auf die Bonität zulassen.

Datenschutzrechtlich bedenklich war ferner, daß die zum Teil unzulässig erhobenen Daten von der Bahn an die Citi Bank AG und deren Rechenzentren in den USA ohne entsprechende Sicherheitsvorkehrungen übermittelt wurden. Ferner sollten die Daten bei Zustimmung der Kunden für Telefonwerbung verwendet werden. Auch bei Zustimmung bestanden Zweifel an der Zulässigkeit der Telefonwerbung, da der Kunde auf dem Formular nicht überblicken konnte, für welche „Beauftragten" der Bahn und der Bank die Einwilligung zur Telefonwerbung überhaupt gelten sollte.

Für datenschutzrechtlich bedenklich hielten wir außerdem die unklare Beschreibung der Electronkarte auf dem Antragsformular. Die Kunden konnten nicht deutlich entnehmen, daß bei der Benutzung der Electronkarte ebenso wie bei der Kreditkarte ein Bewegungsprofil mit den gebuchten einzelnen Reisen einschließlich Datum usw. anhand der Kontoauszüge entsteht. Die Electronkarte ist keineswegs eine Guthabenkarte ohne Kontoverbindung ähnlich wie die Telefonkarte, von der nur die bezahlten Beträge abgebucht werden. Vielmehr werden die Forderungen der Bank aus der Verwendung der Electron-Zahlungsfunktion der BahnCard mit dem Guthaben auf dem Electron-Kartenkonto taggleich verrechnet.

Die Aufsichtsbehörde Hamburg hat zusammen mit den Aufsichtsbehörden Bremen und Niedersachsen die dargestellten datenschutzrechtlichen Einwände gegen die Antragsformulare gegenüber der Deutschen Bahn AG geltend gemacht. Die massiven Datenschutzprobleme und unsere Forderungen wurden wegen der Bedeutung für eine große Zahl von Bürgern öffentlich vertreten. Innerhalb weniger Tage war die Deutsche Bahn AG daraufhin zu grundsätzlichen Verbesserungen bereit. Da seit August 1995 der Berliner Datenschutzbeauftragte für die Kontrolle der Deutschen Bahn AG örtlich zuständig ist, wurde die rechtliche Auseinandersetzung mit der Bahn AG von dort weitergeführt. Nach Verhandlungen zwischen dem Berliner Datenschutzbeauftragten, der Bahn AG und der Citi Bank sind in den erneuerten Antragsformularen für die BahnCard nun Wahlmöglichkeiten zwischen den verschiedenen Varianten der BahnCard vorgesehen. Unzulässige Fragen – insbesondere bei der BahnCard ohne Kreditkartenfunktion – werden nicht mehr gestellt. Auf den auf der Rückseite der Formulare abgedruckten allgemeinen Geschäftsbedingungen wird nunmehr das BahnCard-Verfahren besser dargestellt und für den Kunden etwas transparenter.

Für die Verarbeitung der Antragsdaten in den US-Staaten Nevada und South Dakota, wo für Privatunternehmen keine Datenschutzgesetze existieren, wurde vertraglich abgesichert, daß der Standard des Bundesdatenschutzgesetzes für die Datenverarbeitung in den USA maßgeblich ist. Über den Inhalt des Vertrages muß allerdings noch weiter verhandelt werden.

Auch nach Veränderung des Formulars bleiben aus Datenschutzgesichtspunkten Wünsche offen. Kundenfreundlicher und übersichtlicher wären getrennte Anträge für jede Version der BahnCard. Wünschenswert wäre auch eine noch klarere Abfassung der allgemeinen Geschäftsbedingungen zum gesamten Antrags- und Abrechnungsverfahren.

27. Videoüberwachung in der Wirtschaft

Im Anschluß an unsere letzte Berichterstattung (13. TB, 28.1) hat die Aufsichtsbehörde festgestellt, daß immer mehr Lebensbereiche mit Videokameras überwacht werden. Mittlerweile werden die Bürger nicht nur in Warenhäusern und Kreditinstituten elektronisch beobachtet, sondern geraten zunehmend auch in Bahnhöfen, Parkhäusern, Sporteinrichtungen, Treppenhäusern, Fahrstühlen und Taxis sowie auf öffentlichen Wegen in das Blickfeld elektronischer Augen.

Auf dem eigenen Grundstück ist eine derartige Überwachung aufgrund des Hausrechts zwar grundsätzlich zulässig, wenn sie zur Wahrung überwiegender berechtigter Interessen des Eigentümers erforderlich ist. Der Bundesgerichtshof hat aber mit Urteil vom 25. April 1995 festgestellt, daß eine private Überwachung durch Videoaufzeichnungen auf öffentlichen Wegen einen unzulässigen Eingriff in das Persönlichkeitsrecht des Betroffenen darstellen kann. Ob ein solcher Eingriff gerechtfertigt sei, z. B. um schwerwiegenden Gefahren durch die Überwachung zu begegnen, könne nur anhand der Würdigung aller Umstände des Einzelfalls und durch Vornahme einer Abwägung der verfassungsrechtlich geschützten Positionen der Beteiligten ermittelt werden.

Die Aufsichtsbehörde hat ergänzend die private Videoüberwachung öffentlicher Wege unter dem Gesichtspunkt des Anliegergebrauchs im wegerechtlichen Sinne mit der Baubehörde geklärt. Dabei hat sich ergeben, daß der öffentliche Weg dadurch in Anspruch genommen wird, daß eine Videokamera über öffentlichem Grund – beispielsweise an einer Hauswand – montiert wird. Hierbei handelt es sich nach Auffassung der Baubehörde um eine den Anliegergebrauch überschreitende Sondernutzung, da der Gemeingebrauch an der Stelle, an der die Kamera befestigt ist, dauernd ausgeschlossen ist. Eine solche Sondernutzung bedarf einer wegerechtlichen Genehmigung, die versagt werden kann, wenn die vorgesehene Sondernutzung gegen datenschutzrechtliche Vorschriften verstoßen würde.

Dagegen stellt die Videoerfassung öffentlicher Verkehrsflächen mit Kameras, die außerhalb des Verkehrsraums errichtet sind, keine Wegebenutzung dar und wird deshalb auch weder von den Vorschriften über den Anliegergebrauch noch von den Vorschriften über die Sondernutzung öffentlicher Wege erfaßt.

Die Aufsichtsbehörde wird die von der Baubehörde vertretene Rechtsauffassung bei Beratungsgesprächen mit Bürgern und Unternehmen berücksichtigen. Die Bestimmungen des BDSG sind allerdings häufig nicht auf die Videoüberwachung anzuwenden, weil die Aufzeichnungen in aller Regel nicht den Dateibegriff des BDSG erfüllen. Dann hat die Aufsichtsbehörde keine rechtliche Möglichkeit, den Einsatz von Videosystemen in der gewerblichen Wirtschaft zu kontrollieren. Die Betroffenen müssen in diesen Fällen ihr Persönlichkeitsrecht selbst – gegebenenfalls gerichtlich – durchsetzen.

Selbstverständlich kann die Videoüberwachung durchaus ein geeignetes Mittel sein, Gefahren zu begegnen und insbesondere Straftaten zu verhindern oder zumindest deren Aufklärung zu erleichtern. Die Videoaufnahmen sind dann jedoch kurzfristig darauf zu überprüfen, ob sie zur Gefahrenabwehr oder Strafverfolgung weiter benötigt werden; alle anderen Aufzeichnungen sind zu löschen.

Dennoch bleibt es dabei, daß private Stellen grundsätzlich die Bürger allenfalls klar erkennbar und nicht mit heimlichen Videoaufnahmen durch versteckte Kameras überwachen dürfen. Sie haben jeweils deutlich auf die Videoüberwachung z. B. durch Aufkleber aufmerksam zu machen oder zumindest die Kameras gut sichtbar anzubringen.

28. Workshop der Aufsichtsbehörden für den Datenschutz

Am 21. und 22. September 1995 fand der erste gemeinsame Workshop der Aufsichtsbehörden für den Datenschutz in Hamburg statt. Ziel des Workshops war es, eine Verbesserung der Zusammenarbeit der Aufsichtsbehörden zu erreichen. Es wurde erörtert, wie eine Kooperation künftig aussehen und realisiert werden könnte. Weiterhin sollten auch die Probleme der verschiedenen Aufsichtsbehörden in der täglichen Arbeit besprochen werden.

Alle Teilnehmer stimmten darin überein, daß zukünftig die Zusammenarbeit der Aufsichtsbehörden auch länderübergreifend zu intensivieren ist. Insbesondere aus den neuen Bundesländern kam der Wunsch, bei Einzelproblemen Unterstützung durch andere Aufsichtsbehörden zu erhalten.

Zur möglichen Organisation eines Informationsaustausches zwischen den Aufsichtsbehörden wurde beispielsweise angeregt, eine „Infobörse", eventuell unter Nutzung elektronischer Verbreitungsmöglichkeiten, anzulegen. Auch könnten sich einzelne Aufsichtsbehörden auf ein Thema spezialisieren und sodann den anderen Aufsichtsbehörden als kompetenter Ansprechpartner zur Verfügung stehen. Bei der Prüfung von bundesweit tätigen Unternehmen und bei Anordnungen gegenüber diesen Unternehmen wurde eine Koordinierung zwischen den einzelnen Aufsichtsbehörden für sinnvoll gehalten. Ziel müsse jedenfalls eine einheitliche Vorgehensweise sein, wobei das nunmehr erfolgte persönliche Kennenlernen sicherlich sehr hilfreich sein wird.

Daneben standen weitere Diskussionsthemen auf der Tagesordnung:

- Allgemeine Prüferfahrungen,
- Befugnisse der Aufsichtsbehörden,
- Speicherungen zum Zwecke der Übermittlung,
- Beschwerden von Bürgern und Abgrenzung zum BDSG,
- Technische und organisatorische Anforderungen.

Insgesamt wurde die Durchführung des Workshops von allen Teilnehmern als Bereicherung angesehen und eine Fortsetzung gewünscht. Der Landesbeauftragte für den Datenschutz Niedersachsen erklärte sich bereit, den nächsten Workshop voraussichtlich im Sommer 1996 zu veranstalten.

29. Register nach § 32 BDSG und Prüftätigkeit

29.1 Register und Meldepflicht

Die Aufsichtsbehörde führt nach § 38 Abs. 2 BDSG ein Register der Stellen, die personenbezogene Daten geschäftsmäßig zum Zwecke der personenbezogenen oder der anonymisierten Übermittlung speichern oder im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen. Diese Stellen unterliegen nach § 32 BDSG der Meldepflicht. Derzeit sind zu diesem Register 195 Unternehmen gemeldet. Unterteilt nach der Art der meldepflichtigen Tätigkeit ergibt sich folgendes Bild:

Speicherung zum Zwecke der Übermittlung
Auskunfteien/Warndienste 14
Direktmarketing/Adreßhändler 14

Speicherung zum Zwecke der anonymisierten Übermittlung
Markt- und Meinungsforschung 10

Auftragsdatenverarbeitung
Servicerechenzentren 24
Akten- und Datenträgervernichter 13
Mikroverfilmer 6
Datenerfasser 25
Mailboxen 3
sonst. Auftragsdatenverarbeitung 86

29.2 Prüfungen

Der folgenden Übersicht sind die Zahlen der Überprüfungen im Berichtszeitraum zu entnehmen, die gemäß § 38 Abs. 2 BDSG regelmäßig vor Ort stattfinden:

Auskunfteien/Warndienste 4
Direktmarketing/Adreßhändler 4
Markt- und Meinungsforschung 6
Servicerechenzentren 9
Akten- und Datenträgervernichter 1
Mikroverfilmer 2
Datenerfasser 7
sonstige Auftragsdatenverarbeitung 10
gesamt 43

Im Rahmen der Anlaßaufsicht nach § 38 Abs. 1 BDSG wurden außerdem wieder viele Unternehmen insbesondere aufgrund von Eingaben geprüft.

Geschäftsverteilung (Stand: 15. Dezember 1995)

Der Hamburgische Datenschutzbeauftragte
Baumwall 7, 20459 Hamburg

Tel.: 040/3504-2044
BN: 9.41-2044
Fax: 040/3504-2372

			Durchwahl
Dienststellenleiter:	Dr. Hans-Hermann Schrader	D	–2044–
Stellvertreter:	Peter Schaar		–2231–
Vorzimmer:	Heidi Passow		–2045–

D 1 – Geschäftsstelle

			Durchwahl
Leiter:	Gunnar Hansen	D 1	–2223–
Sachbearbeiterin:	Annelies Franke	D 10	–2063–
Mitarbeiterinnen:	Heidi Passow	D 11	–2045–
	Irene Heinsohn	D 12	–2047–

D 1: Allgemeine Verwaltungsangelegenheiten
Betreuung der Tätigkeitsberichte
Öffentlichkeitsarbeit
Geheimschutzangelegenheiten
(s. a. Referate D 2 und D 3)

D 10: Systemverwaltung
Bibliothek
Register nach § 24 HmbDSG
Verwaltung und Bearbeitung von Eingaben
Verwaltung von Senats-/Bürgerschaftsdrucksachen
Betreuung von Veranstaltungen

D 11: Vorzimmerdienst
Posteingang
Textverarbeitung

D 12: Registratur
Postausgang
PC-Textverarbeitung

D 2 – Referat

			Durchwahl
Leiter:	Dr. Harald Wollweber	D 2	–2046–
Sachbearbeiter:	Gunnar Hansen	D 1	–2223–

D 2: Grundsatzfragen des Datenschutzrechts
Datenschutzgesetze
Parlamentsangelegenheiten
Justiz

Strafvollzug
Verfassungsschutz
Meldewesen
Ausweis- und Paßangelegenheiten
Ausländerwesen
Ausbildungsleiter für die Juristenausbildung

D 1: Personenstandswesen

D 3 – Referat Durchwahl

Leiter:	Ulrich Werner	D 3	–2581–
Sachbearbeiter:	Gunnar Hansen	D 1	–2223–

D 3: Polizei und Feuerwehr
Staatsanwaltschaft
Straßenverkehrsverwaltung
Verkehrsordnungswidrigkeiten

D 1: Bau-, Vermessungs- und Wohnungswesen
Stadtentwicklung

D 4 – Referat Durchwahl

Leiter:	Dr. Hans-Joachim Menzel	D 4	–2558–
Sachbearbeiter:	Achim Kruppke	D 41	–2563–

D 4: Gesundheitswesen mit medizinischer Forschung (öffentlicher und nicht-öffentlicher Bereich)
Kultur

D 41: Soziales
Arbeitsschutz

D 5 – Referat Durchwahl

Leiterin:	Annette Husten	D 5	–2562–
Sachbearbeiter:	Achim Kruppke	D 51	–2563–

D 5: Personalwesen, Gleichstellung
Archivwesen
Wirtschaftschaftsverwaltung und Landwirtschaft

D 51: Hochschule, Schule und Berufsbildung

D 6 – Referat Durchwahl

Leiter:	Peter Schaar	D 6	–2231–
Sachbearbeiter:	Dietmar Nadler	D 61	–2236–

D 6: IuK-Beauftragter
Grundsatzfragen der IuK-Technik und -Organisation
- Telekommunikation
- Online-Datenbanken

Datenschutzrechtliche Betreuung und technisch-organisatorische Beratungs- und Prüftätigkeit für die Bereiche
- Statistik
- Wahlen
- Medien
- Natur- und Umweltschutz

Technisch-organisatorische Beratungs- und Prüftätigkeit für die Bereiche
- Meldewesen
- Ausweis- und Paßangelegenheiten
- Ausländerwesen
- Personalwesen, Gleichstellung
- Personenstandswesen
- Hochschule
- Justiz (außer Staatsanwaltschaft)
- Strafvollzug
- Verfassungsschutz
- Kultur
- nicht-öffentlicher Bereich für die genannten IuK-Techniken

D 61: IuK-Leitung für die Dienststelle
Grundsatzfragen der IuK-Technik und -Organisation bei
- Großrechnern/Rechenzentren
- Archivierung auf analogen und digitalen Datenträgern

Datenschutzrechtliche Betreuung und technisch-organisatorische Beratungs- und Prüftätigkeit für die Bereiche
- Finanz-, Steuer- und Rechnungswesen
- allgemeine Senatsangelegenheiten
- zentrale Informationstechnik (LIT)

Technisch-organisatorische Beratungs- und Prüftätigkeit für die Bereiche
- Parlamentsangelegenheiten
- Bau-, Vermessungs- und Wohnungswesen
- Stadtentwicklung
- Archivwesen
- Polizei und Feuerwehr
- Staatsanwaltschaft
- Straßenverkehrsverwaltung
- Verkehrsordnungswidrigkeiten
- nicht-öffentlicher Bereich für die genannten IuK-Techniken

D 7-Referat Durchwahl

Leiter:	Dr. Uwe Schläger	D 7-1	–2564–
	Ulrich Kühn	D 7-2	–2564–

D 7-1: Grundsatzfragen der IuK-Technik und -Organisation, insbesondere
- Bewertung technischer Methoden, Verfahren und Produkte im IuK-Bereich, insbesondere des Bereichs Arbeitsplatzrechner und deren Vernetzung (PC-Technik)
- Entwicklung von Datensicherheitskonzepten
- Analyse von datenschutzrelevanten Schlüsseltechniken in den Informations- und Kommunikationstechniken, insbesondere Chipkarten
- Bewertung datenschutzrechtlicher Aspekte komplexer DV-Systeme und deren Vernetzung
- Weiterentwicklung von Methoden, Verfahren und dv-gestützter Hilfsmitteln für datenschutz-technische Prüfungen
- Kontakte zu Hochschulen und anderen Forschungseinrichtungen
- Richtlinien zur Datensicherung und Datenverarbeitung für die genannten IuK-Techniken

Technisch-organisatorische Beratungs- und Prüftätigkeit für die Bereiche
- Gesundheitswesen mit medizinischer Forschung
- Soziales
- Arbeitsschutz
- nicht-öffentlicher Bereich für die genannten IuK-Techniken

D 7-2: Grundsatzfragen der IuK-Technik und -Organisation, insbesondere
- Bewertung technischer Methoden, Verfahren und Produkte im IuK-Bereich, insbesondere des Bereichs Abteilungsrechner und deren Vernetzung (UNIX-Technik)
- Entwicklung von Datensicherheitskonzepten
- Analyse von datenschutzrelevanten Schlüsseltechniken in den Informations- und Kommunikationstechniken, insbesondere Verschlüsselungstechnik
- Bewertung datenschutzrechtlicher Aspekte komplexer DV-Systeme und deren Vernetzung
- Weiterentwicklung von Methoden, Verfahren und dv-gestützter Hilfsmitteln für datenschutz-technische Prüfungen
- Kontakte zu Hochschulen und anderen Forschungseinrichtungen
- Richtlinien zur Datensicherung und Datenverarbeitung für die genannten IuK-Techniken

Technisch-organisatorische Beratungs- und Prüftätigkeit für die Bereiche
- Wirtschaftsverwaltung, Landwirtschaft
- Bezirksangelegenheiten
- Schule und Berufsbildung
- nicht-öffentlicher Bereich für die genannten IuK-Techniken

Betreuung der IuK-Trainee-Kräfte

D 8 – Referat Durchwahl

Leiterinnen:	Helga Naujok	D 8-1	–2556–
	Elisabeth Duhr	D 8-2	–2541–
Referent:	Detlef Malessa	D 80	–2089–
Sachbearbeiterin:	Evelyn Seiffert	D 81	–2468–

Aufsichtsbehörde nach §§ 38 Bundesdatenschutzgesetz

D 8-1: Versicherungswirtschaft einschließlich Vorsitz in der Arbeitsgruppe Versicherungswirtschaft der Aufsichtsbehörden
Allfinanz-Gruppen
Handel, Industrie
Düsseldorfer Kreis der Aufsichtsbehörden

D 8-2: Auskunfteien, Wirtschafts- und Handelsauskunfteien
SCHUFA
Kreditwirtschaft
Internationaler Datenverkehr im öffentlichen und nicht-öffentlichen Bereich, insbesondere Datenschutzrecht der Europäischen Gemeinschaften

D 80: Versandhandel
Werbung und Adreßhandel
Bauen und Wohnen, insbesondere Mietangelegenheiten
Transport und Verkehr einschließlich HVV
Freie Berufe und gewerbliche Dienstleistungen
Videoüberwachung in der Wirtschaft
Sonstige Rechtsfragen zum Datenschutz in der Wirtschaft
Kirchen

D 81: Auftragsdatenverarbeitung
Markt- und Meinungsforschung
Datenbankbetreiber und Netzanbieter (mit D 6)
Bildschirmtext und Mailboxen (mit D 6)
Allgemeine Beratung von betrieblichen Datenschutzbeauftragten
Grundsätzliche Fragen zum Register nach §§ 32 BDSG
Mikroverfilmung
Akten- und Datenträgervernichtung

Stichwortverzeichnis

Veröffentlichungen zum Datenschutz

Beim Hamburgischen Datenschutzbeauftragten sind derzeit folgende Veröffentlichungen kostenlos erhältlich:

Broschüren

Datenschutzkonzept für UNIX-Mehrplatzanlagen
Datenschutz in Netzen
Datenschutz in der Arztpraxis
Mobilfunk und Datenschutz

Berichte und Dokumente

Bericht über den Datenschutz bei Automation und Vernetzung der hamburgischen Verwaltung – IuK-Datenschutzbericht –

Informationsblätter

Tips zum Adressenhandel
Datenschutz im privaten Bereich
Die Gesundheits-Chipkarte

Internet

Weitere Informationen des Hamburgischen Datenschutzbeauftragten über
- Tätigkeitsberichte
- Presseerklärungen
- Datenschutzgesetze
- Broschüren (siehe oben)

können auch unter folgender Adresse abgerufen werden:
„http://www.rewi.hu-berlin.de/Datenschutz/DSB/HmbDSB/"