BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG

11. Wahlperiode

Drucksache 11/50

05.01.83

Der Hamburgische Datenschutzbeauftragte

An den
Herrn Präsidenten der Bürgerschaft

Betr.: Erster Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten zum 1. Januar 1983

Gemäß § 20 Absatz 2 Satz 2 des Hamburgischen Datenschutzgesetzes übersende ich der Bürgerschaft meinen Ersten Tätigkeitsbericht, den ich zum 1. Januar 1983 erstellt habe.*

Dem Senat leite ich meinen Tätigkeitsbericht gleichzeitig zu.

Schapper

* Verteilt nur an die Abgeordneten der Bürgerschaft

Bürgerschaftsdrucksachen — außer Senatsvorlagen — sind zu beziehen bei:
Druckerei Wartenberg & Söhne GmbH, Theodorstraße 41 w, 2000 Hamburg 50, Telefon 89 39 48

Erster Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten

vorgelegt zum 1. Januar 1983
gemäß § 20 Absatz 2 Satz 2 des Hamburgischen Datenschutzgesetzes

Inhaltsverzeichnis

1. Vorwort

Das Hamburgische Datenschutzgesetz bestimmt in § 20 Abs. 2 S. 2*), daß der Hamburgische Datenschutzbeauftragte (DSB) jährlich zum 1. Januar Senat und Bürgerschaft einen Tätigkeitsbericht zu erstatten hat. Die Berichtspflicht des DSB ist auf den Anwendungsbereich des Hamburgischen Datenschutzgesetzes beschränkt, das die Verarbeitung personenbezogener Daten durch die hamburgische Verwaltung regelt. Dem Hamburgischen Datenschutzbeauftragten sind aber auch die Aufgaben der Aufsichtsbehörde nach §§ 30/40 Bundesdatenschutzgesetz (BDSG) übertragen. Meines Erachtens liegt es im Interesse der Bürgerschaft, des Senats und auch der Öffentlichkeit, wenn ich über den gesetzlichen Auftrag hinaus in meinem Tätigkeitsbericht auch auf den Datenschutz im nicht-öffentlichen Bereich eingehe; denn erst die Zusammenfassung beider Kontrollfunktionen, der des Landesbeauftragten im öffentlichen Bereich und der der Aufsichtsbehörde im nicht-öffentlichen Bereich, ergibt ein vollständiges Bild des Datenschutzes in der Freien und Hansestadt Hamburg und der Tätigkeit des Hamburgischen Datenschutzbeauftragten.

Der erste Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten betrifft das Jahr 1982. Es ist jedoch zu berücksichtigen,

- daß ich mein Amt erst am 10. Mai 1982 angetreten habe,
- daß die ersten Monate der Amtsführung mit der technischen und organisatorischen Einrichtung der Dienststelle weitgehend ausgefüllt waren,
- daß vor allem der personelle Aufbau sich nicht ohne Schwierigkeiten und – teilweise erhebliche – zeitliche Verzögerungen vollzogen hat,
- daß die Arbeit am Bericht aus technischen Gründen am 20. November 1982 abgeschlossen sein mußte.

Der vorgelegte Bericht umfaßt mithin nur einen Zeitraum von etwa 6 Monaten. Seine Aufgabe besteht weniger darin, Rechenschaft abzulegen über die bisher geleistete Arbeit. Wichtiger erscheint es mir, Bürgerschaft und Senat über die rechtliche und organisatorische Situation des Datenschutzes in Hamburg zu unterrichten, ihnen aktuelle Probleme vor Augen zu führen und – soweit möglich – auf Verbesserungsmöglichkeiten hinzuweisen. Zugleich sollen Inhalt und Zielsetzung meiner künftigen Arbeit dargestellt werden. Naturgemäß konnten im Berichtszeitraum nicht alle aufgegriffenen Hinweise abschließend behandelt werden. Der Bericht enthält auch Vorgänge, deren Erledigung noch aussteht.

2. Rechtliche Grundlagen

2.1 Entstehungsgeschichte und Besonderheiten des Hamburgischen Datenschutzgesetzes

Seit dem 1. Januar 1979 ist das BDSG mit allen Bestimmungen in Kraft. Seine wesentlichen Vorschriften waren schon seit dem 1. Januar 1978 anzuwenden.

Nach § 7 Abs. 2 BDSG erlangte das Datenschutzrecht des Bundes mit Ausnahme der §§ 15 – 21 (Durchführung des Datenschutzes, Bestimmungen über den Bundesbeauftragten) auch Gültigkeit für die Behörden und sonstigen öffentlichen Stellen der Freien und Hansestadt Hamburg sowie aller ihrer Aufsicht unterstehenden juristischen Personen des öffentlichen Rechts, soweit sie Bundesrecht ausführen. Diese besondere Situation – nur ein Teil der öffentlichen Stellen in Hamburg und diese auch nur bezogen auf bestimmte Aufgaben waren dem allgemeinen Datenschutzrecht unterworfen – endete erst mit dem Inkrafttreten des Hamburgischen Datenschutzgesetzes am 1. Mai 1981. Von diesem Zeitpunkt an gilt in Hamburg für alle öffentlichen Stellen dasselbe Datenschutzrecht – und dies auch für die Ausführung von Bundesrecht.

*) Paragraphenangaben ohne Zusatz beziehen sich auf das Hamburgische Datenschutzgesetz (HmbDSG)

Die Freie und Hansestadt Hamburg ist das letzte Bundesland, das – sogar mit mehreren Jahren Abstand von den anderen – ein eigenes Datenschutzgesetz verabschiedet hat. Doch ist diese Verzögerung nicht damit zu erklären, daß der Gesetzgeber hier lange Zeit untätig geblieben ist. Sie zeigt vielmehr, daß – schon bei der Vorbereitung des Gesetzentwurfes durch den Senat, aber erst recht bei den Beratungen der Bürgerschaft – intensiv darüber diskutiert wurde, an welchen Stellen der Datenschutz gegenüber den Regelungen des Bundesdatenschutzgesetzes und der anderen Länder verbessert werden könne.

Auch das Hamburgische Datenschutzgesetz folgt – wie alle anderen Ländergesetze – der Grundstruktur des BDSG. Es hat die Begriffsbestimmungen nahezu unverändert und auch die materiellen Regelungen zum großen Teil übernommen. Damit ist dem Bedürfnis nach weitgehender Rechtseinheitlichkeit in Bund und Ländern Rechnung getragen worden. Das Datenschutzrecht ist eine schwierige Materie. Daher ist es zu begrüßen, wenn die Rechtsanwendung nicht noch durch unnötige Abweichungen zwischen Bundes- und Landesrecht zusätzlich erschwert und der Bürger nicht mit allzuvielen, zum Teil sich nur in Nuancen unterscheidenden Regelungen konfrontiert wird.

In einer Reihe von Punkten weicht das HmbDSG indessen vom BDSG ab, zum Teil geht es auch über die Datenschutzgesetze anderer Länder hinaus. Einmal ist die Stellung des Hamburgischen Datenschutzbeauftragten durch einige Besonderheiten gekennzeichnet, auf die ich unter 3.1 näher eingehe. Es gibt aber auch Änderungen, mit denen der Hamburgische Gesetzgeber unter Berücksichtigung von Erfahrungen und Anregungen anderer Länder den Datenschutz verbessern und die Position des Betroffenen stärken wollte. Zugleich sollten damit Anstöße zur Weiterentwicklung des Datenschutzrechts auch im Bund gegeben werden.

Hier die wichtigsten Änderungen in Kürze:

1. In den Fällen, in denen die Einwilligung Voraussetzung für die Zulässigkeit der Datenverarbeitung ist, muß der Betroffene bis ins einzelne über die Auswirkungen der Einwilligungserklärung aufgeklärt werden (§ 5 Abs. 2).

2. Der Betroffene erhält das Recht, Übermittlungen innerhalb des öffentlichen Bereichs zu sperren, auch ohne ein berechtigtes Interesse darzulegen, soweit die Übermittlung nicht durch Gesetz zugelassen ist (§ 6 Abs. 1 Nr. 4; diese Vorschrift tritt erst am 1. Mai 1984 in Kraft).

3. Die Zulässigkeit mehrfacher Verwendung seiner Daten muß dem Betroffenen bekannt sein (§ 10 Abs. 1 Satz 2).

4. Die behördeninterne Weitergabe von personenbezogenen Daten wird der zwischenbehördlichen Übermittlung gleichgestellt (§ 10 Abs. 2).

5. Bei Übermittlungen an nicht-öffentliche Stellen darf der Empfänger die Daten nur für den angegebenen Zweck verwenden (§ 12 Abs. 2 Satz 2).

6. Bei Darlegung eines berechtigten Interesses kann der Betroffene verlangen, daß die Übermittlung an nicht-öffentliche Stellen gesperrt wird (§ 12 Abs. 3).

7. Das Datenschutzregister, das der Datenschutzbeauftragte zu führen hat, umfaßt nicht nur die automatisch betriebenen Dateien, sondern auch alle manuell geführten Karteien. Der Hamburgische Datenschutzbeauftragte hat jährlich eine Übersicht über die im Register enthaltenen Dateien zu veröffentlichen (§ 13).

8. Die Erteilung von Auskünften an den Betroffenen erfolgt gebührenfrei (§ 14 Abs. 5).

9. Daten, deren Kenntnis für die speichernde Stelle zur Erfüllung ihrer Aufgaben nicht

mehr erforderlich ist, müssen gelöscht werden, es sei denn, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden (§ 15 Abs. 3).

10. Jede öffentliche Stelle hat regelmäßig alle vier Jahre die von ihr gespeicherten Daten auf ihre Erforderlichkeit zu prüfen und ggf. ihre Bestände zu bereinigen (§ 15 Abs. 4).

11. Es wird ein – summenmäßig unbegrenzter – verschuldensunabhängiger Schadensersatzanspruch eingeführt (§ 17).

12. Das auch den anderen Datenschutzgesetzen bekannte Recht auf Anrufung des Datenschutzbeauftragten wird dadurch abgesichert, daß niemand gemaßregelt oder benachteiligt werden darf, weil er davon Gebrauch gemacht hat. Bedienstete der Freien und Hansestadt Hamburg sind von der Pflicht entbunden, den Dienstweg einzuhalten (§ 23).

2.2 Weitere Rechts- und Verwaltungsvorschriften zum Datenschutz

Das Hamburgische Datenschutzgesetz ermächtigt in den §§ 13 Abs. 5 und 14 Abs. 4 den Senat zum Erlaß von Rechtsverordnungen. Zu der in § 13 Abs. 5 vorgesehenen Rechtsverordnung zum Datenschutzregister nehme ich unter 4.4.1 Stellung. Auf den Erlaß einer Rechtsverordnung gem. § 14 Abs. 4 zum Auskunftsverfahren ist „im Interesse der Eindämmung der Normenflut" verzichtet worden; stattdessen ist das Auskunftsverfahren durch Verwaltungsanordnung geregelt worden (Nr. 10 der unten erwähnten Hinweise für die Durchführung des HmbDSG). Die Verwaltungsvorschriften regeln alle Fragen erschöpfend und bürgerfreundlich; ich habe gegen diese Verfahrensweise keine Bedenken.

Der Senat hat von der ihm im § 16 Satz 3 eingeräumten Ermächtigung Gebrauch gemacht und die Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme gem. § 16 Satz 2 Nr. 2 durch Zuständigkeitsanordnung vom 25. Mai 1982 (Amtl. Anzeiger S. 969; ersetzt Zust.AO v. 21.4.81, Amtl. Anzeiger S. 733) auf das Senatsamt für den Verwaltungsdienst übertragen.

Die Senatskommission für den Verwaltungsdienst hat am 16. Juni 1977 die Richtlinie zum Verfahren der Datensicherung im Rahmen der automatisierten Datenverarbeitung (DS-Richtlinie, MittVw S. 205) erlassen. Die DS-Richtlinie regelt im wesentlichen, welche Stelle für welche Teile der Datensicherung verantwortlich ist. Die DS-Richtlinie wird durch die vom Senatsamt für den Verwaltungsdienst am 4. Januar 1979 erlassenen Rahmenregelungen zur Datensicherung für automatisierte Verfahren (DS-Rahmenregelungen, MittVw S. 13) konkretisiert; die DS-Rahmenregelungen enthalten Empfehlungen für konkrete Maßnahmen der Datensicherung. Ich werde prüfen, ob die DS-Richtlinien und die DS-Rahmenregelungen im Lichte neuerer Erkenntnisse fortzuschreiben sind.

Nach Inkrafttreten des Hamburgischen Datenschutzgesetzes hat das Senatsamt am 24. Februar 1982 Hinweise für die Durchführung des Hamburgischen Datenschutzgesetzes herausgegeben (MittVw S. 55). Diese Hinweise regeln einige für die Verwaltungspraxis besonders wichtige Punkte. Auf Anforderung stellt das Senatsamt sehr viel ausführlichere Hinweise für die Durchführung des HmbDSG, des BDSG und X. Buches des Sozialgesetzbuches (SGB X) zur Verfügung.

3. Der Hamburgische Datenschutzbeauftragte

3.1 Rechtsstellung

Gem. § 18 Abs. 1 wird die Verarbeitung personenbezogener Daten durch die Verwaltung von einem in Ausübung seines Amtes unabhängigen, nur dem Gesetz unterworfenen Hamburgischen Datenschutzbeauftragten überwacht. Er untersteht der Dienst- und Rechtsaufsicht des Senats (§ 19 Abs. 1). Gem. Senatsbeschluß vom 14. August 1979 führt der für

die Justiz zuständige Senator die Dienst- und Rechtsaufsicht für den Senat. Die Dienstaufsicht bezieht sich ausschließlich auf die Regelung dienstrechtlicher Fragen und auf die Sicherstellung eines geordneten äußeren Geschäftsablaufs. Sie eröffnet aber keinerlei Einfluß auf die Art und den Inhalt der Amtsausübung. Auch die Rechtsaufsicht ist durch die Unabhängigkeit des DSB und im Hinblick auf seine besondere Wirkungsweise begrenzt. Sie setzt nur dort ein, wo er Maßnahmen ergreift, die unmittelbare Rechtswirkung haben; auf keinen Fall kann sie ein Mittel sein, ihn auf die Rechtsauffassung des Senats festzulegen.

Die Unabhängigkeit des DSB kommt auch darin zum Ausdruck, daß er – neben dem Senat – auch die Bürgerschaft beraten und ihr über das Ergebnis der Überwachung berichten kann (§ 19 Abs. 4 Satz 1). Damit ist sichergestellt, daß er sich jederzeit an die Bürgerschaft wenden und sich zu bestimmten Vorgängen äußern sowie Anregungen einbringen kann.

Umgekehrt kann – ebenso wie der Senat – auch die Bürgerschaft den DSB ersuchen, Gutachten zu erstellen und Berichte zu erstatten (§ 18 Abs. 4 Satz 2, 20 Abs. 2 Satz 1). Seinen Tätigkeitsbericht erstattet er zugleich der Bürgerschaft und dem Senat (§ 20 Abs. 2 Satz 2).

Zur Stärkung seiner Unabhängigkeit hat der DSB außerdem das Recht, Vorschläge für die personelle Ausstattung seiner Dienststelle zu machen; der Senat kann ihm keinen Mitarbeiter aufzwingen. Die Versetzung oder Abordnung seiner Mitarbeiter ist an seine Zustimmung gebunden (vgl. § 19 Abs. 2).

Insgesamt enthält das Hamburgische Datenschutzgesetz also – insoweit über die Regelungen des Bundes und der meisten anderen Länder hinausgehend – eine Reihe von Bestimmungen, die eine von Weisungen freie und nur dem Gesetz unterworfene Ausübung des Amtes des Datenschutzbeauftragten absichern. Die unabhängige Stellung des Datenschutzbeauftragten ist wiederum Vorbedingung für das Vertrauen der Bürger, auf das er bei seiner Kontrolltätigkeit angewiesen ist.

Bei der Berufung des Hamburgischen Datenschutzbeauftragten wirken Senat und Bürgerschaft zusammen. Die Bürgerschaft wählt ihn auf Vorschlag des Senats (§ 18 Abs. 2 Satz 1); der Senat bestellt ihn für eine Amtszeit von 4 Jahren (§ 18 Abs. 3).

Auf Vorschlag des Senats hat mich die Bürgerschaft am 14. April 1982 gewählt. Mit Aushändigung der Ernennungsurkunde am 6. Mai 1982 bin ich mit Wirkung vom 10. Mai zum Hamburgischen Datenschutzbeauftragten bestellt worden.

3.2 Datenschutzkontrolle im nicht-öffentlichen Bereich

Durch Zuständigkeitsanordnung vom 25. Mai 1982 (Amtl. Anzeiger S. 969) hat der Senat dem Hamburgischen Datenschutzbeauftragten die Aufgabe der Aufsichtsbehörde nach §§ 30, 40 BDSG übertragen, die vorher die Behörde für Wirtschaft, Verkehr und Landwirtschaft wahrgenommen hatte. Die Aufsichtsbehörde überprüft die Ausführung des Bundesdatenschutzgesetzes durch private Personen oder Stellen, insbesondere in der Wirtschaft. Damit ist in Hamburg – ebenso wie in Bremen, im Saarland und in Schleswig-Holstein – die Kontrolle der Datenverarbeitung im öffentlichen und im nicht-öffentlichen Bereich in einer Hand zusammengefaßt.

So wird manche Doppelarbeit vermieden und die einheitliche Handhabung der – bis auf wenige Abweichungen – identischen Bestimmungen des Bundes- und des Landesdatenschutzgesetzes sichergestellt. Vor allem für den Bürger erweist sich die Zusammenlegung der Zuständigkeiten als vorteilhaft. Ihn überfordert die Unterscheidung von Datenschutz im öffentlichen und im privaten Bereich. Selbst Kenner tun sich oft schwer, bestimmte Vorgänge dem einen oder dem anderen Bereich zuzuordnen. Hinzu kommt, daß es häufig von eher zufälligen Voraussetzungen abhängt, ob das Bundesdatenschutzgesetz oder das Hamburgische Datenschutzgesetz anzuwenden ist.

3.3 Aufgaben und Befugnisse des Datenschutzbeauftragten (öffentlicher Bereich)

3.3.1 Kontrolle der Verwaltung

Im Mittelpunkt der Tätigkeit des Datenschutzbeauftragten steht seine Kontrollaufgabe. Nach § 20 Abs. 1 hat er die Einhaltung des Datenschutzes bei den Behörden und sonstigen öffentlichen Stellen der Freien und Hansestadt Hamburg zu überwachen. Die Kontrolle beschränkt sich nicht auf die Beachtung des Hamburgischen Datenschutzgesetzes, sie erstreckt sich auch auf andere Datenschutzbestimmungen. Damit wird dem Umstand Rechnung getragen, daß das Datenschutzgesetz den Datenschutz nicht umfassend und abschließend regelt, sondern daß es darüber hinaus noch eine Vielzahl anderer Vorschriften mit datenschutzrechtlicher Zielsetzung gibt. Dazu gehören etwa die Regelungen über Berufsgeheimnisse, das Steuergeheimnis, das Sozialgeheimnis und das Statistikgeheimnis.

Die Verantwortung für die Einhaltung des Datenschutzes tragen die datenverarbeitenden Stellen selbst. Diese Verantwortung kann und darf ihnen der Datenschutzbeauftragte nicht abnehmen.

Alle öffentlichen Stellen, die der Kontrolle des DSB unterworfen sind, sind verpflichtet, ihn bei der Erfüllung seiner Aufgabe zu unterstützen (§ 18 Abs. 4). Sie haben ihm Auskunft auf seine Fragen und Einsicht in alle Unterlagen und Akten zu gewähren, die im Zusammenhang mit der Datenverarbeitung stehen. Außerdem haben sie ihm Zutritt zu allen Räumen zu gewähren. Die Unterstützungspflicht besteht bei Sicherheits- und Steuerbehörden nur gegenüber dem Hamburgischen Datenschutzbeauftragten selbst und den von ihm schriftlich Beauftragten. Ausnahmsweise kann die Einsichtnahme verweigert werden, wenn der Senat im Einzelfall feststellt, daß hierdurch die Sicherheit des Bundes oder eines Landes gefährdet würde.

Eine weitere wichtige Erkenntnisquelle wird das Datenschutzregister sein, daß der Datenschutzbeauftragte nach § 13 zu führen hat. Über den Aufbau des Datenschutzregisters wird unter 4.4 berichtet.

3.3.2 Beratung der Verwaltung

Ebenso wichtig wie die nachgehende Kontrolle ist die Aufgabe, den Senat wie auch einzelne Behörden zu beraten (vgl. § 24 Abs. 1 S. 2). Die Beratung der Verwaltung kann wesentlich dazu beitragen, daß es zu Verstößen gegen Datenschutzbestimmungen gar nicht erst kommt. Zur Beratung gehört auch die Mitwirkung beim Erlaß von Rechtsvorschriften. Es geht darum, den Datenschutz auf allen Ebenen vom Gesetz bis zur verwaltungsinternen Richtlinie (letztlich bis zur organisatorisch-technischen Durchführungsmaßnahme) fortzuentwickeln und so zu gestalten, daß es gar nicht erst zu einer Beeinträchtigung von Bürgerrechten kommen kann.

Hierzu ist es notwendig, daß die Beratung möglichst frühzeitig einsetzt. Ich habe dem Senat angeboten, an der Vorbereitung datenschutzrelevanter Vorhaben mitzuwirken. Die Staatsräte haben zugesagt (Beschluß der Staatsräte vom 22. Juni 1982), sie würden innerhalb ihrer Zuständigkeitsbereiche dafür sorgen, daß ich am Abstimmungsverfahren beteiligt würde, soweit Belange des Datenschutzes berührt seien.

Die Beratung der Behörden im Abstimmungsverfahren besteht darin, beim Erkennen von Problemen zu helfen und auf Regelungsmöglichkeiten hinzuweisen. Wenn ich umfassend unterrichtet und rechtzeitig beteiligt worden bin, bin ich auch bereit, ein Vorhaben in datenschutzrechtlicher Hinsicht mit zu verantworten. Weil ich jedoch auch die Belange der Bürger gegenüber der Verwaltung zu vertreten habe, muß ich diese Verantwortung unter den Vorbehalt stellen, daß sich nach Erlaß der Rechtsvorschrift keine gravierenden neuen Gesichtspunkte ergeben.

3.3.3 Vertretung der Anliegen der Bürger

Nach § 22 kann sich jedermann an den Hamburgischen Datenschutzbeauftragten wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch eine Stelle der hamburgischen Verwaltung in seinen Rechten verletzt worden zu sein. Der Datenschutzbeauftragte ist eine Art Ombudsmann, Bürgeranwalt in Datenschutzfragen.

Es ist seine vornehmste Aufgabe, den Anliegen der Bürger nachzugehen und um die Durchsetzung ihrer Rechte bemüht zu sein. Andere Aufgaben müssen demgegenüber grundsätzlich zurückstehen. Ich möchte aber auch an dieser Stelle um Verständnis dafür bitten, daß die notwendigen Ermittlungen und Verhandlungen mit den Behörden häufig viel Zeit beanspruchen, so daß in Einzelfällen mehrere Wochen vergehen können, ehe ich dem Bürger das Ergebnis meiner Prüfung mitteilen kann.

Besonders wichtig ist es, daß dem Bürger dort geholfen wird, wo er sich selbst nicht die notwendigen Informationen verschaffen kann, um seine Rechte gezielt geltend zu machen. Das gilt vor allem für den Verfassungsschutz, die Polizei und die Staatsanwaltschaft, die nicht verpflichtet sind, dem Bürger Auskunft darüber zu geben, ob und ggf. welche Daten sie über ihn gespeichert haben. Dagegen kann der DSB auch bei diesen Behörden kontrollieren, ob die Datenschutzvorschriften beachtet worden sind. Soweit ich Verstöße feststelle, werde ich auf schnelle Abhilfe dringen. Allerdings darf ich Erkenntnisse, die ich bei der Prüfung gewonnen habe, dem Betroffenen nur mit Zustimmung der Behörde mitteilen. Umsomehr bin ich darauf angewiesen, daß mir der Bürger Vertrauen entgegenbringt.

3.3.4 Berichterstattung

Zu meinen Pflichten gehört schließlich die jährliche Berichterstattung an Bürgerschaft und Senat. Mit dem vorliegenden Tätigkeitsbericht wird dieser Pflicht erstmals entsprochen. Zudem können Senat und Bürgerschaft den DSB jederzeit ersuchen, sich zu Fragen des Datenschutzes gutachtlich zu äußern. Eine derartige Aufforderung ist bislang noch nicht ergangen.

3.3.5 Durchsetzungsmöglichkeiten

Der DSB hat keinerlei Weisungs- oder Eingriffsbefugnisse gegenüber dem Senat oder einzelnen Behörden. Seine Tätigkeit findet ihren Niederschlag in Empfehlungen und Beanstandungen.

Im allgemeinen wird der DSB von dem Mittel der Beratung und Empfehlung Gebrauch machen (vgl. § 20 Abs. 1 Satz 2). Führt dies aber nicht zur Behebung festgestellter Mängel oder zur Vermeidung künftiger Verstöße, hat der Datenschutzbeauftragte die Möglichkeit, die Verletzung von Datenschutzvorschriften zu beanstanden (§ 21). Das ist sein einziges förmliches Mittel. Die rechtliche Durchsetzung der Beanstandung ist dem DSB aufgrund seiner verfassungsrechtlichen Stellung verwehrt.

Wird eine Empfehlung oder Beanstandung nicht beachtet, so hat der DSB die Möglichkeit, sich gem. § 19 Abs. 4 unmittelbar an die Bürgerschaft zu wenden. Er kann solche Fälle auch in seinen Tätigkeitsbericht gem. § 20 Abs. 2 Satz 2 aufnehmen. Ein letztes Mittel, das zwar nicht gesetzlich geregelt ist, sich aber aus der Natur des Datenschutzes ergibt, ist die Unterrichtung der Öffentlichkeit.

Im übrigen lasse ich mich bei meiner Arbeit von folgenden Überlegungen leiten:

Der beste und sicherste Datenschutz ist der, den die bei der Datenverarbeitung Beschäftigten aus eigener Überzeugung leisten. Aus diesem Grunde bin ich vor jeglicher förmlich-bürokratischer Vorgehensweise und Kritik bestrebt, für die Belange des Datenschutzes zu werben und das Verständnis für die Sorgen und Befürchtungen der betroffenen Bürger zu fördern. Sehr wichtig ist, daß die in einzelnen Fällen entstehenden Zielkonflikte zwischen

den Bedürfnissen der speichernden Stelle und den Belangen des Datenschutzes präzise definiert und eingegrenzt werden. Das ermöglicht es, Scheingefechte abzubrechen und Streitigkeiten in Bagatellsachen auf ihre wahre Bedeutung zurückzuführen.

Da die Befugnisse des Datenschutzbeauftragten gering sind, sehe ich in konsequenter Überzeugungsarbeit langfristig das beste Mittel für eine Anerkennung datenschutzrechtlicher Belange.

3.4 Aufgaben und Befugnisse der Aufsichtsbehörde nach §§ 30, 40 BDSG

Im nicht-öffentlichen Bereich wird unterschieden zwischen solchen Stellen, die die Datenverarbeitung für eigene, und solchen, die die Datenverarbeitung für fremde Zwecke betreiben. Die entsprechenden Vorschriften sind im Dritten und im Vierten Abschnitt des BDSG angesiedelt.

Stellung und Rechte der Aufsichtsbehörden sind für den Dritten Abschnitt des BDSG in § 30 und für den Vierten Abschnitt in § 40 geregelt. Die Aufsichtsbehörden ergänzen das Konzept der unternehmensinternen Selbstkontrolle durch ein Organ neutraler, staatlicher Fremdkontrolle.

3.4.1 Anlaßkontrolle nach § 30 BDSG

Nach § 30 Abs. 1 S. 1 BDSG überprüft die Aufsichtsbehörde die Ausführung des BDSG und anderer datenschutzrechtlicher Bestimmungen im Einzelfall, wenn ein Betroffener begründet darlegt, daß er bei der Verarbeitung seiner personenbezogenen Daten durch einen Normadressaten des Dritten Abschnittes in seinen Rechten verletzt ist (Anlaßaufsicht). Wird im Rahmen dieser Anlaßaufsicht allerdings eine bestimmte speichernde Stelle überprüft, so braucht die Aufsichtsbehörde sich nicht auf den auslösenden Einzelfall zu beschränken, sondern kann weiteren Verstößen nachgehen, die ihr bei dieser Gelegenheit bekannt werden.

Entscheidungs- und Durchführungskompetenzen sind mit dem Kontrollauftrag der Aufsichtsbehörde nicht verbunden, was vielen Betroffenen leider unbekannt ist. Die Aufsichtsbehörde kann der speichernden Stelle nur nahelegen, Maßnahmen zur Beseitigung von Verstößen gegen Datenschutzbestimmungen vorzunehmen; sie kann solche Maßnahmen aber nicht anordnen. Im übrigen ist es dem Betroffenen überlassen, aufgrund des Bescheides, den er von der Aufsichtsbehörde erhalten hat, zu entscheiden, ob er weitere Schritte unternehmen, d.h. eines seiner Rechte auf Berichtigung, Sperrung, Löschung oder Schadensersatz geltend machen will. Soweit die Beteiligten ihren Streit fortsetzen, bleibt die Entscheidung stets den Gerichten vorbehalten.

Im Vorfeld gerichtlicher Entscheidungen bleiben der Aufsichtsbehörde aber wichtige Kontroll- und Filterfunktionen. Die Aufsichtsbehörde kann den Sachverhalt ermitteln und gegebenenfalls Beweise sichern:
Nach § 30 Abs. 2 BDSG ist sie berechtigt, bei den speichernden Stellen die zur Prüfung erforderlichen Auskünfte zu verlangen. Sie kann darüber hinaus Geschäftsräume der speichernden Stelle betreten, dort Prüfungen und Besichtigungen vornehmen und in geschäftliche Unterlagen, gespeicherte personenbezogene Daten und Datenverarbeitungsprogramme Einsicht nehmen.

3.4.2 Beratungsaufgaben

Als wesentlich wichtiger als die Anlaßkontrolle hat sich in meiner bisherigen Praxis die Beratungsfunktion der Aufsichtsbehörde erwiesen. Eine sachverständige Beratung trägt im Interesse aller Beteiligten dazu bei, Nachteile, die sich für die Betroffenen aus der Verarbeitung personenbezogener Daten ergeben könnten, von vornherein zu vermeiden. Mögliche Konfliktpunkte können rechtzeitig ausgemacht werden und spätere Beanstandungen können entfallen.

In § 30 Abs. 1 S. 2 BDSG ist ausdrücklich vorgesehen, daß die Aufsichtsbehörde den betrieblichen Datenschutzbeauftragten zu unterstützen hat, wenn dieser sich an sie wendet. Sie soll also gemeinsam mit ihm bestehende Unklarheiten beseitigen und damit der speichernden Stelle dazu verhelfen, die Grenzen ihres Handlungsspielraumes rechtzeitig zu erkennen.

Dies bedeutet nicht, daß der betriebliche Datenschutzbeauftragte der einzig mögliche Gesprächspartner der Aufsichtsbehörde ist. Sie wird einer speichernden Stelle das Gespräch nicht deshalb verweigern, weil die Initiative nicht vom Beauftragten ausgeht. Die Unterstützung durch die Aufsichtsbehörde ist für die zahlreichen kleinen Unternehmen, die einen betrieblichen Datenschutzbeauftragten nicht zu bestellen brauchen, sogar ganz besonders wichtig. Erfreulicherweise wird nach den bisherigen Erfahrungen, die auch bereits die Behörde für Wirtschaft, Verkehr und Landwirtschaft gemacht hat, die Bereitschaft der Aufsichtsbehörde, Gespräche zu führen und Hilfe zu leisten, von allen Beteiligten (betrieblichen Datenschutzbeauftragten, Unternehmensleitungen, Betriebsräten, Verbänden und Gewerkschaften) gern und häufig in Anspruch genommen.

3.4.3 Aufgaben nach § 40 BDSG

Die Unternehmen und Stellen, die die Datenverarbeitung für fremde Zwecke durchführen, sind einer weitergehenden staatlichen Aufsicht unterworfen.

Betroffen davon sind

- Stellen, soweit sie geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung speichern und übermitteln (vor allem Auskunfteien),
- Stellen, soweit sie geschäftsmäßig personenbezogene Daten speichern, diese anonymisieren und in dieser Form übermitteln (u.a. Markt- und Meinungsforschungsinstitute),
- Stellen, soweit sie geschäftsmäßig personenbezogene Daten im Auftrag als Dienstleistungsunternehmen verarbeiten (vor allem Service-Rechenzentren und Datenerfassungsbetriebe).

Zusätzlich zu den Kontrollrechten und -pflichten des Dritten Abschnitts hat die Aufsichtsbehörde nach § 40 BDSG eine ständige Überwachungspflicht. Die Initiative ist also auf die Aufsichtsbehörde verlagert. Weitere Rechte und Sanktionen sind ihr jedoch nicht eingeräumt. Auch im Vierten Abschnitt sind – abgesehen von Verwaltungsakten im Zusammenhang mit Ordnungswidrigkeiten – ihre Äußerungen bloße Rechtsansichten. Gelegentlich wird der Meinungsaustausch zwischen den zu überwachenden Stellen und der Aufsichtsbehörde dadurch allerdings erleichtert.

3.5 Einrichtung der Dienststelle

3.5.1 Stellenausstattung

Die Bürgerschaft hat mit Beschluß vom 26. März 1981 (9. Wahlperiode, 72. Sitzung) im Zusammenhang mit der Verabschiedung des Hamburgischen Datenschutzgesetzes folgende Stellen für die Dienststelle des Hamburgischen Datenschutzbeauftragten geschaffen:

1 Stelle Hamburgischer Datenschutzbeauftragter	B 6
1 Stelle Regierungsdirektor	A 15
1 Stelle Amtsrat	A 12
1 Stelle Büroangestellte	VI b
1 Stelle Angestellte für Textverarbeitung	IXb/VII

Durch die Bewilligung der Stellen sollte dem Hamburgischen Datenschutzbeauftragten ermöglicht werden, nach einer nur durch die Personalauswahl bedingten Anlaufzeit die Arbeit aufzunehmen. In der Vorlage des Senats (vgl. Drucksache 9/1112, S. 23) heißt es hierzu, daß es sich bei den bewilligten Stellen nach Zahl und Wertigkeit um eine Grundausstattung handele und daß dem Hamburgischen Datenschutzbeauftragten Raum für die Entwicklung eigener Vorschläge nach § 19 Abs. 2 Satz 1 bleiben müsse.

Mit der Übertragung der Zuständigkeiten gem. §§ 30, 40 BDSG auf den DSB sind weitere 2 Stellen von der vorher zuständigen Behörde für Wirtschaft, Verkehr und Landwirtschaft übergegangen:

1 Stelle Regierungsrat	A 13
1 Stelle Regierungsamtmann	A 11

Die Stellen konnten inzwischen alle besetzt werden, die letzte zum 1. November 1982.

Schon bald nach Aufnahme der Arbeit mußte ich feststellen, daß die von der Bürgerschaft beschlossene Grundausstattung den Anforderungen nicht entspricht. Die Überwachung des nicht-öffentlichen Bereichs (Tätigkeit als Aufsichtsbehörde gem. §§ 30, 40 BDSG) bindet die übertragenen 2 Stellen. Für die Überwachung des öffentlichen Bereichs sind ebenfalls 2 Stellen (Referent und Sachbearbeiter) erforderlich, um nur die dringlichsten Probleme (Sicherheitsbereich, Gesundheits- und Sozialwesen, Meldewesen, Statistik) bearbeiten zu können. Für die Führung des Datenschutzregisters, die technisch-organisatorischen Prüfungen und die Auseinandersetzung mit den durch die technologische Entwicklung bedingten Datenschutzproblemen (neue Medien, Büroautomation) sind weitere 2 Stellen (Referent und Sachbearbeiter) erforderlich. Bei diesem – angesichts der angespannten Haushaltslage am Notwendigsten orientierten – Personalbedarf sind Kapazitäten für die überregionale Zusammenarbeit, die Öffentlichkeitsarbeit und den Tätigkeitsbericht bereits mit eingeplant.

Ich habe daher zum Stellenplan 1983 zusätzlich

1 Stelle Regierungsdirektor	A 15
1 Stelle Amtsrat	A 12

beantragt. Diesem Antrag hat der Senat zum Stellenplan 1983 nicht mehr entsprochen, weil der Antrag nicht unter Einhaltung der Antragsfristen gestellt und naturgemäß auch noch nicht mit konkreten Angaben begründet werden konnte.

Ich bin aber dankbar dafür, daß das Senatsamt für den Verwaltungsdienst mir spätestens zum 1. Januar 1983 aus dem eigenen Bestand einen Regierungsrat z.A. vorläufig zuweisen will.

3.5.2 Sachausstattung

Die mir zur Verfügung stehenden Haushaltsmittel sind im Kapitel 2050 des Haushaltsplanes der Freien und Hansestadt Hamburg veranschlagt. Ich halte es für notwendig, folgende Ansätze möglichst noch für 1983, spätestens für 1984 zu erhöhen:

Aus- und Fortbildung auf 10.000 DM (statt 5.000 DM in 1982 und 1983)
Reisekosten auf 6.000 DM (statt 1.000 DM in 1982 und 3.000 DM in 1983)

Die verhältnismäßig hohen Mittel für Aus- und Fortbildung sind notwendig, damit meine Mitarbeiter ihre Kenntnisse auf dem Gebiet der automatisierten Datenverarbeitung erhalten und fortentwickeln können. Reisekosten sind in diesem Umfang wegen der unter 4.7 beschriebenen intensiven Kooperation erforderlich.

Ich habe für die Dienststelle eine Unterbringung im DAG-Haus am Karl-Muck-Platz dem angebotenen Standort im Einkaufszentrum Altona vorgezogen, weil das DAG-Haus zentra-

ler liegt und die Büroräume leichter zugänglich sind. Mit der Unterbringung im DAG-Haus war allerdings der Nachteil verbunden, daß erst Ende November alle erforderlichen Räume zur Verfügung standen.

Wegen der angespannten Haushaltssituation mußte die Beschaffung von Büchern und Fachzeitschriften auf ein Minimum beschränkt werden; ich hoffe, daß die Ausstattung in den nächsten Jahren vervollständigt werden kann. Für Veröffentlichungen sind im Entwurf des Haushaltsplanes 1983 ausreichende Mittel veranschlagt.

3.5.3 Defizite

Der Umstand, daß die Institution des Hamburgischen Datenschutzbeauftragten mit mehreren Jahren Verspätung geschaffen wurde, und die Schwierigkeiten, die mit dem Aufbau einer neuen Dienststelle verbunden sind, haben allen Mitarbeitern viel abverlangt, um inzwischen einigermaßen wirkungsvoll arbeiten zu können. Zu den üblichen organisatorischen Problemen kam hinzu, daß einige Beschaffungen überraschend lange Zeit benötigten. Besonders nachteilig macht sich das Fehlen jeglicher Akten bemerkbar; so müssen in mühsamer Arbeit die Akten über die Entstehung wichtiger Gesetze (z.B. für das Hamburgische Datenschutzgesetz oder das Meldegesetz) mit Hilfe von Unterlagen der Bürgerschaftskanzlei und aus den Vorgängen der Justizbehörde rekonstruiert werden. Auch die Datenschutzbeauftragten der Nachbarländer haben mir in vorbildlicher Weise geholfen und aus ihren Unterlagen Kopien zur Verfügung gestellt. Dennoch wird es noch mehrere Monate dauern, bis der Aufbau der Registratur im großen und ganzen abgeschlossen ist. Die organisatorischen Probleme werden durch die Raumnot (zeitweilig mußten einige Mitarbeiter im Ziviljustizgebäude untergebracht werden) und durch die Enge der Haushaltsmittel verschärft.

Auf der anderen Seite war der Geschäftsanfall in der Dienststelle von Anfang an beträchtlich und überstieg die Kapazität des zur Verfügung stehenden Personals. Auch wenn die Zuweisung eines Regierungsrats z.A. Entlastung bringen wird, halte ich eine weitere personelle Verstärkung meiner Dienststelle – auch unter Berücksichtigung der angespannten Haushaltslage – für dringlich.

Ich möchte allerdings schon an dieser Stelle darauf hinweisen, daß trotz personeller Verstärkung der Dienststelle im beantragten Umfang die Kontrolldichte gering bleiben wird. Die systematische Prüfung einer größeren Dienststelle bindet die Arbeitskapazität zweier Mitarbeiter wenigstens einen Monat. Unter Berücksichtigung meiner sonstigen Aufgaben wären daher mehr als 6 größere und daneben einige kleinere Prüfungen jährlich nicht möglich. Der nicht-öffentliche Bereich ist in diese Schätzung nicht einbezogen.

4. Tätigkeit im Berichtszeitraum

4.1 Information über Datenschutz

4.1.1 Ausgangslage und Problem

Eine wichtige Aufgabe des DSB besteht darin, bei den Bürgern ebenso wie bei den Stellen der öffentlichen Verwaltung das Bewußtsein für die Bedeutung und die praktischen Auswirkungen des Datenschutzes zu stärken. Aufgrund der Erkenntnisse, die ich in meiner kurzen Amtszeit gewonnen habe, kann ich die Feststellungen anderer Datenschutzbeauftragter bestätigen: Zwar ist das Interesse der Bürger an Fragen des Datenschutzes groß, auch fehlt es der Verwaltung nicht an Sensibilität. Wünschenswert wäre aber ein größeres Engagement der öffentlichen Stellen, den Datenschutz in ihrem Bereich fortzuentwickeln, und der Bürger, ihre Rechte nach den Datenschutzgesetzen gezielt wahrzunehmen. Erforderlich ist hierfür auf beiden Seiten eine Vertiefung der Kenntnisse.

Fehlendes Wissen, vergröbernde Darstellungen und z.T. emotional geführte Diskussionen haben in der Öffentlichkeit Unruhe und Unsicherheit hervorgerufen. Als Beispiele, die die Situation schlaglichtartig beleuchten sollen, nenne ich:

Die (unzutreffende) Annahme, der Datenschutz verbiete jegliche Weitergabe von Daten. Die (unzutreffende) Vermutung von Bürgern, der Datenschutzbeauftragte habe Kenntnis von allen gespeicherten personenbezogenen Daten und könne daher Auskunft über sie geben.

Eine nennenswerte Anzahl von Bürgern zögert bzw. lehnt es ab, in telefonischen Beratungen über Datenschutzprobleme Namen, Anschrift und Telefonnummer zu nennen, obwohl ich ihnen vertrauliche Behandlung zusichere und auf das Benachteiligungsverbot in § 23 (gilt nicht für meine Tätigkeit als Aufsichtsbehörde nach §§ 30, 40 BDSG) hinweise.

Ich befürchte jedoch, daß die Kompliziertheit und der Abstraktionsgrad des Datenschutzrechts einer verbreiteten und vertieften Kenntnis verhältnismäßig enge Grenzen setzen; viele Bürger, aber auch Verwaltungsangehörige stehen ratlos vor der scheinbar einfachen Frage, welche Datenschutzvorschrift im Einzelfall gilt – spezielle Rechtsvorschrift gem. § 45 BDSG oder § 27, SGB X und BDSG oder HmbDSG je nach der zu erledigenden Verwaltungsaufgabe. Hinzu kommt, daß die persönlichen Vorstellungen der Bürger von der Schutzwürdigkeit einzelner Daten im Widerspruch stehen zu den Intentionen des Gesetzgebers, der an formale Kriterien angeknüpft hat. Deshalb fallen verhältnismäßig wenig sensitive Daten, wenn sie in einer Datei gespeichert werden, unter das Datenschutzgesetz; hingegen sind auf sehr sensitive Daten, wenn sie in Akten gespeichert werden, die Bestimmungen des Datenschutzgesetzes nicht anwendbar. Vielen Bürgern, aber auch manchem Mitarbeiter der Verwaltung fehlt die Kenntnis, daß im öffentlichen Bereich Daten, die nicht unter das Datenschutzrecht fallen, nicht etwa schutzlos sind und nach Belieben verwendet werden dürfen, sondern zumindest aufgrund der Amtsverschwiegenheit nach denselben Regeln zu behandeln sind, die das Datenschutzgesetz ausdrücklich für die von ihm geschützten Daten setzt.

Auch dies gehört zu meinen Aufgaben: falsche oder unklare Vorstellungen über Datenschutz zu berichtigen und auf diese Weise unzutreffende Erwartungen sowie damit verbundene Enttäuschungen abzubauen.

4.1.2 Mittel und Wege

Ein wichtiger Partner des Datenschutzbeauftragten ist die Presse. Ich habe vom Tage meines Amtsantritts an das Interesse der Medien an Fragen des Datenschutzes genutzt, Hintergrundgespräche geführt und Interviews gegeben. Erfreulicherweise haben die Hamburger Zeitungen ihre Leser mehrfach darauf hingewiesen, daß es nunmehr auch in Hamburg einen Datenschutzbeauftragten gibt, und über die von ihm zu leistende Arbeit unterrichtet. Ein Problem ist und wird auch in Zukunft der Widerspruch zwischen dem Interesse der Presse an spektakulären Fällen und dem tatsächlichen Charakter meiner Arbeit sein, geduldiger Kleinarbeit, die in der Regel ohne sensationelle Ergebnisse bleiben wird. Aber auch wenn es nur ausnahmsweise Datenschutzskandale geben wird, hoffe ich doch auf eine Berichterstattung in den Medien, die dazu beiträgt, die Datenverarbeitung transparenter, die Verwaltungsabläufe durchschaubarer zu machen.

Meine Mitarbeiter und ich nehmen jede Möglichkeit wahr, in Vorträgen, Diskussionen und Aus- und Fortbildungsveranstaltungen aufklärend zu wirken und um Verständnis für unsere Arbeit zu werben. Ich habe viele Einzelgespräche mit Mitgliedern der Bürgerschaft und des Senats geführt, in denen mir durchweg volle Unterstützung zugesichert wurde.

Nach meinen ersten und daher vorläufigen Eindrücken ist der Kenntnisstand vieler Mitarbeiter in der Verwaltung der Freien und Hansestadt Hamburg verbesserungsbedürftig. Ich begrüße es daher, daß Behörden an mich mit der Bitte um Fortbildung ihrer Bediensteten

herangetreten sind; darüber hinaus werde ich mich auch darum bemühen, daß Datenschutz allgemein stärker in den Fortbildungsprogrammen berücksichtigt wird. Außerdem nutzen meine Mitarbeiter und ich jeden Kontakt mit Bediensteten, um über Datenschutz zu informieren. Insbesondere im Zusammenhang mit dem Aufbau des Datenschutzregisters hat es zahlreiche Kontakte gegeben.

Einen breiten Raum nehmen – im allgemeinen telefonische – Einzelgespräche mit Bürgern ein. Verständlicherweise konnte ich bisher noch kein Informationsmaterial erarbeiten; ich bin meinen Kollegen, insbesondere dem Bundesbeauftragten für den Datenschutz, sehr dankbar, daß sie mir großzügig ausgeholfen haben. Dieser Bericht wird zugleich die erste Information über meine Arbeit sein; ich beabsichtige, die in § 13 Abs. 1 Satz 3 vorgesehene Veröffentlichung einer Übersicht über die im Datenschutzregister enthaltenen Dateien mit Informationen über den Datenschutz, insbesondere über die Rechte der Bürger zu verbinden und in der ersten Hälfte des nächsten Jahres zu veröffentlichen.

4.2 Eingaben

4.2.1 Überblick

In den ersten Monaten meiner Tätigkeit haben mich verhältnismäßig viele Eingaben erreicht. Einige Zuschriften waren vor meinem Amtsantritt an die Justizbehörde oder den Senat gerichtet und wurden an mich weitergeleitet. In vielen Fällen baten die Einsender um allgemeine Informationen über den Datenschutz oder das Hamburgische Datenschutzgesetz; dann konnte ich mit dem Abdruck des Gesetzestextes oder mit den Broschüren „Bürgerfibel Datenschutz" und „Der Bürger und seine Daten" helfen, die mir der Bundesbeauftragte für den Datenschutz zur Verfügung gestellt hatte. Auf Interesse stieß auch das „Datenschutzscheckheft" des Berliner Datenschutzbeauftragten.

Die Zahl der Eingaben, die sich mit konkreten Fragen beschäftigten oder Beschwerden enthielten, belief sich bis zum 15. November 1982 auf 63. In der Mehrzahl waren die Petenten selbst Betroffene eines Datenverarbeitungsvorgangs. Aber auch betriebliche Datenschutzbeauftragte, Verantwortliche von datenverarbeitenden Stellen und Betriebsräte haben sich an mich gewandt. Die Eingaben verteilen sich auf den öffentlichen und den nichtöffentlichen Bereich je zur Hälfte.

Im öffentlichen Bereich lag das Interesse hauptsächlich bei der Datenverarbeitung von Polizei und Staatsanwaltschaft, ein weiterer Schwerpunkt war das Melderecht. Die Einzelheiten zu den Sachproblemen sind unter 6. näher beschrieben.

4.2.2 Beispiele

1.) Es stellte sich heraus, daß viele Bürger über die Verwaltungsabläufe und die Zusammenarbeit zwischen mehreren Behörden gar keine oder nur verschwommene Vorstellungen haben. Das Unbehagen gegenüber einzelnen Behörden oder allgemein gegenüber dem Staat kann oftmals beseitigt werden durch die Beschreibung der tatsächlichen Handhabung und Hinweise auf die Notwendigkeit und die gesetzliche Grundlage für bestimmte Speicherungen oder Übermittlungen. Beispielsweise wurde ich von zwei Einsendern nach der Zulässigkeit der Übermittlung von Betriebsergebnissen durch das Finanzamt an die Handels- bzw. Handwerkskammer gefragt. Zunächst habe ich klargestellt, daß nur eine Angabe, nämlich der einheitliche Gewerbesteuermeßbetrag, übermittelt wird, den die Kammern für die Beitragserhebung benötigen. Rechtsgrundlagen sind die Abgabenordnung, das Gesetz über die Industrie- und Handelskammern und die Handwerksordnung, die Vorrang vor den allgemeinen Regelungen im Hamburgischen Datenschutzgesetz haben. Diese Klarstellung hat ausgereicht, um die Bedenken der Einsender zu zerstreuen.

2.) Besorgnis beim Betroffenen wird immer dadurch erregt, daß er nicht oder nicht genau weiß, welche Informationen über ihn in welchem Zusammenhang verwendet werden.

Deutlich wird das dadurch, daß die Betroffenen sich oftmals dann beschwerdeführend an mich wenden, wenn sie vermuten, daß „hinter ihrem Rücken" Unrechtes geschehen oder nach einer Befragung in einer konkreten Angelegenheit die Daten für einen ganz anderen Zweck genutzt werden könnten.

So haben sich einige Bürger über Fragebogen beschwert, die zum Teil in Bereiche eindringen, die mit der eigentlichen Zweckerfüllung nicht im Zusammenhang stehen. Dies gilt z.B. für einen von den Sozialdienststellen verwendeten Fragebogen, der sich an Unterhaltsverpflichtete richtet. Dort wird u.a. nach der Krankenkasse des Unterhaltsverpflichteten und bei besonderen Aufwendungen für einen kranken Familienangehörigen nach der Diagnose gefragt. In beiden Punkten konnte die Behörde die Erforderlichkeit dieser Angaben zunächst nicht begründen. Es muß noch genauer geprüft werden, ob die Frage nach der Krankenkasse völlig entfallen kann; die Frage nach der Diagnose soll ersetzt werden durch die Bitte, eine allgemeine Begründung für die höheren Aufwendungen zu geben.

3.) Auch der Fragebogen des Hamburger Verkehrsverbundes (HVV), der die Grundlage dafür bildet, daß ihm vom Bund Ausgleichszahlungen geleistet werden für die verbilligten Beförderungen von Schülern, Studenten und Auszubildenden, war Gegenstand einer Beschwerde. Hierin wird u.a. nach der vollständigen Anschrift gefragt, wobei andererseits völlige Anonymisierung zugesagt wird. Die Adresse wird tatsächlich beim HVV nicht gespeichert; sie dient lediglich dazu, die richtige Bezeichnung von Ein- und Ausstiegshaltestellen zu prüfen. Wie mir der HVV mitteilte, hält er diese Kontrolle nicht mehr für erforderlich und will zunächst versuchsweise auf die Angabe der Adresse verzichten.

Da eine Pflicht zur Abgabe der Fragebogen besteht, die im Tarifvertrag festgeschrieben ist und sich auf die Nachweispflicht des HVV als Zuschußempfänger gründet (§ 45a des Personenbeförderungsgesetzes und § 6a des Allgemeinen Eisenbahngesetzes), habe ich zusätzlich angeregt, die Befragten gleichzeitig mit der Aufforderung, den Fragebogen ausgefüllt wieder abzugeben, deutlicher als bisher über den Grund der Befragung aufzuklären. Dies hat der HVV zugesagt.

4.) Im nicht-öffentlichen Bereich liegt ein Schwerpunkt bei der Tätigkeit der Wirtschaftsauskunfteien. Auf Grund der Tatsache, daß die Auskunfteien nach § 34 BDSG eine Benachrichtigungspflicht trifft, haben viele Bürger nach dem Inkrafttreten des BDSG erstmals von der Existenz solcher Stellen erfahren, die Informationen über ihre Zahlungsfähigkeit und Kreditwürdigkeit sammeln und weitergeben.

Viele sind darüber irritiert, daß sie in ein und demselben relativ kurzen Brief über die Tatsache der Speicherung informiert und gleichzeitig gebeten werden, noch weitere Informationen herauszugeben. Mancher Bürger glaubt gar, er müsse den beigefügten Fragebogen gewissenhaft ausgefüllt der Auskunftei zurückgeben. Ich werde darauf hinwirken, daß die Betroffenen besser aufgeklärt und vor allem auf die Freiwilligkeit zusätzlicher Angaben hingewiesen werden (s. auch 7.1.1 Ziff. 4).

5.) Viele Bürger beklagen sich, daß sie, um in den Genuß der vertraglichen Hauptleistung zu kommen, durch vorgegebene Vertragstexte gezwungen werden, Informationen preiszugeben, die nicht direkt die Durchführung des Vertrages betreffen.

Als Beispiel hierfür sei der sog. Erstbestellschein im Versandhandel genannt, in dem auch Angaben über den Ehegatten erbeten werden und nach Geburtsdatum, früheren Wohnanschriften und bei Ausländern nach der Dauer des bisherigen Aufenthaltes in der Bundesrepublik und der Gültigkeit der Aufenthaltsgenehmigung gefragt wird. Der Erstbestellschein wurde nach dem Inkrafttreten des Bundesdatenschutzgesetzes verschiedentlich geändert. So wurden einige Fragen weggelassen und andere verdeutlicht. Vor allem wird der Kunde durch verschiedene Hinweise darüber aufgeklärt, daß

diese Angaben zur Bonitätsprüfung und für eine Anfrage bei der Schufa benötigt werden. Auch erfährt der Kunde von den notwendigen Mitteilungen, z.B. der Anschrift, an Zulieferer.

Überraschenderweise erreichte mich vor einigen Tagen eine Eingabe, in der sich jemand darüber beschwert, der sich mit einer Bestellung in Höhe von ca. 200,– DM an ein Versandhaus gewandt hatte und bei Lieferung zahlen wollte. Nach Darstellung des Petenten bestand das Versandhaus gleichwohl auf den für die Schufa-Anfrage notwendigen Daten. Diesen Fall habe ich noch nicht näher untersuchen und abschließend behandeln können.

6.) In einigen Fällen konnte ich Bürgern, die sich an mich wandten, bedauerlicherweise nicht weiterhelfen:

Ein arbeitsloser Bürger hatte sich z.B. auf eine chiffrierte Stellenanzeige gemeldet und seine Bewerbungsunterlagen eingeschickt. Die erhielt er einige Tage später mit einem Ablehnungsschreiben zwar zurück; das Schreiben ließ jedoch den Absender nicht erkennen, so daß der Bürger nicht wußte, wer seine Daten möglicherweise verwertet hatte. Ich konnte dem Bürger nicht behilflich sein und den Datenempfänger nicht ermitteln.

In solchen Fällen besteht sicherlich eine Mißbrauchsgefahr. Wer ihr entgehen will, darf entweder gar nicht auf chiffrierte Stellenanzeigen reagieren oder sollte sich damit begnügen, nur kurz – ohne Unterlagen – sein Interesse zu bekunden.

Überhaupt sollte sich jeder darüber im klaren sein, daß er kostenlos seine Adresse (evtl. mit Alter, Berufsbezeichnung und weiteren Angaben) zur Verfügung stellt, wenn er sich an Preisausschreiben und ähnlichen Werbeaktionen beteiligt.

4.3 Beobachtung der automatisierten Datenverarbeitung

4.3.1 Stand der Automation in der hamburgischen Verwaltung

Zu meinen Aufgaben gehört es auch, den Stand und die Entwicklung der automatisierten Datenverarbeitung in der hamburgischen Verwaltung zu beobachten. Hierfür stehen mit den Niederschriften über die Sitzungen des Unterausschusses Stellenplan des Haushaltsausschusses der Bürgerschaft am 6. und 19.2.1981 umfassende und aussagekräftige Unterlagen zur Verfügung, die mir die eigene Bestandsaufnahme für die Behörden und Ämter der Freien und Hansestadt Hamburg sehr erleichtern, ein im Hinblick auf meine knappe Personalausstattung glücklicher Umstand. (Die Niederschriften sind vom Senatsamt für den Verwaltungsdienst unter dem Titel „Automation in der hamburgischen Verwaltung" im September 1981 als Broschüre veröffentlicht worden.) Die Feststellungen des Unterausschusses treffen nach meinen Ermittlungen auch heute noch weitgehend zu. Aus Sicht des Datenschutzes ist zu Stand und Entwicklung der Automation in der hamburgischen Verwaltung folgendes zu bemerken:

Die Behörden der Freien und Hansestadt Hamburg bedienen sich zur Verarbeitung ihrer automatisierten Verfahren der Datenverarbeitungszentrale bei der Finanzbehörde. Die weit überwiegende Zahl der dort durchgeführten automatisierten Verfahren ist in der Form der zentralen Stapelverarbeitung organisiert, d.h. die zu verarbeitenden Dateien werden auf Papierbelegen zur Datenverarbeitungszentrale transportiert und dort unter jederzeitiger Kontrolle des Personals verarbeitet.

Nach den Feststellungen im Unterausschuß Stellenplan ist der Stand der äußeren Datensicherung (Abwehr eines Angriffs von außen) gut, und auch die innere Datensicherung bietet bei dem praktizierten Konzept der physischen Trennung von Test und echter Verarbeitung zu Bedenken kaum Anlaß. Die Gefahr mißbräuchlicher Datenverarbeitung ist daher bei diesen Verfahren gering. Der Stand der inneren Datensicherung muß aber – auch unter dem Aspekt der weiteren technischen und betrieblichen Entwicklung – laufend beobachtet werden.

Bislang werden in der Datenverarbeitungszentrale nur zwei – aber umfangreiche und bedeutsame – ADV-Verfahren, das polizeiliche Informationssystem (POLAS) und – mit Einschränkungen – der Auskunftsbetrieb der Steuerverwaltung im Dialogbetrieb abgewickelt. In dieser Verarbeitungsform hat der Sachbearbeiter über Terminal (im allgemeinen Bildschirm und Tastatur) direkten Zugang zur Datenverarbeitungsanlage; über das Terminal kann er Daten eingeben, verändern und abrufen. Diese Aktivitäten stehen beim Dialogbetrieb nicht unter Kontrolle des Personals in der Datenverarbeitungszentrale; daher muß die leichter mögliche mißbräuchliche Benutzung durch technische und organisatorische Maßnahmen sowie durch Sicherheitsvorkehrungen in den Programmen verhindert werden. Auch wenn für die Dialogverfahren schon im Interesse der Integrität der Verfahren ein hohes Maß an Datensicherung angestrebt wird, ist es doch meine Aufgabe, das Erreichte kritisch zu prüfen und – soweit notwendig – Verbesserungsvorschläge zu machen. Dies gilt auch für die künftigen Dialogverfahren, die sich z.T. schon im Stadium der Planung oder Realisierung befinden (z.B. Umstellung der Datenerfassung für die Berechnung und Zahlung der Bezüge der Beamten, Angestellten und Arbeiter).

Neben der Datenverarbeitungszentrale bei der Finanzbehörde bestehen weitere Rechenzentren im Universitätskrankenhaus Eppendorf und in der Universität Hamburg. Über diese Rechenzentren und kleinere autonome Datenverarbeitungsanlagen in einigen Behörden sowie die Datenverarbeitungsanlagen bei den juristischen Personen des öffentlichen Rechts muß ich mich noch informieren.

Durch die Mitwirkung in verschiedenen Arbeitskreisen ist sichergestellt, daß ich über Stand und Entwicklung der automatisierten Datenverarbeitung in den Behörden der Freien und Hansestadt Hamburg informiert bleibe. Hier sind insbesondere der Behördenausschuß für automatisierte Datenverarbeitung (Austausch von Informationen und Erfahrungen über automatisierte Datenverarbeitung im Kreise leitender Beamter) und der Arbeitskreis ADV-Organisation und -Planung (regelmäßige Dienstbesprechung des Senatsamtes mit den Leitern der programmierenden Stellen in den Behörden und Ämtern der Freien und Hansestadt Hamburg) zu nennen.

4.3.2 Mitwirkung an Automationsvorhaben

Zu den datenschutzrelevanten Vorhaben, an denen ich aufgrund der Absprache mit den Staatsräten frühzeitig beteiligt werden soll, gehört auch und gerade die Entwicklung automatisierter Verfahren. Dadurch habe ich die Möglichkeit, die Anliegen des Datenschutzes in die weitere Entwicklung der Automation in der hamburgischen Verwaltung einzubringen.

Bisher habe ich an zwei Automationsvorhaben mitgewirkt (s. 6.4 und 6.10.2):

- Automatisiertes Verfahren zum Abbau der Fehlsubventionierung und der Mietverzerrung (Fehlbelegungsabgabe) und

- Teilnahme des Versorgungsamtes Hamburg am Niedersächsischen automatisierten Verfahren für die Zahlung der Versorgungsrente.

4.4 Datenschutzregister nach § 13

4.4.1 Rechtsgrundlagen

Nach § 13 führt der DSB das Datenschutzregister. Es enthält Angaben zu allen Dateien, die unter das Hamburgische Datenschutzgesetz fallen, und gliedert sich in zwei Teile:

1.) Dateien der Behörden und sonstigen öffentlichen Stellen der Freien und Hansestadt Hamburg (mit Ausnahme des Landesamtes für Verfassungsschutz – s. § 13 Abs. 4 – und der unter 2.) genannten Behörden) und

2.) Dateien der Staatsanwaltschaft und der Polizei sowie der Landesfinanzbehörden, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung in Dateien speichern; dieser Teil wird besonders geführt (§ 13 Abs. 3 Nrn. 1 und 2).

In dem Datenschutzregister sind alle automatisierten Dateien enthalten sowie die nicht automatisierten Dateien, deren Daten zur Übermittlung bestimmt sind. Nicht automatisierte Dateien, deren Daten nicht zur Übermittlung bestimmt sind (sog. interne Dateien – § 1 Abs. 2 Satz 2), werden nicht in das Datenschutzregister aufgenommen.

Das Datenschutzregister ist

- Informationsgrundlage für den Bürger über die von der Verwaltung gespeicherten personenbezogenen Daten, damit er gezielt sein Recht auf Auskunft und weitere Rechte wahrnehmen kann. Zu diesem Zweck hat jeder ein Recht auf Einsicht in das Datenschutzregister und auf Auszüge daraus (§ 13 Abs. 2). Der Bürger hat diese Rechte jedoch nicht bezüglich des oben unter 2.) erwähnten besonderen Teils des Datenschutzregisters.

- Arbeitsgrundlage für meine Überwachungstätigkeit; die Übersicht über alle Dateien (einschl. der Dateien im besonderen Teil des Datenschutzregisters) macht es mir möglich, meine Kontrollmaßnahmen z.B. nach dem Gefährdungspotential zu planen, das von den Dateien ausgeht (Art der gespeicherten Daten, betroffener Personenkreis, Verwendungszweck).

§ 13 Abs. 5 ermächtigt den Senat, Einrichtung und Führung des Datenschutzregisters sowie Meldungen zum Datenschutzregister durch Rechtsverordnung zu regeln. Ein erster Entwurf liegt vor. Ich habe angeregt, hieran zunächst nicht weiterzuarbeiten, weil ich die Erfahrungen aus dem Aufbau des Datenschutzregisters auswerten und in die endgültige Fassung der Verordnung einfließen lassen möchte.

4.4.2 Dateien der öffentlich-rechtlichen Wettbewerbsunternehmen

§ 2 Abs. 2 regelt, welche Datenschutzvorschriften auf öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen (sog. öffentlich-rechtliche Wettbewerbsunternehmen), anzuwenden sind. Damit diese Unternehmen keine Nachteile gegenüber ihren Wettbewerbern erleiden, werden auf sie

- nur § 16 (datenschutzrechtliche Eigenkontrolle), § 17 (Schadensersatzanspruch) und der Dritte Abschnitt HmbDSG (hier relevant: Vorschriften über die Überwachung durch den DSB) und

- im übrigen die Vorschriften des BDSG angewendet, die für die privaten Konkurrenten ebenfalls gelten.

§ 2 Abs. 2 zählt § 13 nicht als anzuwendende Vorschrift auf. Da die öffentlich-rechtlichen Wettbewerbsunternehmen meiner Überwachung unterliegen und das Datenschutzregister die Arbeitsgrundlage hierfür ist, müssen die in den öffentlich-rechtlichen Wettbewerbsunternehmen geführten Dateien ebenfalls im Datenschutzregister enthalten sein. Aus den Gesetzesmaterialien ergeben sich auch keine Hinweise darauf, daß die Anwendung des § 13 auf die öffentlich-rechtlichen Wettbewerbsunternehmen bewußt ausgeschlossen worden ist. Ich werde mich bei der nächsten Novellierung um eine Klarstellung bemühen.

4.4.3 Dateien der Sozialleistungsträger

Gem. § 79 Abs. 1 SGB X ist auf die Datenverarbeitung im Sozialleistungsbereich (§§ 11 ff SGB I) das BDSG anzuwenden, auch wenn die entsprechenden Aufgaben von Landesbehörden ausgeführt werden; damit ist das ursprünglich angestrebte Prinzip durchbrochen,

daß für die Landesverwaltung einheitlich das jeweilige Landesdatenschutzgesetz gelten soll (vgl. § 7 Abs. 2 Satz 1 BDSG). Das Nebeneinander von BDSG (über § 79 SGB X) und HmbDSG hat – neben anderen Problemen – für das Datenschutzregister zur Folge, daß

- alle unter das BDSG fallenden Dateien des Sozialleistungsbereichs gem. § 12 BDSG zu veröffentlichen sind,

- nur die automatisierten Dateien des Sozialleistungsbereichs zum Datenschutzregister gemeldet werden müssen, weil § 13 auf sie nicht anzuwenden ist und nach § 19 Abs. 4 BDSG (der gem. § 79 Abs. 3 SGB X entsprechend anzuwenden ist) nur die automatisierten Dateien in das Datenschutzregister aufzunehmen sind.

Ich habe die für Sozialleistungen zuständigen Behörden und Ämter gleichwohl gebeten, auch ihre nicht automatisierten Dateien zum Datenschutzregister zu melden, weil zum einen der Bürger für das Fehlen dieser Dateien im Register und den Hinweis auf die – noch nicht erfolgte – Veröffentlichung kein Verständnis hätte und zum anderen das Register als Arbeitsgrundlage des DSB unvollständig wäre. Eine Veröffentlichung der Dateien aus dem Sozialleistungsbereich unter Beachtung von § 12 BDSG läßt sich auf der Grundlage des Datenschutzregisters ohne Schwierigkeiten durchführen.

4.4.4 Verwertung früherer Arbeitsergebnisse

Das Senatsamt für den Verwaltungsdienst hat im Jahre 1978 für die Veröffentlichung der Dateien gem. § 12 BDSG (das damals für die hamburgische Verwaltung galt, soweit sie Bundesrecht ausführte) und – vorsorglich – auch für das nach dem zu erwartenden Hamburgischen Datenschutzgesetz erforderliche Datenschutzregister Meldungen über folgende Dateien der Behörden der Freien und Hansestadt Hamburg erstatten lassen:

- Dateien, die der Ausführung von Bundesrecht dienen,
- Dateien, die der Ausführung von Landesrecht dienen,
- Dateien im rechtsfreien Raum,
- Dateien der Personalverwaltung (die nach § 7 Abs. 3 BDSG nicht unter die Veröffentlichungspflicht fallen),
- gesetzlich vorgeschriebene Register oder sonstige aufgrund von Rechts- oder veröffentlichten Verwaltungsvorschriften zu führende Dateien (§ 12 Abs. 2 Nr. 3 BDSG).

Das Datenschutzregister gem. § 13 wird die oben aufgeführten Dateien und zusätzlich die Dateien der juristischen Personen des öffentlichen Rechts, die der Aufsicht der Freien und Hansestadt Hamburg unterstehen einschließlich der Dateien der öffentlich-rechtlichen Unternehmen, die am Wettbewerb teilnehmen (mit Ausnahme der öffentlich-rechtlichen Kreditinstitute), enthalten.

Es bot sich daher an, auf den im Jahre 1978 geleisteten Vorarbeiten aufzubauen. Da für das Datenschutzregister zusätzliche Angaben gefordert werden, mußten die Behörden und Ämter alle früheren Meldungen überarbeiten.

4.4.5 Stand des Registers

Mit Rundschreiben vom 5. Juli 1982 habe ich die Behörden und Ämter aufgefordert,

- alle beigefügten früheren Meldungen zu überarbeiten und zu ergänzen,
- neue Dateien zu melden und
- entsprechende Rundschreiben an die ihrer Aufsicht unterstehenden juristischen Personen des öffentlichen Rechts weiterzugeben, damit auch diese mir ihre Dateien melden.

Die Meldungen sind zu einem großen Teil termingerecht eingegangen; einige Behörden haben Terminverlängerung erbeten. Die Meldungen der juristischen Personen des öffentlichen Rechts gehen nur zögernd ein. Dennoch hoffe ich, das Datenschutzregister, wie beabsichtigt, zum 31. Dezember 1982 einrichten zu können.

Damit wird auch die Voraussetzung dafür geschaffen sein, daß in der ersten Hälfte des Jahres 1983 die Übersicht gem. § 13 Abs. 1 Satz 3 erarbeitet und veröffentlicht werden kann.

4.4.6 Sonstige Probleme

Aus Rückfragen der Behörden während der Bearbeitung der Meldungen und aus der ersten Durchsicht der Meldungen haben sich einige Probleme ergeben, die hier nur skizziert werden sollen:

1.) Was sind nicht-automatisierte Dateien, deren Daten nicht zur Übermittlung bestimmt sind

Es wird häufig verkannt, daß es zur Beurteilung dieser Frage auf die Zweckbestimmung ankommt. Wenn die Daten nach den Rechts- und Verwaltungsvorschriften oder den organisatorischen Festlegungen, die der Datei zugrundeliegen, übermittelt werden sollen oder können, kommt es nicht darauf an, ob und in welchem Umfang auch tatsächlich Daten übermittelt werden; die Datei ist dann nicht intern und zum Datenschutzregister zu melden. Eine interne Datei liegt vor, wenn die Daten nicht zur Übermittlung bestimmt sind. In diesem Falle bleiben die Zweckbestimmung („Nicht-Übermittlung") und damit die Eigenschaft „interne Datei" erhalten, auch wenn im Einzelfall entgegen der sonst aufrechterhaltenden Zweckbestimmung Daten aufgrund gerichtlicher oder behördlicher Anweisung oder zu vertraglichen Prüfungen übermittelt werden.

2.) Übereinstimmung des Inhalts von Akten und Datei

Wenn der Inhalt einer Datei identisch ist mit dem Inhalt von parallel geführten Akten, kommt es nicht darauf an, ob Daten aus der Datei oder aus den Akten übermittelt werden. Für die Übermittlung der Daten gelten – unabhängig davon, ob die Übermittlung im Einzelfall aus der Datei erfolgt – die §§ 10 und 12. Die Datei ist zum Datenschutzregister zu melden.

3.) Dateien in der Personalverwaltung

Die Dateien in den Personalverwaltungen der Behörden und Ämter sind weitgehend einheitlich. Da die Behörden und Ämter dennoch bei der Meldung zum Datenschutzregister unterschiedlich verfahren, habe ich das Senatsamt für den Verwaltungsdienst gebeten, die Meldungen der Dateien in der Personalverwaltung zu koordinieren.

4.) Dateien in der Steuerverwaltung

Die Steuerverwaltungen des Bundes und der Länder haben bisher den Standpunkt vertreten, daß alle in der Steuerverwaltung geführten Dateien „in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung" gespeichert werden und daher zum besonderen Teil des Datenschutzregisters zu melden sind, der der Einsicht durch den Bürger entzogen ist (s. § 13 Abs. 3 Nr. 2). Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu die Ansicht vertreten, daß die Ausnahmeregelung einer Vorschrift wie § 13 Abs. 3 Nr. 2 nach dem Zweck dieser Vorschrift, eine Ausforschung der Steuerverwaltung zu verhindern, beurteilt und daher im einzelnen geprüft werden muß, welche Dateien der Steuerverwaltung zum allgemeinen, der Einsicht zugänglichen Teil und welche zum besonderen Teil des Datenschutzregisters gehören. Ich werde nach Vorliegen der Meldungen der Finanzbehörde Gespräche mit dieser aufnehmen.

4.5 Register nach § 40 BDSG

Nach § 39 Abs. 1 BDSG haben die dem Vierten Abschnitt des BDSG unterstehenden Stellen die Aufnahme ihrer Tätigkeit innerhalb eines Jahres der Aufsichtsbehörde anzumelden. Die der Aufsichtsbehörde mitzuteilenden Angaben ergeben sich aus § 39 Abs. 2 BDSG. Nach § 40 BDSG hat die Aufsichtsbehörde hierüber ein öffentliches Register zu führen.

Für Hamburg wurde dieses Register Anfang 1978 von der bisher zuständigen Behörde für Wirtschaft, Verkehr und Landwirtschaft eingerichtet. Es wird in Form von Karteikarten geführt und bildet die Grundlage für die Überwachungstätigkeit der Aufsichtsbehörde nach dem Vierten Abschnitt des BDSG.

Im Register sind zur Zeit 182 datenverarbeitende Stellen verzeichnet, sie gliedern sich wie folgt:

- Dem § 31 Abs. 1 Nr. 1 BDSG sind 14 Stellen zuzuordnen. Dazu zählen vor allem die Schufa Hamburg und einige Wirtschaftsauskunfteien, aber auch zentrale Auskunfteien, die bei überregional, z.T. bundesweit wirkenden Wirtschaftsverbänden oder Vereinen angesiedelt sind.

- Dem § 31 Abs. 1 Nr. 2 BDSG sind 10 Stellen zuzuordnen. Dabei handelt es sich hauptsächlich um Markt- und Meinungsforschungsinstitute, aber auch um Institutionen, die für gezielte Vorhaben (z.B. Stadtsanierung) Planungsdaten zusammentragen.

- Dem § 31 Abs. 1 Nr. 3 BDSG sind 158 Stellen zuzuordnen. Hierher gehören vor allem Service-Rechenzentren und Datenerfassungsunternehmen. Es haben sich viele Stellen zum Register angemeldet, die ihre Auftrags-Datenverarbeitung nur im Rahmen verbundener Unternehmen durchführen.

  Eine weitere große Gruppe sind die Unternehmen, die eine Auftrags-Datenverarbeitung nur in relativ geringem Umfang (z.B. zur Kapazitätsauslastung) durchführen. Es gibt auch Stellen, die Datenverarbeitungs-Aufträge entgegennehmen und zur Durchführung einen oder mehrere Subunternehmer einsetzen.

  Weiter sind auch die Unternehmen meldepflichtig, die geschäftsmäßig das Löschen von Daten auf Datenträgern besorgen, wenn sie in ihrer Vertragsgestaltung und Werbung den Schwerpunkt ihrer Tätigkeit auf diese Phase der Datenverarbeitung verlagern und bestimmte Sicherheiten garantieren.

  Schließlich sind Unternehmen registriert, die im Auftragsverhältnis Adressen anderer Unternehmen verwalten und diese weisungsgemäß einsetzen.

Seit Beginn meiner Tätigkeit sind etwa 25 Registeränderungen erforderlich gewesen. Neu aufgenommen wurden 7 Stellen, während 4 Stellen gelöscht wurden.

4.6 Beratungen und Prüfungen

4.6.1 Beratungen und Prüfungen im öffentlichen Bereich

In meiner kurzen Amtszeit sind von den Behörden und Ämtern der Freien und Hansestadt Hamburg und den ihrer Aufsicht unterstehenden juristischen Personen des öffentlichen Rechts zahlreiche allgemeine Fragen und Einzelprobleme an mich herangetragen worden; hierüber wird unter 6. im jeweiligen Sachzusammenhang berichtet. Ich werte die vielen Anfragen als einen Beweis für die Kooperationsbereitschaft der Stellen, die ich zu kontrollieren habe. Trotz der – auch wegen der anderen zu erledigenden Aufgaben – knappen Personalkapazität bemühen wir uns, allen Wünschen nach Beratung unverzüglich nachzukommen. Angesichts der Fülle der vordringlich zu erledigenden Aufgaben war es bisher nicht

möglich, Stellen, die personenbezogene Daten verarbeiteten oder durch andere Stellen verarbeiten lassen (speichernde Stellen), oder Stellen, die im Auftrag verarbeiten (Rechenzentren), systematisch zu prüfen. Wir haben aber drei Ortsbesichtigungen durchgeführt, über die unter 6.5.2, 6.7.4 und 6.9.1 im Sachzusammenhang berichtet wird.

4.6.2 Beratungen und Prüfungen im nicht-öffentlichen Bereich

Da das BDSG die Beratung der betrieblichen Datenschutzbeauftragten besonders hervorhebt, hat es schon vor meiner Amtszeit zahlreiche Kontakte zwischen Unternehmen und Aufsichtsbehörde gegeben. Systematische Kontrollen bei den Unternehmen des Vierten Abschnitts sind noch nicht durchgeführt worden. Ich werde jedoch Anfang nächsten Jahres mit turnusmäßigen Überwachungen beginnen.

4.7 Kooperation im Datenschutz

Wegen der Übereinstimmung der Probleme und der Aufgabenstellung ist eine enge Zusammenarbeit der Beteiligten, insbesondere der für die Überwachung zuständigen Behörden, wichtig, um Doppelarbeit und widersprüchliche Entscheidungen zu vermeiden. Ich werde mich an der bestehenden Zusammenarbeit rege beteiligen.

4.7.1 Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Die Konferenz ist im Dezember 1978 eingerichtet worden und hat seither 13 Sitzungen abgehalten. In der Konferenz werden allgemein interessierende Probleme erörtert mit dem Ziel, eine gemeinsame Auffassung zu erarbeiten. In den letzten Sitzungen hat die Konferenz z.B.

- zur Novellierung des BDSG,
- zu Datenschutzproblemen in der Steuerverwaltung und zu den Datenschutzregelungen im vorgesehenen Staatsvertrag über Bildschirmtext Stellung genommen.

Die Stellungnahmen der Konferenz werden in Arbeitskreisen vorbereitet, in denen Erfahrungen ausgetauscht und Datenschutzprobleme im Detail erörtert werden. Die knappe Personalausstattung zwingt mich, bei der Mitwirkung in den Arbeitskreisen Prioritäten zu setzen, die sich nach den Schwerpunkten meiner künftigen Arbeit richten werden.

4.7.2 Kooperation mit Aufsichtsbehörden anderer Bundesländer

Seit Bestehen des BDSG treffen sich die obersten Aufsichtsbehörden der Bundesländer im sog. „Düsseldorfer Kreis" mit dem Ziel, eine möglichst einheitliche Anwendung des BDSG in allen Bundesländern zu gewährleisten.

Zu diesem Zweck beschäftigte sich der „Düsseldorfer Kreis" zunächst mit Grundsatzfragen und Definitionen; dies geschah in enger Zusammenarbeit mit Spitzenverbänden der Wirtschaft. Ergebnis waren vorläufige Verwaltungsvorschriften, die in Hamburg als „Hinweise zur Anwendung des BDSG" (Amtlicher Anzeiger 1978, S. 953 ff., S. 2171 ff. und 1981 S. 533 ff.) veröffentlicht sind.

Im Jahr 1982 tagte der „Düsseldorfer Kreis" dreimal. Herausragendes Thema war auch hier die Novellierung des BDSG. Ständig werden Angelegenheiten der Schufa und der Wirtschaftsauskunfteien behandelt, auch über den Verlauf der Grenze zwischen Drittem und Viertem Abschnitt muß anhand von Einzelfällen immer wieder diskutiert werden. Von aktueller Bedeutung gerade für Hamburg ist die Beurteilung zentraler Karteien von Versicherungsverbänden und der damit zusammenhängenden Übermittlungsverfahren; zwei betroffene Verbände haben hier ihren Sitz.

4.7.3 Kooperation mit betrieblichen Datenschutzbeauftragten

Die Aufsichtsbehörde in Hamburg ist regelmäßig Gast in einigen Arbeitskreisen betrieblicher Datenschutzbeauftragter.

Bei diesen Treffen bietet sich Gelegenheit, die Haltung der Aufsichtsbehörde zu aktuellen Fragen zu verdeutlichen und die im „Düsseldorfer Kreis" erarbeiteten Ergebnisse an diejenigen weiterzuleiten, die es vornehmlich angeht. Als vorteilhaft für die praktische Arbeit hat sich der Kontakt zu den betrieblichen Datenschutzbeauftragten auch insofern herausgestellt, als die Auswirkungen und Schwierigkeiten bei der Umsetzung mancher Beschlüsse der Aufsichtsbehörde direkt vorgetragen werden können. In den Arbeitskreisen werden oftmals grundsätzliche Fragen aufgeworfen, deren Klärung der Fortentwicklung des Datenschutzrechts dient.

5. Allgemeine Fragen des Datenschutzes

5.1 Zur Lage des Datenschutzes in Hamburg

Zur Lage des Datenschutzes haben sich die anderen Datenschutzbeauftragten in ihren letzten Tätigkeitsberichten und sonstigen Veröffentlichungen ausführlich geäußert. Ich möchte ihrer Beurteilung mit meinem 1. Tätigkeitsbericht keinen eigenen Beitrag hinzufügen. Hierzu reichen die Erfahrungen, die ich in meiner kurzen Amtszeit gesammelt habe, nicht aus. Auch kann ich nicht ausschließen, daß sich die Verhältnisse in Hamburg von der Situation in anderen Ländern aus mancherlei Gründen unterscheiden.

Die noch junge Institution des Hamburgischen Datenschutzbeauftragten wird im allgemeinen positiv aufgenommen. Die Beteiligten warten in vielen Fällen noch ab, welche Richtung der DSB einschlagen und welchen Stil er praktizieren wird. Soweit ich zur Klärung von Einzelfällen mit Bürgern, Verwaltung oder Wirtschaft Kontakt habe, habe ich ich mich bemüht deutlich zu machen, daß ich mich bei der Lösung von Konflikten nach allen Seiten fair verhalten will. Ich habe den Eindruck, daß die Beteiligten diese Haltung würdigen und mir ein gewisses Maß an Vertrauen entgegenbringen.

Um weitere Klarheit über meine Einstellung zu vermitteln, habe ich im folgenden meine Position zu einigen Fragen umrissen, die in der allgemeinen Diskussion um den Datenschutz immer wieder eine Rolle spielen, häufig zu völlig falschen Frontstellungen führen und eine sachliche Konfliktlösung behindern. Ich hoffe, damit zur Erhaltung und Verstärkung des Datenschutzbewußtseins und zur Akzeptanz des DSB beizutragen.

5.2 Datenschutz in der Kritik

Die Erwartungen, denen der Datenschutz als eine im Spannungsfeld zwischen den Bürgern einerseits sowie Verwaltung und Wirtschaft andererseits angesiedelte Einrichtung ausgesetzt ist, sind naturgemäß unterschiedlicher Art. Dementsprechend unterscheiden sich auch die Blickwinkel, aus denen Kritik geübt wird. Der DSB muß sich dieser Kritik von allen Seiten stellen, denn die Fähigkeit zum Meinungsaustausch mit den Beteiligten sowie die Bereitschaft, daraus zu lernen, sind Grundbedingungen seiner Tätigkeit. Allgemein gilt, daß mit dem Datenschutz vorsichtig umgegangen werden sollte.

5.2.1 Datenschutz als Vorwand

Häufig muß der Datenschutz als Begründung für Dinge herhalten, die mit ihm nichts oder sehr wenig zu tun haben. Folgende Beispiele (wie auch die späteren aus der Arbeit der letzten Tage vor Abfassung dieses Berichts) seien dazu genannt:

- Die Meldestelle in einem Bezirksamt verweigert einem Bürger die Auskunft über die neue Anschrift eines verzogenen Bürgers, weil das Datenschutzrecht das verbiete. Tatsächlich kann sie die neue Anschrift nicht bekanntgeben, weil sie sie nicht mehr hat; sie wird nur im Einwohnerzentralamt gespeichert.

- Immer wieder kommt es vor, daß Übermittlungen unter Hinweis auf den Datenschutz abgelehnt werden, obwohl sie datenschutzrechtlich durchaus zulässig wären; man will aus anderen Gründen nicht übermitteln, z.B. weil der Aufwand für zu hoch gehalten wird.

In diesen Fällen wird der Datenschutz als Vorwand benutzt, um lästige Diskussionen über die wahren Gründe zu vermeiden.

Hierdurch wird der Datenschutz diskreditiert; ich werde daher in solchen Fällen, soweit sie mir bekannt werden, dafür werben, daß die wahren Gründe ehrlich genannt werden, und ggf. klarstellen, daß der Datenschutz mißbraucht wird.

5.2.2 Mißverstandener Datenschutz

Häufig werden Übermittlungen „aus Gründen des Datenschutzes" abgelehnt, obwohl die Voraussetzungen für eine Weitergabe vorliegen. In diesen Fällen ist entweder überhaupt nicht geprüft worden, ob eine Übermittlung hätte erfolgen dürfen, oder aber die übermittelnde Stelle ist sich über die Voraussetzungen im unklaren gewesen und hat die Übermittlung vorsichtshalber abgelehnt.

Diese Entscheidungen stoßen zu Recht auf Unverständnis. Folgende Beispiele mögen das belegen:

- Jemand erleidet während der Teilnahme an einem Sportlehrgang einen Unfall. Für die Auseinandersetzung mit der Versicherung benötigt er die Adressen der übrigen Kursusteilnehmer, die als Zeugen benannt werden sollen. Der veranstaltende Verein verweigert die Herausgabe unter Berufung auf den Datenschutz, obwohl das berechtigte Interesse des Geschädigten offensichtlich auch dann höher zu bewerten ist, wenn ein Teilnehmer wider Erwarten nicht bereit sein sollte, zur Aufklärung des Sachverhalts beizutragen.

- Sog. Klassenlisten (Verzeichnis aller Schüler mit Namen, Anschrift, Telefonnummer, u.U. Geburtsdatum) werden unter Berufung auf Datenschutz nur dann angefertigt und verteilt, wenn alle Eltern – schriftlich – ihr Einverständnis erklären, obwohl die schutzwürdigen Belange der Eltern auch dann gewahrt sind, wenn ihnen die Möglichkeit des Widerspruchs gegeben wird.

Ich habe Verständnis dafür, daß man sich in der Anfangsphase des Datenschutzes aus Unkenntnis häufig für Abwarten entschieden hat. Aber: Heute kann Unkenntnis als Rechtfertigung für Nichtstun nicht mehr akzeptiert werden. Soweit noch Unsicherheiten bestehen, sind die Entscheidungsbefugten in Verwaltung und Wirtschaft verpflichtet, durch geeignete Maßnahmen (Fortbildung) Klarheit herbeizuführen. Ich bin bereit, dazu meinen Beitrag zu leisten. Im übrigen bin ich mir darüber im klaren, daß Datenschutz für alle Beteiligten ein fortwährender Lernprozeß ist.

5.2.3 Datenschutz contra Effizienz

Bisweilen wird in der Verwaltung die Neigung erkennbar, den Datenschutz als Hindernis für vernünftiges Verwaltungshandeln hinzustellen. Es bleibt aber wenig übrig, wenn diese Befürchtungen substantiiert werden sollen. Ich begrüße es allerdings, wenn diese Befürchtungen ausgesprochen werden. Erst aufgrund eines regen Meinungsaustausches und einer intensiven Kooperation mit der Verwaltung können ausgewogene Ergebnisse erzielt werden, die den Belangen beider Seiten Rechnung tragen.

Die modernen Datenverarbeitungs- und Kommunikationstechniken ermöglichen der Verwaltung beträchtliche Steigerungen der Effizienz; allerdings muß die Ausnutzung der technischen Möglichkeiten dort ihre Grenze finden, wo die Persönlichkeitsrechte beeinträchtigt werden. Dieses Spannungsverhältnis zwischen effizienter Datenverarbeitung einerseits und dem Schutz der Privatsphäre andererseits muß in jedem konkreten Fall neu aufgelöst werden. Dabei haben weder die Effizienz noch der Datenschutz absolut und immer Vorrang. Beides liegt im Interesse des Bürgers.

Zweifellos hat der Datenschutz Erschwerungen in der Verwaltung und damit zumindest unsichtbare Kosten verursacht (z.B. macht die Beachtung zusätzlicher Formalitäten die Abläufe starrer). Zugleich hat er aber auch für mehr Transparenz und damit Klarheit in der Verantwortlichkeit gesorgt, z.B.

- dient die schriftliche Auftragserteilung in einem Rechenzentrum der Kontrolle der datenschutzrechtlichen Zulässigkeit und dem Nachweis der Kostenverantwortung;
- soll die formelle Freigabe automatisierter Verfahren durch die fachlich zuständige Stelle aufgrund eigener Prüfungen diese dazu veranlassen, sich von der datenschutzrechtlichen Zulässigkeit des Verfahrens zu überzeugen; zugleich bewirkt sie, daß die fachlich zuständige Stelle sich auf ihre fachliche Verantwortung für das automatisierte Verfahren besinnt.

In vielen Fällen führt der Datenschutz sogar zu einer Rationalisierung der Informationsverarbeitung, wenn z.B.

- in einer jährlich neu zu erhebenden Statistik durch Wegfall von Namen, Anschriften sowie weiteren, für die Statistik nicht unbedingt erforderlichen Daten der Aufwand für die Erhebung auf die Hälfte reduziert werden kann,
- die Forderung des Datenschutzes nach einer laufenden Bereinigung der zentralen Namenskartei der Staatsanwaltschaft das Vorhaben einer Automatisierung dieser Kartei beschleunigt, die vor allem das Ergebnis hat, daß der Aufwand für die Führung der Kartei beträchtlich vermindert wird.

Je länger sich die Verwaltung mit den Belangen des Datenschutzes auseinandersetzen muß, umso deutlicher wird sie erkennen, daß Datenschutz und Effizienz keine Gegensätze sein müssen.

6. Einzelne Probleme des Datenschutzes im öffentlichen Bereich

In der kurzen Berichtszeit konnte ich naturgemäß nur wenige konkrete Datenschutzprobleme bearbeiten, in den meisten Fällen aufgrund äußerer Anstöße. Erst die Tätigkeit im nächsten (ein volles Jahr umfassenden) Berichtszeitraum wird es mir ermöglichen, die Datenschutzprobleme im öffentlichen (wie auch im nicht-öffentlichen) Bereich vollständig aufzuarbeiten.

6.1 Neue Medien

Von den unter dem Titel „neue Medien" zusammengefaßten Zukunftstechnologien steht der Bildschirmtext kurz vor der Realisierung. Die Konferenz der Datenschutzbeauftragten hat im April 1982 Vorschläge für eine bereichsspezifische Datenschutzregelung verabschiedet, die aufgrund des besonderen Gefährdungspotentials von Bildschirmtext notwendig ist. Die Vorschläge wollen verhindern, daß mit den beim Betrieb von Bildschirmtext zwangsläufig anfallenden Daten – gleichgültig von wem – Persönlichkeitsprofile erstellt werden können. Aus dem gleichen Grund sollen auch die Möglichkeiten der Anbieter, Daten der Teilnehmer zu erheben und zu verarbeiten, eingeschränkt werden.

Der jetzt vorliegende Entwurf des Staatsvertrages berücksichtigt weitgehend die Vorschläge der Datenschutzbeauftragten; wegen der weiteren Verhandlungen über den Staatsvertrag habe ich mit der Senatskanzlei Kontakt.

In Hamburg wird nach dem gegenwärtigen Stand der Planung im November 1983 eine Bildschirmtextzentrale eingerichtet werden.

6.2 Archivwesen

6.2.1 Hauskartei

Das Staatsarchiv hat die sog. Hauskartei (das bis 1968 manuell geführte Melderegister, nach Straßen und Hausnummern geordnet) nach Ablösung durch die noch heute bestehende Lochkartenkartei übernommen. Das Staatsarchiv hat die Hauskartei auf Mikrofilm übertragen. In ihrer heutigen Form ist sie also keine Datei, da sie nicht nach anderen Merkmalen als Straße/Hausnummer umgeordnet und ausgewertet werden kann. Nur die Hauskartei ermöglicht den regionalen Nachweis der Wohnbevölkerung vor dem 1. Januar 1968. Deshalb muß gelegentlich auch heute noch auf die Hauskartei zurückgegriffen werden; in Amtshilfe für die Meldebehörden werden aus ihr Auskunft erteilt. Rechtliche Bedenken hiergegen bestehen nicht.

6.2.2 Archivklausel

Das Hamburgische Datenschutzgesetz schreibt in § 15 Abs. 3 vor, daß personenbezogenen Daten zu löschen sind, wenn ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und – ausnahmsweise – kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden. Daraus ergibt sich, daß das Staatsarchiv nur in den Fällen Dateien aus der Verwaltung übernehmen kann, in denen spezielle Rechtsvorschriften sog. Archivklauseln enthalten (vgl. z.B. § 11 Hamburgisches Meldegesetz (HmbMG)). In allen anderen Fällen wären die personenbezogenen Daten in den Dateien, die dem Staatsarchiv zur Übernahme angeboten werden, gem. § 15 Abs. 3 zu löschen. Denn das Angebot an das Staatsarchiv erfolgt ja nur, wenn die anbietende Stelle die angebotenen Daten nicht mehr zur Erfüllung ihrer Aufgaben benötigt.

Ich habe dieses Problem mit dem Staatsarchiv erörtert. Es hat keine aktuelle Bedeutung, weil das Staatsarchiv augenblicklich keine Dateien übernimmt. Es ist aber nicht auszuschließen, daß künftig auch Dateien in die Bestände des Staatsarchivs übernommen werden sollen. Nach den Parlamentsmaterialien hat das Archivproblem bei den Beratungen des Rechtsausschusses keine Rolle gespielt. Es dürfte bei der endgültigen Fassung des § 15 Abs. 3 schlicht übersehen worden sein.

Ich halte daher die baldige Einfügung einer Archivklausel in das HmbDSG nach dem Vorbild anderer Landesdatenschutzgesetze für erforderlich. Ich weise allerdings darauf hin, daß damit nicht alle Probleme gelöst würden, die mit der Speicherung und Verarbeitung personenbezogener Daten in Archiven verbunden sind. Die Konferenz der Bundesbeauftragten und der Landesbeauftragten für den Datenschutz hat im April 1982 Empfehlungen zur Sicherstellung des Datenschutzes im Archivwesen verabschiedet und darin eine gesetzliche Regelung für die Arbeit der Archive vorgeschlagen.

6.3 Steuerwesen

Die Konferenz der Datenschutzbeauftragten hat im September 1982 eine Entschließung verabschiedet, die nach langen kontroversen Auseinandersetzungen mit der Steuerverwaltung den Standpunkt der Datenschutzbeauftragten bekräftigt. Es geht dabei im wesentlichen um drei Probleme:

- Die Steuerverwaltungen geben den Datenschutzbeauftragten nur dann Auskünfte und Akteneinsicht über Vorgänge, die unter das Steuergeheimnis fallen, wenn die Datenschutzbeauftragten aufgrund von Bürgereingaben tätig werden. Im übrigen lassen die Steuerverwaltungen Kontrollen nicht zu, soweit das Steuergeheimnis berührt ist.

Sie übersehen dabei, daß § 30 der Abgabenordnung (Steuergeheimnis) eine bereichsspezifische Geheimhaltungs- und Übermittlungsvorschrift ist, die nur insoweit den Datenschutzgesetzen vorgeht. Weder § 30 noch eine andere Vorschrift der Abgabenordnung sagen etwas über die Überwachung durch die Datenschutzbeauftragten aus; daher gelten insoweit die entsprechenden Vorschriften der Datenschutzgesetze, in Hamburg § 20. Es wäre unverständlich und mit dem eindeutigen Wortlaut der Datenschutzgesetze nicht vereinbar, wenn dem Datenschutzbeauftragten als gesetzlichem Kontrollorgan das Steuergeheimnis entgegengehalten wird, dessen Einhaltung er zu kontrollieren hat.

Zudem ist § 20 Abs. 4 Nr. 1, aufgrund dessen die Behörden dem Datenschutzbeauftragten „. . . . Auskunft zu seinen Fragen sowie Einsicht in alle Unterlagen und Akten zu gewähren haben, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen . . . .", eine Vorschrift im Sinne von § 30 Abs. 4 Nr. 2, die eine Offenbarung zuläßt.

- Die Steuerverwaltungen melden ihre Dateien zum besonderen Teil des Datenschutzregisters, weil sie nach ihrer Ansicht ausnahmslos „im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung" geführt werden (hierauf bin ich unter 4.4.6 näher eingegangen).

- Die Steuerverwaltungen erhalten von Behörden und privaten Stellen sog. Kontrollmitteilungen über steuererhebliche Sachverhalte. Die Datenschutzbeauftragten halten die gegenwärtige Praxis der Kontrollmitteilungen für unzulässig, weil die rechtlichen Grundlagen (§§ 85, 93, 111 AO) entweder keine materiellen Eingriffsbefugnisse einräumen oder die Inanspruchnahme Nichtbeteiligter (Dritter) nur für den Fall vorsehen, daß die Sachverhaltsaufklärung durch den Beteiligten (Steuerpflichtigen) tatsächlich nicht zum Ziele führt oder keinen Erfolg verspricht; sie lassen es nicht zu, generell und vorsorglich im voraus Auskünfte zu verlangen.

Ich habe Gespräche mit der Steuerverwaltung in Hamburg aufgenommen.

6.4 Bauwesen

Im Berichtszeitraum stand hier die Stellungnahme zu dem beabsichtigten Automationsverfahren zur Erhebung der Fehlbelegungsabgabe nach dem Gesetz zum Abbau der Fehlsubventionierung und der Mietverzerrung im Wohnungswesen (AFWoG) in der Fassung des Art. 27 des Zweiten Gesetzes zur Verbesserung der Haushaltsstruktur (2. HStrukG) vom 22.12.1981 (BGBl. I S. 1523) im Vordergrund. Ich habe gegen das vorgesehene Verfahren und seine Nutzung durch die Clearingstelle für die Wohnungsvergabe an ausländische Wohnungssuchende keine Bedenken erhoben.

Das automatisierte Verfahren sieht vor, daß zunächst aus den Unterlagen der Wohnungsbaukreditanstalt, der Baubehörde und der Bezirksämter eine Datei aufgebaut wird, die alle (noch) öffentlich geförderten Wohnungen enthält. Für jede öffentlich geförderte Wohnung werden aus einer automatisierten, aus dem Melderegister abgeleiteten Datei die Daten über die Inhaber der Wohnung übernommen. Diese Datei wird benutzt, um dem Inhaber der Wohnung Erklärungsbogen zuzusenden. Die Angaben aus dem Erklärungsbogen ergänzen die Datei und dienen als Grundlage für die Berechnung der Fehlbelegungsabgabe. Ferner soll die Datei die bisher manuell geführte Wohnraumkartei ersetzen.

Die Speicherung der in dieser Datei vorgesehenen personenbezogenen Daten ist bis auf zwei Ausnahmen – die mit der Baubehörde diskutiert werden – nach Vorschriften des Gesetzes zur Sicherung der Zweckbestimmungen von Sozialwohnungen vom 30.7.1980 und des AFWoG (z.T. in Verbindung mit dem 2. Wohnungsbaugesetz) erforderlich und damit zulässig. Auch die vorgesehenen Übermittlungen von Daten aus dem Melderegister sind zulässig.

Die im automatisierten Verfahren vorgesehene Datei soll auch für die Clearingstelle für die Wohnungsvergabe an ausländische Wohnungssuchende genutzt werden. Der Senat hat die Clearingstelle eingerichtet; sie soll die Wohnungsvergabe an ausländische Wohnungssuchende lenken und überwachen, jedoch selbst keine Wohnungen vergeben. Auf diese Weise sollen zusätzliche Ausländerkonzentrationen nach Möglichkeit vermieden und vorhandene abgebaut werden (vgl. Antwort des Senats auf eine Große Anfrage betr. bisherige und zukünftige Ausländerpolitik in Hamburg, Drucksache 9/4390, S. 8). Zu diesem Zweck legt die Clearingstelle Vergabequoten für die Belegung von Sozialmietwohnungen in aufnehmenden und abgebenden Bezirken fest und überprüft die Erfüllung der Vergabequoten (vgl. Antwort des Senats auf eine Schriftliche Kleine Anfrage betr. Clearingstelle für die Wohnungsvergabe an ausländische Wohnungssuchende, Drucksache 10/99). Für ihre Aufgabe benötigt die Clearingstelle statistische Auswertungen über den Anteil von Ausländern in den Bezirken und die Belegung von Sozialmietwohnungen mit Ausländern. Hierfür kann die Datei für die Fehlbelegungsabgabe mitgenutzt werden, wenn sie um die Angabe „Staatsangehörigkeit" ergänzt wird. Ich halte die Speicherung des Merkmals „Staatsangehörigkeit" für zulässig, weil ohne sie eine Steuerung der Wohnungsvergabe an Ausländer nicht möglich ist; es ist aber nicht erforderlich, daß die Clearingstelle selbst personenbezogene Daten erhält. Verhandlungen mit der Baubehörde sind im Gange.

6.5 Statistik

6.5.1 Statistikklausel

Das Hamburgische Datenschutzgesetz enthält in § 11 eine besondere Regelung für die durch Rechtsvorschriften angeordneten statistischen Erhebungen und Auswertungen von personenbezogenen Daten (Amtliche Statistik).

Danach gelten für die Amtliche Statistik von den Vorschriften des HmbDSG

- nur § 8, der sie zu technischen und organisatorischen Maßnahmen der Datensicherung verpflichtet, und
- der Dritte Abschnitt, der sie der Überwachung durch den Hamburgischen Datenschutzbeauftragten unterwirft.

Die Speicherung und Übermittlung personenbezogener Daten richtet sich nach der jeweiligen anordnenden Rechtsvorschrift.

Mithin gelten u.a. nicht die Vorschriften über die Rechte des Betroffenen. Diese Ausnahme hat der Gesetzgeber wegen des besonderen Charakters der Datenverarbeitung in der Amtlichen Statistik gemacht, die zwar sehr viele personenbezogene Daten verarbeitet, aber den Personenbezug nur für gelegentliche Rückfragen oder Korrekturen, nicht aber für die statistische Auswertung nutzt. Ferner hat er berücksichtigt, daß die Amtliche Statistik eine lange und bewährte Tradition in der Geheimhaltung der ihr anvertrauten – nicht nur personenbezogenen – Daten hat (Statistikgeheimnis). Da der Betroffene seine Rechte nicht selbst wahrnehmen kann, hat die Überwachung durch den DSB umso größere Bedeutung.

6.5.2 Mikrozensus

Mehrere Bürger haben mich angerufen und sich besorgt und unwillig über den Mikrozensus geäußert. Ich habe dies zum Anlaß genommen, mich im Statistischen Landesamt über den Mikrozensus zu informieren.

Der Mikrozensus ist eine Bundesstatistik über die Bevölkerung auf repräsentativer Grundlage; er richtet sich nach dem Gesetz über die Durchführung einer Repräsentativstatistik der Bevölkerung und des Erwerbslebens vom 15.7.1975 (BGBl. I S. 2909). Das Gesetz schreibt vor, daß bestimmte Tatbestände in bestimmten Zeitabständen mit unterschiedlichen Auswahlsätzen erhoben werden. Mit den Ergebnissen des Mikrozensus werden die Ergebnisse der Großzählungen (letzte Volks- und Berufszählung 1971) fortgeschrieben. Das Mikrozensus-Gesetz gilt nur bis einschl. 1982; ein neues Mikrozensus-Gesetz ist in der parlamentarischen Beratung. Bei den Anrufen der Bürger zum Mikrozensus spielten drei Fragen eine besondere Rolle:

1.) Der Zwang zur Teilnahme an dem Mikrozensus

Die Anrufer vermißten die Möglichkeit, sich der Befragung entziehen zu können. Da der Mikrozensus eine Repräsentativstatistik ist, müssen die an der Befragung teilnehmenden Personen nach statistischen Methoden ausgewählt werden. Die am Mikrozensus teilnehmenden Personen werden über ihre Wohnungen ausgewählt. Die Wohnadressen werden zu Teileinheiten zusammengefaßt, die jede etwa gleich viele Wohnungen enthalten. Aus diesen wird über das gesamte Stadtgebiet verteilt 1% der Wohnungen nach dem Zufallsprinzip ausgewählt. Die Auswahl nach dem Zufallsprinzip ist sehr wichtig, weil nur sie die Repräsentativität der Ergebnisse gewährleistet. Daher ist es unverzichtbar, daß alle in den ausgewählten Wohnungen lebenden Personen an der Befragung teilnehmen.

2.) Die Intensität der Befragung

Nach Meinung der Anrufer dringt das Fragenprogramm des Mikrozensus tief in ihre

persönliche Sphäre ein. Das ist richtig. Das Erhebungsprogramm ist zwar in vollem Umfang durch das Mikrozensus-Gesetz gedeckt, jedoch ist die Gefahr gegeben, daß der Staat für sich das Recht in Anspruch nimmt, „. . . . den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist" (BVerfGE 27,1). Das Bundesverfassungsgericht hält in dem zitierten Beschluß eine statistische Befragung insbesondere dort für unzulässig, „. . . . wo sie den Bereich des menschlichen Eigenlebens erfaßt, der von Natur aus Geheimnischarakter hat, und damit auch diesen inneren Bezirk zu statistisch erschließbarem und erschließungsbedürftigem Material erklärt." Nach meiner Ansicht trägt das gegenwärtige Erhebungsprogramm, zumal die Fragen zur Gesundheit auf freiwilliger Basis beantwortet werden, den vom Bundesverfassungsgericht aufgestellten Kriterien gerade noch Rechnung und hält damit verfassungsrechtlichen Bedenken Stand.

3.) Die Geheimhaltung der Befragungsergebnisse

Mehrere Anrufer gaben ihrer Sorge Ausdruck, daß die z.T. sehr persönlichen Daten auch für andere Zwecke verwendet werden. Hier ist die Gesetzeslage ganz eindeutig; eine andere Verwendung ist unter keinen Umständen zulässig.

In diesem Zusammenhang gibt es ein Randproblem. Der Mikrozensus wird durch nebenberufliche, aufgrund eines Werkvertrages beschäftigte Interviewer durchgeführt; ein Anrufer bemängelte mir gegenüber, daß ihn ein Interviewer aufgesucht habe, der in seiner Nähe wohne und ihn von Ansehen kenne. Das Statistische Landesamt erklärte hierzu, daß zur Vermeidung hoher Wegekosten – die vom Interviewer aus der Pauschalvergütung zu tragen sind – ein wohnungsnaher Einsatz angestrebt werde, daß aber der beanstandete Fall ein Einzelfall sei, dem in aller Regel sofort durch einen Einsatz des Interviewers in einer anderen Gegend abgeholfen werde. Ich habe das Statistische Landesamt gebeten, diesem Problem weiterhin besondere Aufmerksamkeit zu widmen, auch wenn es nur selten auftritt, und ggf. die vorhandene Möglichkeit zu nutzen, Fahrkosten zusätzlich zur Pauschale zu zahlen.

Ich habe mich im Statistischen Landesamt an Ort und Stelle über die Maßnahmen unterrichtet, die zur Gewährleistung der Geheimhaltung getroffen worden sind.

Mit den Daten eines Haushalts kommen jeweils in Berührung:

- 1 Interviewer
- 1 Sachbearbeiter und 1 Mitarbeiter
- 1 weiterer Interviewer, der in Heimarbeit die Verschlüsselung und Plausibilitäten prüft.

Der Sachbearbeiter und der Mitarbeiter sind als Bedienstete des Statistischen Landesamtes, die Interviewer durch Vertrag zur Geheimhaltung verpflichtet.

Die Interviewer sind durch Vertrag verpflichtet, die ihnen anvertrauten Unterlagen so aufzubewahren, daß kein Dritter von seinem Inhalt Kenntnis nehmen kann. Das Statistische Landesamt behält sich in dem Vertrag das Recht vor, die vertrauliche Behandlung der Unterlagen durch Besichtigung der Wohnung zu überprüfen. Ich habe das Statistische Landesamt gebeten, von diesem Recht gelegentlich Gebrauch zu machen.

Der Sachbearbeiter und der Mitarbeiter arbeiten in einem durch Sicherheitsschloß gesicherten besonderen Raum, in dem auch die Unterlagen aus dem Mikorzensus aufbewahrt werden. Diese Sicherheitsmaßnahmen reichen nach meiner Überzeugung aus.

6.6 Einwohnerwesen

6.6.1 Hamburgisches Meldegesetz

Am 23.8.1982 ist in Hamburg das Hamburgische Meldegesetz in Kraft getreten. Damit hat Hamburg fristgerecht den Auftrag des Melderechtsrahmengesetzes erfüllt und sein Meldegesetz den bundesrechtlichen Vorgaben angepaßt. Das Meldewesen ist nun im Sinne eines sehr viel konsequenteren bereichsspezifischen Datenschutzes neu strukturiert worden.

Ich habe am Gesetzgebungsverfahren noch nicht mitwirken können. Meine Aufgabe sehe ich nunmehr darin, die Umsetzung dieses Gesetzes in die Praxis, und zwar sowohl durch untergesetzliche Rechts- und Verwaltungsvorschriften als auch durch die technische Neukonzeption der Verfahren des Einwohnerwesens, aufmerksam zu begleiten.

In diesem Sinne habe ich bereits am Erlaß der Meldescheinverordnung mitgewirkt, die in der am 5.10.1982 in Kraft getretenen Fassung keinen datenschutzrechtlichen Bedenken unterliegt. Im nächsten Jahr wird die Beratung der aus datenschutzrechtlicher Sicht besonders wichtigen Verordnung gem. § 31 Abs. 5 HmbMG anstehen, in der die regelmäßigen Übermittlungen von Daten aus dem Melderegister an andere öffentliche Stellen (z.B. Polizei) näher geregelt werden sollen: Dabei wird besonders darauf zu achten sein, daß die datenschutzrechtliche Substanz des Meldegesetzes nicht wieder verlorengeht.

6.6.2 Stand der Automation

Bei einem Inforamtionsbesuch im Einwohnerzentralamt haben meine Mitarbeiter sich über den derzeitigen Stand der Automation im Einwohnerwesen informiert.

Zur Zeit gibt es

- das zentrale Personenregister im Einwohnerzentralamt (EZA) der Behörde für Inneres und
- die regionalen Einwohnerkarteien in den Einwohnerdienststellen der Bezirksverwaltung.

Das zentrale Einwohnerregister ist nach Namen geordnet und wird manuell geführt.

Die regionalen Einwohnerkarteien bestehen aus Lochkarten, die in den Einwohnerdienststellen als manuelle Karte genutzt und bei Bedarf nach Übernahme auf Magnetband als automatisierter Datenbestand verarbeitet werden. Die regionalen Einwohnerkarteien sind nach Straßen und Hausnummern geordnet; für jeden Einwohner gibt es eine Lochkarte. Bei Meldevorgängen (An- und Abmeldung) wird eine neue Lochkarte hergestellt, die bestimmte Daten des Meldevordrucks enthält. Die in der Lochkarte enthaltenen Daten werden zusätzlich zur Lochung in Klarschrift auf die Lochkarte geschrieben; die Klarschriftzeilen ermöglichen die Nutzung als manuelle Kartei. Für die Herstellung der Lohnsteuerkarten und die Vorbereitung von Wahlen werden die Lochkarten an einem Wochenende zur Datenverarbeitungszentrale der Finanzbehörde transportiert und dort auf Magnetband übernommen; danach werden sie zu den Einwohnerdienststellen zurückgebracht, damit sie am Montag wieder als Kartei zur Verfügung stehen.

Der auf Magnetbändern gespeicherte automatisierte Datenbestand wird außer für den Druck von Lohnsteuerkarten und für die Vorbereitung der Wahlen auch für andere Zwecke verwendet (z.B. Liste der schulpflichtigen Kinder, Wehrerfassung, Planungsauswertungen).

Die Lochkartenlösung für die regionalen Einwohnerkarteien ist technisch und organisatorisch überholt; sie erlaubt zudem nur ein geringes Maß an Datensicherung (insbesondere keine Eingabekontrolle), so daß sie durch ein neues Verfahren ersetzt werden muß. Die Planungen hierzu sind noch nicht abgeschlossen.

6.6.3 Einzelne Probleme

Während des Berichtszeitraumes haben mich auch einige Eingaben erreicht, die das Einwohnerzentralamt betrafen.

Im Bericht sollen nur zwei Probleme erwähnt werden: die regelmäßige Übermittlung von Daten an öffentlich-rechtliche Religionsgesellschaften und der Schutz von Inkognito-Adoptionen.

Zum einen ging es darum, ob eine Übermittlung von Meldedaten an öffentlich-rechtliche Religionsgesellschaften auch dann zulässig ist, wenn diese Daten mit einer Auskunftssperre gem. § 34 Abs. 5 HmbMG belegt sind. Ich habe diese Frage bejaht, denn aus der Systematik des Gesetzes ergibt sich, daß die Auskunftssperre sich nur auf die – in § 34 HmbMG geregelten – Auskünfte aus dem Melderegister an private Stellen bezieht. Bei Übermittlungen an öffentlich-rechtliche Religionsgesellschaften gem. § 33 Abs. 1 HmbMG ist allerdings sicherzustellen, daß der Sperrvermerk mit übermittelt wird. Dies hat die Bfl zwischenzeitlich akzeptiert.
Beim Problem der Gefährdung von Inkognito-Adoptionen ging es darum, daß eine kirchliche Stelle noch Jahre nach vollzogener Adoption als ihr übermittelten Namen eines adoptierten Kindes den ursprünglichen Familiennamen gespeichert hatte, so daß das Kind unter seinem Geburtsnamen mit dem Zusatz bei . . . . (Name der Adoptiveltern) angeschrieben wurde. Daß ein solches Vorkommnis schutzwürdige Belange des betroffenen Kindes erheblich beeinträchtigen kann, liegt auf der Hand.

Ich habe die Angelegenheit mit den betroffenen Stellen, soweit sie meiner Aufsicht unterliegen (EZA, Adoptionsvermittlungsstelle) erörtert. Inzwischen wurden Regelungen erreicht, die geeignet sind, solche Pannen in Zukunft zu verhindern. Es ist sichergestellt, daß bei der Begründung von Adoptionspflegschaften (nach § 2744 BGB) von der Adoptionsvermittlungsstelle unverzüglich die Eintragung einer Übermittlungssperre im Melderegister veranlaßt wird. Dieser Sperrvermerk wird in Zukunft nicht nur beim zentralen Personenregister des EZA, sondern auch auf den Einwohnerkarten der Einwohnerdienststellen bei den Bezirksämtern eingetragen. Die Sperrvermerke werden bei einer Übermittlung von Meldedaten an andere öffentliche Stellen mit übermittelt. Schließlich hat die Adoptionsvermittlungsstelle durch eine entsprechende Vereinbarung mit dem Kirchenkreisamt sichergestellt, daß diese nur den geltenden Familiennamen des betr. Kindes (ggf. einschl. des Sperrvermerks) speichert.

6.7 Sicherheitsbereich

6.7.1 Sonderregelungen im HmbDSG

Dieser Bereich hat für die Datenschutzkontrolle eine besondere Bedeutung, denn an keiner Stelle werden in solchem Umfang empfindliche personenbezogene Daten in hochtechnisierten und außerordentlich leistungsfähigen Verbundsystemen mit vielfältigen Verknüpfungsmöglichkeiten und zahlreichen Abrufvorrichtungen verarbeitet. Zwar benötigen die Sicherheitsbehörden zur Erfüllung ihrer Aufgaben, verfassungsfeindliche Bestrebungen zu beobachten, strafbare Handlungen zu verfolgen und Gefahren abzuwehren, zahlreiche Informationen, und sie sind auf eine besondere Diskretion angewiesen. Dem stehen jedoch – auch wegen der eingeschränkten Transparenz der Datenverarbeitung in diesem Bereich – die bei derartig umfassenden Informationssystemen nicht auszuschließenden Gefahren für die Persönlichkeitsrechte einzelner Bürger gegenüber.

Auch die Sicherheitsbehörden haben das HmbDSG anzuwenden. Es enthält allerdings – wie die anderen Datenschutzgesetze – einige der besonderen Aufgabenbestimmung der Sicherheitsbehörden Rechnung tragende Sonderregelungen:

- Die von der Polizei und der Staatsanwaltschaft zu meldenden Dateien werden in einem besonderen, nicht-öffentlichen Datenregister erfaßt (§ 13 Abs. 3 Nr. 1).

- Das Landesamt für Verfassungsschutz ist ganz von der Meldepflicht ausgenommen (§ 13 Abs. 4).

- Der den Betroffenen nach § 14 Abs. 1 gewährte Auskunftsanspruch über die zu seiner Person gespeicherten Daten entfällt gegenüber den Sicherheitsbehörden (§ 14 Abs. 2). Diese können die erbetene Auskunft verweigern, sie ist ihnen aber nicht verboten. Sowohl für die Polizei als auch für den Verfassungsschutz gibt es verwaltungsinterne Richtlinien (KpS/NADIS), die im einzelnen regeln, unter welchen Voraussetzungen die zuständige Behörde Auskünfte erteilen kann (Näheres hierzu unter 6.7.2.2 und 6.7.3).

Die Kontrollbefugnisse des DSB sind im Bereich der öffentlichen Sicherheit und Ordnung in zweierlei Hinsicht eingeschränkt: Die Rechte auf Auskunft, Akteneinsicht und Betreten der Diensträume stehen nur dem Datenschutzbeauftragten selbst und den von ihm schriftlich besonders damit beauftragten Mitarbeitern zu. Die Sicherheitsbehörden können ihm die Akteneinsicht verwehren, wenn der Senat im Einzelfall feststellt, daß dadurch die Sicherheit des Bundes oder eines Landes gefährdet ist (§ 24 Abs. 4 S. 3 und 4).

Die bisher an mich herangetragenen Eingaben, die sich durchweg auf die Frage bezogen, ob bei Polizei und Verfassungsschutz personenbezogene Daten über die Einsender gespeichert seien, oder den Wunsch zum Ausdruck brachten, evtl. gespeicherte Daten zu löschen, führten – auch wegen der Aufgeschlossenheit der Sicherheitsbehörden für Belange des Datenschutzes – zu befriedigenden Ergebnissen. Den Löschungsersuchen gab die Polizei in den meisten Fällen statt.

Da der allgemeine Auskunftsanspruch aus § 14 gegenüber den Sicherheitsbehörden nicht gilt, darf auch der DSB Auskünfte nur in dem Umfang erteilen, der von den Sicherheitsbehörden gebilligt wird. Wenn diese eine Auskunft ablehnen, kann der DSB dem Einsender lediglich mitteilen, die Überprüfung habe keine Verletzung datenschutzrechtlicher Bestimmungen ergeben. Diese Aussage kann sowohl bedeuten, daß eine Speicherung erfolgt ist, als auch, daß eine erfolgte Speicherung rechtens ist. Ein solches Verfahren ist für den Anfragenden natürlich unbefriedigend, angesichts der geltenden gesetzlichen Regelungen, die der Verhinderung von Ausforschungsversuchen dienen, darf der DSB aber nicht weitergehen.

Für das Vertrauen des Bürgers in die Wirksamkeit der Arbeit des Datenschutzbeauftragten ist es von großer Bedeutung, daß die Sicherheitsbehörden – wie bisher schon – weiter bereit sind, auch ohne Verpflichtung selbst Auskünfte zu erteilen oder aber den DSB zur Erteilung von Auskünften zu ermächtigen, soweit nicht überragende Sicherheitsbelange dem entgegenstehen.

6.7.2 Polizei

6.7.2.1 Das polizeiliche Informationssystem

Im Berichtszeitraum habe ich auch bei der Polizei noch keine systematischen Prüfungen durchgeführt, sondern mir zunächst nur einen ersten Überblick über die von der Polizei geführten Dateien und über das von den Polizeidienststellen des Bundes und der Länder betriebene Verbundsystem verschafft. Bereits seit mehr als 10 Jahren bedient sich die Polizei bei ihren Fahndungs- und Ermittlungsaufgaben der Unterstützung durch Computer, um Unzulänglichkeiten des bisherigen Fahndungssystems (mit Fahndungsbuch und Fahndungskarteien) zu überwinden. 1972 wurde das arbeitsteilige INPOL-System in Betrieb genommen. Dabei handelt es sich um einen Aufgaben- und Datenverbund, in dem heute die DV-Systeme von 7 Ländern (incl. Hamburg) und das DV-System des Bundeskriminalamtes zusammengeschlossen sind.

Die derzeit geltende Konzeption des INPOL-Systems ist enthalten in dem am 12.6.1981 von der Innenministerkonferenz beschlossenen „Konzept zur Fortentwicklung des polizeilichen Informationssystems INPOL". Dieses Konzept unterscheidet zwischen solchen Pro-

jekten, die bundesweit zu realisieren sind (INPOL-Bund) und solchen von lediglich regionaler Bedeutung (INPOL-Land). Zu den im INPOL-Bund zu realisierenden Aufgaben gehören die Personen- und Sachfahndung, der Kriminalaktennachweis (KAN), die Haftdatei, die Datei mit erkennungsdienstlichen Daten, zentrale Aktenerschließungs- und Spurendokumentationssysteme für Straftaten von bundesweiter Bedeutung und zentrale Tatmittelnachweise für bestimmte Kriminalitätsbereiche.

Nach den im INPOL-Fortentwicklungskonzept enthaltenen Vorgaben werden die Projekte in den einzelnen Systemen der Länder realisiert. Das alle INPOL-Anwendungen (Bund + Land) umfassende Auskunftssystem des Landes Hamburg trägt den Namen POLAS (**POL**izeiliches **A**uskunfts **S**ystem).

Die in POLAS/INPOL zusammengefaßten Dateien enthalten insbesondere die folgenden Informationen:

Die Personenfahndungsdatei hält Fahndungsnotierungen bereit über Personen, die regional, national oder international zur Festnahme, Inverwahrname, Aufenthaltsermittlung, Identitätsprüfung oder polizeilichen Beobachtung ausgeschrieben worden sind.

Die Haftdatei enthält Notierungen über Personen, die sich aufgrund richterlich angeordneter Freiheitsentziehung in Verwahrung befinden.

Die Sachfahndungsdatei beinhaltet Informationen über Kraftfahrzeuge und andere Sachen, die regional, national oder international zur Beweissicherung, Einziehung, Eigentumssicherung, Eigentümerübermittlung oder zur Beobachtung ausgeschrieben sind.

Der Kriminalaktenindex enthält Hinweise auf Fundstellen von personenbezogenen Unterlagensammlungen, die bei der Polizei geführt werden.

Verantwortlich für den Inhalt der gespeicherten Daten sind grundsätzlich die erfassenden Dienststellen, die zum überwiegenden Teil den Ländern zugeordnet sind. Neben den bereits genannten Dateien liefert die Polizei auch personenbezogene Daten für die ausschließlich beim BKA betriebenen INPOL-Anwendungen, PIOS-Terrorismus und PIOS-Rauschgiftdatei. Die Datenschutzkontrolle der zum INPOL-System gehörenden Dateien ist angesichts der durch den gegenseitigen Verbund bedingten Komplexität nur im Zusammenwirken zwischen allen Landesbeauftragten und dem Bundesbeauftragten für den Datenschutz möglich. Diese Zusammenarbeit wird koordiniert im Arbeitskreis „Sicherheit" der ständigen Konferenz der Landesbeauftragten und des Bundesbeauftragten für den Datenschutz.

Die nächste INPOL-Anwendung, die im Verbund-System für Bund und Länder (in HH 1984) realisiert werden soll, ist der zentrale Kriminalaktennachweis (KAN) beim BKA. Nach dem von der Innenministerkonferenz beschlossenen KAN-Konzept ist dieser ein Verzeichnis von Kriminalakten, die beim Bund und bei den Ländern in Fällen schwerer oder überregional bedeutsamer Straftaten über Beschuldigte oder sonst tatverdächtige Personen angelegt sind. Die Bewertungskriterien für die überregionale Bedeutung von Straftaten wurden unter Berücksichtigung von datenschutzrechtlichen Belangen bundeseinheitlich festgelegt. Überregional bedeutsam sind nach dem z.Z. geltenden KAN-Konzept Straftaten, wenn Verdacht besteht auf

- gewohnheits-, gewerbs- oder bandenmäßige Begehung
- Mittäterschaft
- planmäßige überörtliche Begehung
- Handeln zur Verfolgung extremistischer Ziele
- Begehung unter Mitführung von Schußwaffen
- internationale Betätigung

- erneute Straffälligkeit des Beschuldigten außerhalb seines Wohn- und Aufenthaltsbereichs.

Die Realisierung des KAN-Konzepts soll in Hamburg im Jahre 1984 erfolgen. Dabei wird darauf zu achten sein, daß die oben genannten Bewertungskriterien bei der Auwahl der in den KAN aufzunehmenden Akten strikt eingehalten werden. Darüber hinaus werde ich aufmerksam zu prüfen haben, ob und inwieweit die Beschränkung des KAN auf überregionale Täter durch das demnächst ebenfalls zu realisierende Konzept einer zentralen Datei für erkennungsdienstliche Unterlagen wieder aufgehoben wird.

Abschließend ist zu bemerken, daß die Hamburger Polizei auch noch zahlreiche manuell geführte, zumeist nach Delikten geordnete Karteien unterhält.

6.7.2.2 Stand des Datenschutzes

Einen wichtigen Schritt zur bereichsspezifischen Regelung datenschutzrechtlicher Belange stellen die bundeseinheitlichen Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien) dar, die in Hamburg am 1. März 1982 erlassen wurden. Diese Richtlinien enthalten Regeln für die Datenübermittlung, die Aufbewahrungsdauer, die Voraussetzungen einer Auskunftserteilung an den Betroffenen, und sie begründen Pflichten zur Aussonderung und technischen Datensicherung. Wichtigen datenschutzrechtlichen Belangen ist damit Rechnung getragen.

Besonders bedeutsam sind die Vorschriften über die Dauer der Aufbewahrung. Die kürzeren Fristen haben dazu geführt, daß die Polizei aus ihrem früheren Bestand, der ca. 370.000 Personendatensätze umfaßte, ca. 170.000 gelöscht und die dazugehörigen Akten vernichtet hat. Dadurch, daß in alle Verfahren Lösch- bzw. Prüfroutinen eingebaut sind, ist die polizeiliche Informationsverarbeitung auf „programmiertes Vergessen" eingerichtet.

Die Erteilung einer Auskunft lassen die Richtlinien zu, wenn eine Abwägung ergibt, daß das Interesse des Betroffenen an der Auskunft das öffentliche Interesse an der Geheimhaltung überwiegt. Diese Regelung, die die Polizei zur Ermessensausübung verpflichtet, hat nach den bisherigen Erfahrungen nicht zu einer Behinderung der polizeilichen Aufgabenerfüllung und schon gar nicht zu einem „gläsernen Sicherheitsapparat", wie bisweilen behauptet wird, geführt, obwohl die Polizei bis auf einen kleinen Rest alle gestellten Auskunftsersuchen beantwortet hat. In einer Reihe von Fällen ergaben die Auskünfte, daß unrichtige oder nicht mehr erforderliche Daten gespeichert waren.

Bemerkenswert ist, daß die Polizei mit den KpS-Richtlinien nicht nur das ihr vom DSG abverlangte Minimum an Datenschutz realisiert, sondern auf ihre gesamte Datenverarbeitung datenschutzrechtliche Grundsätze anwendet, ohne danach zu unterscheiden, ob sie ihre Vorgänge in Akten, manuellen oder elektronischen Dateien verarbeitet. Es ist anzuerkennen, daß damit das Schutzbedürfnis der Bürger unabhängig von der konkreten Art der Verarbeitung gleich hoch veranschlagt wird.

Nicht geregelt ist bisher, welche Bediensteten der Polizei zu welchen Daten der polizeilichen Auskunftssysteme Zugang haben. Die Polizei hat jedoch erste im großen und ganzen akzeptable Vorschläge für eine differenzierte Zugangsregelung bereits erarbeitet und diese auch mir vorgelegt. Die Diskussion ist noch nicht abgeschlossen, so daß ich noch keine endgültige Beurteilung abgeben kann. Es geht darum, den Zugang so zu begrenzen, daß jeder Bedienstete nur auf solche Daten zugreifen darf, die er zur Aufgabenerfüllung in der ihm übertragenen Funktion benötigt.

Ein Defizit der in Hamburg geltenden KpS-Richtlinien sehe ich darin, daß sie keine präzisen Regelungen zur Errichtung einzelner polizeilicher Dateien enthalten. Auf Bundesebene wie auch in einigen Bundesländern gelten „Dateirichtlinien", in denen vorgesehen ist, daß jede Einrichtung einer polizeilichen Datei einer besonderen Anordnung bedarf, in der u.a.

- die Rechtsgrundlage,
- der Zweck,
- der Personenkreis,
- die Art der Daten,
- sowie die Stellen, an die Auskunft erteilt wird,

festgelegt werden.

Ich bin der Auffassung, daß auch in Hamburg solche Datei-Statuten (Feststellungs- bzw. Errichtungsanordnungen) errichtet werden sollten, um möglicherweise unzulässige Speicherungen und Datenflüsse besser erkennen und im voraus verhindern zu können.

Leider sind die KpS-Richtlinien in Hamburg nicht im Amtl. Anzeiger veröffentlicht worden, wie das in anderen Bundesländern schon geschehen ist. Erfahrungen aus anderen Ländern (etwa den USA) haben gezeigt, daß eine möglichst umfassende Unterrichtung der Öffentlichkeit die Effizienz der Polizeiarbeit nicht herabsetzt, sondern eher das Gegenteil bewirkt hat, weil der „Vorhang des Unheimlichen" von den polizeilichen Datensammlungen gelüftet wird. Erhöhte Transparenz kommt fast immer auch der Aufgabenerfüllung der Behörden zugute.

6.7.2.3 Einzelne Probleme

Neben der allgemeinen Bestandsaufnahme über Probleme des Datenschutzes bei der Polizei habe ich mich aufgrund von Eingaben oder Anfragen auch mit einer Reihe von Einzelproblemen befaßt, deren Bewertung jedoch z.Z. noch nicht abgeschlossen ist.

- Zum einen geht es um das Problem, ob, in welchem Umfang und unter welchen Voraussetzungen die Polizei Sozialdaten von Sozialleistungsträgern im Wege der Amtshilfe erhalten kann. Nach Inkrafttreten des Sozialgesetzbuches hatten sich einige Sozialleistungsträger zunächst geweigert, der Polizei weiterhin über die Stammdaten bestimmter Mitglieder (Name, Geburtsdatum, Geburtsort, derzeitige Anschrift, sowie Name und Anschrift des derzeitigen Arbeitgebers) ohne richterliche Anordnung Auskunft zu erteilen. Diese Haltung wurde damit begründet, daß § 73 SGB X als Spezialgesetz die allgemeine Amtshilfeverpflichtung gem. § 68 SGB X verdränge.

  Demgegenüber wurde von der Behörde für Inneres und von der Behörde für Arbeit, Jugend und Soziales der Standpunkt vertreten, daß § 68 SGB X neben der Vorschrift des § 73 SGB X zu beachten sei. Amtshilfeersuchen seien demnach zu erfüllen, soweit sie sich auf die in § 68 SGB X genannten Stammdaten erstreckten und kein Grund zu der Annahme bestehe, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt würden.

  Ohne Beteiligung des DSB ist dieser Streit im Juni 1982 zwischen den beteiligten Stellen im Sinne der Behörde für Inneres entschieden worden. In Abstimmung mit den anderen DSB bin ich dabei zu klären, ob das erzielte Ergebnis aus datenschutzrechtlicher Sicht akzeptabel ist.

- In einem weiteren Fall geht es darum, daß die Polizei bei einer Häufung von Straftaten in bestimmten Bereichen verstärkte Überwachungsmaßnahmen durchführt und präventivpolizeiliche Personenkontrollen vornimmt. Über diese Personenkontrollen werden von den Polizeibeamten Aktennotizen gefertigt („sog. Anhaltemeldungen"), in denen neben den Personalien des Überprüften Angaben über Ort, Zeit, Art und Rechtscharakter der polizeilichen Maßnahme aufgenommen werden. Diese Anhaltemeldungen werden von der Polizei in Sammlungen, die jedenfalls den KpS-Richtlinen unterliegen, mehrere Jahre aufbewahrt. Ob, in welchem Umfang und wie lange eine solche Speicherung zulässig ist, wird von mir z.Z. noch geprüft.

- Schließlich ist von ärztlicher Seite die Frage an mich herangetragen worden, ob die Speicherung von Daten über Suizid-Versuche im POLAS erforderlich ist. Diese Speicherung halte ich für problematisch. Ärztlicherseits werden insbesondere deswegen Bedenken geäußert, weil die Speicherung ein fortdauerndes Gefühl der Ausweglosigkeit und Ohnmacht gegenüber Staat und Gesellschaft bei den Betroffenen bewirken kann und dadurch geeignet ist, ärztliche Therapien zu gefährden. Die Polizei hält die Speicherung aus Gründen der Gefahrenabwehr für erforderlich, um bei erneuten Freitodversuchen sehr rasch die für den jeweiligen Fall individuell richtigen Maßnahmen ergreifen zu können. In dieser Angelegenheit ist das Gespräch mit den Beteiligten noch nicht abgeschlossen.

6.7.3 Datenschutz beim Landesamt für Verfassungsschutz (LfV)

Auch beim Landesamt für Verfassungsschutz habe ich noch keine systematische Überprüfung vorgenommen, sondern mir lediglich einen ersten Überblick verschaffen können und eine vorläufige Bestandsaufnahme über die anstehenden Probleme gemacht.

Das Bundesamt für Verfassungsschutz und die Verfassungsschutzbehörden der Länder führen als Gemeinschaftseinrichtung das „Nachrichtendienstliche Informations- und Verbundsystem" (NADIS). In NADIS werden nicht die Inhalte eines Vorgangs, sondern nur Grundinformationen zu einer Person, wie zum Beispiel Name, Anschrift, Geburtsdatum etc. gespeichert, im übrigen nur Aktenzeichen der speichernden Stellen. NADIS ist also im wesentlichen eine Hinweisdatei, Einzelinformationen über Personen können nur durch Einsichtnahme in die durch NADIS erschlossenen Vorgänge erzielt werden; eine gewisse Aussagekraft hat für den Fachkundigen allerdings auch schon das Aktenzeichen. NADIS ist im übrigen keine Belastetendatei, da zum Beispiel auch Zielpersonen gegnerischer Nachrichtendienste beziehungsweise Personen, für die eine Sicherheitsüberprüfung wegen des Zugangs zu Verschlußsachen durchgeführt wird, gespeichert werden.

Die materiell-rechtliche Zuständigkeit des LfV Hamburg für die Sammlung und Speicherung von Informationen über Personen und Organisationen ergibt sich aus § 3 des Gesetzes über den Verfassungsschutz in der Freien und Hansestadt Hamburg (HmbVerfSchG). Danach hat der Verfassungsschutz Informationen zu sammeln und auszuwerten über

- Bestrebungen, die gegen die freiheitliche demokratische Grundordnung oder die gegen den Bestand und die Sicherheit des Bundes oder eines Landes gerichtet sind,
- geheimdienstliche Tätigkeiten für eine fremde Macht sowie
- Bestrebungen, die durch Anwendung von Gewalt auswärtige Belange der Bundesrepublik Deutschland gefährden.

Das Landesamt für Verfassungsschutz wirkt ferner mit bei der Überprüfung von Personen, die Zugang zu Verschlußsachen erhalten sollen oder ihn sich dienstlich verschaffen können, und bei der Überprüfung von Personen, die an sicherheitsempfindlichen Stellen von lebens- und verteidigungswichtigen Einrichtungen beschäftigt sind oder werden sollen.

Die dem Verfassungsschutz entsprechend den vorstehenden Aufgaben obliegende Art der Informationsverarbeitung wirft für den Datenschutz eine Reihe von Problemen auf. Seine Tätigkeit ist umso weniger problematisch, je mehr sie darauf konzentriert ist, der politischen Führung Lageberichte allgemeiner oder spezieller Art – insbesondere im Hinblick auf die Aktivitäten bestimmter Organisationen – zu liefern. Soweit das LfV jedoch Daten über einzelne Personen erhebt und verarbeitet, von denen diese nach Lage der Aufgaben in der Regel keine Kenntnisse haben, stellt sich die Frage nach den rechtlichen Grenzen zwischen den Erfordernissen eines rechtsstaatlichen Verfassungsschutzes einerseits und der geschützten Individualsphäre andererseits.

Gerade beim Verfassungsschutz kann sich die Art der Gewinnung einer Information auch auf die Rechtmäßigkeit ihrer nachfolgenden Speicherung auswirken. Ich werde daher – un-

ter Beachtung der genannten Grenzziehung – im Einzelfall auch zu prüfen haben, ob die Erhebung der Daten rechtmäßig und zur Aufgabenerfüllung erforderlich ist.

Ein weiteres Problem, das ich einer genaueren Betrachtung unterziehen werde, liegt im Bereich der Zusammenarbeit des LfV mit anderen Stellen, insbesondere der Polizei. Die rechtliche Problematik dieser Zusammenarbeit liegt darin begründet, daß ein Spannungsverhältnis besteht zwischen der Verpflichtung zur Amtshilfe einerseits, der strikten Trennung der Aufgaben von Verfassungsschutz und Polizei andererseits. Die Aufgabentrennung wird durch § 2 HmbVerfSchG deutlich, wonach das LfV ausschließlich für die in § 3 HmbVerfSchG beschriebenen Aufgaben zuständig ist und einer polizeilichen Dienststelle nicht angegliedert werden darf. Darüber hinaus ist in § 4 HmbVerfSchG festgelegt, daß dem LfV polizeiliche Befugnisse nicht zustehen. Gerade im Verhältnis Verfassungsschutz/Polizei ist es also wichtig, daß die wechselseitigen Datenflüsse auf das unbedingt notwendige Maß beschränkt werden, damit das Trennungsprinzip nicht unterlaufen wird. Aus datenschutzrechtlicher Sicht kommt besondere Bedeutung der Frage zu, inwieweit mit polizeilichen Befugnissen erlangte personenbezogene Daten an den Verfassungsschutz übermittelt und dort verarbeitet werden dürfen.

Zur Wahrung datenschutzrechtlicher Belange haben die Verfassungsschutzämter intern sog. NADIS-Löschungsrichtlinien erlassen. Durch sie wird bundeseinheitlich geregelt, in welchen Zeiträumen Daten zu überprüfen und zu löschen sind. Aufgrund dieser Richtlinien ist ein große Anzahl von Datensätzen gelöscht worden. Zur Durchführung der alle 4 Jahre vorzunehmenden Erforderlichkeitsprüfung nach § 15 Abs. 4 hat das LfV zusätzlich interne Ausführungsbestimmungen erlassen; das danach praktizierte Verfahren ist aus meiner Sicht akzeptabel.

Die Überprüfung von Einzelfällen ergab keine Beanstandungen.

6.7.4 Staatsanwaltschaft

Auch die Staatsanwaltschaft (StA) gehört als Strafverfolgungsorgan zu den Behörden des Sicherheitsbereichs, die nur begrenzte Pflichten zur Publizierung ihrer Datenverarbeitungsmaßnahmen haben.

Die bei der StA anfallenden Daten werden zum weitaus überwiegenden Teil in Akten verarbeitet. Sie unterliegen mithin nicht unmittelbar den Regelungen des Datenschutzgesetzes, wohl aber den allgemeinen Grundsätzen der Verhältnismäßigkeit und Erforderlichkeit, die durch §§ 9 ff lediglich konkretisiert werden.

Die StA bei dem Landgericht Hamburg führt als manuelle Datei die sog. „Zentralkartei" (ZK). In dieser Kartei, über die wir uns bei einem Informationsbesuch haben unterrichten lassen, werden die Personalien der Beschuldigten (Name, Vorname, Geburtsdatum und -ort), das in einem eingeleiteten Verfahren jeweils vergebene Aktenzeichen sowie – soweit dies für die Bediensteten der ZK ohne weiteres erkennbar ist – die Paragraphen-Angabe der dem Beschuldigten vorgeworfenen Straftat festgehalten.

Die ZK dient zwar in erster Linie als Hilfsmittel der Aktenführung, zur Erleichterung und Beschleunigung des Geschäftsablaufs bei der Staatsanwaltschaft; sie ist jedoch keine interne Datei i.S.v. § 1 Abs. 2 Satz 2; denn die gespeicherten Daten sind auch zur Übermittlung an Dritte bestimmt. Auskünfte aus der ZK werden neben den Bediensteten der StA auch den hamburgischen Strafgerichten, den Sachbearbeitern der Kriminalpolizei und bestimmten Angehörigen der Justizbehörde gegeben. Wie oft solche Übermittlungen vorkommen, ist ohne Belang; entscheidend ist, daß die Daten auch von anderen Stellen verwendet werden.

Da mithin die Datenschutzgesetze bei der Beurteilung der Zentralkartei voll zur Anwendung kommen, hat die 9. Konferenz der Datenschutzbeauftragten am 28./29. Sept. 1981

„Mindestanforderungen für den Datenschutz bei den Zentralen Namenskarteien der Staatsanwaltschaften" beschlossen. Diese habe ich im Oktober der Justizbehörde zur Stellungnahme übersandt. Die Datenschutzbeauftragten gehen in ihrem Beschluß davon aus, daß die Zentralkarteien wegen des in der Natur der Sache liegenden Bezugs zu Straftaten zu den besonders sensiblen Datensammlungen gehören, die schutzwürdige Belange der Betroffenen nachhaltig berühren können. Dies gilt vor allem für die Daten von Unschuldigen, weil bereits der Ort der Speicherung einen belastenden Zusammenhang vermitteln kann.

Daher dürfen über die zur Identifizierung der im Namensverzeichnis geführten Personen notwendigen Daten hinaus nur Daten gespeichert werden, die für die Verbindung zu den Vorgängen bei der StA erforderlich sind. Es ist fraglich, ob die Speicherung des Tatvorwurfs in der Zentralkartei notwendig ist. Zwar soll die Kartei als solche nicht als Entscheidungsgrundlage dienen, es erscheint mir jedoch – insbesondere bei den Übermittlungen aus der Kartei – zweifelhaft, ob den schutzwürdigen Belangen der Betroffenen hinreichend Rechnung getragen wird. Dieses Problem werde ich mit der StA zu klären versuchen.

Bei den Übermittlungen aus der Zentralkartei besteht die Gefahr, daß hier eine Art Ersatzzentralregister entsteht, das auch Daten enthält, die im Bundeszentralregister bereits getilgt sind. Die Staatsanwaltschaft hat jedoch Regelungen getroffen, die darauf hinzielen, daß nur noch solche Daten übermittelt werden, die im BZR nicht getilgt sind. Wieweit diese Regelungen ausreichend sind, werde ich ebenfalls zu prüfen haben.

Schließlich werde ich auf angemessene Sperr- und Löschungsfristen hinwirken. Die Löschung ist bisher so geregelt, daß die einzelnen Karteikarten frühestens zehn Jahre nach der letzten Eintragung vernichtet werden, ohne daß die Einhaltung wenigstens dieser Frist durch regelmäßige Überprüfungen gewährleistet ist. Die bisherige Praxis der StA ist meiner Auffassung nach mit § 15 Abs. 3 und 4 nicht in Einklang zu bringen. Danach sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange der Betroffenen beeinträchtigt werden. Die Frage der Erforderlichkeit ist regelmäßig alle 4 Jahre zu überprüfen.

Zu berücksichtigen ist jedoch, daß es der StA insbesondere im Hinblick auf den Umfang der manuell betriebenen Datei sehr schwer fällt, den Anforderungen des HmbDSG gerecht zu werden. Das bedeutet einen erheblichen zusätzlichen Personalbedarf. Diese Schwierigkeiten können die StA jedoch nicht aus den Pflichten des Gesetzes entlassen.

Da bereits Untersuchungen zur Automation der Zentralkartei geführt worden sind und die Absicht besteht, das Automationsvorhaben Mitte 1983 zu realisieren, habe ich von einer Beanstandung nach § 21 abgesehen. Durch Einführung der Automation kann die Problematik der Löschung befriedigend geregelt werden; es wäre nicht vertretbar, für den kurzen Zwischenzeitraum einen aufwendigen Personaleinsatz zu fordern.

6.8 Justiz

Besonders sensible personenbezogene Daten fallen auch im Rahmen der Straf- und Zivilgerichtsbarkeit (sowie der Freiwilligen Gerichtsbarkeit) an.

Die Kontrollbefugnis des HmbDSG gilt bei den Gerichten gem. § 20 Abs. 1 allerdings nur insoweit, als diese in Verwaltungsangelegenheiten tätig werden. Wie diese Abgrenzung im einzelnen vorzunehmen ist, werde ich noch mit der Justizbehörde abzustimmen haben.

Zwar werden personenbezogene Daten bei den Gerichten zum überwiegenden Teil aktenmäßig – also nicht in Dateien – verarbeitet. Auch hier gilt es jedoch, die Einhaltung der rechtsstaatlichen Grundsätze von Verhältnismäßigkeit und Übermaßverbot zu überwa-

chen. Im übrigen finden die bei den Gerichten verarbeiteten Daten durch Übermittlung häufig Eingang in Dateien, die bei anderen Stellen geführt werden.

Ich habe mir zunächst einen Überblick über die zahllosen Übermittlungen seitens der Gerichte verschafft sowie mehrere Eingaben bearbeitet, die die Auskunftspraxis beim Schuldnerverzeichnis und beim Grundbuchamt betrafen.

6.8.1 Anordnung über Mitteilungen in Strafsachen (MiStra)

Die Anordnung über Mitteilungen in Strafsachen ist eine bundeseinheitliche interne Verwaltungsvorschrift, die vom Bundesminister der Justiz im Einvernehmen mit den Justizministern und -senatoren der Länder erlassen worden ist. Die MiStra geht aus von der Feststellung, daß es in vielen Strafverfahren Vorgänge gibt, die auch für andere öffentliche Stellen wichtig sind und Anlaß zu Maßnahmen geben können. Sie regelt im einzelnen, in welchen Fällen und zu welchem Zeitpunkt die Justizbehörden zu Mitteilungen verpflichtet sind.

Die derzeit noch breit gestreuten Mitteilungen verbleiben vielfach über die Löschungsfristen des Bundeszentralregistergesetzes hinaus in den Akten der empfangenden Stelle. Schon dieser Umstand gibt Anlaß zur strengen Prüfung der Frage, ob der Katalog der zu übermittelnden Informationen und der Datenempfänger dem datenschutzrechtlichen Grundsatz der Erforderlichkeit entspricht. Im übrigen sollte nicht verkannt werden, daß die Mitteilungen wegen der Auswirkungen, die sie auslösen, den Charakter zusätzlicher Sanktionen erhalten können. Daraus ergibt sich, daß sie nicht nur auf eine einwandfreie gesetzliche Grundlage gestellt, sondern auch restriktiv geregelt werden müssen.

Auf der Konferenz der Datenschutzbeauftragten vom 29. September 1980 ist das Thema bereits ausführlich behandelt und ein entsprechender Beschluß gefaßt worden. Die Justizministerkonferenz hat einen Unterausschuß mit der Überarbeitung der MiStra beauftragt, der bereits einzelne Ergebnisse erzielt hat. Erfreulicherweise hat er sich mehrheitlich für eine spezialgesetzliche Regelung der MiStra ausgesprochen, d.h. der Bundesminister soll zum Erlaß einer entsprechenden Rechtsverordnung ermächtigt werden. Es ist auch anerkannt worden, daß der Umfang der Mitteilungspflichten mit dem Ziel einer „generellen Reduktion" überprüft werden muß.

Die Diskussion der Ergebnisse innerhalb der Verwaltung sowie zwischen den einzelnen Ländern ist noch nicht abgeschlossen. Viele Ressorts halten die gegenwärtigen Regelungen für unverzichtbar, einige drängen sogar auf eine Ausweitung der Mitteilungspflichten.

Ich werde den Fortgang der Diskussion aufmerksam verfolgen und das Ergebnis der Bemühungen gemeinsam mit meinen Kollegen kritisch zu würdigen haben.

6.8.2 Anordnung über Mitteilungen in Zivilsachen (MiZi)

Ähnlich problematisch wie die MiStra ist die Anordnung über Mitteilungen in Zivilsachen. Diese Mitteilungen beziehen sich auf personenbezogene Sachverhalte, die in Verfahren der streitigen und freiwilligen Gerichtsbarkeit bekannt werden. Finanzbehörden, Sozialbehörden, Staatsanwaltschaft, Polizei, Standesämter und andere öffentliche Stellen erhalten dadurch Informationen über gerichtliche Entscheidungen, die sie zur Erfüllung ihrer Aufgaben mehr oder auch weniger dringend benötigen. Bei vielen Mitteilungspflichten ist ihre Notwendigkeit zwar evident und auch durch einschlägige Rechtsvorschriften gedeckt; diverse Fälle sind aber auch problematisch.

Zumindest zweifelhaft erscheint mir z.B. der folgende Fall, mit dem ich aufgrund einer Eingabe befaßt war: Das Amtsgericht hat dem Verkehrsamt die Anordnung einer auf eigenen Antrag angeordneten Vermögenspflegschaft mitgeteilt mit dem Ziel, eine Untersuchung der Tauglichkeit des Betroffenen für den Kraftverkehr zu veranlassen. Die endgültige Beurteilung dieses Falles habe ich wegen noch ausstehender Stellungnahmen noch nicht vornehmen können.

Als weiterer bereits in der Diskussion befindlicher, besonders problematischer Tatbestand ist die Benachrichtigung der Träger der örtlichen Sozialhilfe beim Eingang von Räumungsklagen wegen Zahlungsverzuges eines Mieters zu nennen. Die Sozialdienststelle soll dadurch in die Lage versetzt werden, zügig im Interesse des Mieters tätig zu werden; dessen behaupteter Verzug beruht jedoch möglicherweise gar nicht auf finanziellen, sondern auf rechtlichen Gründen. Der Mieter hat vielleicht sogar ein erhebliches Interesse daran, nicht als potentieller Sozialhilfeempfänger geführt zu werden.

Die Datenschutzbeauftragten des Bundes und der Länder beabsichtigen, sich der Problematik in einer Arbeitsgruppe anzunehmen und Empfehlungen für zufriedenstellende datenschutzrechtliche Regelungen zu erarbeiten.

6.8.3 Schuldnerverzeichnis

Durch mehrere Eingaben bin ich darauf aufmerksam geworden, wie öffentliche Stellen in zunehmendem Maße als Datenquelle für Informationsströme im privaten Bereich genutzt werden. In diesem Zusammenhang ist an erster Stelle das beim Amtsgericht geführte Schuldnerverzeichnis zu nennen. In dieses Verzeichnis sind nach § 915 ZPO die Personen einzutragen, die eine eidesstattliche Versicherung (§§ 807 ZPO, 284 AO) abgegeben haben oder gegen die gem. § 901 ZPO Haft angeordnet ist. Die Eintragung wird nach Ablauf bestimmter, im Gesetz festgelegter Fristen – zum Teil, etwa bei Nachweis der Befriedigung des Gläubigers, auch vorzeitig – gelöscht. In das Schuldnerverzeichnis kann jedermann Einsicht nehmen. Auch können Abschriften erteilt werden, wenn die Einhaltung der Löschungsfristen gewährleistet erscheint. Das Verfahren ist in den „Allgemeinen Vorschriften über die Erteilung und die Entnahme von Abschriften oder Auszügen aus dem Schuldnerverzeichnis" vom 16.8.55 näher geregelt.

Auf der Grundlage dieser Vorschriften übermittelt das Amtsgericht Hamburg – wie eine aus den Akten vorgenommene Bestandsaufnahme ergeben hat – Durchschriften der Karteikarten des Schuldnerverzeichnisses an den Verlag Günther Heinrich. Dieser gibt monatlich sog. „Vertrauliche Mitteilungen" heraus, in denen die Eintragungen im Schuldnerverzeichnis in listenmäßiger Form enthalten sind. Diese „Vertraulichen Mitteilungen" werden von der Handelskammer Hamburg – gemäß einer den geltenden Vorschriften entsprechenden Bewilligung – an ihre und an die Mitglieder weiterer Berufsverbände und an Behörden weitergegeben.

Auf der Grundlage dieser Übermittlungen werden die Daten des Schuldnerverzeichnisses auch bei der „Schufa" und bei den Kreditauskunfteien gespeichert.

Der Kreis derjenigen, die auf diese Art und Weise vollständige Listen des Schuldnerverzeichnisses empfangen, ist, wie man sieht, sehr groß. Es besteht die große Gefahr, daß die vorgesehenen Auflagen – insbesondere die Einhaltung der Löschungsbestimmungen – nicht erfüllt werden, denn die informierten Personen und Unternehmen haben oftmals ein Interesse daran, die Informationen auch über die vorgesehenen Fristen hinaus zu besitzen. Eine Kontrolle findet praktisch nicht statt und ist jedenfalls bei der großen Anzahl der unter den Dritten Abschnitt des BDSG fallenden Unternehmen auch kaum möglich, da diese nur der Anlaßaufsicht unterliegen. Ob die dem Vierten Abschnitt des BDSG unterliegenden Unternehmen (insbesondere Kreditauskunfteien und Schufa) die gesetzlichen Löschungsfristen einhalten, werde ich bei meinen demnächst vorzunehmenden allgemeinen Prüfungen festzustellen haben.

Zur Lösung der bundesweit aufgetretenen Probleme und Eingrenzung der Informationsflüsse hat der Bundesminister der Justiz auf Anregung des Bundesbeauftragten für den Datenschutz im Dezember 1980 eine „Verordnung über Abschriften aus dem Schuldnerverzeichnis" entworfen und den Landesjustizverwaltungen und den DSB zur Stellungnahme zugeleitet. Die Diskussion darüber ist noch nicht abgeschlossen. Insbesondere der Deutsche Industrie- und Handelstag lehnt die geplanten Einschränkungen ab. Auch den

Anforderungen des Datenschutzes entspricht der Entwurf nicht in allen Einzelheiten (vgl. 4. Tätigkeitsbericht des BfD, 4.1.8, S. 44).

6.8.4 Abschriften aus dem Grundbuch

Auch mit dem Problem der Grundbuchauszüge war ich im Berichtszeitraum befaßt. So hat der bisherige Eigentümer eines Grundstückes vom Grundbuchamt unaufgefordert eine Mitteilung über Änderungen im Grundbuch erhalten, in der nicht nur der Eigentumsübergang (aus Abt. I des Grundbuchs), sondern auch die vom Käufer eingegangenen dinglichen Belastungen (Abt. III) ausgewiesen waren.

Da die Sachverhaltsaufklärung bis zum Redaktionsschluß nicht abgeschlossen werden konnte, ist eine abschließende Beurteilung noch nicht möglich. Der Fall gibt mir jedoch Veranlassung, die Übermittlungen aus dem Grundbuch im nächsten Jahr einer genaueren Überprüfung zu unterziehen.

6.9 Gesundheitswesen

Im Bereich des Gesundheitswesens habe ich mich einerseits um eine Bestandsaufnahme der zahlreichen Probleme bemüht. andererseits auch an einigen Projekten beratend mitgewirkt.

6.9.1 Bestandsaufnahme

Die Bestandsaufnahme für den Bereich Gesundheitswesen konnte im Berichtszeitraum noch nicht abgeschlossen werden; dieser Komplex umfaßt nicht nur verschiedene speichernde Stellen (u.a. zwei Fachbehörden,hzahlreiche Krankenhäuser und Beratungseinrichtungen), sondern ist darüber hinaus nach verschiedenen, zum Teil unterschiedlichen datenschutzrechtlichen Bestimmungen zu beurteilen (HmbDSG, BDSG, SGB X, § 203 StGB, ärztliche Schweigepflicht).

Ein Schwerpunktproblem soll schon einmal hervorgehoben werden: Ich habe festgestellt, daß psychisch Kranke derzeit in diversen Zusammenhängen Gegenstand umfangreicher Datensammlungen sind. Zu nennen sind hier verschiedene Projekte im Rahmen des Modellprogramms Psychiatrie der Bundesregierung, die im Aufbau befindliche „Basisdokumentation psychiatrischer Krankenhäuser", neue „Sozialberichte" der Rehabilitationsträger usw. Den dort gesammelten höchst sensiblen Daten gilt meine besondere Aufmerksamkeit: Meine Mitarbeiter haben im Berichtszeitraum die zur Begleitung des Modellprogramms Psychiatrie eingerichtete Psychosoziale Arbeitsgemeinschaft beim AK Eilbek besucht und datenschutzrechtliche Probleme diskutiert. Ferner haben wir uns bei einem Informationsbesuch im AK Ochsenzoll umfassend in die dort geplante psychiatrische Basisdokumentation einführen lassen. Bezüglich der für die Rehabilitationsträger zu verfassenden Sozialberichte stehe ich in Kontakt mit einem psychiatrischen Beratungszentrum.

6.9.2 Krebsregistergesetz

Ein wichtiges Projekt, an dem ich während des Berichtszeitraumes mitgewirkt habe, sind die Vorarbeiten zum Referentenentwurf für ein hamburgisches Krebsregistergesetz.

Ich begrüße es, daß das bereits seit langen Jahren betriebene Krebsregister nunmehr auf eine gesetzliche Grundlage gestellt werden soll. Dies ist wegen des mit der Einspeicherung in das Krebsregister verbundenen Eingriffs in Grundrechtpositionen der Betroffenen dringend erforderlich.

Ich sehe es vorrangig als meine Aufgabe an, auch bei gesundheitspolitisch bedeutsamen Vorhaben, wie dem Krebsregister, für die Wahrung der schutzwürdigen Belange der Patienten einzutreten. Die bisherigen Beratungen haben m.E. gezeigt, daß es möglich ist, Re-

gelungen zu finden, die nicht nur den Interessen der Krebsforschung, sondern zugleich auch dem Schutz der Individualsphäre gerecht werden.

Ich habe insbesondere mit Erfolg darauf hinwirken können, daß bereits im Referenten-Entwurf von der grundsätzlichen Notwendigkeit einer Einwilligung des Patienten in die Übermittlung seiner Daten an das Krebsregister ausgegangen wird. Weiter ist es gelungen, geeignete Regelungen für die verschiedenen Arten der Übermittlung von Daten aus dem Krebsregister an Dritte zu finden.

6.10 Arbeits-, Jugend- und Sozialwesen

6.10.1 Umsetzung des SGB X

Bei der Beurteilung der datenschutzrechtlichen Probleme im Bereich der Behörde für Arbeit, Jugend und Soziales bin ich noch nicht weit vorgedrungen. In ersten Gesprächen konnte ich feststellen, daß es dort noch große Schwierigkeiten bei der Umsetzung der datenschutzrechtlichen Regelungen des SGB X gibt. So gibt es in der Behörde für Arbeit, Jugend und Soziales unterschiedliche „Hinweise" zur Anwendung der §§ 35 SGB I, 67 ff SGB X. Diese Hinweise werden zur Zeit überarbeitet und einander angeglichen.

Nach § 79 Abs. 1 SGB X haben die Behörden und sonstigen öffentlichen Stellen der Freien und Hansestadt Hamburg sowie die der Aufsicht der Freien und Hansestadt Hamburg unterstehenden juristischen Personen des öffentlichen Rechts – wenn sie Sozialleistungsträger sind – die §§ 28 und 29 BDSG entsprechend anzuwenden. Das bedeutet, daß sie wie juristische Personen des Privatrechts betriebliche Datenschutzbeauftragte bestellen müssen. Es ist wiederholt auf den zweifelhaften Sinn dieser Vorschrift hingewiesen worden, die einen betrieblichen Datenschutzbeauftragten mit Aufgaben vorsieht, wie sie nach anderen Vorschriften des BDSG bzw. des HmbDSG von den Leistungsträgern ohnehin schon wahrzunehmen sind (z.B. Führung von Übersichten über die Dateien und Prüfung der ordnungsmäßigen Anwendung der Datenverarbeitungsprogramme). Dennoch besteht die gesetzliche Pflicht; sie muß erfüllt werden.

Die juristischen Personen des öffentlichen Rechts, die Leistungsträger sind, haben betriebliche Datenschutzbeauftragte bestellt. Die Behörden und sonstigen öffentlichen Stellen der Freien und Hansestadt Hamburg haben das bislang nicht getan. Diese Haltung wird damit begründet, daß in Hamburg die verfassungsrechtlichen Bedenken geteilt würden, die die kommunalen Spitzenverbände gegen diese Vorschrift erhoben haben. Neuerdings wird überlegt, wie die gesetzliche Pflicht zur Bestellung betrieblicher Datenschutzbeauftragter mit geringem Aufwand erfüllt werden kann. Ich erwarte, daß die gesetzlich geforderten betrieblichen Datenschutzbeauftragten bald bestellt werden.

6.10.2 Automatisiertes Verfahren für die Kriegsopferversorgung

Die Behörde für Arbeit, Jugend und Soziales beabsichtigt, für die Berechnung und Zahlung der Kriegsopferrenten das niedersächsische automatisierte Verfahren zu nutzen und die hamburgischen Fälle von Niedersachsen verarbeiten zu lassen; sie will ein entsprechendes Verwaltungsabkommen abschließen.

Ich habe gegen diese Absicht keine Bedenken erhoben und den Niedersächsischen Landesbeauftragten für den Datenschutz informiert, dessen Kontrolle das Verfahren und das Rechenzentrum, in dem verarbeitet wird, unterstehen.

7. Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich

7.1 Auskunfteien

7.1.1 Handels- und Wirtschaftsauskunfteien

Das Bundesdatenschutzgesetz gilt selbstverständlich auch und gerade für Handels- und Wirtschaftsauskunfteien. Anfängliche Abwehrversuche mit der Begründung, das BDSG sei nicht anwendbar, weil die Archive nicht den Dateibegriff erfüllten, blieben auf der Strecke. Heute gehen alle Beteiligten von der vollen Anwendung des BDSG aus – auch die Gerichte.

Sehr häufig werde ich gefragt, ob die Arbeit der Auskunfteien, nämlich das Sammeln, Zusammenstellen und Weitergeben von Auskünften, ohne die Mitwirkung des Betroffenen und ohne seine Zustimmung erlaubt ist und ob der Betroffene nicht die Löschung der über ihn gespeicherten Daten erreichen kann.

Dazu ist zu sagen, daß das BDSG die Tätigkeit der Auskunfteien nicht verbietet, jedoch gerade für ihren Umgang mit personenbezogenen Daten in den §§ 32 – 35 einige neue Regeln setzt. Eine Einwilligung des Betroffenen braucht zur Speicherung bei der Auskunftei und zur Übermittlung an eine anfragende Stelle nicht eingeholt zu werden, wenn sich die Auskunftei und der Auskunftsuchende an diese Vorschriften halten.

Einen Löschungsanspruch kennt das BDSG nur dann, wenn die Speicherung von vornherein unzulässig war und wenn die Löschung von mehr als fünf Jahre alten Daten verlangt wird. Dem Betroffenen bleibt in allen anderen Fällen – und das dürfte die Regel sein – nur die Möglichkeit, unrichtige Daten berichtigen oder streitige Daten sperren zu lassen.

Über einzelne Probleme haben die Aufsichtsbehörden mit den Wirtschaftsauskunfteien eingehend gesprochen. Als wichtigste Ergebnisse sind zu erwähnen:

1.) Bei unzulässiger Beschaffung von Informationen ist die anschließende Speicherung ebenfalls unzulässig, weil dadurch die schutzwürdigen Belange des Betroffenen beeinträchtigt sind. Es ist nicht auszuschließen, daß z.B. eine Nachbarschaftsbefragung unangenehme Folgen für den Betroffenen haben kann. Die Aufsichtsbehörden haben auf die Verhältnismäßigkeit der Mittel hingewiesen und empfohlen, bei Anfragen wegen Bagatellbeträgen auf diese Art der Datenerhebung zu verzichten. Die Auskunfteien haben erklärt, daß sie in einigen Fällen auf die Nachbarschaftsbefragung angewiesen seien; sie wollen sich jedoch auf die Fragen nach Wohnort, Aufenthaltsdauer, Einkommen, Arbeitgeber, wirtschaftlichen Verhältnissen und Bankverbindungen beschränken; auf keinen Fall wird eine persönliche Beurteilung abgefragt.

2.) In den Wirtschaftsauskünften finden unterschiedlichste Informationen ihren Niederschlag, z.B. auch geschätzte Angaben und ungenaue, teils mißverständliche Formulierungen. Es hat sich sogar eine besondere Sprache herausgebildet, ähnlich wie bei Zeugnissen von Arbeitnehmern.

   Die Wirtschaftsauskunfteien haben folgende Zugeständnisse gemacht: Über die Persönlichkeit des Betroffenen darf nur positiv in einem kurzen Satz Auskunft gegeben werden. Geschätzte Daten dürfen nur in einem eng begrenzten Umfang gespeichert werden, soweit sie sich nämlich auf das Geburtsjahr, das Einkommen, Betriebszahlen und Grundstückswerte beziehen und von einer zutreffenden Schätzgrundlage ausgegangen und eine korrekte Schätzmethode angewandt wird.

   Soweit Angaben gespeichert werden, die wegen ihrer Unschärfe Anlaß zu Spekulationen beim Empfänger über den Betroffenen geben, sind nach Meinung der Aufsichtsbehörden jedenfalls dann schutzwürdige Belange des Betroffenen beeinträchtigt, wenn

derartige Informationen als positive Aussage weitergegeben werden, jedoch beim Empfänger Anlaß zu nachteiligen Schlüssen geben.

3.) Die Auskunfteien übernehmen regelmäßig Informationen aus den öffentlichen Schuldnerregistern. Sie sehen sich jedoch nicht in der Lage, die vorgeschriebenen Löschungsfristen für diese Daten einzuhalten. Bisher wird eine veraltete Information erst dann vernichtet, wenn der Sachbearbeiter aus irgendeinem Grund auf sie stößt. Die Wirtschaftsauskunfteien haben betont, es sei gewährleistet, daß die überalteten Daten nicht mehr berücksichtigt würden. Die Aufsichtsbehörden haben einen Verstoß gegen § 915 ZPO festgestellt und ein systematisches Löschen dieser Daten gefordert (vgl. auch 6.8.3).

4.) Die für jede datenverarbeitende Stelle geltende Verpflichtung zur Benachrichtigung des Betroffenen über die Tatsache, daß über ihn personenbezogene Daten gespeichert sind, wurde von den Wirtschaftsauskunfteien anfangs verbunden mit der Bitte um zusätzliche Informationen. Die Verbindung dieser beiden so unterschiedlichen Anliegen – vor allem redaktionell im selben Vordruck – wurde von den Aufsichtsbehörden sehr kritisch beobachtet. Schon zu Beginn der Gespräche haben sich die Wirtschaftsauskunfteien bereit erklärt, die Benachrichtigung deutlicher von der Bitte um mehr Daten abzusetzen, damit dem Angeschriebenen klar wird, daß er nicht etwa eine gesetzliche Pflicht zum Ausfüllen und Zurücksenden des beigefügten Fragebogens hat. Auf die Freiwilligkeit dieser Leistung soll besonders hingewiesen werden.

Diese Übereinkunft ist jedenfall bei einer hamburgischen Auskunftei noch nicht in hinreichendem Maße umgesetzt worden.

5.) Die erste Frage des Betroffenen, der seine Auskunft über die eigenen Daten erhalten hat, richtet sich auf die Herkunft der Informationen und den Empfänger der Wirtschaftsauskunft.

Der Auskunftsanspruch des Betroffenen nach § 34 Abs. 2 BDSG bezieht sich auf alle zu seiner Person gespeicherten Daten.

Es ist schwierig abzugrenzen, welche Informationen der Auskunfteien in einer Datei gespeichert sind und dementsprechend auch in der Auskunft an den Betroffenen angegeben werden müssen. Die Aufsichtsbehörden zählen alle in der Wirtschaftsauskunft genannten Angaben als Bestandteile der Datei. Deshalb muß dem Betroffenen die vollständige Wirtschaftsauskunft bekanntgegeben werden, hierzu gehören auch der Empfänger der Auskunft und das sog. Krediturteil. Die Aufsichtsbehörden haben darauf hingewiesen, daß diese Angaben bereits in den Verwaltungsvorschriften, die mit Verbänden der Wirtschaft abgestimmt worden sind, als zur Person des Betroffenen gespeichert gewertet werden.

Die Auskunfteien meinen, diese beiden Angaben dem Betroffenen nicht mitteilen zu können. Die Angabe des Empfängers sei nicht als Datum zur Person des Betroffenen zu betrachten, sie sei vielmehr ein internes Datum. Die Angabe über das Krediturteil lasse den Schluß auf den Auskunftsempfänger zu, was die Geschäftsbeziehung zwischen Auskunftei und Auskunftsempfänger erheblich beeinträchtigen würde. Auch habe das Krediturteil, da es sich jeweils auf eine konkrete Anfrage beziehe, objektiv keinerlei Aussagewert – es sei ebenfalls ein internes Datum.

Die Aufsichtsbehörden haben die Frage nach dem Auskunftsempfänger zunächst zurückgestellt. Hinsichtlich des Krediturteils haben sie mit Nachdruck die Auffassung vertreten, daß dies kein internes Datum sei und die Auskunftspflicht des § 34 BDSG nur in besonderen Ausnahmefällen eingeschränkt werden könne. Im Normalfall müsse – wenn das Krediturteil in der Wirtschaftsauskunft genannt ist – dem Betroffenen diese Auskunft gegeben werden.

7.1.2 Auskunftsstelle über den Versicherungsaußendienst e.V. (AVAD)

In Hamburg hat eine Auskunftsstelle über den Versicherungsaußendienst (AVAD) ihren Sitz, sie hat die Rechtsform eines eingetragenen Vereins. Nach ihrer Satzung ist es ihre Aufgabe zu erreichen, daß nur vertrauenswürdige Personen im Versicherungsaußendienst tätig sind. Hierzu unterhält sie einen Auskunftsverkehr mit allen Versicherungsgesellschaften im Bundesgebiet. Entsprechend den Auskunftsrichtlinien der AVAD werden über alle bei den Versicherungsunternehmen ausgeschiedenen angestellten und freien Mitarbeiter formularmäßig vorgegebene Auskünfte gefertigt und der AVAD zugesandt. Sobald sich jemand für eine Außendienstarbeit bei einem Versicherungsunternehmen bewirbt, wird bei der AVAD nachgefragt und die evtl. vorliegende Auskunft abgefordert.

Bisher hat die Aufsichtsbehörde das Speichern auf der Grundlage des § 32 BDSG ohne Einwilligung des Betroffenen für zulässig gehalten. Die Rechtsprechung einiger Arbeitsgerichte hat mich veranlaßt, diese Position zu überprüfen.

Ich habe ein Gespräch mit der AVAD verabredet.

7.1.3 Schufa

Als Schutzgemeinschaften für allgemeine Kreditsicherung verstehen sich die verschiedenen Schufa-Gesellschaften im Bundesgebiet und die ihnen angeschlossenen Firmen. Auch in Hamburg hat eine Schufa GmbH ihren Sitz.

Schon bald nach Inkrafttreten des BDSG hatten sich die Schufa-Gesellschaften mit ihren Anschlußfirmen auf eine Formulierung geeinigt, mit der die betreffenden Kunden über die Speicherung bei der Schufa informiert werden sollten.

Die Aufsichtsbehörden hatten Zweifel am Sinn dieser Schufa-Klausel, da verschiedene Kreditinstitute keine Verträge annahmen, wenn die Klausel gestrichen worden war. Dies sprach dafür, daß die Klausel als Einwilligung in die Übermittlung an die Schufa, die dortige Speicherung und ggf. die weiteren Übermittlungen verstanden wurde.

Diese Frage war Anlaß für eine Gesprächsrunde, zu der die Aufsichtsbehörden mit der Schufa sowie den Verbänden der Kreditwirtschaft und des Versandhandels zusammenkamen. Im Verlauf dieser Gespräche sind zahlreiche Klarstellungen und Verbesserungen erreicht worden. Wesentlichstes Ergebnis sind eine neue Schufa-Klausel und eine stark überarbeitete „Technische Anleitung", die Bestandteil des Schufa-Vertrages ist.

Da die Informationen an die Schufa pauschal und ohne Prüfung im Einzelfall gemeldet werden, kann nicht immer von der Zulässigkeit der Datenübermittlung nach § 24 Abs. 1 BDSG ausgegangen werden. Aus diesem Grunde ist die Klausel dahingehend erweitert worden, daß der Betroffene über die Übermittlung an die Schufa und die dortige Speicherung aufgeklärt wird und mit seiner Unterschrift eine formell korrekte Einwilligung i.S. des § 3 BDSG abgibt.

Beim Schufa-Meldeverfahren stellt sich ein auch in anderem Zusammenhang immer wieder auftauchendes Problem: Ist es besser, wenn keine Informationen weitergegeben werden, oder kommt es vor allem darauf an, daß die ausgetauschten Informationen ein möglichst genaues Bild ergeben? Das Ergebnis wird wohl immer ein Kompromiß sein.

So sind jetzt einige nicht so wesentliche und andere nicht ganz eindeutige Merkmale weggelassen. Auf Meldungen über Bagatellbeträge ist ganz verzichtet worden. Andererseits ist klarer festgelegt, was im Einzelfall vorgefallen sein muß, bevor z.B. das Merkmal „Letzte Mahnung" gemeldet werden darf. Auch ist geregelt, daß die Informationen fortlaufend zu aktualisieren sind (z.B. Anfechtung und Aufhebung eines Mahnbescheides). Anfragen zu Personaleinstellungen sind nach den Schufa-Verträgen nicht mehr zulässig.

Bei Anfragen an die Schufa muß die fragende Stelle jedesmal angeben, worin ihr Interesse an der Auskunft liegt. Die Begründung für das berechtigte Interesse hat die Schufa aufzuzeichnen. Da sich die Anfragegründe ständig wiederholen, wird mit bestimmten Kürzeln bei der Schufa angefragt, wobei dieses Kürzel gleichzeitig den Grund der Anfrage angibt.

Da es nun relativ einfach ist, mit einem Kürzel bei der Schufa anzufragen, haben die Aufsichtsbehörden empfohlen, daß sich die Schufa in ihrem Vertrag ein Kontrollrecht für Stichproben einräumen läßt. Dieser Empfehlung ist die Schufa gefolgt. Diese Überprüfungen des berechtigten Interesses sind bei den Anschlußfirmen zur normalen Routine geworden.

Der Schufa sind hauptsächlich Kreditinstitute angeschlossen. Daneben haben jedoch auch Wirtschaftsunternehmen aller Branchen, vor allem Versand- und Kaufhäuser und Handelsfirmen einen – allerdings eingeschränkten – Zugang zu den Informationen der Schufa, wenn sie sich ihr mit dem sog. B-Vertrag anschließen. Im Rahmen dieses Vertrages werden nur ausgewählte Negativ-Daten weitergegeben, da die übrigen Daten für die B-Anschlußfirmen ohne Bedeutung sind.

Aus einigen Beschwerden wurde bekannt, daß die Schufa Informationen aus ihren Beständen an Wohnungseigentümer zum Zwecke der Überprüfung der Bonität übermittelt.

Bei den Aufsichtsbehörden bestehen Zweifel, ob dieses Meldeverfahren mit dem Selbstverständnis der Schufa – die kreditgebende Wirtschaft vor Verlusten im Kreditgeschäft schützen zu wollen – zu vereinbaren ist. Bedenken ergeben sich auch, weil der Kreis der Auskunftsempfänger eine Dimension annimmt, die über den ursprünglichen Geschäftszweck der Schufa hinausgeht.

Der Schufa-Vertrag und die dazugehörige Technische Anleitung enthalten für dieses Meldeverfahren keine besonderen Regelungen. Die Begründung der Anfragen mit dem Merkmal „AV" (Anfrage wegen Vorleistung oder Lieferung mit kreditorischem oder geschäftlichem Risiko) beschreibt den Fall nicht genau genug, um ein entsprechendes Interesse substantiiert belegen zu können. Die Bedenken verstärken sich, wenn dieses Merkmal für geschäftliche Risiken aller Art verwendet werden sollte.

Die Problematik soll in weiteren Gesprächen mit der Schufa erörtert werden.

7.2 Versicherungswirtschaft

7.2.1 Versicherungsklausel

Um die durch die Datenverarbeitung erzielten Rationalisierungserfolge zu erhalten und die Datenverarbeitung im Hinblick auf das BDSG rechtlich abzusichern, hielt die Versicherungswirtschaft die Einführung einer Datenschutz-Ermächtigungsklausel für erforderlich. Mit ihr wurden im wesentlichen zwei Anliegen verfolgt. Zum ersten sollte sie die Zulässigkeit der Datenverarbeitung auch in den Fällen sicherstellen, in denen die Voraussetzungen der §§ 23 oder 24 Abs. 1 BDSG nicht gegeben oder zweifelhaft waren. Sie sollte zum anderen eine Benachrichtigung durch die Datenempfänger, die selbst speichern, entbehrlich machen.

In mehreren Gesprächen zwischen den Aufsichtsbehörden und der Versicherungswirtschaft unter Beteiligung des Bundesaufsichtsamtes für das Versicherungswesen wurde näher untersucht, inwieweit die Ermächtigungsklausel notwendig und in welcher Form sie zulässig ist. Dabei wurde herausgearbeitet, daß Informationen über den einzelnen Versicherungsnehmer an sehr verschiedene Empfänger weitergegeben werden, das können sein

- Rückversicherer,
- andere Versicherungsunternehmen der Versicherungsgruppe,

- Verbände einer Sparte,
- andere Versicherungsunternehmen derselben Sparte und
- Versicherungsvermittler.

Es stellte sich heraus, daß viele Datenübermittlungen erfolgen, ohne daß im Einzelfall die Zulässigkeit durch den jeweiligen Bearbeiter geprüft werden kann. Wegen der fehlenden Einzelfallprüfung sind die Voraussetzungen für eine zulässige Datenübermittlung nach § 24 Abs. 1 BDSG nicht gegeben. Die Zulässigkeit kann deshalb nur durch Einwilligung des Betroffenen herbeigeführt werden.

Für eine Einwilligung ist Voraussetzung, daß der Betroffene erfährt, in was er einzuwilligen gedenkt. Deshalb ist die Klausel so gestaltet, daß jedes Versicherungsunternehmen die üblichen Datenempfänger konkret bezeichnen kann. Außerdem ist vorgesehen, daß dem Betroffenen auf Wunsch ein Merkblatt zugesandt oder ausgehändigt wird, in dem die Datenübermittlungen und ihr Zweck ausführlich beschrieben sind.

Mit Ausnahme der Kfz-Haftpflicht-Versicherung gibt es keinen Anspruch auf Abschluß eines Versicherungsvertrages; das bedeutet, daß ein Versicherungsunternehmen generell kein Vertragsangebot anzunehmen braucht, wenn die Ermächtigungsklausel gestrichen wurde. Unter versicherungsaufsichtsrechtlichen Gesichtspunkten ist eine endgültige Ablehnung des Vertrages erst dann gerechtfertigt, wenn der Antragsteller von dem Unternehmen in ausreichender Weise darüber unterrichtet worden ist, weshalb in seinem konkreten Fall die Durchführung des Vertrages unmöglich ist, wenn eine Einwilligung nicht erteilt ist.

7.2.2 Zentrale Dateien bei Verbänden

Nach dem Verständnis der Versicherungswirtschaft deckt die Klausel auch den Fall ab, daß personenbezogene Daten, die auf ein vergrößertes Versicherungsrisiko hindeuten, an Verbände der einzelnen Sparten übermittelt werden. Das sind im wesentlichen Informationen über Auffälligkeiten bei Schadensabwicklungen. Ziel ist es, die Versicherungsunternehmen und damit auch die Gemeinschaft der Versicherten vor Ungerechtigkeiten und Betrug zu schützen.

1.) Bei dem in Hamburg ansässigen Verband der Haftpflicht-, Unfall-, Auto- und Rechtsschutzversicherer (HUK-Verband) gibt es beispielsweise eine zentrale Registrierstelle. Hier können alle Kraftfahrzeug-Haftpflicht-Versicherer des Bundesgebietes für eine Schadensregulierung nachfragen, ob der Schädiger schon einmal wegen Versicherungsbetruges verurteilt wurde oder ob er schon früher an auffälligen Schäden beteiligt war. Diese Fragen sind bei einer Schadensmeldung ohnehin zu beantworten; wenn Angaben hierüber fehlen, hat der Versicherungsnehmer seine vertraglichen Pflichten verletzt. Der Verband kann mit Hilfe der zentralen Registrierstelle angeben, bei welchen Gesellschaften und unter welchen Schadensnummern Vorgänge existieren. Die Registrierstelle führt eine angereicherte Hinweisdatei. Einzelheiten können jedoch nur bei den direkt betroffenen Versicherungsgesellschaften erfragt werden.

   Dieses Meldeverfahren, in dem der Verband einzelne Auskunftsersuchen beantwortet, ist insoweit nicht zu beanstanden.

2.) Im Rechtsschutzbereich ist geregelt, daß dem HUK-Verband alle Vertragskündigungen zu melden sind, die die Versicherer ausgesprochen haben. Diese Kündigung erfolgt i.d.R. dann, wenn ein Versicherungsnehmer auffällig häufig seine Rechtsschutzversicherung in Anspruch genommen hat. Dies wird als Indiz für ein nicht normales Versicherungsrisiko angesehen.

   Die Aufsichtsbehörden haben gegen die Meldung an den HUK-Verband nichts einzuwenden, wohl aber dagegen, daß dieser alle ihm zugegangenen Meldungen vervielfältigt und – teils per Magnetband – an alle im Bundesgebiet ansässigen Rechtsschutz-

versicherer weiterleitet. Die so weit gestreuten Datenübermittlungen sind meiner Meinung nach nicht erforderlich. Es müßte genügen, wenn die entsprechende Information nur auf eine Einzelanfrage hin weitergegeben wird. Die Versicherungswirtschaft hält dem praktische und wirtschaftliche Gründe entgegen, die mich bisher nicht überzeugen.

In einer Gesprächsrunde mit den Versicherungsverbänden soll nach Lösungsmöglichkeiten gesucht werden.

3.) Für die Sparte der Reisegepäckversicherung ist ein Meldedienst zum Deutschen Transportversicherer-Verband (DTV) eingerichtet. Die auffälligen Schadensabwicklungen werden auf Karteikarten mitgeteilt. Der Verband kopiert die Karten und gibt sie den angeschlossenen Gesellschaften bekannt. Das Original wird zu Beweiszwecken in einer alphabetisch geordneten Kartei verwahrt, aus der nur äußerst selten Auskünfte erfragt werden.

Auch in diesem Falle erscheint mir die Verbreitung der Informationen an alle Reisegepäckversicherer nicht zulässig. Die oben erwähnte Gesprächsrunde wird sich auch hiermit beschäftigen.

7.3 Adreßhandel

Viele Beschwerden richten sich gegen die unverlangte Zusendung von direkt adressiertem Werbematerial. Ich werde oft gefragt, wie die Absender die Anschriften erhalten, ob ein Verstoß gegen Datenschutzvorschriften vorliegt und ob und wie man sich gegen die Werbung wehren kann.

Zunächst soll die Arbeitsweise in der Direktwerbung beschrieben werden.

Vor dem Inkrafttreten des Bundesdatenschutzgesetzes wurden Adressen im wesentlichen in ganzen Beständen (auf Magnetband oder auf Listen mit Aufklebern) zur einmaligen Nutzung verkauft. Es kam also zur tatsächlichen Übergabe des Adreßmaterials. Oftmals wurden ein oder mehrere Vermittler zwischengeschaltet, um die Adressen einer bestimmten Zielgruppe zusammenzustellen.

Neuerdings hat sich die sog. Adressenmittlung durchgesetzt. Hierbei werden die Adressen genutzt, ohne daß sie den Herrschaftsbereich eines rechtmäßig speichernden Unternehmens verlassen. Adreß-Eigentümer kann ein Adressenverlag, ein Versandhaus oder irgendein Handelsunternehmen sein. Ein Vermittler bringt die Interessen des werbenden und des die Adressen besitzenden Unternehmens zusammen. Die eine Seite stellt das Werbematerial zur Verfügung, die andere die Adressen. Der Vermittler oder in seinem Auftrag ein sog. Letter-Shop adressieren das Material und geben es zur Post auf. Als Absender sind entweder das werbende Unternehmen oder ein Postfach des Letter-Shop angegeben.

Die an der Adressenmittlung Beteiligten haben ursprünglich die Meinung vertreten, es komme bei diesem Verfahren gar nicht zu einer Datenübermittlung im Sinne des BDSG.

Um die Problematik aufzuhellen, haben die Aufsichtsbehörden mit dem Adressenverleger- und Direktwerbeunternehmer Verband e.V. verhandelt, der mit 22 Mitgliedern etwa ein Drittel des Marktanteils vertritt. Die Gespräche hatten im wesentlichen folgende Ergebnisse:

1.) Zu Unrecht erlangte Daten dürfen nicht gespeichert werden, weil wegen der Art der Erhebung schutzwürdige Belange des Betroffenen beeinträchtigt sind. Konsequenterweise sind solche Daten zu löschen (§ 35 BDSG).

In diesem Zusammenhang hat der Verband darauf hingewiesen, daß seine Mitglieder ein eigenes Interesse haben, nur die Adressen solcher Personen zu speichern und zu vermitteln, die sich nicht belästigt fühlen.

Deshalb wurde auch die sog. „Robinsonliste" eingerichtet, in die aufgenommen wird, wer nicht umworben werden möchte. Die Aufnahme in die „Robinsonliste" kann erbeten werden beim

Adressenverleger- und Direkt-
werbeunternehmer-Verband e.V.
Postfach 2149
6000 Frankfurt 1.

Ähnliche Karteien wurden auch bei weiteren Stellen eingerichtet, so kann man sich wenden an die

Deutsche Postreklame GmbH
Wiesenhüttenstr. 18
6000 Frankfurt

und das

Kraftfahrtbundesamt
Fördestr. 16
2390 Flensburg.

2.) Es besteht nunmehr Einigkeit darüber, daß bei der Adressenmittlung eine Datenübermittlung dann vorliegt, wenn dem werbenden Unternehmen (oder seinem Auftragnehmer) personenbezogene Daten bekannt werden, also auch dann, wenn der Umworbene durch seine Rückantwort unfreiwillig zu erkennen gibt, daß er die Voraussetzungen der Zielgruppenbeschreibung erfüllt.

Die Tätigkeit der Adressenanbieter ist demzufolge nach den Kriterien des Vierten Abschnitts des BDSG zu beurteilen.

Die unfreiwillige Übermittlung durch die Rückäußerung des Betroffenen kann dadurch vermieden werden, daß ihm die Selektionskriterien genannt werden, die dazu führten, daß seine Anschrift genutzt wurde. Wenn er sich dann dem werbenden Unternehmen offenbart, geschieht dies eigenverantwortlich und in vollem Bewußtsein der Tragweite seiner Rückmeldung.

Die Adressenmieter haben vorgeschlagen, den Umworbenen mit einem Beilagezettel oder in Form eines herausgestellten Kästchens darüber aufzuklären, nach welchen Kriterien die Adressen für dieses Werbeangebot ausgewählt wurden, und ihm auf Einzelanfrage individuelle Auskunft über die Herkunft der Adresse sowie der Selektionskriterien anzubieten.

3.) Eine Datenübermittlung liegt auch dann vor, wenn dem Vermittler Anschriften zur eigenverantwortlichen Nutzung überlassen werden. In diesem Fall wird der Vermittler selbst zur speichernden Stelle. Sofern er keine eigenen Nutzungsrechte hat, ist er Auftragnehmer im Sinne des § 37 BDSG. Herr der Daten bleibt der Vermieter. Aus § 37 BDSG ist aber die Verpflichtung herauszulesen, daß der Betroffene – zumindest auf Anfrage – über die Identität der speichernden Stelle in Kenntnis zu setzen ist, da er sonst seine Rechte nicht geltend machen kann.

Diese Ergebnisse bedeuten bereits eine Verbesserung der Situation des Betroffenen. Noch mehr würde erreicht werden, wenn die mir als Vorentwurf bekanntgewordene Empfehlung des Europarats zum Schutz personenbezogener Daten bei der Verwendung für Zwecke der Direktwerbung umgesetzt würde.

Darin wird im einzelnen empfohlen,

- den Betroffenen über die beabsichtigte Nutzung zu Werbezwecken zu unterrichten,
- ihm das Recht zuzugestehen, die Weitergabe zu untersagen,
- Listen mit besonders sensiblen Daten nur mit seiner Zustimmung weiterzugeben,
- bei der Aufforderung des Betroffenen an einen Werbenden, seine Adresse zu löschen, diese Aufforderung an alle bei der Vermittlung beteiligten Stellen weiterzureichen, damit er künftig nicht umworben wird,
- ihm auf Anfrage den Usprung seiner Adresse zu nennen.

7.4 Daten über Mietinteressenten

Durch eine Eingabe bin ich mit dem Problem der Erhebung von Daten über Mietinteressenten konfrontiert worden. Wie auch der Presse zu entnehmen war, verlangen manche Vermieter – allen voran die großen Wohnungsgesellschaften – von Mietinteressenten detaillierte Auskünfte über Einkommens- und Vermögensverhältnisse (Arbeitseinkommen, sonstige regelmäßige Einkünfte etc.), sowie über familiäre Verhältnisse (von Alter und Geschlecht der Kinder und sonstigen Haushaltsangehörigen bis hin zur Frage nach Schwangerschaften). Weiter wird nach dem Namen des letzten Hauswirts, dem Grund der Kündigung und der Dauer des Mietverhältnisses gefragt. In dem mir vorgelegten Fragebogen mußten Mieter auch versichern, daß sie ihre Miete bisher immer pünktlich entrichtet, keine Mahnbescheide erhalten und niemals einen Offenbarungseid geleistet haben.

Darüber hinaus sind große Wohnungsbaugesellschaften dazu übergegangen, generell bei der SCHUFA anzufragen und Bewerber, die dort (z.B. mit Schulden aus Versandhausgeschäften) registriert sind, abzulehnen. Weiterhin ist es fast schon als üblich anzusehen, daß etwa Sozialhilfeempfänger Bürgen für die Mietzahlung zu benennen haben. Nach dem letzten Jahresbericht des Amtes für Heime über die Obdachlosenbetreuung (vom Sept. 1982) führen diese Praktiken dazu, daß immer weniger Familien oder Alleinstehende die Chance haben, eine Obdachlosigkeit zu überwinden.

Das Problem liegt darin, daß die Mietinteressenten den Datenwünschen der Vermieter praktisch hilflos ausgeliefert sind, denn sie müssen damit rechnen, daß sie von vornherein aus der Liste der Bewerber gestrichen werden, wenn sie auch nur einzelne der geforderten Angaben oder Einwilligungen nicht erteilen.

Das geltende Datenschutzrecht kann den Betroffenen leider keinen Schutz bieten, da die Angaben von dem Bewerber auf „freiwilliger" Basis erhoben werden.

Ein rechtlicher Ansatz zur Lösung der Probleme könnte allenfalls darin liegen, daß bestimmte Fragen als unzulässiger Eingriff in die zu schützende Individualsphäre zu werten sein könnten; solche Fragen brauchte der Wohnungssuchende dann analog der zum Arbeitsverhältnis entwickelten Grundsätze nicht oder nicht wahrheitsgemäß zu beantworten. Ich habe jedoch Zweifel, ob dieser Lösungsweg tragfähig ist.

Sicherer wäre es jedoch, wenn der Gesetzgeber der o.g. Entwicklung mit gesetzlichen Maßnahmen entgegenträte. Die entsprechende Empfehlung des Bundesbeauftragten für den Datenschutz in seinem 4. Tätigkeitsbericht (Ziff. 4.1.9) findet meine volle Unterstützung.

7.5 Schutz von Arbeitnehmerdaten

Ein auch in quantitativer Hinsicht bedeutsamer Anteil meiner Beratungstätigkeit im nichtöffentlichen Bereich bezog sich auf die mit dem Schutz von Arbeitnehmerdaten im Betrieb zusammenhängenden Probleme.

7.5.1 Personalinformationssysteme

Das Arbeitsverhältnis ist schon seit langem zu einem Schnittpunkt privater und staatlicher Informationsansprüche geworden: Zum einen sehen sich viele Unternehmen bei der heutigen Wirtschaftslage veranlaßt, sämtliche Rationalisierungsmöglichkeiten zu nutzen; hierzu benötigen sie mehr und schnellere Informationen. Zum anderen haben die Unternehmen in erheblichem Umfang staatliche Melde- und Auskunftspflichten im Personalbereich zu erfüllen. Als herausragende Beispiele sind in diesem Zusammenhang etwa die Datenerfassungs-Verordnung (DEVO) vom 24.11.1972 und die Datenübermittlungs-Verordnung (DÜVO) vom 18.12.1972 zu nennen, in denen Inhalt und Form der Meldungen nach der RVO, dem Angestelltenversicherungsgesetz und dem Arbeitsförderungsgesetz näher geregelt werden.

Die ständig wachsende Menge der so beanspruchten Informationen kann in vielen Unternehmen nur noch mit Hilfe von automatisierter Datenverarbeitung bewältigt werden. Umfang, Intensität und Regelmäßigkeit der Datenverarbeitung begründen die Gefahr, daß das Arbeitsverhältnis damit gleichzeitig zu einem Experimentierfeld für neue und bessere Verarbeitungsmethoden wird.

Von den Arbeitnehmern und ihren Gewerkschaften wird in diesem Zusammenhang die Gefahr des „gläsernen Menschen" gesehen, wenn Tausende von Daten über Belegschaftsangehörige in Personal-Informations-Systemen gespeichert werden. Daß solche Systeme dem Arbeitnehmer auch Nachteile bringen und jedenfalls zu einem nicht unerheblichen Machtzuwachs der Arbeitgeber führen können, soweit ihm die Verwendung von Personalinformationen freigestellt ist, liegt auf der Hand. Diese Gefahren sollten jedoch nicht überbetont und emotionalisiert werden; durch die individualrechtlichen Regelungen der §§ 3, 23, 24 BDSG einerseits und die kollektiv-rechtlichen Mitbestimmungs- und Beteiligungsregelungen des Betriebsverfassungsgesetzes andererseits werden die Nutzungsmöglichkeiten von Personalinformationen bereits wesentlich eingeschränkt.

Ein Abbau der vielerorts vorhandenen Befürchtungen bei den Arbeitnehmern wie auch die Wahrnehmung von Rechten setzt allerdings voraus, daß sie besser unterrichtet werden. Diese Aufforderung richtet sich gleichermaßen an Arbeitgeber und Gewerkschaften. Auch ich werde meinen Beitrag zur Information und zur Versachlichung der Diskussion leisten. Zur Einschränkung möglicher Konflikte trete ich gerade bei der Planung neuer Personalinformationssysteme für eine möglichst große Transparenz ein. Die Unternehmen sollten darauf Wert legen, die Vertretungsorgane der Arbeitnehmer so frühzeitig wie möglich zu beteiligen. Im übrigen sollte immer der Grundsatz beachtet werden: Je weniger Personalinformationen automatisiert verarbeitet und je konkreter die Verarbeitungszwecke festgelegt werden, desto besser läßt sich die Verwendung von Personalinformationen kontrollieren und desto geringer ist dementsprechend das Mißtrauen auf Seiten der Belegschaft.

7.5.2 Verhältnis BDSG – Betriebsverfassungsgesetz (BetrVG)

Schwierigkeiten ergeben sich bei der Frage nach dem Verhältnis zwischen dem BDSG und den arbeitsrechtlichen Vorschriften, vor allem dem BetrVG. Häufig mußte ich zu Fragen Stellung nehmen, in denen das BDSG kaum berührt ist: So ändert das BDSG überhaupt nichts an den Aufgaben und Mitbestimmungsrechten von Betriebsräten, diese richten sich ausschließlich nach dem BetrVG. Der Betriebsrat ist auch nach dem Inkrafttreten des BDSG wie bisher berechtigt und verpflichtet, die Informationsverarbeitung in Unternehmen zu kontrollieren. Probleme treten auf, wenn der Betreiber einer Datenverarbeitungsanlage vom BDSG (§ 6) vorgeschriebene Sicherheitsvorkehrungen zu treffen hat. Soweit diese Maßnahmen gleichzeitig geeignet sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen (§ 87 Abs. 1 Ziff. 6 BetrVG), unterliegen sie der Mitbestimmung des Betriebsrats.

Auch dieses Mitbestimmungsrecht bleibt durch die datenschutzrechtlichen Bestimmungen grundsätzlich unberührt, denn § 6 Abs. 1 BDSG räumt den Unternehmern einen Ermessensspielraum für die zu treffenden Sicherungsmaßnahmen ein. Diese Gestaltungsmöglichkeiten sind der Mitbestimmung voll zugänglich.

Auch heute noch wird darüber gestritten, ob Betriebsräte sich trotz ihrer Geheimhaltungspflichten nach § 79 BetrVG auch vom Arbeitgeber auf das Datengeheimnis nach § 5 BDSG verpflichten lassen müssen. Eine solche zusätzliche Verpflichtung wäre nur dann entbehrlich, wenn (vgl. § 45 BDSG) die betriebsverfassungsrechtlichen Vorschriften eine dekkungsgleiche Regelung wie § 5 Abs. 1 BDSG enthielten. Dies ist nach meiner Auffassung nicht der Fall: Im Gegensatz zum BDSG, nach dem alle personenbezogenen Daten geschützt werden, beschränken sich die Verschwiegenheitspflichten des BetrVG im wesentlichen auf Betriebs- und Geschäftsgeheimnisse sowie auf personenbezogene Daten mit einem gewissen Intim- bzw. Vertraulichkeitscharakter. Soweit die Verschwiegenheitspflicht nach § 79 BetrVG sich nicht auf in Dateien gespeicherte personenbezogene Daten erstreckt, ist deshalb auch eine Verpflichtung von Betriebsratsmitgliedern auf das Datengeheimnis geboten.

8. Ausblick

8.1 Schwerpunkte meiner künftigen Tätigkeit

Nachdem die Bestandsaufnahme jedenfalls in den sensiblen Bereichen im wesentlichen abgeschlossen und die Personal-Soll-Stärke erreicht ist, wird eine der wichtigsten Aufgaben im nächsten Jahr die umfassende Prüfung von ausgewählten speichernden Stellen (voraussichtlich Dienststellen in den Bereichen Gesundheitswesen, öffentliche Sicherheit und Bezirksverwaltung) sowie von Stellen, die im Auftrag verarbeiten (voraussichtlich die Rechenzentren der Universität und des Universitätskrankenhauses Eppendorf, eine dezentrale Datenverarbeitungsanlage einer Behörde und das Rechenzentrum einer juristischen Person des öffentlichen Rechts), sein. Es wird sich erweisen, ob die Kapazität ausreicht, zusätzlich einige Automationsverfahren zu prüfen. Im nicht-öffentlichen Bereich wird der Schwerpunkt meiner Prüfungstätigkeit bei den Wirtschaftsauskunfteien sowie den Zentraldateien der Versicherungsverbände liegen.

Ein weiterer Schwerpunkt wird – nach Fertigstellung des Registers – eine verstärkte Öffentlichkeitsarbeit sein.

8.2 Rechtsentwicklung in Hamburg

Ob und inwieweit das HmbDSG sich in der praktischen Anwendung bewährt hat, läßt sich so kurze Zeit nach dem Inkrafttreten naturgemäß noch nicht abschließend beurteilen. Deshalb möchte ich mich damit begnügen, die Aufmerksamkeit darauf zu lenken, daß einzelne Vorschriften und deren praktische Auswirkungen in Teilen der Verwaltung kritisch gesehen und diskutiert werden.

1.) Eine dieser Vorschriften ist § 6 Abs. 1 Nr. 4. Danach hat jeder in Bezug auf die zu seiner Person gespeicherten Daten das Recht auf Sperrung der Übermittlung an Behörden und sonstige öffentliche Stellen, soweit die Übermittlung nicht durch Gesetz zugelassen ist. Zwar tritt diese Regelung gem. § 29 Nr. 3 erst am 1. Mai 1984 in Kraft; doch wird bereits jetzt die Befürchtung geäußert, daß damit die Amtshilfe zwischen hamburgischen Behörden und den Behörden anderer Länder beeinträchtigt werden könnte. In welchem Umfang dies der Fall sein wird und ob daher bereichsspezififsche Übermittlungsregelungen geschaffen werden müßten, ist jedoch noch offen.

   Einen konkreten Regelungsbedarf für Übermittlungen an andere Behörden hat bisher lediglich die Polizei geltend gemacht, weil die vorhandenen spezialgesetzlichen Grundlagen (wie BKA-Gesetz, StPO) nicht alle für erforderlich gehaltenen Übermittlungen an andere Polizeidienststellen und sonstige Behörden absichern.

Es wird erwogen, zusätzliche Vorschriften über die Informationsflüsse der Polizei an externe Stellen in das Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung aufzunehmen. Eine solche gesetzliche Regelung wäre aus der Sicht des DSB zu begrüßen. Sie sollte allerdings nicht auf die Übermittlungen beschränkt werden. Vielmehr sollte die Gelegenheit genutzt werden, die Informationsbeschaffung und -verarbeitung durch die Polizei insgesamt auf einwandfreie gesetzliche Grundlagen zu stellen.

Das HmbDSG (§§ 9, 10, 12) enthält zwar allgemeine Befugnisnormen für die Speicherung und Übermittlung personenbezogener Daten durch öffentliche Stellen. Diese können jedoch für sich genommen nicht hinreichend klar abgrenzen, ob eine Datenverarbeitung durch die Polizei im Einzelfall zulässig ist oder nicht. Im übrigen enthalten sie keine Vorschriften über die Beschaffung von Informationen, so daß nur die polizeiliche Generalklausel als Rechtsgrundlage in Betracht kommt. Zusätzlich regelungsbedürftig ist schließlich die genauere Abgrenzung der Aufgabenbereiche von Gefahrenabwehr und Strafverfolgung und der daraus folgenden Konsequenzen für die Informationsarbeit.

Ich verkenne nicht, daß die Polizei intern bereits Anstrengungen unternommen hat, um datenschutzrechtlichen Belangen Rechnung zu tragen (KpS-Richtlinien). Es gibt auch eine Reihe von Richtlinien und Erlassen, die die polizeilichen Aufgaben präzisieren und ihr Informationsverhalten näher regeln. Dies vermag aber nichts daran zu ändern, daß es in Hamburg – wie in den anderen Bundesländern – an eindeutigen, hinreichend abgesicherten Befugnisnormen nach wie vor fehlt. Die Schaffung klarer gesetzlicher Maßstäbe für die Zulässigkeit der polizeilichen Informationsbeschaffung und -verarbeitung wäre geeignet, viele Rechtsunsicherheiten zu beseitigen und würde insofern auch dazu beitragen, das gelegentlich verkrampfte Verhältnis zwischen Datenschutz und Polizei zu lockern.

2.) Eine andere Vorschrift, die von Teilen der Verwaltung in ihrer praktischen Anwendbarkeit kritisch gesehen wird, ist § 15 Abs. 4. Danach sind gespeicherte Daten regelmäßig alle 4 Jahre auf ihre Erforderlichkeit hin zu überprüfen und die Datenbestände gem. Abs. 3 zu bereinigen.

Diesen Begriff der regelmäßigen vierjährlichen Überprüfung legt die Polizei – unterstützt vom Senatsamt für den Verwaltungsdienst – so aus, daß die Überprüfungspflicht grundsätzlich bestehe, in besonders gelagerten Fällen aber Ausnahmen möglich seien. Eine solche Ausnahmelage sei dann gegeben, wenn eine Datenaussonderung nach 4 Jahren – etwa wegen der längerfristigen Aufbewahrungszeiten nach den KpS-Richtlinien – nicht in Betracht komme.

Diese Auslegung kann ich – im Ergebnis in Übereinstimmung mit der Justizbehörde – nicht teilen: Der Begriff „regelmäßig" läßt keine Durchbrechung der vierjährlichen Überprüfungspflicht nach dem Regel-Ausnahme-Prinzip zu, sondern ist – wie auch in den Ausschußberatungen hervorgehoben wurde – ein „präziser Gesetzesbefehl". Alle Daten einer Datei sind demnach mindestens einmal in 4 Jahren auf ihre Erforderlichkeit hin zu überprüfen. Diese Überprüfung kann auch im Hinblick auf die Geltung verwaltungsinterner Aufbewahrungsbestimmungen – wie der KpS-Richtlinien – nicht entfallen. Dies ergibt sich schon daraus, daß untergesetzliche Vorschriften nicht Gesetze abändern können.

Darüber hinaus beruhen die in den KpS-Richtlinien geregelten Aufbewahrungsfristen nur auf verallgemeinernden Interessenabwägungen. Es ist demnach keineswegs ausgeschlossen, daß eine schon nach 4 Jahren – also vor Ablauf der meisten KpS-Aufbewahrungsfristen – vorgenommene Überprüfung eines Einzelfalles zu dem Ergebnis führt, daß Daten zu löschen sind, weil sie zur Aufgabenerfüllung nicht mehr erforderlich sind.

Folgendes Beispiel aus der Praxis mag dieses verdeutlichen: Eine Person wird (mit 10-jähriger Aufbewahrungsfrist) im POLAS gespeichert, weil gegen sie wegen schwerer Körperverletzung ermittelt und Anklage erhoben worden ist. Bei einer Überprüfung nach 4 Jahren wird festgestellt, daß das Ergebnis des Strafverfahrens bei der Polizei nicht vorliegt, was leider wegen fehlender oder zu langsamer Rückmeldungen von Verfahrensergebnissen häufig vorkommt. Eine Nachfrage bei der Staatsanwaltschaft ergibt Freispruch wegen erwiesener Unschuld. Konsequenz: Die Eintragung ist unverzüglich zu löschen.

Ich verkenne nicht, daß die vierjährliche Überprüfung für Stellen mit Massendatenverarbeitung (wie der Polizei) einen nicht unerheblichen Verwaltungsaufwand bedeuten kann. Dieser Umstand kann bei der Anwendung des Gesetzes jedoch nur insoweit berücksichtigt werden, als eine praktikable Rahmenregelung für die in den einzelnen Fällen anzustellenden Relevanzprüfungen zu entwickeln ist. Dabei kann auch bereits auf Erfahrungen mit der auch aus meiner Sicht akzeptablen Vorgehensweise beim LfV zurückgegriffen werden.

8.3 Rechtsentwicklung im Bund und in anderen Ländern

Der Hamburgische Datenschutzbeauftragte hat sein Amt zu einem Zeitpunkt angetreten – und damit in Hamburg eine neue Phase des Datenschutzes eingeleitet –, in dem der Datenschutz in anderen Ländern in ein zunehmend kritisches Stadium eingetreten ist. Die Abschaffung des Datenschutzes wird zwar nur vereinzelt verlangt; doch immer häufiger fordern Kritiker, daß Positionen, die bei der Beratung des Bundesdatenschutzgesetzes noch selbstverständlich waren, nunmehr wieder zurückgenommen werden.

Der Referentenentwurf eines Gesetzes zur Änderung des BDSG scheint wieder in der Versenkung verschwunden zu sein. Deswegen versage ich es mir, mich an dieser Stelle erneut hierzu zu äußern.

Empfindliche Rückschläge hat der Datenschutz besonders in Baden-Württemberg erfahren:

Nach der Änderung des Landesdatenschutzgesetzes ist die Übermittlung personenbezogener Daten von Behörde zu Behörde dort in der Form geregelt, daß nur noch der Empfänger (nicht mehr auch die übermittelnde Stelle) die Verantwortung dafür trägt, daß die Übermittlung personenbezogener Daten zur rechtmäßigen Erfüllung der in seiner Zuständigkeit liegenden Aufgaben erforderlich ist. Nach dieser Neuregelung muß der Bürger in Baden-Württemberg jetzt wieder mit einem weitgehend unkontrollierten Datenaustausch zwischen den Behörden rechnen, denn die ersuchende Behörde, die Daten zur Erfüllung ihrer Aufgaben erhalten will, wird die Erforderlichkeit der Übermittlung wesentlich leichter bejahen, als die ersuchte Behörde, die dem Ersucher in der Regel neutral gegenübersteht.

Die in Baden-Württemberg ebenfalls beschlossene ausdrückliche Beschränkung der Kontrollkompetenzen des Datenschutzbeauftragten auf Vorgänge der Datenverarbeitung in Dateien schwächt nachhaltig die Wirksamkeit der Kontrolle, insbesondere die Möglichkeiten der Datenschutzbeauftragten, Eingaben nachzugehen. Dadurch wird die Glaubwürdigkeit des Datenschutzes in den Augen der Bürger stark beeinträchtigt.

Schließlich ist in Baden-Württemberg geplant, im Wege einer Änderung des Datenschutzgesetzes die wissenschaftliche Forschung weitgehend von der Einhaltung der Berufs- und besonderen Amtsgeheimnisse freizustellen. Dieser fast einen datenschutzrechtlichen „Freibrief" enthaltende Vorschlag geht weit über das hinaus, was selbst bei großzügiger Betrachtungsweise im Interesse der Forschung geboten ist.

Die bisherige Beratung eines Gesetzentwurfs für das Krebsregister in Hamburg hat gezeigt, daß sich bei vorsichtiger und sachlicher Analyse der möglichen Konflikte zwischen medizinischer Forschung und Datenschutz befriedigende Lösungen finden lassen, die den Bedürfnissen der Forschung Rechnung tragen, ohne substantielle Belange des Datenschutzes zu beeinträchtigen.

Ich hoffe, daß es mir auch im nächsten Jahr gelingen wird, die bisherige positive Entwicklung des Datenschutzes in Hamburg zu erhalten und zu verstärken.

Hamburg, den 31.12.1982

Claus Henning Schapper

Übersicht über die vorläufige Organisation der Dienststelle des Hamburgischen Datenschutzbeauftragten