1. Einleitung

1.1 Vorbemerkung

In den vergangenen zwei Jahren waren Situation und Perspektiven des Datenschutzes thematisch vor allem bestimmt durch die Volkszählung 1987, durch die rasante Entwicklung auf dem Gebiet neuer Informations- und Kommunikationstechniken, die auch in den Büros der öffentlichen Verwaltungen mehr und mehr eingesetzt werden, und durch die immer dringlicher werdende Notwendigkeit, gesetzgeberische Konsequenzen aus dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 zu ziehen. Von besonderer Bedeutung für das Land Nordrhein-Westfalen war das Inkrafttreten des Gesetzes zur Fortentwicklung des Datenschutzes vom 15. März 1988, das eine grundlegende Neufassung des Datenschutzgesetzes Nordrhein-Westfalen enthält.

Das neue Datenschutzgesetz bringt auch für den Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Änderungen mit sich. § 27 dieses Gesetzes sieht vor, daß der Berichtszeitraum nicht mehr wie bisher auf ein Jahr festgelegt ist, sondern sich auf zwei Kalenderjahre erstreckt. Da der letzte Tätigkeitsbericht nach früherem Recht noch die Zeit bis zum 31. März 1987 erfaßte, gilt der vorliegende Bericht für die Zeit vom 1. April 1987 bis zum 31. Dezember 1988.

Nicht zuletzt diese Umstellung bedingt eine strukturelle und inhaltliche Neugestaltung des Tätigkeitsberichts. Statt der ausführlichen Darstellung einer großen Zahl von Einzelfällen ist es erforderlich geworden, Schwerpunkte zu bilden und nur die wichtiger erscheinenden Probleme abzuhandeln. Diese Gründe bestimmen auch den Aufbau des vorliegenden Berichts. So sind die ersten Erfahrungen mit dem neuen Datenschutzgesetz, soweit sie besondere Auslegungs- und Anwendungsprobleme mit sich gebracht haben, in einem Abschnitt zusammengefaßt. Ein weiterer Abschnitt bietet die Zusammenstellung der wichtigsten Bereiche, für die inzwischen datenschutzrechtliche Neuregelungen getroffen worden sind oder aber – weitaus überwiegend – dringender gesetzlicher Regelungsbedarf besteht. In den Abschnitten über die Rechtsprechung zum informationellen Selbstbestimmungsrecht und über den Datenschutz in den Bereichen der Verwaltung habe ich mich auf die Behandlung von Einzelfragen und Fällen beschränkt, denen ich eine allgemeine oder exemplarische Bedeutung zumesse. Gleiches gilt für den Abschnitt über die organisatorischen und technischen Maßnahmen. Die wichtigsten Feststellungen, Anregungen und Forderungen habe ich in einem Überblick meinem Bericht in Kurzform vorangestellt. Erstmalig enthält der Bericht ein Stichwortverzeichnis.

1.2 Amtswechsel

In den Berichtszeitraum fällt auch ein Wechsel im Amt des Landesbeauftragten für den Datenschutz.

Mein Amtsvorgänger Dr. Heinrich Weyer ist am 4. September 1987 nach Ablauf seiner achtjährigen Berufungszeit aus dem Amt ausgeschieden. Die Lan-

desregierung sprach ihm Dank und Anerkennung aus und würdigte ihn als kritischen und höchst fachkundigen Beobachter und Ratgeber des Datenschutzes. Auch von Vertretern der drei Landtagsfraktionen wurden seine Verdienste hervorgehoben, die er sich über die Landesgrenzen hinaus erworben hat. Er hat das Amt des Landesbeauftragten mit Leben erfüllt und wesentlich dazu beigetragen, daß in Nordrhein-Westfalen ein nachhaltiges Bewußtsein für den Stellenwert und die Belange des Datenschutzes gewachsen ist.

Ich habe mein Amt als neuer Landesbeauftragter für den Datenschutz am 1. Dezember 1987 angetreten. Meinem Vorgänger bin ich dankbar dafür, daß er mir ein wohlbestelltes Feld überlassen hat, das ich ohne besondere Übergangsprobleme weiter bearbeiten konnte. Wie er verstehe ich die mir übertragenen Aufgaben nicht als einseitige Interessenvertretung. Vielmehr geht mein Bemühen dahin, die Privatsphäre des Einzelnen soweit wie möglich zu schützen, ohne dem gegenüberstehende Allgemeininteressen bei der gebotenen Abwägung zu vernachlässigen. Dabei handelt es sich, wie mir viele Eingaben von Bürgern zeigen, häufig nicht um Fragen von Rechtsverstößen gegen den Datenschutz durch öffentliche Stellen oder deren Beschäftigte, sondern vielfach geht es dem Bürger um eine Aufklärung, auf welcher Grundlage personenbezogene Daten über ihn erhoben werden, welche Stellen davon unterrichtet werden (können) und inwieweit die Zweckbindung der Datenverarbeitung gesichert ist. Besonderes Gewicht lege ich auch auf eine praxisnahe Beratung der öffentlichen Stellen, soweit dies im Rahmen meiner personellen und sächlichen Ausstattung möglich ist.

An dieser Stelle möchte ich nicht versäumen, den Mitarbeiterinnen und Mitarbeitern meiner Dienststelle zu danken, deren sachkundiges und engagiertes Mitwirken die Erfüllung meiner Aufgaben erst ermöglicht.

1.3 Schwerpunkte der Tätigkeit

Das Schwergewicht meiner Tätigkeit lag in der Beantwortung von **Bürgereingaben**, die für mich schon wegen ihrer Zahl, aber auch wegen ihrer Bedeutung – Datenschutz ist Bürgerschutz! – den Hauptanlaß für meine Kontrolltätigkeit bilden. Darüber hinaus suchten viele öffentliche Stellen meinen Rat. **Beratungsschwerpunkte** waren u. a. Fragen der Volkszählung, die Datenverarbeitung für wissenschaftliche Zwecke und die Zulässigkeit der Bekanntgabe personenbezogener Umweltdaten, insbesondere im Bereich der Altlasten. Ebenfalls im Sinne vorbeugenden Datenschutzes habe ich zu einer Reihe datenschutzrechtlich relevanter **Gesetzesvorhaben** Stellung genommen.

Bei zahlreichen **Kontrollbesuchen** wurden die Zulässigkeit der Verarbeitung personenbezogener Daten und die getroffenen organisatorischen und technischen Maßnahmen überprüft. Die Prüfungen erfolgten u. a. bei Kommunen, Polizeibehörden, im Sozialversicherungsbereich sowie bei kommunalen und staatlichen Rechenzentren.

Eine Reihe von **Informationsbesuchen** vertiefte mein Bild vom Stand des Datenschutzes in unterschiedlichen Bereichen. Als Beispiele seien das Stel-

lenverwaltungssystem SIS beim Minister für Wissenschaft und Forschung sowie das „Generelle Schulinformationssystem GESI" genannt, das von verschiedenen Städten im westlichen Ruhrgebiet angewandt wird. Außerdem habe ich beim Landesrechnungshof und beim Justizminister eingehende **Beratungsgespräche** über Fragen des Datenschutzes geführt; dabei konnte das gegenseitige Verständnis gefördert werden.

In einundzwanzig Fällen habe ich gegenüber öffentlichen Stellen förmliche **Beanstandungen** auf Grund von Verstößen gegen Vorschriften über den Datenschutz ausgesprochen (vgl. § 30 DSG NW a.F, § 24 DSG NW n.F). Die Beanstandungen betrafen vorwiegend Fälle aus den Bereichen Sozialwesen, Ausländerangelegenheiten und Volkszählung, bei der es um Fragen der Bestellung von städtischen Bediensteten zu Zählern und zu Leitern von Erhebungsstellen ging. Bei einer um ein Vielfaches größeren Zahl von Verstößen konnte ich von einer Beanstandung absehen, insbesondere deshalb, weil die Behebung der Mängel entsprechend meinen Empfehlungen sichergestellt schien. Eine Auflistung aller Beanstandungsfälle im Tätigkeitsbericht halte ich für entbehrlich, da die Notwendigkeit der Beanstandungen nicht in erster Linie von der Schwere des Verstoßes abhängt und unbeanstandete Fälle der Sache nach bedeutsamer sein können. Dies schließt nicht aus, daß im Bericht zum Teil auch auf Beanstandungen eingegangen wird, soweit damit eine über den Einzelfall hinausweisende Problematik verbuden ist.

1.4 Öffentlichkeitsarbeit

Die anhaltende Nachfrage verschiedener Institutionen und einer breiten Öffentlichkeit war für mich weiterhin Beweggrund, durch intensive Öffentlichkeitsarbeit das Datenschutzbewußtsein der Bürger zu fördern.

In Presseerklärungen, Zeitungs-, Rundfunk- und Fernsehinterviews, Podiumsdiskussionen, Vorträgen, Seminaren sowie Veröffentlichungen in Fachzeitschriften haben ich oder meine Mitarbeiter zu verschiedenen Themen Stellung genommen. Im Vordergrund standen dabei die Volkszählung des Jahres 1987 und die neue Landesgesetzgebung zum allgemeinen Datenschutzrecht. Auch in anderen Bereichen, wie z. B. beim Datenschutz im Gesundheits-, Sozial-, Kommunal- und Schulwesen sowie bei der Datensicherung gab es eine erhebliche Nachfrage. In besonderem Maße habe ich mich an Lehrgängen im Rahmen des ADV-Fortbildungsprogramms des Innenministers beteiligt. Angesichts der Personalsituation meiner Dienststelle war es meinen Mitarbeitern und mir leider nicht möglich, allen Wünschen zu entsprechen.

Daneben habe ich in großer Zahl Informationsmaterial an interessierte Stellen und Bürger abgegeben. Auf dem Gebiet der Datensicherung gehörten hierzu außer meiner Organisationshilfe zur Datensicherung ein an mehr als tausend öffentliche Stellen verteilter Sammelband mit den entsprechenden Auszügen aus meinen ersten acht Tätigkeitsberichten einschließlich Stichwortverzeichnis. Zum neuen Datenschutzgesetz Nordrhein-Westfalen habe ich ein Faltblatt herausgegeben, das auch einen Überblick über die Datenschutzkontrollinstanzen nach anderen Gesetzen enthält. Ferner konnte ich eine Informa-

tionsschrift des Innenministers mit dem Text des neuen Datenschutzgesetzes in die Verteilung einbeziehen. Erneut betraf eine Vielzahl von Anforderungen meine Tätigkeitsberichte.

1.5 Zusammenarbeit im Datenschutz

Die **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** hat im Berichtszeitraum in fünf Sitzungen wiederum eine Reihe aktueller Datenschutzfragen behandelt, die sich insbesondere auf Grund zunehmender Gesetzgebungsaktivitäten auf diesem Felde stellten. Erörtert wurden u. a. folgende Themen:

- Neukonzeption des Ausländerzentralregisters
- Rückmeldung von der Justiz an die Polizei über den Ausgang von Strafverfahren
- Speicherung von AIDS-Daten in polizeilichen Informationssystemen
- Polizeiliche Datenverarbeitung bis zum Erlaß bereichspezifischer gesetzlicher Regelungen
- Neufassung des Bundesdatenschutzgesetzes
- Gesundheitsreform
- Poststrukturreform und Telekommunikation
- Datensicherheit beim Einsatz kleinerer Datenverarbeitungsanlagen.

Außer in den Sitzungen der Konferenz wirkte ich in einer Reihe ihrer Arbeitskreise an den Beratungen mit. In den Arbeitskreisen Steuerverwaltung und Statistik habe ich den Vorsitz. Schwerpunktmäßig wurde über Fragen der Steuergesetzgebung und der Volkszählung diskutiert.

Zusammen mit dem Bundesbeauftragten für den Datenschutz habe ich im September 1988 an einem vom Bundesminister für Arbeit und Sozialordnung angeregten Informationsbesuch bei der AOK Dortmund bezüglich des dortigen Modellversuchs „Effizienz und Wirtschaftlichkeit der durch Kassenärzte erbrachten und veranlaßten Leistungen“ teilgenommen (vgl. dazu 6. Tätigkeitsbericht, S. 52 bis 55). Dieser Besuch diente auch der Gewinnung von Erkenntnissen für das anstehende Gesundheitsreformgesetz. Dabei konnten in die Diskussion wesentliche Aspekte der Entschließung eingebracht werden, welche die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. Juni 1988 zu dem Entwurf des Gesetzes gefaßt hatte.

Im „Düsseldorfer Kreis“ der Datenschutzreferenten der obersten **Aufsichtsbehörden für den nicht-öffentlichen Bereich** habe ich weiter in der Arbeitsgruppe Versicherungswirtschaft mitgearbeitet. Hier ist eine Neuformulierung der Schweigepflichtentbindungsklauseln für die Kranken-, Lebens- und Unfallversicherung sowie der Einwilligungsklausel nach dem Bundesdatenschutzgesetz nebst einem erläuternden Merkblatt zur Datenverarbeitung erreicht worden. Trotz des damit erzielten Fortschritts habe ich Bedenken, die umfangreiche Datenverarbeitung der Versicherungswirtschaft auf die Einwilligung der Betroffenen zu stützen (s. unten S. 31).

2. Überblick

Folgende Aussagen des Berichts hebe ich hervor:

Neues Datenschutzgesetz

Zum neuen Datenschutzgesetz Nordrhein-Westfalen kann insgesamt eine **positive Bilanz** gezogen werden. Allerdings hätte die Einführung von Benachrichtigungspflichten die Transparenz der Datenverarbeitung für die Bürger erhöht (3.1).

Der Grundsatz der **informationellen Gewaltenteilung** ist innerhalb öffentlicher Stellen nicht nur bei der Weitergabe, sondern auch der Erhebung der Daten und der Auskunftserteilung an betroffene Bürger zu berücksichtigen (3.2.1.4, 3.2.5.1, 3.2.5.3).

Bei der **Forschungsklausel** (§ 28) stellt sich die Frage nach der Normenklarheit der Ausnahmen vom Grundsatz der Einwilligung. In Bereichen von insgesamt besonderer Eingriffstiefe ist die Vorschrift nicht anwendbar (3.2.6, 3.2.6.2).

Unabhängige Datenschutzkontrolle

Die von der Bundesregierung beabsichtigte **Einschränkung der Kontrollbefugnisse** der Landesdatenschutzbeauftragten im Bundesdatenschutzgesetz, insbesondere durch den Ausschluß systematischer Kontrollen bei der Erhebung und Verwendung personenbezogener Informationen außerhalb von Dateien, ist keinesfalls hinnehmbar (4.1.1).

Bereichspezifischer Datenschutz

Die Liste der **Regelungsdefizite** ist immer noch lang. Angesichts in Kürze auslaufender Übergangsfristen sind im Landesrecht bereichspezifische Datenschutzregelungen vordringlich u. a. für Polizei, Verfassungsschutz, Gesundheitswesen, Personalverwaltung, Schule und Statistik (4., 4.4).

Die **Sicherheitsüberprüfungen** in sicherheitsempfindlichen Bereichen der öffentlichen Verwaltung und der Privatwirtschaft bedürfen einer gesetzlichen Regelung, da die vorhandenen verwaltungsinternen Richtlinien nur noch für eine eng begrenzte Übergangszeit herangezogen werden können. Soweit nicht vorrangig der Bundesgesetzgeber tätig wird, ist eine landesrechtliche Regelung erforderlich, etwa in einem Geheimschutzgesetz oder im Verfassungsschutzgesetz, das auf Grund des Volkszählungsurteils und der anstehenden Sicherheitsgesetze des Bundes ohnehin novelliert werden muß (4., 4.4.1).

Im Landesmedienrecht sollten normenklare Rechtsvorschriften für die Übermittlung von Bürgerdaten durch öffentliche Stellen an die Medien geschaffen werden, nicht zuletzt, um der Verwaltung für ihre **Öffentlichkeitsarbeit** verläßliche Maßstäbe an die Hand zu geben (4.4.9).

Daten an politische Parteien

Mit dem Innenminister besteht Einigkeit, daß außer im Zusammenhang mit Wahlen die Übermittlung von Namen und Anschriften von Bürgern aus dem **Melderegister** an Parteien für Einladungen zu Kaffeetafeln, Bürgerfesten oder ähnlichen Veranstaltungen nicht zulässig ist (6.1.1).

Bei Elternbefragungen im Schulbereich dürfen Parteien aus dem Melderegister keine Anschriften erhalten, wohl aber vom **Schulverwaltungsamt,** soweit die Eltern nicht widersprochen haben (6.9.3).

Pauschale Einwilligungen

Öffentliche Stellen fordern von den Bürgern häufig auf **Antragsformularen** Einwilligungserklärungen, die zu nahezu unbeschränkten Datenerhebungen bei beliebigen dritten Stellen ermächtigen sollen. Der Bürger kann jedoch über die Preisgabe seiner Daten nur dann frei entscheiden, wenn er weiß, was konkret mit ihnen geschieht (6.2).

Datenweitergabe durch Gerichte

Einer Reihe von Bürgereingaben ist zu entnehmen, daß die Verfahrensregelungen aller Gerichtszweige einer Überarbeitung bedürfen, um insbesondere für die Weitergabe, aber auch Anforderung von Daten durch die Gerichte präzise Datenschutzvorgaben zu schaffen (6.3.3).

Polizeiliche Datenerhebung

Nach meinen Ermittlungen werden bei der Polizei Karteien, Dateien oder sonstige Sammlungen mit Angaben über Sexualverhalten (wie etwa **„Rosa Listen"**) nicht geführt. In diesem Zusammenhang war die Einsichtnahme der Polizei in **sämtliche** Karteikarten einer **Bahnhofsverbotskartei** unzulässig (6.4.1).

Sozialwesen

Das Recht des Bürgers auf informationelle Selbstbestimmung und das Gebot des geringstmöglichen Eingriffs schränken die Wahl der Informationsbeschaffung durch Sozialleistungsträger ein: Bei der Feststellung von Leistungssachverhalten hat die **Mitwirkung des Betroffenen** grundsätzlich **Vorrang** vor der Amtsermittlung bei anderen Stellen (6.5.1).

Mit der Aufgabe der Sozialhilfe, die Menschenwürde zu wahren, ist es unvereinbar, wenn Leistungsträger ohne konkrete Anhaltspunkte für eine zweckwidrige Verwendung von Geldleistungen Sachleistungen gewähren und dabei Dritten gegenüber die **Anschrift des Hilfsempfängers** als Lieferadresse offenbaren, so daß ihnen die Tatsache des Sozialhilfebezuges bekannt wird. Der Betroffene darf auch nicht zu einer **Selbstoffenbarung** verpflichtet werden (6.5.6).

Das **Sozialgeheimnis** schützt, soweit weder eine Offenbarungsbefugnis nach dem Sozialgesetzbuch noch die Einwilligung des Betroffenen vorliegt, auch gegen Aktenanforderungen durch Gerichte und ist damit **gerichtsfest** (6.5.8).

AIDS

Die Speicherung von AIDS-Hinweisen in **polizeilichen Informationssystemen** ist in Nordrhein-Westfalen abgeschafft worden (6.4.2).

Die Verwendung einer **Blutprobe** für eine HIV-Untersuchung bedarf einer gesetzlichen Grundlage oder der ausdrücklichen Einwilligung des Betroffenen. Mit Patienten geschlossene Behandlungsverträge, die keine derartige Einwilligung enthalten, rechtfertigen die HIV-Untersuchung nicht (6.6.1).

Amtsärztliche Untersuchungen

Die von Bewerbern und Beschäftigten im Landesdienst bei amtsärztlichen Untersuchungen geforderten **„Angaben zur Vorgeschichte"**, deren Erhebung tief in ihre Privatsphäre eindringt, dürfen nicht unzumutbar sein. Das Verlangen, die behandelnden und begutachtenden Ärzte von der Schweigepflicht zu entbinden, und die damit verbundene Möglichkeit, bei allen angegebenen Krankheiten die ärztlichen Unterlagen anzufordern, eröffnet eine nahezu unbegrenzte Ausforschung der gesundheitlichen Verhältnisse der Betroffenen (6.6.2).

Automatisierte Personaldatenverarbeitung

Der Einsatz der automatisierten Datenverarbeitung im Personalwesen bringt wegen der erhöhten Verfügbarkeit und Vergleichbarkeit der Daten eine besondere Gefährdung der Persönlichkeitsrechte der Betroffenen mit sich. Deshalb sind an die Erforderlichkeit und Verhältnismäßigkeit automatisierter Personalverwaltungssysteme besonders strenge Maßstäbe anzulegen (6.7.1).

Beihilfen

Wegen der Gefahr einer Verwendung der besonders sensiblen Beihilfedaten für sonstige Personalangelegenheiten ist die **Abschottung der Beihilfestelle** von der Personalverwaltung erforderlich. Diese notwendige Schutzvorkehrung folgt aus der informationellen Selbstbestimmung wie auch aus der Fürsorgepflicht des Dienstherrn. Insoweit sind präzise bereichspezifische Regelungen durch den Gesetzgeber dringend geboten (4.4.4, 6.7.5).

Volkszählung 1987

Dem gestiegenen Bewußtsein der Bürger für den korrekten Umgang mit ihren Volkszählungsdaten stand vielfach eine mangelnde Sensibilität der Verantwortlichen in den Gemeinden für die berechtigten Interessen der Auskunftspflichtigen gegenüber. Zahlreiche Mängel bei der Durchführung der Volkszählung haben das Vertrauen vieler Bürger in eine strikte Trennung von statistischer Erhebung und Verwaltungsvollzug erschüttert. Insgesamt erfolgte die Volkszählung jedoch auf rechtmäßiger Grundlage (6.8).

Umweltdaten

Datenschutz und Umweltschutz sind keine Gegensätze, enthalten jedoch in manchen Fällen einen Zielkonflikt. Soweit Kartierungen, Dateien oder besondere Verzeichnisse wie etwa Wasserbücher und Altlastenkataster personen-

bezogene Daten enthalten, können Erwägungen des Gesetzgebers zur Herstellung von **Aktenöffentlichkeit** ergeben, daß die Information der Allgemeinheit über Umweltdaten als wesentliche Voraussetzung für einen wirksamen Umweltschutz in gewissen Grenzen Vorrang vor dem Datenschutz erhält (6.10).

Gesundheitsangaben für Fahrerlaubnis

Bei Beantragung einer Fahrerlaubnis der Klassen 3 und 1 dürfen Fragen zum Gesundheitszustand des Antragstellers nur gestellt werden, soweit sie für die Kraftfahrtauglichkeit erheblich und für den Betroffenen nicht unzumutbar sind; eine Rechtspflicht zur Beantwortung besteht nicht (6.11.1).

Datensicherheit

Die Bedeutung der **dezentralen Datenverarbeitung** und der kleineren Datenverarbeitungsanlagen nimmt weiter zu. Leider sind aber die Stellen, die ihre Daten selbständig zu verarbeiten beabsichtigen, häufig nicht in der Lage, den daraus resultierenden Anforderungen zu entsprechen. Die Datenzentralen, bei denen die Arbeiten früher durchgeführt wurden, werden dennoch verkleinert oder gar aufgelöst. Die Träger von Datenzentralen sollten daher prüfen, ob bei einer Dezentralisierung der automatisierten Datenverarbeitung einige Funktionen der bisherigen Datenzentrale zentral zu erhalten und evtl. sogar auszubauen sind (7.1.1).

Bei Einsatz eines **PC** oder einer sonstigen **kleineren Datenverarbeitungsanlage** sollte der Anwender prüfen, ob die dabei erzielbare Datensicherheit ausreicht. Die Verarbeitung personenbezogener Daten mit einem automatisierten Verfahren, das keine angemessene Datensicherheit bietet, verstößt gegen die Datenschutzgesetze (7.2.1 und Anlage 4).

Öffentliche Stellen sollten bei Anfragen an Hersteller auch nach der Möglichkeit des Einsatzes von **Chipkarten** zur Zugriffssicherung fragen (7.3, S. 114).

Wer **Daten anderer Stellen** in deren Auftrag verarbeitet, hat selbst die Sicherung dieser Daten gegen unbefugte Zugriffe Dritter zu gewährleisten (7.5, S. 120/121).

3. Das neue Datenschutzgesetz Nordrhein-Westfalen

3.1 Bilanz

Nach den Novellierungen des allgemeinen Datenschutzrechts in Hessen und Bremen ist am 23. April 1988 auch in Nordrhein-Westfalen mit dem Gesetz zur Fortentwicklung des Datenschutzes (GV. NW. S. 160) ein durch das Volkszählungsurteil bedingtes neues Datenschutzgesetz in Kraft getreten. Ungeachtet der relativ geringen Aufmerksamkeit, die es bei seiner Verkündung in den Medien gefunden hat, bedeutet es für die Bürger des Landes eine neue Dimension des Datenschutzes.

Bei den Vorbereitungen zu diesem Gesetz habe ich wiederholt Stellungnahmen abgegeben; außerdem habe ich mich in einem öffentlichen Anhörungstermin des Landtags geäußert. Gegenüber dem Gesetzentwurf konnten einige Verbesserungen erreicht werden. So müssen in Akten enthaltene, zur Aufgabenerfüllung nicht mehr erforderliche Daten auf Verlangen des Betroffenen gelöscht werden, wenn die weitere Speicherung ihn in unangemessener Weise beeinträchtigen würde. Dies geht im wesentlichen auf eine meiner Anregungen zurück. Entgegen der Entwurfsregelung hat der Gesetzgeber auch davon abgesehen, die Behörden der Staatsanwaltschaft der Datenschutzkontrolle durch den Landesbeauftragten zu entziehen, soweit diese nicht Verwaltungsaufgaben wahrnehmen.

Zu meinem Bedauern sind aber eine Reihe von Vorstellungen, die ich schon zu Beginn in das Gesetzgebungsverfahren eingebracht hatte, nicht aufgegriffen worden. Dies gilt insbesondere hinsichtlich der in Anlehnung an den ersten Regierungsentwurf von 1985 gegebenen Anregung, zugunsten des Betroffenen Benachrichtigungspflichten über ihm nicht bekannte Erhebungen bei Dritten und Abweichungen vom Erhebungszweck vorzusehen. Angesichts des vom Gesetz gewollten Ausnahmecharakters wäre meines Erachtens durch eine nachträgliche Unterrichtung die zügige Abwicklung der Verwaltungsaufgaben nicht ernsthaft behindert worden.

Insgesamt kann jedoch eine positive Bilanz gezogen werden. Wesentliche Neuregelungen, die auch schon im Gesetzentwurf enthalten waren, sind bereits im 8. Tätigkeitsbericht (S. 179 bis 181) angesprochen. Zusammenfassend hebe ich folgende Änderungen hervor:

- **Anwendungsbereich:** Ausdehnung auf Akten, Bild- und Tonträger, Erfassung der internen Daten, Regelung der Zulässigkeit von Datenerhebung und Datennutzung, Anpassung des Dateibegriffs an die technische Entwicklung;
- **Transparenz:** Grundsatz der offenen Informationsbeschaffung beim Bürger mit Aufklärungspflichten, zusätzliche Hinweispflichten bei Einholung der Einwilligung, Regelung eines Akteneinsichtsrechts, Erweiterung des Auskunftsrechts auf Zweck und Rechtsgrundlage der Speicherung, auf die Datenherkunft und die Empfänger von Übermittlungen, Geltung des Aus-

kunfts- und Einsichtsrechts grundsätzlich auch gegenüber den Sicherheits- und Finanzbehörden;

- **Zweckbindung:** Verbot der Abweichung vom Erhebungszweck bei der Weiterverarbeitung der Daten, Zweckänderungen nur als Ausnahmen gemäß abschließendem Katalog, kein Vorliegen einer Zweckänderung u. a. bei Wahrnehmung von Aufsichts- und Kontrollbefugnissen;
- **Besonderer Datenschutz:** U. a. Datenverarbeitung bei Dienst- und Arbeitsverhältnissen im öffentlichen Dienst, Fernmessen und Fernwirken.

3.2 Erste Erfahrungen, Auslegungs- und Anwendungsprobleme

Eine ganze Reihe von Bürgereingaben und Anfragen von Behörden zeigen, daß das neue Datenschutzgesetz auch schwierige Auslegungsfragen ausgelöst hat. Nachfolgend werden einige der Probleme behandelt, die sich mir bisher bei der Anwendung dieses Gesetzes gestellt haben und die mir für die Praxis der Verwaltung besonders bedeutsam erscheinen. Inzwischen liegen auch Kommentierungen des neuen Gesetzes vor, denen weitere Hinweise entnommen werden können.[1)]

3.2.1 Erhebung (§ 12)

3.2.1.1 Begriff

Erheben ist das Beschaffen von Daten über den Betroffenen (§ 3 Abs. 2 Satz 2 Nr. 1). Nach der Begründung des Gesetzentwurfs umfaßt die Erhebung jede Form gezielt betriebener Gewinnung personenbezogener Daten durch Befragung oder zweckgerichtete Beobachtung; der Begriff erfaßt nicht zufällig erlangte Informationen oder die in eigener Initiative erfolgenden Mitteilungen etwa von Hinweisgebern.

Die Zulässigkeitsanforderungen für die Erhebung (§ 12) müssen demnach auch erfüllt werden, wenn eine Behörde bei einer anderen öffentlichen Stelle eine Sammlung von Karteikarten durchsucht (unten S. 54/55) oder Akten mit personenbezogenen Daten einsieht, selbst wenn sie nur einen Teil der Informationen benötigt und die Betroffenen vorher nicht kennt.

Die Erhebung setzt, anders als die Speicherung, nicht die Zweckrichtung der weiteren Verarbeitung der Daten voraus. So sind auch Informationen, die bei einem Einstellungsgespräch offenbart, aber nicht protokolliert werden, durch das Recht auf informationelle Selbstbestimmung geschützt.

---

1) **Bergmann/Möhrle/Herb**, Datenschutzrecht, Teil V (Länderdatenschutzgesetze/Kirchen), 7. Ergänzungslieferung, Boorberg Verlag, Stuttgart, München, Hannover; **Stähler,** Datenschutzgesetz Nordrhein-Westfalen, 2. Auflage (1988), Deutscher Gemeindeverlag, Köln; **Weyer,** Datenschutzgesetz Nordrhein-Westfalen, 1988, Verlag für Wirtschaft und Verwaltung Hubert Wingen, Essen

3.2.1.2 Aufklärungs- und Hinweispflichten

Von besonderer Bedeutung sind die Aufklärungs- und Hinweispflichten der Verwaltung nach § 12 Abs. 2. Sie sollen den Bürger im Sinne der Selbstbestimmung in die Lage versetzen, die Rechtmäßigkeit der Datenbeschaffung zu beurteilen und sich über die weitere Datenverarbeitung zu vergewissern. Die Belehrungspflichten sind gegenüber dem alten Recht im Gesetz deutlich erweitert und erfordern – ebenso wie die Überprüfung der geforderten Angaben auf die Erforderlichkeit – eine grundlegende Anpassung der Praxis, insbesondere der Hinweise in Antragsformularen und Fragebogen. Soweit es der Einwilligung des Betroffenen zur Datenpreisgabe bedarf, ist er nicht nur gemäß § 12 Abs. 2 Satz 3 auf die Freiwilligkeit seiner Angaben hinzuweisen; selbstverständlich müssen zusätzlich die für jede Einwilligung nach § 4 Satz 3 und 4 geltenden Belehrungspflichten erfüllt werden.

3.2.1.3 Aufsichts- und Kontrollbefugnisse

Das Geseuz nennt in § 12 Abs. 1 Satz 3 bei den Voraussetzungen, unter denen eine Erhebung auch bei anderen Stellen oder Personen als beim Betroffenen zugelassen ist, nicht die Fälle des § 13 Abs. 3. Gleichwohl halte ich es für zulässig, daß eine Behörde in Wahrnehmung ihrer Aufsichts- und Kontrollbefugnisse bei einer Dienststelle im hierzu erforderlichen und verhältnismäßigen Umfang personenbezogene Daten erhebt. Dies läßt sich dem Gesetz selbst entnehmen, das für die Phase der Übermittlung die Wahrnehmung von Aufgaben nach § 13 Abs. 3 als Befugnisgrund nennt (§ 14 Abs. 1, letzter Halbsatz).

Gleiches dürfte übrigens im Blick auf § 14 Abs. 1 Satz 2 für die Erhebung von Daten bei anderen öffentlichen Stellen gelten, soweit es zur Entscheidung in einem Verwaltungsverfahren deren Beteiligung bedarf.

3.2.1.4 Erhebung innerhalb der öffentlichen Stelle

Die Regelungen des § 12 gelten auch für die Erhebung innerhalb einer öffentlichen Stelle. Auch wenn benötigte Daten bei einer anderen Organisationseinheit derselben Stelle mit anderer Aufgabenzuweisung schon vorhanden sind, sind personenbezogene Daten regelmäßig beim Betroffenen mit seiner Kenntnis zu erheben. Ein Zugriff auf die Daten an ihm vorbei darf nach § 12 Abs. 1 Satz 3 nur unter den Voraussetzungen des § 13 Abs. 2 Satz 1 Buchstaben a und c bis g erfolgen; die andere Organisationseinheit ist insoweit „andere Stelle“ im Sinne dieser Rechtsvorschrift (funktionaler Behördenbegriff).

Nur so wird der aus dem informationellen Selbstbestimmungsrecht folgende Grundsatz der informationellen Gewaltenteilung gewahrt, der nach dem Beschluß des Bundesverfassungsgerichts vom 18. Dezember 1987 (NJW 1988, 959) auch behördenintern Geltung hat. Das Gesetz selbst erkennt dies in § 14 Abs. 5 für die interne Weitergabe ausdrücklich an. Überdies ergibt sich aus § 14 Abs. 5 i.V.m. § 14 Abs. 3 Satz 2 und 3, daß die weitergebende Organisationseinheit bei Ersuchen des Empfängers grundsätzlich nur eine Plausibili-

tätsprüfung vorzunehmen hat, während in der Regel die Verantwortung für die gemäß der Erhebung erfolgende Weitergabe bei der ersuchenden Organisationseinheit liegt.

3.2.2 Zweckbindung und Zweckänderung (§ 13)

Die Weiterverarbeitung erhobener Daten (Speicherung, Veränderung, Nutzung, Übermittlung, interne Weitergabe) ist in der Regel nur für die Zwecke zulässig, für die sie erhoben sind. Die Bindung an den Erhebungszweck dient der Selbstbestimmung, dem Vertrauensschutz und dem Rechtsschutz des Betroffenen, der bei ihm gegenüber erfolgter Erhebung über den Verwendungszweck aufzuklären war. Eine Verarbeitung zu anderen Zwecken liegt nach dem Gesetz nicht vor in den Fällen des § 13 Abs. 3 (u. a. Wahrnehmung von Aufsichts- und Kontrollbefugnissen). Abweichungen vom Erhebungszweck sind nur unter den Katalog-Voraussetzungen des § 13 Abs. 2 Satz 1 statthaft. Für die Übermittlung in einem Verwaltungsverfahren gilt die Sonderregelung, daß sie zulässig ist, soweit es zur Entscheidung der Beteiligung mehrerer öffentlicher Stellen bedarf (§ 14 Abs. 1 Satz 2).

Der Grundsatz der Zweckbindung darf nicht dadurch unterlaufen werden, daß die Bestimmung des Erhebungszwecks zu weit gefaßt wird. Mit dem Selbstbestimmungsrecht wäre eine Sammlung von Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren; der Grundsatz der Verhältnismäßigkeit erfordert die Beschränkung auf das in sachlicher und zeitlicher Hinsicht erforderliche Minimum (BVerfGE 65, 1, 46). Die Abgrenzung im einzelnen kann problematisch sein. Jedoch wird soviel gesagt werden können, daß für ein bestimmtes Verfahren erhobene Daten grundsätzlich nicht für ein anderes Verfahren verarbeitet werden dürfen, wenn dies nicht in der Zweckbestimmung des ersten Verfahrens mit angelegt oder als Ausnahme von der Zweckbindung besonders erlaubt ist. Stets muß die Erhebung zur Erfüllung bestimmter einzelner Aufgaben der öffentlichen Stelle erforderlich sein. So wäre es verfehlt, beispielsweise im Bereich des Ordnungsrechts generell von dem Erhebungszweck „Gefahrenabwehr" auszugehen und nicht auf die Abwehr der jeweiligen Gefahr im Einzelfall abzustellen.

Von den Ausnahmen von der Zweckbindung in dem Katalog des § 13 Abs. 2 Satz 1 sei hier nur eine der Ausnahmen des Buchstaben a angesprochen, nach der eine Zweckänderung zulässig sein soll, wenn die Wahrnehmung einer durch Gesetz oder Rechtsverordnung zugewiesenen einzelnen Aufgabe die Verarbeitung dieser Daten **„zwingend voraussetzt"**. Selbst wenn Zweifel an der Normenklarheit dieser Ausnahmevorschrift zurückgestellt werden, kann jedenfalls nur eine besonders restriktive Handhabung in Frage kommen. Demnach ist zumindest zu fordern, daß bestimmte Daten einer bestimmten öffentlichen Stelle in einem eng begrenzten Umfang zum jetzigen Zeitpunkt für die Wahrnehmung einer genau definierten einzelnen Aufgabe zwingend benötigt werden, weil andernfalls die Aufgabe nicht erfüllt werden könnte.

Bedenken hinsichtlich einer derartigen Eingrenzbarkeit können etwa bei der Prüfung der Eignung/Nichteignung zum Führen von Kraftfahrzeugen oder der

Zuverlässigkeit/Unzuverlässigkeit im Gewerbe- und Gaststättenrecht entstehen. Dies insbesondere bezüglich der Frage, bei welchen Stellen entsprechende Erkundigungen angestellt werden dürfen. Insoweit sollten bereichspezifische Regelungen angestrebt werden.

3.2.3 Übermittlung innerhalb des öffentlichen Bereichs (§ 14)

Die Anfrage eines Landtagsabgeordneten gab mir Veranlassung, erneut Überlegungen zur Zulässigkeit der Übermittlung personenbezogener Daten an Mitglieder des **Landtags** zu Zwecken der parlamentarischen Kontrolle anzustellen.

Der Landtag ist als „öffentliche Stelle" im Sinne der Übermittlungsvorschrift des § 14 Abs. 1 Satz 1 anzusehen, wenngleich für seine eigene Datenverarbeitung das Datenschutzgesetz nicht gilt, soweit er nicht Verwaltungsaufgaben wahrnimmt (§ 2 Abs. 1 Satz 2). Nach § 14 Abs. 1 Satz 1 sind Übermittlungen u. a. zur Wahrnehmung von Aufgaben nach § 13 Abs. 3 zulässig; zu diesen Aufgaben gehört die Wahrnehmung von Aufsichts- und Kontrollbefugnissen. In der Kommentarliteratur werden insoweit nur Befugnisse von Verwaltungsbehörden genannt (z. B. Dienst- und Fachaufsicht). Ich habe jedoch keine grundsätzlichen Bedenken, wenn öffentliche Stellen im Falle einer Übermittlung an den Landtag § 13 Abs. 3 zumindest entsprechend anwenden, solange es in der Landesverfassung an einer ausdrücklichen Regelung fehlt.

Das parlamentarische Kontrollrecht steht aber nur dem Landtag und im Umfang ihrer Zuständigkeit auch dessen Ausschüssen zu, nicht jedoch einzelnen Abgeordneten, die Auskunft über personenbezogene Daten nur für sich begehren. Zu beachten ist darüber hinaus stets, daß die Übermittlung personenbezogener Daten zur Ausübung des Kontrollrechts erforderlich sein muß. Oft werden anonymisierte Angaben ausreichen. Ist dies nicht der Fall, muß der Grundsatz der Verhältnismäßigkeit beachtet werden. Ferner gebietet das Recht auf informationelle Selbstbestimmung eine hinreichende Abschottung gegen Kenntnisnahme der Daten durch Stellen und Personen, die hierzu nicht auf Grund einer Rechtsvorschrift befugt sind. In vielen Fällen wird jedenfalls die Herstellung der Vertraulichkeit geboten sein (vgl. § 31 Abs. 2 der Geschäftsordnung des Landtags, § 1 Abs. 2 der Verschlußsachenanordnung des Landtags, § 9 Abs. 5 des Gesetzes über die Einsetzung und das Verfahren von Untersuchungsausschüssen des Landtags Nordrhein-Westfalen).

3.2.4 Übermittlung an nicht-öffentliche Stellen (§§ 16, 29 Abs. 1 Satz 2)

3.2.4.1 Rechtliches, berechtigtes und öffentliches Interesse

Das neue Datenschutzgesetz unterscheidet in § 16 Abs. 1 Satz 1 Buchstaben c und d in begrüßenswerter Klarheit zwischen einem rechtlichen, einem berechtigten und einem öffentlichen Interesse für die Übermittlung an nicht-öffentliche Stellen und stellt dementsprechend unterschiedliche Anforderungen.

Ließ das frühere DSG NW bei der Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs ein „berechtigtes" Interesse des Empfängers an der

Kenntnis der Daten genügen, sofern dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt wurden, so fordert das neue Datenschutzgesetz ein **„rechtliches" Interesse**; zudem darf kein Grund zu der Annahme bestehen, daß das Geheimhaltungsinteresse des Betroffenen überwiegt (Buchstabe c). In der Tat kommt einem nur berechtigten Interesse, für das schon durch die Sachlage gerechtfertigte vernünftige Erwägungen wirtschaftlicher oder ideeller Art auf seiten des Datenempfängers ausreichen, nicht die Qualität eines Allgemeininteresses zu, das bei Einzelfallabwägung ggf. das Geheimhaltungsinteresse des Betroffenen verdrängt. Anders verhält es sich bei einem rechtlichen Interesse, das etwa durch einen vom Empfänger glaubhaft gemachten Rechtsanspruch begründet ist.

Kann der Antragsteller lediglich ein **„berechtigtes" Interesse** (Buchstabe d) geltend machen, dürfen ihm Daten des Betroffenen nur dann bekanntgegeben werden, wenn dieser über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck in geeigneter Weise unterrichtet worden ist und der Datenübermittlung nicht widersprochen hat. Obwohl im Gesetz nicht ausdrücklich gefordert, ist der Betroffene auch über sein Widerspruchsrecht zu belehren, wobei eine angemessene Überlegungsfrist festgesetzt werden sollte.

Eine im **„öffentlichen" Interesse** (Buchstabe d) liegende Datenübermittlung an Private knüpft der Gesetzgeber an die Voraussetzungen, die auch bei einem nur berechtigten Interesse gegeben sein müssen. Das Meldegesetz für das Land Nordrhein-Westfalen läßt für die sog. Gruppenauskunft ein öffentliches Interesse in Abwägung mit den Belangen der Betroffenen genügen. Die Folge davon ist, daß ein und dieselben Daten vom Meldeamt u. U. herausgegeben werden dürften, eine andere Stelle der Gemeinde oder eine andere Behörde daran jedoch gehindert wäre, wenn der Betroffene nach vorheriger Unterrichtung widerspricht.

3.2.4.2 Öffentliche Rats- und Ausschußsitzungen

Einer Betrachtung bedarf auch, ob Buchstabe d (Bekanntgabe im „öffentlichen" Interesse) im Blick auf öffentliche Rats- und Ausschußsitzungen nach der Gemeindeordnung (GO) Anwendung findet. Dies hätte zur Folge, daß privaten Zuhörern, die nicht Mitglieder dieser Gremien sind, personenbezogene Daten Dritter in öffentlichen Sitzungen nur zur Kenntnis gebracht werden dürfen, wenn hierfür ein öffentliches Interesse besteht und die betroffenen Mitbürger der Übermittlung nach vorheriger Übermittlung nicht widersprochen haben. Anders als § 16 Abs. 1 Satz 1 Buchstabe d enthält § 33 Abs. 2 Satz 1 GO („Die Sitzungen des Rates sind öffentlich.") keine auch dem Bürger klar ersichtliche Ermächtigung zur Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs.

Demgegenüber läßt sich die Auffassung vertreten, die Gemeindeordnung enthalte insoweit eine abschließende Regelung und gehe der Regelung des Datenschutzgesetzes vor (§ 2 Abs. 3 DSG NW). Hierfür spricht, daß die Gemeindeordnung in § 33 Abs. 2 Satz 2 die Möglichkeit vorsieht, durch die Geschäfts-

ordnung die Öffentlichkeit für Angelegenheiten einer bestimmten Art auszuschließen. Allerdings hat die Geschäftsordnung selbst nicht die für die Zulässigkeit von Informationseingriffen erforderliche Rechtssatzqualität; auch macht die Gemeindeordnung keine ausdrücklichen Vorgaben für die Frage des Ausschlusses der Öffentlichkeit bei vorgesehener Behandlung personenbezogener Informationen.

Um die bestehenden Zweifel auszuräumen, empfiehlt es sich, daß der Gesetzgeber eine dem Gebot der Normenklarheit und dem Grundsatz der Verhältnismäßigkeit entsprechende Änderung der Gemeindeordnung vornimmt.

3.2.4.3 Daten von Beschäftigten

§ 16 findet keine Anwendung bei der Übermittlung der Daten von Beschäftigten an nicht-öffentliche Stellen. Für derartige Personaldaten sieht der Gesetzgeber in § 29 Abs. 1 Satz 2 einen besonderen Schutz vor. Die Übermittlung ist danach „nur" zulässig, wenn der Empfänger ein rechtliches Interesse darlegt, der Dienstverkehr es erfordert oder der Betroffene eingewilligt hat.

Soweit ein **„rechtliches Interesse"** anzunehmen ist, darf nicht hinter die allgemeinen Voraussetzungen des vergleichbaren § 16 Abs. 1 Satz 1 Buchstabe c zurückgegangen werden; es ist eher ein strengerer Maßstab anzulegen, da der Gesetzgeber im Bereich der Arbeitnehmerdaten bewußt einengend von § 16 Abs. 1 abweicht. So darf bei gesetzes- und verfassungskonformer Auslegung des § 29 Abs. 1 Satz 2 ebenfalls kein Grund zu der Annahme bestehen, daß das Geheimhaltungsinteresse des Betroffenen überwiegt. Da Personaldaten an sich ihrem Wesen nach geheimzuhalten sind, wird bei sorgfältiger Abwägung nur in seltenen Fällen das rechtliche Interesse der als Empfänger in Betracht kommenden Stelle als höherrangig zu bewerten sein.

Der **„Dienstverkehr"** kann es zum Beispiel erfordern, an Türen der Diensträumen mit Publikumsverkehr Schilder mit Name und Amtsbezeichnung der Beschäftigten anzubringen oder bei Schreiben an den Bürger ihre Amtsbezeichnung anzugeben. Schon wegen des anderen Wortlauts in § 29 Abs. 1 Satz 2 dürfte es nicht möglich sein, die Zulässigkeit einer Übermittlung – wie in § 16 Abs. 1 Satz 1 Buchstabe a vorgesehen – immer bereits dann anzunehmen, wenn diese zur rechtmäßigen Aufgabenerfüllung erforderlich ist und die Voraussetzungen des § 13 Abs. 1 vorliegen.

3.2.5 Anspruch auf Auskunft und Akteneinsicht (§ 18)

3.2.5.1 Inhalt

Das Gesetz sieht leider keine Benachrichtigungspflichten bei Datenerhebungen ohne Kenntnis des Betroffenen und bei Abweichungen vom Erhebungszweck vor. Deshalb kommt dem erweiterten Auskunftsrecht und dem jetzt gesetzlich geregelten Akteneinsichtsrecht eine ganz besondere Bedeutung zu, damit der Bürger so weit wie rechtlich möglich über die ihn betreffende Informationsverarbeitung Klarheit erhält und seine Rechte auf Berichtigung, Sperrung, Löschung, Schadensersatz und Anrufung des Landesbeauftragten für den Datenschutz geltend machen kann.

Das Auskunftsrecht des Betroffenen erstreckt sich nunmehr auch auf den Zweck und die Rechtsgrundlage der Speicherung sowie auf die Herkunft der Daten und die Empfänger auch von nicht regelmäßigen Übermittlungen (§ 18 Abs. 1 Satz 1 Nr. 2 und 3). Die Angaben müssen in einer dem Bürger verständlichen Form gegeben werden.

Zur Angabe des **Zwecks** gehört die Mitteilung der Aufgabe, zu deren Erfüllung die Speicherung erforderlich ist. Die **Herkunft** der Daten erfaßt nicht nur die Fälle, in denen die zur Auskunft verpflichtete Stelle Daten von anderen – öffentlichen oder nicht-öffentlichen – Stellen ohne Ersuchen erhalten hat, sondern auch die Fälle eigener Erhebung bei anderen Stellen (§ 12 Abs. 1 Satz 3).

Die Angaben müssen so differenziert sein, daß der Betroffene auch erkennen kann, ob **innerhalb** der öffentlichen Stelle der Grundsatz der informationellen Gewaltenteilung beachtet wird, soweit er betroffen ist.

Die Erfüllung des Auskunftsanspruchs bedingt auch **Aufzeichnungen** und Vermerke, jedenfalls über die Herkunft der Daten und die Empfänger von Übermittlungen. Andernfalls würde dem Anspruch nicht hinreichend Rechnung getragen werden können. Löschungspflichten nach § 19 bleiben unberührt.

3.2.5.2 Mitwirkung des Betroffenen

Begehrt der Betroffene ohne nähere Darlegung und ohne Einschränkung Auskunft über seine Daten, ist dem Antrag im Hinblick auf die in **Dateien** enthaltenen Daten auch ohne Angaben des Betroffenen zu entsprechen, soweit nicht ein Fall des § 18 Abs. 1 Satz 2 oder des Absatzes 3 vorliegt. Die Antwort muß nicht nur die gespeicherten Daten bezeichnen, sondern auch die Angaben nach Absatz 1 Nr. 2 und 3 enthalten.

Auskunft aus **Akten** oder Akteneinsicht sind nach Absatz 2 Satz 2 nur zu gewähren, soweit der Betroffene **Angaben** macht, die das **Auffinden der Daten mit angemessenem Aufwand** ermöglichen, und es sich um Akten handelt, die nicht Gegenstand eines Verwaltungsverfahrens nach dem Verwaltungsverfahrensgesetz sind (insoweit soll für alle Verfahrensbeteiligten einheitlich die Regelung des § 29 VwVfG NW gelten). Ermöglicht der Betroffene mit seinen Angaben die Auffindbarkeit seiner Daten nur zu einem Teil, so ist seinem Begehren insoweit nachzukommen. Hinsichtlich weiterer Daten brauchen Nachforschungen nicht angestellt zu werden. Allerdings sollte der Betroffene auf diese Folge aufmerksam gemacht werden, indem er zugleich Gelegenheit erhält, fehlende Angaben nachzuholen oder gemachte Angaben zu präzisieren, was auch die Beschränkung seines Antrags auf ihn allein interessierende Daten bei bestimmten Organisationseinheiten bedeuten kann.

Weiß der mit dem Antrag befaßte Bearbeiter auch im Fall einer unsubstantiierten Antragstellung vom Vorhandensein bestimmter Daten und bedarf es insoweit keiner besonderen Suche, wird es keinen Grund geben, dem Selbstbestimmungsrecht des Betroffenen nicht Rechnung zu tragen.

3.2.5.3 Informationelle Gewaltenteilung

Im Lichte der informationellen Gewaltenteilung stellt sich die Frage, ob der Antrag **dezentral** von den jeweils speichernden Organisationseinheiten **oder zentral** von nur einer Organisationseinheit der speichernden Stelle zu bearbeiten ist, bei der damit alle Daten aus den unterschiedlichen Aufgabenbereichen zusammengeführt würden. Eine spezielle Aussage hierzu fehlt in § 18. Von Verfassungs wegen dürfte eine zentrale Bearbeitung nicht ausgeschlossen sein. Jedoch muß durch organisatorische und technische Maßnahmen gewährleistet werden, daß die Daten ausschließlich zu Zwecken der Auskunft oder Gewährung von Akteneinsicht verwendet werden und Unbefugte keinen Zugriff erhalten. Hierzu trägt eine baldige Löschung bei; zur Dokumentation des Antragsverfahrens angemessen erscheint eine Frist bis zu einem Jahr.

Soweit Mitteilungen über besonders **sensible Daten** (z. B. Gesundheitsdaten) in Rede stehen, sollte dem Bürger von den betroffenen Organisationseinheiten (z. B. Gesundheitsamt) gesondert geantwortet werden. Wird dies nicht als zweckmäßig erachtet, sollte der Betroffene gefragt werden, ob er auch in dieser Hinsicht mit einer zentralen Zusammenführung und einheitlichen Antwort einverstanden ist. Insoweit handelt es sich um grundrechtsangemessene Maßnahmen im Sinne des § 10 Abs. 1 Satz 2.

3.2.6 Datenverarbeitung für wissenschaftliche Zwecke (§ 28)

3.2.6.1 Ausnahmen vom Grundsatz der Einwilligung

Wie bereits in einer Reihe von Fällen deutlich geworden, können Auslegung und Anwendung des § 28 in der Praxis der öffentlichen Stellen dazu führen, daß dem Datenschutz der Betroffenen nicht hinreichend Rechnung getragen wird. Es stellt sich deshalb die Frage nach der Normenklarheit. Dies gilt jedenfalls im Blick auf einige der Ausnahmen in Absatz 2 Satz 1, die zu einer Datenverarbeitung ohne Einwilligung des Betroffenen berechtigen.

Nach **Buchstabe a** dürfen öffentliche Stellen personenbezogene Daten ohne Einwilligung für ein bestimmtes Forschungsvorhaben verarbeiten, wenn „die Einholung der Einwilligung **unmöglich** ist". Angesichts des klaren Wortlauts sehe ich keine Möglichkeit, diese Ausnahme auch dann als gegeben anzusehen, wenn die Einholung der Einwilligung zwar nicht unmöglich, aber nur mit unvertretbarem Aufwand möglich ist. Eine derartige Formulierung enthält das Gesetz in § 14 Abs. 2 (ähnlich auch § 13 Abs. 2 Satz 1 Buchstabe e). Im Umkehrschluß folgt daraus, daß Buchstabe a den Fall des unvertretbaren Aufwands nicht meinen kann. Vielmehr muß nach dem Wortlaut die Einholung der Einwilligung objektiv unmöglich sein. Dies ist etwa anzunehmen, wenn der Aufenthalt des Betroffenen nicht ermittelt werden kann oder die Kontaktaufnahme aus sonstigen tatsächlichen Gründen ausgeschlossen ist.

Nach dem Bremischen Datenschutzgesetz in der Fassung der Änderung von 1987 bedarf es der Einwilligung u. a. dann nicht, wenn der Zweck der Forschung „nur mit unverhältnismäßigem Aufwand erreicht werden kann"; die

Forderung der Unmöglichkeit der Einholung wurde nicht normiert. Hätte hier auch der Gesetzgeber in Nordrhein-Westfalen ein Weniger gegenüber der Unmöglichkeit ausreichen lassen wollen, so hätte er dies sicherlich nach dem Gebot der Normenklarheit auch für den Bürger deutlich zum Ausdruck gebracht.

Unabhängig hiervon mag es öffentlichen Stellen rechtspolitisch wünschenswert erscheinen, schon im Fall des unvertretbaren Aufwands von der Einholung der Einwilligung durch entsprechende Gesetzesänderung absehen zu können. So ist einzuräumen, daß etwa die Durchsicht Hunderter von Akten, in denen jeweils die Daten mehrerer Betroffener enthalten sein können, auf außerordentliche Schwierigkeiten stößt. Auch Folgerungen hieraus können sich indes nur an der gegebenen Gesetzeslage orientieren.

Im Fall des **Buchstabe b** muß „die Einholung der Einwilligung dem Betroffenen **unzumutbar**" sein. Dabei ist zu berücksichtigen, daß der Betroffene in Ausübung seines Selbstbestimmungsrechts regelmäßig selbst zu entscheiden hat, ob er ihm unangenehme Angaben machen will oder nicht. Erst dann, wenn ihn im konkreten Einzelfall schon das Abverlangen einer Einwilligung, etwa im Hinblick auf eine Erkrankung oder die Bekanntgabe des Forschungsvorhabens und der Art der dafür benötigten Daten, subjektiv in unerträglicher Weise belasten würde, kann Buchstabe b in Betracht kommen. Keinesfalls wird Buchstabe b bei einem Forschungsvorhaben generell auf alle Betroffenen Anwendung finden können, nur weil die Voraussetzungen im Falle eines der Betroffenen als gegeben angesehen werden. Häufig wird es auch an der weiteren Voraussetzung des § 28 Abs. 2 Satz 1 fehlen, daß das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt.

Auch der Ausnahmefall des **Buchstaben c,** nach dem es der Einwilligung dann nicht bedarf, wenn „durch das Einholen der Einwilligung der **Forschungszweck gefährdet** würde", darf nicht zum Einfallstor für einen weitgehenden Verzicht auf das Einverständnis des Betroffenen gemacht werden. Die Vorschrift wird zunächst dahin verstanden werden können, daß bei bestimmten Forschungsvorhaben der Zweck wissenschaftlich fundierter Forschung wegen der Art der Themenstellung, der Art der benötigten Daten und der Zusammensetzung des Kreises der Betroffenen dadurch gefährdet würde, daß die Einwilligung zwar erteilt wird, wegen sachbedingter Voreingenommenheit jedoch mit unwahren oder unvollständigen Angaben gerechnet werden muß. Eine derartige Befangenheit kann u. U. auch die Folge haben, daß Betroffene auf Einwilligungsersuchen nicht reagieren oder eine Einwilligung verweigern würden.

Insgesamt wird man wegen des Ausnahmecharakters strenge Anforderungen stellen müssen. Es müssen jeweils konkrete Anhaltspunkte für die befürchtete Reaktion und eine sich daraus ergebende Gefährdung des Forschungszwecks vorliegen. Ferner muß ausgeschlossen sein, daß der Zweck der Forschung durch Auswahl und Einbeziehung weiterer Betroffener, bei denen eine

Gefährdung im Sinne des Buchstaben c nicht anzunehmen ist, erreicht werden kann. Dies folgt schon aus dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz und gilt gleichermaßen für die Ausnahmetatbestände der Buchstaben a und b.

Im Zweifel hat das Selbstbestimmungsrecht des Betroffenen Vorrang. Steht das Vorliegen der Voraussetzungen einer der Ausnahmen in den Buchstaben a bis c nicht fest, gilt die Regel des § 28 Abs. 1, nach welcher die Daten nicht ohne Einwilligung des Betroffenen, dem das Recht zur Verweigerung zusteht (!), verarbeitet werden dürfen. Im übrigen vermittelt § 28 der Forschung keinen Rechtsanspruch, sondern enthält Zulassungskriterien für den Fall, daß eine Datenverarbeitung zugunsten der Forschung erwogen wird.

Im Anwendungsbereich des § 28 ist die Datenverarbeitung ohne Einwilligung des Betroffenen nicht bereits bei Vorliegen einer der Ausnahmen der Buchstaben a bis c zulässig. **Zusätzlich** muß vielmehr das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Betroffenen **erheblich überwiegen**, und es darf der **Forschungszweck nicht auf andere Weise erreicht werden** können (Abs. 2 Satz 1).

Eine **Anonymisierung** in der Weise, daß der Empfänger die Daten Betroffener nur ohne Personenbezug erhält, schützt den Bürger am wirkungsvollsten. Als Ausprägung des Verhältnismäßigkeitsgrundsatzes steht die Frage der **Anonymisierbarkeit an erster Stelle der Prüfung.** Sie darf nicht mit personalwirtschaftlichen und ähnlichen Überlegungen, mögen diese für sich gesehen durchaus begründet sein, abgetan werden. Scheidet eine Vorweganonymisierung objektiv aus, sollte der Kreis der Wissensträger so eng wie möglich gehalten werden, um dem Gebot der Interessenabwägung zwischen Betroffenen- und Forschungsinteresse zu entsprechen. Eine etwaige Akteneinsicht sollte nach Möglichkeit durch nur einen Wissenschaftler in den Räumen der öffentlichen Stelle erfolgen, damit dieser die Daten anonymisiert auf Erhebungsbögen übertragen kann (vgl. auch § 28 Abs. 3). Voraussetzung ist selbstverständlich, daß personenbezogene Daten, die einem vorrangigen Berufs- oder Amtsgeheimnis unterliegen (vgl. z. B. § 30 AO, § 35 SGB I), zuvor von der öffentlichen Stelle herausgenommen oder unkenntlich gemacht worden sind.

3.2.6.2 Nichtanwendbarkeit des § 28

In Bereichen von insgesamt besonderer Eingriffstiefe findet § 28 nach meiner Auffassung, die sich sowohl auf das Volkszählungsurteil als auch auf die Gesetzesbegründung stützt, keine Anwendung. Hier bedarf es **bereichspezifischer Forschungsklauseln** in anderen Gesetzen, in denen der Gesetzgeber die Grundsatzentscheidung trifft, ob er Forschung gestattet, und in denen er präzise die Voraussetzungen ihrer Zulässigkeit regelt. Für Bereiche wie Strafverfahren und Polizei ist inzwischen anerkannt, daß die allgemeinen Normen der Datenschutzgesetze keine tragfähige Grundlage sein können. So enthält der Referentenentwurf für ein Strafverfahrensänderungsgesetz 1988 (Stand: 3. November 1988) eine Bestimmung, welche unter bestimmten Vorausset-

zungen eine Auskunft zu Forschungszwecken auch ohne Einwilligung des Betroffenen sowie entsprechende Akteneinsicht vorsieht, letzteres allerdings nur insoweit, als die Erteilung von Auskünften einen unverhältnismäßigen Aufwand erfordern oder nach Darlegung der die Akteneinsicht begehrenden Stelle für die Durchführung des Vorhabens nicht ausreichen würde. Zu denken ist aber auch an andere Bereiche, wie etwa das Gesundheitswesen oder Verfahren in Ehescheidungs-, Vormundschafts- und Pflegschaftssachen.

Für die Richtigkeit dieser Auffassung spricht auch, daß in besonders sensitiven Bereichen bei Anwendung des § 28 DSG NW die Gefahr bestehen würde, daß die Ausnahmetatbestände der Buchstaben b und c in der Praxis regelmäßig zugrunde gelegt werden. So könnte man etwa die Konfrontation von Straftätern mit ihrem Fall zu Forschungszwecken generell als unzumutbar ansehen (Buchstabe b) oder von vornherein mit einer ablehnenden Reaktion rechnen (Buchstabe c). Damit aber würde die Konzeption des § 28 in ihr Gegenteil verkehrt.

Soweit § 28 nicht anwendbar ist und bereichspezifische Regelungen fehlen, kommt eine Fortführung der bisherigen Praxis allenfalls für eine **Übergangszeit** in Betracht, sofern durch bestimmte Forschungsvorhaben eine sonst eintretende Funktionsunfähigkeit staatlicher Einrichtungen vermieden wird und Informationseingriffe auf das für die geordnete Weiterführung einer funktionsfähigen Verwaltung unerläßliche Mindestmaß beschränkt werden. Diese Voraussetzungen dürften nur selten gegeben sein, so möglicherweise im Falle der Forschung zur Behebung eines dringenden legislatorischen Regelungsdefizits. Liegen die Voraussetzungen nicht vor, kann nicht etwa nach einer Forschungsklausel verfahren werden, die sich erst in einem Referentenentwurf abzeichnet. Hinzu kommen mit zunehmender Dauer erhebliche Zweifel, ob die Übergangsfrist nicht schon abgelaufen ist.

In bestimmten Fällen findet § 28 **von Gesetzes wegen keine Anwendung.** So gilt die Vorschrift nicht für die Gerichte und für die Behörden der Staatsanwaltschaft, soweit diese Stellen keine Verwaltungsaufgaben wahrnehmen (§ 2 Abs. 1 Satz 2). Nach § 2 Abs. 3 gehen vorhandene bereichspezifische Forschungsklauseln vor (vgl. etwa Krebsregistergesetz NW, § 75 SGB X).

4. Bundesdatenschutzgesetz und bereichspezifische Gesetzgebung

Im Berichtszeitraum haben die Aktivitäten für die Schaffung bereichspezifischer Datenschutzvorschriften erheblich zugenommen. Daneben sind die Bemühungen zur Neufassung des Bundesdatenschutzgesetzes fortgesetzt worden. Insgesamt muß aber festgestellt werden, daß die Liste der Defizite immer noch lang ist und erst verhältnismäßig wenige Gesetzgebungsvorhaben auf dem Gebiet des Datenschutzes zum Abschluß gebracht wurden. Dies gilt auch für den Bereich des Landes. Angesichts dessen, daß nach der Rechtsprechung des Bundesverfassungsgerichts zum sog. Übergangsbonus die Übergangsfristen in Kürze auslaufen, erscheint ein baldiges Handeln der Gesetzgeber nunmehr dringend geboten.

Zusammengefaßt in einem Abschnitt, wird nachfolgend eine Übersicht gegeben, die neben Hinweisen auf verabschiedete Gesetze eine Aufzählung der Bereiche enthält, in denen nach meiner Auffassung datenschutzrechtliche Regelungslücken vordringlich geschlossen werden müssen. Der Katalog erhebt keinen Anspruch auf Vollständigkeit, zumal er vorwiegend Bereiche betrifft, die im Berichtszeitraum durch Gesetz- und Referentenentwürfe besondere Aktualität erlangt haben. Ebenfalls beschleunigt zu verabschieden sind etwa das Justizmitteilungsgesetz, das Ausländerzentralregistergesetz sowie Änderungen des Strafvollzugsgesetzes, des Verfassungsschutzgesetzes Nordrhein-Westfalen und der Gemeindeordnung. Im übrigen verweise ich auf von mir gesehene Regelungsnotwendigkeiten in früheren Tätigkeitsberichten.

Die Übersicht erstreckt sich auch auf Gegenstände der Bundesgesetzgebung, soweit diese einer Umsetzung im Landesbereich bedarf. So ist etwa das Bundesdatenschutzgesetz in Teilen anwendbar u. a. für die Staatsanwaltschaft im Bereich der Rechtspflege (§ 7 Abs. 2 BDSG, § 2 Abs. 1 DSG NW), für öffentlich-rechtliche Wettbewerbsunternehmen wie z. B. Sparkassen (§ 2 Abs. 2 DSG NW) und für unter Landesaufsicht stehende Sozialleistungsträger (§ 79 SGB X). Die Novellierung der Strafprozeßordnung hat hinsichtlich der Strafverfolgung zentrale Bedeutung sowohl für die Landesgesetzgebung zum Polizeirecht als auch für die Praxis von Staatsanwaltschaft und Polizei. Daß ferner beispielsweise die Gesundheitsreform und das Sozialgesetzbuch für öffentliche Stellen des Landesbereichs maßgebend sind, bedarf keiner Erläuterung.

4.1 Aktivitäten des Bundesgesetzgebers

4.1.1 Bundesdatenschutzgesetz

Nachdem der in der letzten Wahlperiode von den Koalitionsfraktionen eingebrachte Gesetzentwurf zur Änderung u. a. des Bundesdatenschutzgesetzes und des Verwaltungsverfahrensgesetzes (Bundestagsdrucksache 10/4737) der Diskontinuität anheimgefallen war, hat die Bundesregierung am 20. Dezember 1988 einen daran anknüpfenden neuen Entwurf eines Gesetzes zur

Fortentwicklung der Datenverarbeitung und des Datenschutzes beschlossen (Bundesratsdrucksache 618/88).

Der Regierungsentwurf enthält hinsichtlich des Bundesdatenschutzgesetzes und des Verwaltungsverfahrensgesetzes im wesentlichen die gleichen Mängel wie der Entwurf der Koalisitionsfraktionen (vgl. 7. Tätigkeitsbericht, S. 189). So werden die Datenverarbeitung in Akten und die Zulässigkeit der Datenerhebung weiterhin im Bundesdatenschutzgesetz ausgeklammert und in das Verwaltungsverfahrensgesetz verwiesen, das weite und wichtige Verwaltungsbereiche (z. B. Finanz- und Sozialverwaltung) ebensowenig erfaßt wie die Strafverfolgung. Die neuen Datenschutzgesetze in Hessen, Bremen und Nordrhein-Westfalen bleiben nahezu unberücksichtigt. Die Kontrollbefugnis des Bundesbeauftragten für den Datenschutz wird insgesamt eingeschränkt, insbesondere durch den Ausschluß systematischer Kontrollen bei der Erhebung und Verwendung personenbezogener Informationen außerhalb von Dateien.

Erstmals sollen auch die Kontrollbefugnisse der Datenschutzbeauftragten der Länder durch den Bundesgesetzgeber eingeschränkt werden. Dies ist keinesfalls hinnehmbar, wie die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. Juni 1988 in einer Entschließung, die einen entsprechenden Referentenentwurf betraf, ausdrücklich klargestellt hat.

Die SPD-Fraktion hat im Bundestag am 13. Dezember 1988 den Entwurf eines Gesetzes zum Schutz personenbezogener Informationen eingebracht (Bundes-Informationsschutzgesetz, Bundestagsdrucksache 11/3730), der ebenfalls das Bundesdatenschutzgesetz ablösen soll. Hierbei handelt es sich um eine Weiterentwicklung des Gesetzentwurfs der SPD-regierten Bundesländer von Februar 1986 (Bundesratsdrucksache 121/86). Wie dieser bezieht er die Datenverarbeitung in Akten sowie die Erhebung ein. Darüber hinaus berücksichtigt er die neuen Landesdatenschutzgesetzte in Hessen, Bremen und Nordrhein-Westfalen. So übernimmt er aus dem nordrhein-westfälischen Datenschutzgesetz das Gebot der informationellen Gewaltenteilung bei der Datenweitergabe innerhalb öffentlicher Stellen sowie die Verpflichtung, auf Antrag des Betroffenen zur Aufgabenerfüllung nicht mehr erforderliche Daten in Akten zu löschen, wenn die weitere Speicherung ihn in unangemessener Weise beeinträchtigen würde. Auch die neu aufgenommene Vorschrift über Fernmessen und Fernwirken (TEMEX) entspricht der Regelung im Datenschutzgesetz Nordrhein-Westfalen. Bisher ohne Vorbild ist eine besondere Bestimmung über die Zulässigkeit von Videoüberwachungen und -aufzeichnungen.

4.1.2 Sicherheitsgesetze

Die Notwendigkeit, für die Verarbeitung personenbezogener Daten im Bereich der Sicherheitsbehörden bereichspezifische gesetzliche Grundlagen zu schaffen, wird allgemein anerkannt. Bereits in der letzten Wahlperiode des Bundestages hat es zahlreiche Vorentwürfe über die Informationsverarbeitung der Verfassungsschutzbehörden und anderer Bundesbehörden aus dem

Sicherheitsbereich gegeben, zu denen sich die Datenschutzbeauftragten des Bundes und der Länder geäußert haben. Auch in dieser Legislaturperiode wurden wiederholt Referentenentwürfe (wie etwa Bundesverfassungsschutzgesetz, BKA-Gesetz, BND-Gesetz, MAD-Gesetz, Zusammenarbeitsgesetz, Verfassungsschutzmitteilungsgesetz) vorgelegt. Dabei ist zu kritisieren, daß ein Entwurf dem anderen mit einer Schnelligkeit folgte, die eine eingehende Überprüfung der jeweiligen Entwürfe nahezu unmöglich machte.

In dem von der Bundesregierung am 20. Dezember 1988 beschlossenen Entwurf eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (Bundesratsdrucksache 618/88) ist in Artikel 3 der Entwurf eines Bundesverfassungsschutzgesetzes enthalten. Das ursprüngliche Vorhaben, den Austausch von Informationen im Sicherheitsbereich in einem eigenen Gesetz – zunächst im Zusammenarbeitsgesetz, dann im Verfassungsschutzmitteilungsgesetz – zu regeln, wurde aufgegeben. Die vorgesehenen Regelungen sind in den neuen Entwurf eines Bundesverfassungsschutzgesetzes einbezogen worden.

Inhaltlich bleibt der jetzt von der Bundesregierung eingebrachte Gesetzentwurf aus datenschutzrechtlicher Sicht durchweg hinter dem bereits hinsichtlich seiner Vorgänger in der letzten Wahlperiode Erreichten zurück. Gegen den Entwurf bestehen gravierende verfassungsrechtliche Bedenken. Insbesondere sind folgende Gesichtspunkte zu erwähnen:

- Der Entwurf entspricht nicht den Anforderungen, die an die Normenklarheit von Vorschriften zu stellen sind. So fehlt eine abschließende, möglichst genaue gesetzliche Beschreibung der Aufgaben, nach der sich der zulässige Umfang der Informationsbeschaffung und -verarbeitung durch die datenverarbeitende Stelle bemißt. Statt dessen gibt es zahlreiche generalklauselartige Regelungen und unbestimmte Begriffe, wie etwa „Bestrebungen gegen die freiheitlich-demokratische Grundordnung“ oder „Gefährdung auswärtiger Belange“.
- Der Grundsatz der Zweckbindung ist nicht hinreichend beachtet. So darf jede Behörde des Bundes von sich aus dem Bundesamt für Verfassungsschutz ihr bekannt gewordene Informationen übermitteln, wenn nach ihrer Auffassung tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung für die Erfüllung der Aufgaben des Bundesamts für Verfassungsschutz erforderlich ist. Innerhalb des Bundesamts für Verfassungsschutz darf jede Information unabhängig von ihrer Herkunft für jede Aufgabe verwendet werden.
- Im Gegensatz zur Regelung im Land Nordrhein-Westfalen steht dem Verfassungsschutz ein generelles Auskunftsverweigerungsrecht zu.
- Die rechtsstaatlichen Grenzen der Zusammenarbeit von Nachrichtendiensten und Polizei werden durch das Trennungsgebot bestimmt. Das Ziel, eine nicht nur rein organisatorische Trennung zu schaffen, sondern durch die Verteilung polizeilicher Befugnisse auf die Polizei und nachrichtendienstlicher Befugnisse auf die Verfassungsschutzbehörde auch eine Bün-

delung der mit diesen unterschiedlichen Befugnissen gewonnenen Informationen zu vermeiden, wird in dem vorliegenden Gesetzentwurf verfehlt.

4.1.3 Rentenversicherungsnummer

In meinem 8. Tätigkeitsbericht (S. 58/59) habe ich zu dem Referentenentwurf eines Gesetzes zur Regelung der Verwendung der Versicherungsnummer kritisch Stellung genommen. Dabei habe ich hervorgehoben, daß die Rentenversicherungsnummer aus verfassungsrechtlichen Gründen nicht die Funktion eines allgemeinen Personenkennzeichens übernehmen darf.

Das vom Bundestag am 20. Juli 1988 beschlossene und inzwischen in Kraft getretene Gesetz (BGBl. I S. 1046) berücksichtigt meine Bedenken allerdings nur zum Teil. Insbesondere hat der Gesetzgeber auch der Arbeitsvermittlung, der Berufsberatung und der Kindergeldkasse die Erhebung, Speicherung und Verwendung der Versicherungsnummer gestattet, obwohl dies für die Aufgabenerfüllung der genannten Stellen nicht zwingend notwendig ist. Zudem dürfen die überbetrieblichen arbeitsmedizinischen Dienste, auch soweit sie das Arbeitssicherheitsgesetz anwenden und damit außerhalb des Sozialgesetzbuchs tätig werden, bei bestimmten Untersuchungen für Zwecke der Prävention, der Rehabilitation und der Forschung die Versicherungsnummer verwenden.

4.1.4 Gesundheitsreform

Der Bundestag hat am 25. November 1988 das Gesetz zur Strukturreform im Gesundheitswesen (Gesundheitsreformgesetz – GRG –, BGBl. I S. 2477) beschlossen. Der Beschlußfassung war eine lebhafte Diskussion auch unter datenschutzrechtlichen Aspekten vorausgegangen. Die Datenschutzbeauftragten des Bundes und der Länder haben in ihrer Entschließung vom 6. Juni 1988 gegenüber dem Regierungsentwurf Verbesserungen des Persönlichkeitsschutzes der Krankenversicherten für notwendig gehalten (vgl. Anlage 1, S. 130 bis 133).

Diesen Forderungen ist im wesentlichen entsprochen worden. So wird es insbesondere ein umfassendes Leistungskonto für den Versicherten nicht geben. Die ärztlichen Leistungen werden – mit Ausnahme der für 2 % der Ärzte zu erhebenden Stichproben – nicht versichertenbezogen erfaßt. Zudem konnte die Einführung eines einheitlichen Sozialversicherungskennzeichens verhindert werden, denn ab 1. Januar 1992 darf die Rentenversicherungsnummer nicht mehr als Krankenversichertennummer verwendet werden. Bedenklich ist allerdings, daß das Gesetz Regelungen des Abrechnungsverfahrens zwischen den Ärzten und den Kassenärztlichen Vereinigungen nicht in dem gebotenen Umfang selbst trifft, sondern weitgehend den Verbänden überläßt.

4.1.5 Sozialversicherungsausweis

Der Gesetzentwurf der Bundesregierung zur Einführung eines Sozialversicherungsausweises und zur Änderung anderer Sozialgesetze vom 22. August 1988 (Bundestagsdrucksache 11/2807) sieht vor, daß alle geringfügig be-

schäftigten Personen für die gesamte Bundesrepublik zentral bei der Datenstelle des Verbandes Deutscher Rentenversicherungsträger (VDR) mit Anschrift und Angaben über Arbeitgeber, Beschäftigungsdauer und Beschäftigungsart gespeichert werden.

Die personenbezogenen Daten sollen der Zentraldatei von den Krankenkassen (Einzugsstellen) zugeleitet werden, die die Daten wiederum von den Arbeitgebern übermittelt erhalten sollen. Innerhalb ihres Zuständigkeitsbereichs prüfen die Krankenkassen, ob geringfügig beschäftigte Personen von verschiedenen Arbeitgebern gemeldet werden. Mit Hilfe der Zentraldatei für die gesamte Bundesrepublik soll darüber hinaus geprüft werden, ob Personen in den Zuständigkeitsbereichen verschiedener Krankenkassen gemeldet werden.

Der beabsichtigte Kontrollzweck wird nach meiner Auffassung bereits mit der vorgesehenen Kontrolle durch die Krankenkasse selbst im wesentlichen erfüllt. Eine bundesweite Zentraldatei einzurichten, um die verbleibenden restlichen Fälle durch Abgleich zu erkennen, ist daher unverhältnismäßig.

Insgesamt sieht der Gesetzentwurf zu weitgehende Überwachungsmaßnahmen vor, die zusammen mit Handlungs- und Duldungspflichten (Meldepflicht, Ausweispflicht) tief in das informationelle Selbstbestimmungsrecht eingreifen und ganz überwiegend Personen treffen werden, die eigentlich nicht gemeint sind, weil sie keiner illegalen Beschäftigung oder Schwarzarbeit nachgehen. Besonders bedenklich erscheint mir die Einbeziehung von Jugendlichen unter 18 Jahren in die vorgesehene Regelung.

4.1.6 Poststrukturreform

Der Gesetzentwurf der Bundesregierung für ein Poststrukturgesetz (Bundestagsdrucksache 11/2854), in dem eine teilweise Privatisierung des Fernmeldewesens vorgesehen ist, enthält hinsichtlich des Datenschutzes lediglich eine Verordnungsermächtigung, die auch inhaltlich erheblichen Bedenken begegnet.

Die Datenschutzbeauftragten des Bundes und der Länder haben in einem Beschluß vom 10. Oktober 1988 über aktuelle Probleme des Datenschutzes in der Telekommunikation im Blick auf die sogenannte Wesentlichkeitstheorie des Bundesverfassungsgerichts die Auffassung vertreten, daß nicht die Bundesregierung als Verordnungsgeber, sondern der Gesetzgeber selbst eine bereichspezifische Regelung treffen muß, die den besonderen Risiken der Telekommunikation angemessen Rechnung trägt. Die gesetzliche Regelung muß den Umfang der Daten auf das unerläßliche Ausmaß beschränken, eine strenge Zweckbindung vorsehen und für den Bürger die Datenflüsse offenlegen. Soweit das Fernmeldewesen privatisiert wird, müssen ebenso strenge Datenschutzbestimmungen wie für den öffentlichen Bereich gelten. Von den Unternehmen der Deutschen Bundespost und den privaten Unternehmen sollten auch Datensicherungsmaßnahmen nach dem neuesten Stand von Wissenschaft und Technik verlangt werden (z. B. Verschlüsselungsverfahren, Codesicherheit, Schutz vor Fehleingaben).

4.2 Handlungsbedarf im Bundesbereich

4.2.1 Strafprozeßordnung

Noch immer enthält das Strafprozeßrecht in wesentlichen Bereichen keine den Anforderungen der Rechtsprechung des Bundesverfassungsgerichts genügenden Vorschriften über den Umgang mit personenbezogenen Daten. Die Schwierigkeiten für den Bürger, sein Recht auf informationelle Selbstbestimmung in diesem Bereich von der Polizei, der Staatsanwaltschaft und den Gerichten gewahrt zu sehen, werden nahezu täglich an mich herangetragen. Die Notwendigkeit, die Strafprozeßordnung vordringlich grundlegend zu überarbeiten, ergibt sich insbesondere auch deshalb, weil die Polizeigesetze der Länder eine Reihe von korrespondierenden Vorschriften enthalten müssen. Eine Mehr- oder Minderregelung von Befugnissen im jeweils anderen Bereich würde die Rechtmäßigkeit derartiger Befugnisnormen in Frage stellen und auf Unverständnis in der Öffentlichkeit und beim betroffenen Bürger stoßen.

Bereits im Jahre 1986 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz eine umfangreiche Stellungnahme mit Überlegungen zur Regelung der Informationsverarbeitung im Strafverfahren beschlossen (vgl. 8. Tätigkeitsbericht, S. 36 f.). Nunmehr liegt ein zwischen den Ressorts noch nicht abgestimmter Referentenentwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts – Strafverfahrensänderungsgesetz 1988 – (StVÄG 1988) vor.

Im Entwurf geregelt sind insbesondere: Fragen der Fahndung, Rasterfahndung, polizeiliche Beobachtung, längerfristige Observation, Einsatz technischer Mittel, Einsatz verdeckter Ermittler, Auskunft und Akteneinsicht, Daten- und Aktenüberlassung zu wissenschaftlicher Forschung, Führung von kriminalpolizeilichen Sammlungen und deren Verwendung zur jeweiligen polizeilichen Aufgabenerfüllung, Führung von Datensammlungen zur Strafverfolgungsvorsorge, Einrichtung automatisierter Verfahren.

Im Interesse der betroffenen Bürger ist zu begrüßen, daß nunmehr eine Reihe von datenschutzrechtlichen Problemfällen eine klare Regelung erfahren. Endlich wird auch eine Unterrichtungsverpflichtung der Staatsanwaltschaft gegenüber den Polizeibehörden über den Ausgang des Ermittlungsverfahrens (§ 479 Abs. 2 StVÄG) geregelt; damit werden wesentliche Voraussetzungen für die ordnungsgemäße Führung der polizeilichen Datensammlungen geschaffen.

Andererseits sollte der Gesetzgeber die Notwendigkeit der Schaffung neuer Vorschriften nicht zur Festschreibung der Wünsche der Praxis nutzen, ohne zuvor die Praxis nach den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit und der Abwägung mit dem Recht auf informationelle Selbstbestimmung kritisch zu überprüfen. Deutlich wird dies u. a. bei der Forschungsklausel, die einseitig auf die Interessen der Forscher ausgerichtet ist, oder bei der Ausgestaltung des Auskunftsrechts für Privatpersonen, das weiter geht und unter erleichterten Voraussetzungen zu verwirklichen ist als das Auskunftsrecht des Betroffenen selbst, sowie bei der Regelung über die Speicherung der Daten von Zeugen zur Vorsorge für künftige Strafverfolgung.

4.2.2 Personenstandsgesetz

Der Bundesminister des Innern hat inzwischen eine überarbeitete Fassung des Vorentwurfs eines Fünften Gesetzes zur Änderung des Personenstandsgesetzes (PStG) vorgelegt (Stand: Juli 1988). Zu einer früheren Fassung des Vorentwurfs hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 15. März 1988 einen Beschluß gefaßt. Die Datenschutzbeauftragten bewerten an dem Vorentwurf insbesondere die Absicht positiv, die Mitteilungspflichten des Standesbeamten gesetzlich zu verankern, die Einsicht in die Personenstandsbücher und die Erteilung von Auskünften und Urkunden präziser zu regeln sowie das öffentliche Aufgebot wegfallen zu lassen.

Insbesondere haben die Datenschutzbeauftragten empfohlen:

- Auf die Eintragung des Berufs in die Personenstandsbücher ist zu verzichten.
- Für Orts- bzw. Zeitangaben in Urkunden, namentlich in Sterbeurkunden, sollte eine Regelung vorgesehen werden, durch die Peinlichkeiten für die Betroffenen vermieden werden. Insbesondere sollten Sterbeurkunden so gefaßt werden, daß sie Dritten keinen Anlaß zu Spekulationen über die näheren Umstände des Todes geben.
- Schaffung einer Rechtsgrundlage für die Mitteilungspflichten der Standesbeamten. Die als Mitteilungsempfänger vorgesehenen Behörden und Stellen sollten im Gesetz abschließend genannt, der Umfang der Mitteilungsinhalte beschrieben und klargestellt werden, daß die Mitteilungen nur zu einem bestimmten Verwendungszweck des Empfängers bestimmt sind.
- Die Berechtigung von Behörden und bestimmten öffentlichen Stellen, Auskunft aus einem und Einsicht in einen Personenstandseintrag sowie Erteilung von Personenstandsurkunden zu verlangen, ist in einer besonderen Vorschrift bereichspezifisch zu regeln.
- Eine Durchsicht der Bücher, wie sie bislang in § 61 PStG vorgesehen ist, sollte entfallen.
- Regelung der Gewährung von Informationen zum Zwecke wissenschaftlicher Forschung durch eine bereichspezifische gesetzliche Vorschrift. Dabei sollte das Prinzip der Gewährung von Auskunft und Einsicht nur mit Einwilligung der Betroffenen als Regelfall an den Anfang gestellt werden.
- Benachrichtigung des Betroffenen über die Gewährung von Informationen an Behörden und bestimmte sonstige Stellen.
- Bei der Inkognito-Adoption Minderjähriger sollte eine Unterrichtung der Meldebehörde am Wohnsitz der leiblichen Eltern des adoptierten Kindes über das Erlöschen des Verwandtschaftsverhältnisses bzw. die Änderung des Namens des adoptierten Kindes nicht erfolgen.
- Bei Vorliegen von Anhaltspunkten für eine Adoptionsvermittlung sollte die Geburt eines Kindes erst dann (acht Wochen nach der Geburt) der zuständigen Meldebehörde gemeldet werden, wenn feststeht, ob und ggf. zu wem das Kind in die Adoptionspflege gegeben wird.

Die überarbeitete Fassung des Vorentwurfs enthält bereits einzelne Empfehlungen der Datenschutzbeauftragten. Viele Empfehlungen sind jedoch noch unberücksichtigt geblieben. An den Verbesserungsvorschlägen der Datenschutzbeauftragten halte ich nach wie vor fest.

4.2.3 Schuldnerverzeichnis

In der letzten Zeit haben die Eingaben, die die Erteilung von Auskünften aus den bei den Amtsgerichten geführten Schuldnerverzeichnissen betreffen, wieder zugenommen. Es ist den Betroffenen, wenn überhaupt, nur sehr schwer verständlich zu machen, daß sich die Datenschutzbeauftragten seit acht Jahren ernsthaft für eine Änderung der Rechtslage einsetzen, aber bisher nicht sehr viel erreicht haben.

Der Bundesminister der Justiz hat im August 1987 einen neuen Entwurf eines Gesetzes zur Änderung von Vorschriften über das Schuldnerverzeichnis und den Entwurf einer Verordnung über die Erteilung von Abdrucken und Listen aus dem Schuldnerverzeichnis den Landesjustizverwaltungen übersandt. In meiner Stellungnahme gegenüber dem Justizminister des Landes Nordrhein-Westfalen habe ich unter anderem folgende Bedenken und Anregungen aus der Sicht des Datenschutzes aufgeführt:

- Zur sicheren Identifizierung des Schuldners sollten Eintragungen in das Schuldnerverzeichnis, Abdrucke, Listen und Auskünfte das Geburtsdatum des Schuldners enthalten.
- Ausdrücklicher Hinweis im Gesetz, daß die Nutzung der Schuldnerdaten ausschließlich für die Beurteilung der Zahlungsfähigkeit eines Schuldners im Rechtsverkehr zulässig ist.
- Bessere Aufklärung der Betroffenen als bisher über den Inhalt der Eintragung in das Schuldnerverzeichnis und die Löschung der Eintragung, insbesondere aber über die Art und den Umfang der Auskunftserteilung an Dritte.
- Erteilung einer Auskunft aus dem Schuldnerverzeichnis nur bei Darlegung eines berechtigten Interesses gegenüber dem Urkundsbeamten der Geschäftsstelle.
- Die Bestimmung des Kreises, der neben den Kammern den Bezug von Abdrucken aus dem Schuldnerverzeichnis erhalten kann, sollte nicht allein dem Bewilligungsverfahren überlassen werden. Der Kreis sollte bereits im Gesetz eingegrenzt werden.
- Die Erteilung von Auskünften durch die zum Bezug von Abdrucken Berechtigten an Dritte sollte nicht nur davon abhängig gemacht werden, daß dies zur ordnungsgemäßen Tätigkeit dieser Stellen gehört; Dritte sollten auch nur bei Nachweis eines berechtigten Interesses Auskunft erhalten.
- Dokumentationspflicht, die den Körperschaften auferlegt, Aufzeichnungen über die Erteilung von Auskünften zu führen, sowie eine Dokumentationspflicht der Listenempfänger, Aufzeichnungen über die Erteilung von Auskünften zu machen.

– Die Löschungspflicht sollte sich nicht nur auf Daten in Dateien beziehen, sondern auch auf Eintragungen, Vermerke und Hinweise in Akten oder sonstigen Unterlagen.

Der Justizminister des Landes Nordrhein-Westfalen hat meine Stellungnahme zu dem Gesetzentwurf dem Bundesminister der Justiz zur Kenntnis gebracht. Im Interesse der betroffenen Bürger bleibt zu hoffen, daß der Gesetzentwurf möglichst bald in Kraft tritt.

4.2.4 Sozialgesetzbuch

Aus zahlreichen Eingaben ist mir bekannt, daß Behörden dem Bürger die Einsicht in über ihn geführte Akten verwehren. Das **Akteneinsichtsrecht** ist jedoch eine wesentliche verfahrensrechtliche Vorkehrung zum Schutze des Rechts auf informationelle Selbstbestimmung und für einen effektiven Rechtsschutz. Dementsprechend habe ich bereits in meinem 3. Tätigkeitsbericht (S. 15) die Auffassung vertreten, daß aus dem Grundrecht auf Datenschutz ein allgemeines Akteneinsichtsrecht hergeleitet werden kann.

Diese verfassungsrechtlichen Anforderungen sind im neuen Datenschutzgesetz Nordrhein-Westfalen (§ 18 Abs. 2 Satz 1) dadurch konkretisiert, daß dem Betroffenen auf Verlangen Akteneinsicht zu gewähren ist. Diese Regelung findet jedoch im Bereich des Sozialgesetzbuchs keine Anwendung. Hier gilt § 25 SGB X, der ein Akteneinsichtsrecht nur im Rahmen eines Verwaltungsverfahrens vorsieht. Ich halte es für geboten, auch in dieser Vorschrift durch Regelung eines allgemeinen Akteneinsichtsrechts die verfassungsrechtlichen Anforderungen normenklar zu konkretisieren.

Nach dem vom Bundesverfassungsgericht ausdrücklich formulierten Grundsatz der **Zweckbindung** ist die Verwendung personenbezogener Daten auf den gesetzlich bestimmten Zweck begrenzt. „Schon angesichts der Gefahren der automatischen Datenverarbeitung ist ein – amtshilfefester – Schutz gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote erforderlich“ (BVerfGE 65, 1, 46). Zwar enthält das Zehnte Buch des Sozialgesetzbuchs bereits bereichspezifische Datenschutzregelungen, die, wie das Bundesverfassungsgericht hervorhebt, in die richtige Richtung weisen. Gleichwohl halten die Datenschutzbeauftragten des Bundes und der Länder hier weitere Verbesserungen für geboten (vgl. 6. Tätigkeitsbericht, S. 200). Dies gilt insbesondere für die Vorschrift des § 69 SGB X, der, gebunden lediglich an die Aufgabenerfüllung nach dem Sozialgesetzbuch und an das Erforderlichkeitsprinzip, einen großzügigen Datenaustausch der Sozialleistungsträger untereinander zuläßt. Damit besteht innerhalb des Sozialleistungsbereichs keine ausreichende informationelle Gewaltenteilung. Die deshalb notwendige Aufgabe, dem Datenaustausch auch innerhalb der Solzialverwaltung klarere Grenzen zu ziehen, hat der Gesetzgeber noch nicht in Angriff genommen.

4.2.5 Fahrerlaubnis

Mir ist bekanntgeworden, daß der Bundesminister für Verkehr eine bereichspezifische gesetzliche Regelung für die Erhebung, Speicherung, Übermittlung und Löschung personenbezogener Daten im Zusammenhang mit der Erteilung einer Fahrerlaubnis vorbereitet. Ich halte dieses Vorhaben für dringend notwendig. Seit Beginn meiner Tätigkeit habe ich auf zahlreiche datenschutzrechtliche Probleme im Zusammenhang mit der Erteilung und dem Entzug einer Fahrerlaubnis hingewiesen. Vielfach haben sich Bürger in Eingaben darüber beschwert, daß die Polizei bzw. Ordnungsbehörden oder Gerichte und Staatsanwaltschaften der Fahrerlaubnisbehörde Tatsachen über körperliche oder geistige Gebrechen mitgeteilt hatten und daß die Fahrerlaubnisbehörde in diesen Fällen zur weiteren Aufklärung die Akten gerichtlicher Verfahren – z. B. Vormundschafts- oder Pflegschaftsakten – ohne Zustimmung des Betroffenen eingesehen hatte (4. Tätigkeitsbericht, S. 122/123; 5. Tätigkeitsbericht, S. 132 bis 134; 7. Tätigkeitsbericht, S. 133/134; 8. Tätigkeitsbericht, S. 119/120).

Für derartige Informationsflüsse gibt es bisher keine normenklare gesetzliche Grundlage. Auf das Datenschutzgesetz Nordrhein-Westfalen kann nach meiner Auffassung bei solchen Informationseingriffen von hoher Eingriffsintensität nicht zurückgegriffen werden. Auch die Datenerhebung im Zusammenhang mit der Erteilung der Fahrerlaubnis weist nach der jetzigen Regelung Lücken auf: So wird z. B. von dem Bewerber um eine Fahrerlaubnis der Klasse 3 das Ausfüllen eines Gesundheitsfragebogens verlangt, obwohl eine gesetzliche Verpflichtung zur Beantwortung solcher Fragen derzeit nicht besteht (s. unten S. 99/100). Ich hoffe, daß mit dem Vorhaben des Bundesministers für Verkehr die aufgezeigten Regelungsdefizite ausgeräumt werden können.

4.2.6 Kreditinformationen

Ein Handlungsbedarf für den Bundesgesetzgeber besteht nach meiner Auffassung – zumindest mittelfristig gesehen – auch im Bereich der **Kreditinstitute.** Zwar konnten zur Erteilung von Bankauskünften und zum Schufa-Verfahren durch Verhandlungen und Vereinbarungen der Datenschutzbeauftragten mit der Kreditwirtschaft Regelungen getroffen werden, durch welche die vor Jahren aufgetretenen Probleme im großen und ganzen zunächst beseitigt worden sind (vgl. dazu 6. Tätigkeitsbericht, S. 136 bis 138; 7. Tätigkeitsbericht, S. 141 bis 143). Der Bundesminister der Justiz befaßt sich zur Zeit in Umsetzung einer entsprechenden Richtlinie der Europäischen Gemeinschaften mit dem **Entwurf eines Verbraucherkreditgesetzes.** Es bietet sich an, in dieses Gesetz bereichspezifische Vorschriften über die Erhebung, Speicherung und Übermittlung personenbezogener Kreditdaten und ihre weitere Verwendung in Kreditinformationssystemen aufzunehmen.

4.2.7 Versicherungswesen

Noch dringender tritt nach meiner Auffassung ein Regelungsbedarf im Bereich des Versicherungswesens hervor: Hier haben die Versicherungsgesellschaften mittlerweile ein umfassendes **System zentraler Warndateien** ein-

gerichtet, die zur Erkennung besonderer Risiken – etwa im Bereich der Lebensversicherung – oder sonstiger Auffälligkeiten dienen sollen. Über bekanntgewordene Fälle dieser Art tauschen die Versicherungsgesellschaften Erkenntnisse aus. Für einen derartigen „Informationsverbund", der den Betroffenen bisher weitgehend unbekannt ist, können die Generalklauseln des Bundesdatenschutzgesetzes keine ausreichende gesetzliche Grundlage sein.

Die Möglichkeit, hier ähnlich wie beim Schufa-Verfahren die Zulässigkeit der Datenverarbeitung über eine **Einwilligungsklausel** zu begründen, muß als äußerst problematisch angesehen werden. Einmal sind die von der Versicherungswirtschaft verwendeten Klauseln sehr allgemein gehalten, so daß es eines von ihr verwendeten mehrseitigen „Merkblatts zur Datenverarbeitung" zu ihrer Erläuterung bedarf. Man wird insoweit davon ausgehen können, daß das Merkblatt – falls überhaupt – von den Kunden erst nach Vertragsschluß gelesen wird. Vor allem aber müssen gegen eine Einwilligungsklausel deswegen Bedenken erhoben werden, weil der Betroffene in vielen Fällen faktisch zum Abschluß einer Versicherung und damit zur Unterzeichnung der von allen Versicherern gleichlautend verlangten Einwilligungsklausel gezwungen ist.

Jemand, der nicht den Schutz der gesetzlichen Krankenversicherung oder Alterssicherung genießt, kann nicht darauf verzichten, sich privat entsprechend zu versichern. Ohne Abschluß einer Gebäudeversicherung bekommt kein Bauherr ein hypothekarisches Darlehen.

Der Zwang zum Vertragsschluß und damit zur Unterzeichnung einer vorgegebenen „Einwilligung" ist damit im Versicherungsbereich größer als im Kreditwesen, wo immerhin die Möglichkeit besteht, ohne Unterzeichnung der Schufa-Klausel ein Postgirokonto zu eröffnen oder aber bei einem Kreditinstitut ein Konto auf Guthabenbasis zu führen, bei dem die Unterzeichnung der Schufa-Klausel nicht verlangt werden kann (vgl. 6. Tätigkeitsbericht, S. 138). Aus diesen Gründen haben die Datenschutzbeauftragten des Bundes und der Länder für die Datenverarbeitung auf Grund einer Einwilligung stets gefordert, den Betroffenen durch besondere Regelungen davor zu schützen, daß er durch soziale, wirtschaftliche oder psychische Zwänge in seiner Entscheidungsfreiheit unangemessen eingeschränkt wird.

Der in dem Bereich der Versicherungswirtschaft geforderte gerechte Ausgleich zwischen den Interessen der Versicherer an einer Datenverarbeitung, die der Verhinderung von Mißbrauchs- und Betrugsfällen dienen soll, und den Interessen der Bürger, diese Datenverarbeitung auf das wirklich Notwendige zu begrenzen, wird nach meiner Auffassung letztlich nur durch eine gesetzliche Regelung erreicht werden können.

4.2.8 Abgabenordnung

Ende November 1988 hat der Bundesminister der Finanzen einen Gesetzentwurf bereichspezifischer Datenschutzvorschriften im Anwendungsbereich der Abgabenordnung bekanntgegeben. Dieser Entwurf ist mit den obersten Finanzbehörden der Länder erarbeitet und abgestimmt worden.

Nach der Begründung des Bundesministers der Finanzen soll durch den Gesetzentwurf eine Rechtszersplitterung, die durch unterschiedliche Regelungen in der Abgabenordnung, dem Bundesdatenschutzgesetz und in den Datenschutzgesetzen der Länder bedingt sei, vermieden und ein einheitliches Datenschutzrecht in dem Verfahren nach der Abgabenordnung gewährleistet werden. Ich vermag diese Begründung jedoch nicht nachzuvollziehen. In meiner langjährigen Kontrollpraxis im Bereich der Finanzverwaltung im Land Nordrhein-Westfalen bin ich in Übereinstimmung mit dem Landesfinanzminister davon ausgegangen, daß Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen nicht zur Anwendung gelangen, soweit die Abgabenordnung eine Regelung zum gleichen Sachverhalt enthält bzw. auf die gleiche Konfliktlage eingeht. Dies ergibt sich unmittelbar aus dem Vorrang des Bundesrechts nach Artikel 31 des Grundgesetzes und ist, soweit mir bekannt, auch von anderen Landesbeauftragten nicht in Zweifel gezogen worden. Alle wichtigen Fälle aus dem Bereich der Finanzverwaltung, auf die ich in meinen Tätigkeitsberichten eingegangen bin, betrafen Fragen zur Anwendung der Abgabenordnung. Viele dieser Fälle sind ähnlich auch in anderen Bundesländern aufgetreten und von den dort zuständigen Landesbeauftragten ebenfalls nach den Vorschriften der Abgabenordnung beurteilt worden. Durch die Zusammenarbeit der Landesbeauftragten für den Datenschutz im Arbeitskreis Steuerverwaltung ist darüber hinaus in nahezu allen Fällen eine einheitliche Beurteilung erreicht worden.

Nach meiner Einschätzung soll mit dem Gesetzesvorhaben des Bundesministers der Finanzen in erster Linie ein weitgehendes **Zurückdrängen der Kontrollbefugnisse unabhängiger Datenschutzbeauftragter** im Bereich der Finanzverwaltung erreicht werden.

Nach der in § 107 d des Entwurfs vorgesehenen Regelung soll nämlich künftig die Datenerhebung und -übermittlung nicht mehr der Kontrolle der Datenschutzbeauftragten unterliegen und die Kontrolle im übrigen auf eine dateimäßige Datenverarbeitung beschränkt werden. Damit würde etwa die wichtige Frage der Einhaltung des Verhältnismäßigkeitsgrundsatzes bei der Aufklärung von steuerlich relevanten Sachverhalten, auf die sich viele Bürgereingaben beziehen, in Zukunft nicht mehr geprüft werden können.

Das Gesetzgebungsvorhaben bleibt nicht nur wesentlich hinter den Anforderungen des Volkszählungsurteils von 1983 zurück, in dem das Bundesverfassungsgericht die Notwendigkeit einer Kontrolle durch unabhängige Datenschutzbeauftragte hervorgehoben hat. In seiner Entscheidung vom 9. März 1988 (NJW 1988, 2031) hat das Bundesverfassungsgericht darüber hinaus ausdrücklich betont, das Recht auf informationelle Selbstbestimmung schütze wegen seiner persönlichkeitsrechtlichen Grundlage generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten und sei nicht auf den jeweiligen Anwendungsbereich der Datenschutzgesetze des Bundes und der Länder beschränkt. Die Nichtbeachtung solcher verfassungsrechtlicher Vorgaben durch den Gesetzentwurf muß nach alledem als ungewöhnlich bezeichnet werden.

Schwerwiegende Unzuträglichkeiten sind auch aus der Regelung zu erwarten, die in § 107 d Abs. 6 und 7 des Entwurfs vorgesehen ist: Danach dürfen geschützte Daten den Datenschutzbeauftragten nur offenbart werden, soweit der Betroffene eingewilligt oder nach vorheriger schriftlicher Benachrichtigung durch die Datenschutzbeauftragten unter Hinweis auf diese Folge einer Offenbarung nicht wiedersprochen hat. Die Finanzbehörde darf den Datenschutzbeauftragten für diesen Zweck Name und Anschrift des Betroffenen offenbaren.

Sicherlich ist es nicht die Absicht der Datenschutzbeauftragten, gegen den Willen eines Betroffenen die Offenbarung seiner Steuerdaten zu erreichen. Die Regelung würde aber praktisch auf eine erhebliche Behinderung der Datenschutzkontrolle hinauslaufen. Wenn z. B. im Rechenzentrum einer Finanzverwaltung eine Kontrolle durchgeführt werden soll, wird es sich vorher nicht absehen lassen, welche personenbezogenen Daten welcher Steuerpflichtiger im Verlauf dieser Kontrolle eingesehen werden müssen.

Der Gesetzentwurf enthält über die aufgezeigten Bereiche hinaus zahlreiche weitere Bestimmungen, gegen die datenschutzrechtliche Bedenken erhoben werden müssen. Insgesamt gesehen muß der Entwurf aus meiner Sicht als unverständlicher Rückschritt angesehen werden. Ich würde nicht anstehen, die Verabschiedung des Gesetzentwurfs in der vorgesehenen Form als „schwarzen Tag für den Datenschutz" zu bezeichnen.

4.3 Aktivitäten des Landesgesetzgebers

4.3.1 Meldegesetz

Durch das Gesetz zur Fortentwicklung des Datenschutzes vom 15. März 1988 (GV. NW. S. 160) ist auch das Meldegesetz für das Land Nordrhein-Westfalen (MG NW) in einigen Bestimmungen geändert worden. Aus datenschutzrechtlicher Sicht ist insbesondere zu begrüßen, daß nunmehr auch im Meldegesetz Nordrhein-Westfalen entsprechend der Regelung in den Meldegesetzen aller anderen Bundesländer ein Widerspruchsrecht der Betroffenen gegen die Datenübermittlung an Adreßbuchverlage enthalten ist.

In früheren Stellungnahmen habe ich die Auffassung vertreten, daß der Beruf und die Seriennummer des Personalausweises und des Passes nicht zu den Daten gehören, die im unmittelbaren Zusammenhang mit den Aufgaben der Meldebehörden, Identifizierung und Wohnungsfeststellung der Einwohner, stehen und daher nicht im Melderegister zu speichern sind. Die Speicherung des Berufs (§ 3 Abs. 2 Nr. 7 MG NW) entfällt nunmehr. Statt dessen wird für die Mitwirkung bei der Erfüllung der Aufgaben nach der Dritten Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens vom 30. März 1935 (RGS. NW. S. 7) nur noch die Berufsausübung im Gesundheitswesen gespeichert. Mit Wirkung vom 1. September 1991 entfällt auch die Speicherung der Seriennummer des Personalausweises und des Passes.

Die Meldebehörden stießen bei Familienforschern selten auf Verständnis, wenn sie ihnen nach den bisher geltenden Vorschriften keine Auskunft über Verwandte erteilten, die vor langer Zeit verzogen oder verstorben waren. Insoweit ist nunmehr eine Änderung eingetreten. Nach Ablauf von fünf Jahren nach Ende des Kalenderjahres, in dem ein Einwohner weggezogen oder verstorben ist, sind die bis dahin gespeicherten Daten gesondert aufzubewahren (§ 11 Abs. 3 Satz 1 MG NW). Während der Zeit der gesonderten Aufbewahrung dürfen die Daten nicht mehr verarbeitet oder sonst genutzt werden, es sei denn, daß dies unter anderem zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot unerläßlich ist oder der Betroffene schriftlich eingewilligt hat (§ 11 Abs. 3 Satz 2 MG NW). Ausgenommen von dieser Regelung sind jetzt Anschrift, Sterbetag und -ort der Einwohner. Zusammen mit beabsichtigten Änderungen des Personenstandsgesetzes dürfte dies die Familienforschung erleichtern.

4.3.2 Enteignungs- und Entschädigungsgesetz

Der Entwurf eines Gesetzes über Enteignung und Entschädigung für das Land Nordrhein-Westfalen (Landesenteignungs- und -entschädigungsgesetz – EEG NW –, Drucksache 10/3177) wird derzeit im Landtag beraten. Zu dem Referentenentwurf des Gesetzes habe ich seinerzeit eine Stellungnahme abgegeben. Die Landesregierung ist mir lediglich in zwei, allerdings als wesentlich zu bezeichnenden Punkten gefolgt. Unberücksichtigt blieb insbesondere meine Forderung nach mehr bereichspezifischen Datenschutzregelungen im Enteignungsgesetz.

Der mit der Enteignung verbundene Eingriff in das Recht auf informationelle Selbstbestimmung und in das Grundrecht auf Datenschutz der von der Enteignung betroffenen Grundeigentümer, Nebenrechtigten und anderen Personen kann von solcher Intensität sein, daß nach den Grundsätzen des Bundesverfassungsgerichts in seinem Volkszählungsurteil sowie nicht zuletzt auch nach der Begründung der Landesregierung zum Gesetz zur Fortentwicklung des Datenschutzes bereichspezifische Datenschutzregelungen zwingend notwendig sind. So sind etwa

- die Verpflichtung zur umfassenden Aufklärung des Bürgers über das Verfahren und seine Rechte,
- die Stellen und Personen, an die zulässigerweise übermittelt werden darf,
- Aufbewahrungs- und Löschungsregelungen,
- die Datenweitergabe zur wissenschaftlichen Forschung,
- die Unterwerfung der Gutachter unter die öffentlich-rechtlichen Datenschutzbestimmungen,
- besondere technische und organisatorische Maßnahmen, etwa bei Auswahl des Verhandlungsraumes,

im Enteignungsgesetz zu regeln.

Über die hiernach erforderlichen Datenschutzregelungen habe ich den Landtag (Vorlage 10/1918) unterrichtet. Das Ergebnis meiner Bemühungen bleibt abzuwarten.

4.3.3 Archivgesetz

Für den Bereich des Bundes ist Anfang des Jahres 1988 das Bundesarchivgesetz in Kraft getreten (BGBl. I S. 62). Als erstes Bundesland hatte Baden-Württemberg bereits am 31. Juli 1987 ein Landesarchivgesetz erlassen. Nunmehr hat auch die Landesregierung Nordrhein-Westfalen im Landtag den Entwurf eines Gesetzes über die Sicherung und Nutzung öffentlichen Archivguts im Lande Nordrhein-Westfalen – Archivgesetz Nordrhein-Westfalen – eingebracht (Drucksache 10/3372).

Ich habe in der Vergangenheit immer wieder darauf hingewiesen, daß für die Benutzung der in öffentlichen Archiven im Land Nordrhein-Westfalen verwahrten Unterlagen eine gesetzliche Regelung zwingend notwendig ist (vgl. zuletzt 8. Tätigkeitsbericht, S. 109). Wie zahlreiche Eingaben zeigen, herrscht gegenwärtig sowohl bei den Archiven, insbesondere im kommunalen Bereich, als auch bei potentiellen Benutzern eine große Unsicherheit darüber, ob und gegebenenfalls unter welchen Voraussetzungen die in den Archiven vorhandenen Unterlagen eingesehen werden können. Da ein immer stärkeres Interesse an der Beschäftigung mit geschichtlichen Fragen des 20. Jahrhunderts festzustellen ist, muß diese Lücke so bald wie möglich geschlossen werden.

Bei der Vorbereitung des Landesarchivgesetzes bin ich von Anfang an beteiligt gewesen. Ich habe mich vor allem dafür eingesetzt, daß das Archivgut von öffentlichen Stellen nach der Abgabe an die Archive möglichst den gleichen Datenschutzstandard behält, wie er für die abgebende Stelle maßgeblich ist.

4.3.4 Polizeigesetz

Auch fünf Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts gibt es für die Datenverarbeitung durch die Vollzugspolizei noch keine den Anforderungen der Rechtsprechung genügenden präzisen gesetzlichen Regelungen über den Umgang mit personenbezogenen Daten. Bereits mit Beschluß vom 24. Januar 1985 haben die Datenschutzbeauftragten des Bundes und der Länder die Mindestanforderungen für die Datenschutzregeln im Polizeirecht aufgestellt (vgl. insoweit meine Ausführungen in meinem 6. Tätigkeitsbericht, S. 27 bis 31). Darüber hinaus haben die Datenschutzbeauftragten des Bundes und der Länder in ihrem Beschluß vom 14. März 1988 zur polizeilichen Datenverarbeitung bis zum Erlaß bereichspezifischer Regelungen darauf hingewiesen, daß im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts zum sog. Übergangsbonus bereits jetzt die Datenverarbeitung durch die Polizei auf das zu beschränken ist, was für die geordnete Weiterführung der polizeilichen Aufgabenerfüllung unerläßlich ist (vgl. Anlage 2, S. 133 bis 135).

Für das Land Nordrhein-Westfalen hat die Fraktion der F.D.P. im Juli 1988 den Entwurf eines Gesetzes zur Änderung des Polizeigesetzes im Landtag einge-

bracht (Drucksache 10/3421). Die Beschlußfassung der Landesregierung über einen Regierungsentwurf stand bei Ende des Berichtszeitraums kurz bevor. Zu dem vom Innenminister vorgelegten Referentenentwurf eines Gesetzes zur Änderung des Polizeigesetzes Nordrhein-Westfalen (PolG NW), des Polizeiorganisationsgesetzes Nordrhein-Westfalen (POG NW) sowie des Ordnungsbehördengesetzes (OBG) habe ich Stellung genommen. In meiner Stellungnahme habe ich zum Ausdruck gebracht, daß der Entwurf den Anforderungen, die an eine gesetzliche Regelung im Bereich der Polizei zu stellen sind, nur in geringem Umfang gerecht wird. Insbesondere habe ich folgende Punkte benannt:

- Der Entwurf enthält mehrere generalklauselartige Regelungen, die für den Bürger nicht erkennen lassen, unter welchen Voraussetzungen die Polizei Daten über ihn erhebt und weiter verarbeitet. Diese nicht normenklaren Regelungen können bei der Anwendung in der täglichen Praxis zu Mißverständnissen und Unklarheiten führen.

- Bedenken gelten auch für die vorgesehene Datenverarbeitung zur Gefahrenabwehr, zum Schutz privater Rechte und zur Vollzugshilfe. Die zugrunde liegende Vorschrift könnte als eine Ermächtigungsgrundlage für die Polizei mißverstanden werden, je nach Einschätzung der allgemeinen Gefahrensituation Daten über alle Bürger zu erheben.

- Der Grundsatz der Zweckbindung der zu polizeilichen Zwecken gewonnenen personenbezogenen Daten ist in dem Entwurf nicht hinreichend berücksichtigt; insbesondere ist für den Bürger nicht mehr erkennbar, unter welchen Voraussetzungen die einmal über ihn erhobenen Daten weiterverarbeitet werden. Es fehlt eine präzise Festlegung im Gesetz, wann eine Zweckänderung im Einzelfall zulässig ist.

- Darüber hinaus bestehen gegen die vorgesehene Nutzung nicht anonymisierter Daten zu Aus- und Fortbildungszwecken, zu statistischen Zwecken oder zur Vorgangsverwaltung und Dokumentation Bedenken. Auch eine Abschottung der verschiedenen zu diesen Zwecken angelegten Datensammlungen voneinander ist nicht gewährleistet.

- Die im Entwurf geregelte allgemeine Befugnis der Polizei, einen Datenabgleich vorzunehmen, ist zu weitgehend, da sie einen nahezu anlaßlosen Abgleich ermöglicht. Dies würde dazu führen, daß jeder Bürger im Rahmen des Abgleichs erfaßt werden kann. Ein Abgleich unverdächtiger Personen mit dem Fahndungsbestand kann jedoch nur im Ausnahmefall hingenommen werden.

- Die Regelung zur polizeilichen Befragung und Auskunftspflicht ist nicht normenklar und würde zu einer uneingeschränkten Befragungsbefugnis der Polizei führen. Es kommt nicht klar zum Ausdruck, daß es sich bei jeder polizeilichen Befragung, soweit personenbezogene Daten erfragt werden, um eine Datenerhebung handelt, die nur unter den für eine solche Erhebung genannten Voraussetzungen zulässig ist.

Inwieweit die vorgenannten Punkte in dem Gesetzentwurf der Landesregierung und in den Beratungen im Landtag Beachtung finden, werde ich weiterverfolgen.

4.4 Handlungsbedarf im Landesbereich

4.4.1 Geheimschutzgesetz

Im Zusammenhang mit einer Stellungnahme gegenüber dem Innenminister des Landes Nordrhein-Westfalen zum Bereich der Sicherheitsüberprüfungen in der Privatwirtschaft habe ich deutlich gemacht, daß dieser Bereich normenklarer gesetzlicher Regelungen bedarf. Der Innenminister teilt meine Auffassung, daß die Durchführung von Sicherheitsüberprüfungen sowohl in der öffentlichen Verwaltung als auch in der Privatwirtschaft gesetzlich – etwa in einem Geheimschutzgesetz – geregelt werden muß. Er hat mir gegenüber zum Ausdruck gebracht, daß er insoweit auf den Bundesgesetzgeber wartet.

Im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts zum sog. Übergangsbonus ist allerdings darauf hinzuweisen, daß die bisherige Praxis bei der Durchführung von Sicherheitsüberprüfungen in eingeschränktem Umfang bis zum Ende der Legislaturperiode des Bundes- bzw. des Landtages hingenommen werden kann. Eine Fortführung über diesen Zeitraum hinaus wäre nicht vertretbar. Sollten die erforderlichen gesetzlichen Regelungen durch den Bundesgesetzgeber nicht rechtzeitig erfolgen, müßten solche Regelungen auf Landesebene getroffen werden.

4.4.2 Vermessungs- und Katastergesetz

Zum Referentenentwurf des Gesetzes zur Änderung des Vermessungs- und Katastergesetzes – VermKatG NW – (Stand: 2. Juni 1987) habe ich aus der Sicht des Datenschutzes Bedenken und Anregungen aufgezeigt.

Bedenken bestehen insbesondere gegen einen unmittelbaren Zugriff der öffentlich bestellten Vermessungsingenieure auf das automatisiert geführte Liegenschaftskataser ohne bereichspezifische Regelung der hiermit im Zusammenhang stehenden datenschutzrechtlichen Probleme.

In ähnlicher Weise bedenklich ist die Zulassung automatischer Datenübermittlungsverfahren für juristische Personen des Privatrechts. Es ist nicht erkennbar, wie etwa die Anlage von (Zweit-)Katastern in privater Hand und die mißbräuchliche Datenweitergabe von dort an interessierte private Dritte verhindert bzw. auch nur kontrolliert werden könnte.

Erhebliche datenschutzrechtliche Bedenken bestehen auch dagegen, daß die personenbezogenen Katasterdaten zur Erfüllung (beliebiger) Landesaufgaben, insbesondere zum Aufbau und zur Fortführung von Informationssystemen, von den Katasterbehörden nach Weisung des Innenministers zur Verfügung zu stellen sind. Auf Grund dieser weiten Regelung kann der Bürger nicht mehr wissen, wer was wann über ihn weiß (BVerfGE 65, 1, 43).

Es bleibt zu hoffen, daß die in meiner Stellungnahme aufgezeigten Datenschutzprobleme durch entsprechende bereichspezifische gesetzliche Regelungen verfassungskonform gelöst werden.

4.4.3 Gesundheitswesen

Aus der verfassungsrechtlichen Verpflichtung des Gesetzgebers, für jede Einschränkung des informationellen Selbstbestimmungsrechts eine gesetzliche Grundlage zu schaffen, ergibt sich ein beträchtlicher Regelungsbedarf im Gesundheitswesen. Das allgemeine Datenschutzgesetz mit seinen unspezifischen Generalklauseln reicht jedoch für die schwerwiegenden Eingriffe in diesem besonders sensiblen Bereich nicht aus. Hier sind präzise bereichspezifische Regelungen zu treffen. Dies gilt insbesondere für die Erhebung und Verarbeitung medizinischer Daten in der öffentlichen Gesundheitsverwaltung.

Das in Nordrhein-Westfalen noch geltende Gesetz über die Vereinheitlichung des Gesundheitswesens aus dem Jahre 1934 enthält keinerlei Regelungen über die Erhebung, Speicherung, Verwendung und Löschung von Daten durch die Gesundheitsämter. Zwar gilt die ärztliche Schweigepflicht auch für den Amtsarzt; sie betrifft aber nur die Phase der Weitergabe personenbezogener Daten. Unter anderem sollte festgeschrieben werden, daß öffentliche Stellen Gesundheitsdaten nur für den Zweck verarbeiten dürfen, zu dem sie sie erhoben oder sonst zur erforderlichen Aufgabenerfüllung erhalten haben; Ausnahmen, für die ein überwiegendes Allgemeininteresse vorliegen muß, bedürfen besonderer gesetzlicher Regelung (vgl. jetzt auch § 35 E-BDSG, Bundesratsdrucksache 618/88).

Erhebliche Regelungsdefizite bestehen auch im Krankenhausbereich. Hier erscheint eine bereichspezifische Regelung ebenfalls dringend geboten. Dabei sollten die Feststellungen und Forderungen der Datenschutzbeauftragten des Bundes und der Länder, wie bereits in meinem 7. Tätigkeitsbericht (S. 68 bis 70) ausgeführt, Berücksichtigung finden.

Wie mir inzwischen bekanntgeworden ist, erarbeitet der Minister für Arbeit, Gesundheit und Soziales derzeit einen Entwurf für ein Gesetz über den Datenschutz im Gesundheitswesen. Darin sollen bereichspezifische Regelungen für die Krankenhäuser, für die Datenverarbeitung im Rahmen des Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten, für den Maßregelvollzug, für das Krebsregister sowie für sonstige Bereiche des Gesundheitswesens getroffen werden. Ein derartiges Gesetzesvorhaben, das an die Stelle des vorhandenen lückenhaften und zum Teil archaischen Regelwerks treten soll, ist zu begrüßen.

4.4.4 Abschottung der Beihilfe

Im Beihilfewesen muß der Grundsatz gelten, daß der Beihilfeberechtigte durch die Art der Organisation der Beihilfegewährung weder davon abgehalten werden darf, zum Arzt zu gehen, noch davon, entstandene Rechnungen zur Beihilfegewährung einzureichen. Daraus folgt, daß grundrechtssichernde

Schutzvorkehrungen erforderlich sind, die eine Kenntnisnahme der zur Beihilfegewährung offenbarten Gesundheitsdaten durch die Personalverwaltung verhindern.

Weder die Beihilfenverordnung noch das Landesbeamtengesetz treffen eine den Anforderungen des Datenschutzes genügende Regelung. Durch den Gesetzgeber sind daher für die Abschottung der Beihilfestelle von der Personalverwaltung ausdrückliche und normenklare Vorschriften zu schaffen. Hierzu gehört auch, daß die Beihilfeakte von den üblichen Personalakten getrennt aufzubewahren und vor dem Zugriff der Mitarbeiter außerhalb der Beihilfestelle zu schützen ist (s. auch unten S. 79).

4.4.5 Dienst- und Arbeitsverhältnisse, Personalakten

Die für das Personalwesen geltende Vorschrift des § 29 DSG NW regelt nur die Weiterverarbeitung der bei ärztlichen oder psychologischen Untersuchungen und Tests **zum Zwecke der Eingehung** eines Dienst- oder Arbeitsverhältnisses erhobenen Daten; in ihr fehlt aber die wichtige Regelung des Umgangs mit sensiblen Gesundheitsdaten der Beschäftigten, die etwa bei der Prüfung der Dienstfähigkeit erhoben werden. Hier bedarf es vor allem der Festlegung, an wen und zu welchem Zweck diese Daten übermittelt und in welchem Umfang sie genutzt werden dürfen.

Die allgemeine Norm des § 29 DSG NW dürfte auch nicht der Forderung nach einer bereichspezifischen Neuregelung des Personalaktenrechts genügen (vgl. 6. Tätigkeitsbericht, S. 89). Personalakten haben den Zweck, über lange Zeiträume, meist über ein ganzes Berufsleben, ein möglichst vollständiges Persönlichkeitsbild zu vermitteln. Die Datenverarbeitung in Personalakten weist folglich eine besondere Eingriffstiefe auf. Daher bedürfen die Zulässigkeit des Sammelns und der weiteren Verarbeitung personenbezogener Daten sowie der Zugang zu diesen Daten einer präzisen bereichspezifischen Regelung.

4.4.6 Schule und Schulgesundheitswesen

Der Kultusminister hat durch die Verwaltungsvorschriften zu § 5 Abs. 4 ASchO – Richtlinien zum Schülerstammblatt und zum sonstigen Datenbestand in der Schule – (VVzASchO) Einzelheiten für die Erhebung, Speicherung und Übermittlung personenbezogener Daten an den Schulen geregelt. Diese Richtlinien, die verschiedentlich angepaßt worden sind, sind für den Umgang mit personenbezogenen Schülerdaten in der Praxis eine wertvolle Hilfe. Nach dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 ist jedoch für Eingriffe in das Recht der Betroffenen auf informationelle Selbstbestimmung eine gesetzliche Grundlage erforderlich, die dem Gebot der Normenklarheit entsprechen muß; aus ihr müssen sich die Voraussetzungen und der Umfang der Einschränkung klar und für den Bürger erkennbar ergeben. Soweit in den nordrhein-westfälischen Schulgesetzen überhaupt Rechtsgrundlagen für die Datenerhebung und Datenverarbeitung an Schulen enthal-

ten sind, entsprechen sie nicht dem Grundsatz der Normenklarheit. In den Ländern Saarland, Rheinland-Pfalz und Bremen sind bereits gesetzliche Neuregelungen in Kraft getreten.

Ich habe daher den Kultusminister des Landes Nordrhein-Westfalen darauf hingewiesen, daß eine gesetzliche Regelung der Erhebung und Verarbeitung von Schüler- und Elterndaten in den Schulen und im Schulgesundheitswesen erforderlich ist (vgl. 7. Tätigkeitsbericht, S. 110). Der Kultusminister hat mir mitgeteilt, daß er einen entsprechenden Referentenentwurf erarbeitet habe, der auch bereits zwischen den Ressorts abgestimmt worden sei. Zur Einbringung des Gesetzentwurfs könne er allerdings derzeit noch keine verbindlichen Angaben machen.

4.4.7 Landes- und Kommunalstatistiken

Für die Durchführung statistischer Erhebungen auf Landes- und kommunaler Ebene bedarf es einer bereichspezifischen landesrechtlichen Regelung, die dem Gebot der Normenklarheit entsprechen und den verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz beachten muß. Darüber hinaus muß der Gesetzgeber organisatorische und verfahrensrechtliche Vorkehrungen für die Durchführung und Organisation der Datenerhebung und -verarbeitung treffen; insbesondere sind Löschungsregelungen für solche Angaben, die als Identifikationsmerkmale zur Durchführung der Erhebung verlangt werden, sowie wirksame Abschottungsregelungen nach außen erforderlich.

Eine gesetzliche Regelung muß vor allem definieren, was unter statistischer Erhebung zu verstehen und wie sie von einer Befragung abzugrenzen ist. Sie müßte u. a. auch eine Regelung zur Einschaltung kommunaler Erhebungsstellen bei der Durchführung von Bundes- und Landesstatistiken enthalten, soweit in den speziellen Statistikgesetzen keine entsprechende Ermächtigung vorgesehen ist. Im Bereich bundesrechtlich geregelter Agrarstatistiken wurden beispielsweise die Kommunen durch das Landesamt für Datenverarbeitung und Statistik bei der Durchführung der Bodennutzungshaupterhebung als Erhebungsstellen eingeschaltet, ohne daß hierfür eine gesetzliche Ermächtigung gegeben war; erst der Entwurf eines Gesetzes über Agrarstatistiken sieht eine entsprechende Ermächtigung vor, die allerdings immer noch einer landesrechtlichen Umsetzung bedarf.

Nach dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz ist im Gesetzgebungsverfahren insbesondere zu prüfen, ob und inwieweit die Durchführung eigener statistischer Erhebungen zur Erfüllung der Aufgaben der Gemeinden und Gemeindeverbände erforderlich ist, sowie ob und inwieweit die Belastung der Betroffenen in einem angemessenen Verhältnis zu dem zu erreichenden Zweck steht. Die Durchführung kommunaler statistischer Erhebungen ist dementsprechend nur zuzulassen, soweit die benötigten statistischen Einzelangaben nicht in dem erforderlichen Umfang vom Landesamt für Datenverarbeitung und Statistik oder von anderen Verwaltungsstellen der Kommune übermittelt werden können.

Außerdem ist zu prüfen, ob es zur Erfüllung kommunaler gesetzlicher Aufgaben ausreicht, wenn den Kommunen nur statistische Erhebungen **ohne** Auskunftspflicht zugestanden werden. Allerdings bedarf es auch dann einer gesetzlichen Ermächtigung, die u. a. vorschreibt, wer die Entscheidung über die Durchführung einer statistischen Erhebung trifft, in welcher Form die statistische Erhebung angeordnet wird, daß der Verwendungszweck der Daten festzulegen ist und Löschungsregelungen zu treffen sind. Bei Zulassung kommunaler statistischer Erhebungen **mit** Auskunftspflicht sollen die Bereiche gesetzlich festgeschrieben werden, in denen solche Erhebungen zugelassen werden.

Weiter sind Vorgaben erforderlich, ob und inwieweit eine Nutzung statistischer Daten für Verwaltungsvollzugszwecke erlaubt sein soll. Dabei ist sicherzustellen, daß alle statistischen Einzelangaben dem Statistikgeheimnis unterliegen und nicht an andere Verwaltungsstellen übermittelt werden dürfen. In diesem Zusammenhang bedarf die Erstellung, Aktualisierung und Nutzung von Adreßdateien im Bereich der Kommunalstatistik ebenfalls einer normenklaren Regelung.

4.4.8 Nutzung der Telekommunikation

Mit Inkrafttreten der Telekommunikationsordnung am 1. Januar 1988 hat die Deutsche Bundespost den Übergang von bisher getrennten Fernmeldediensten zu einem einzigen, diensteintegrierten und digitalen Telekommunikationsnetz eingeleitet. Digitalisierung, programmgesteuerte Vermittlungstechnik und Diensteintegration führen dazu, daß bei Übertragung, Vermittlung und Nutzung der einzelnen Dienste an zentralen Stellen erheblich mehr Daten als bisher anfallen, die je nach Dienstart mehr oder weniger präzise Rückschlüsse auf die Nutzung der Teilnehmer erlauben. Die Daten werden infolge der neuen Technik leichter auswertbar sein als bisher. Die Fortentwicklung von Methoden der automatischen Spracherkennung wird es u. U. ermöglichen, mittels eines Stichwortes Kommunikationsinhalte programmgesteuert aus einer Informationsmenge auszuwählen, zu speichern und zu übermitteln; auch private Betreiber könnten hierzu in der Lage sein.

Die Zuständigkeit zum Erlaß von Regelungen, die dieser Entwicklung Rechnung tragen, ist geteilt:

- Soweit sich die Daten lediglich auf das **Netz** beziehen (Bestandsdaten, Verbindungsdaten, Gebührendaten, Betriebsdaten), fällt die Regelung in den Zuständigkeitsbereich des Bundes.
- Die Regelung des Umgangs mit den Inhaltsdaten sowie mit den Daten, die sich auf die **Nutzung** der Dienste beziehen (Angebotsdaten, Entgeltdaten) ist Angelegenheit der Länder.

Für bestimmte Dienste haben die Länder Nutzungsregelungen bereits erlassen, so für den Bildschirmtext den Btx-Staatsvertrag. Ein weiteres Beispiel ist § 30 des neuen Datenschutzgesetzes Nordrhein-Westfalen, der die Zulässigkeit von Fernmeß- und Fernwirkdiensten regelt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder geht in einem Beschluß vom 10. Oktober 1988 von der Notwendigkeit aus, daß die Länder angesichts der eingangs aufgezeigten Gefahren weitere Nutzungsregelungen treffen, die auch bereichspezifische Datenschutzvorschriften enthalten. Der Btx-Staatsvertrag kann hierzu als Vorbild dienen. In einem derartigen Staatsvertrag müssen auch die materiellen Voraussetzungen zum Betrieb privater Telekommunikationsdienste und deren Zulassung geregelt werden. Die Genehmigung von Diensten muß u. a. von der Zuverlässigkeit des Anbieters auch im Blick auf Datenschutz und Datensicherung abhängig gemacht werden.

4.4.9 Datenübermittlung an Presse und Rundfunk

Schon in meinem 6. Tätigkeitsbericht (S. 152; vgl. auch 8. Tätigkeitsbericht, S. 143) hatte ich angeregt, die Vorschrift des § 4 Landespressegesetz (LPG) präziser zu fassen, da es zweifelhaft erscheint, ob § 4 Abs. 1 und 2 Nr. 2 und 3 LPG eine dem Gebot der Normenklarheit entsprechende gesetzliche Grundlage für die Bekanntgabe personenbezogener Daten durch öffentliche Stellen an die **Presse** darstellt. Eine Neuregelung würde nicht nur der Sicherung des Grundrechts auf Datenschutz dienen, sondern insoweit auch der Öffentlichkeitsarbeit der Verwaltung eine feste Grundlage geben.

Nach § 4 Abs. 2 Nr. 2 LPG besteht ein Anspruch der Presse auf Auskunft nicht, soweit Vorschriften über die Geheimhaltung entgegenstehen. Insoweit waren nach meiner Auffassung (6. Tätigkeitsbericht, S. 150, 5. Tätigkeitsbericht, S. 114) bei Bekanntgabe in Dateien gespeicherter personenbezogener Daten auch die Einschränkungen des § 13 Abs. 1 Satz 1 2. Alternative DSG NW a.F zu beachten. Danach war eine Übermittlung nur zulässig, soweit der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft machte und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt wurden. Im neuen Datenschutzgesetz kommt in dieser Hinsicht die Vorschrift des sowohl für Dateien als für Akten geltenden § 16 Abs. 1 Satz 1 Buchstabe d DSG NW in Betracht. Sie erlaubt die Übermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs, wenn sie im öffentlichen Interesse liegt oder hierfür ein berechtigtes Interesse geltend gemacht wird und der Betroffene in diesen Fällen der Datenübermittlung nicht widersprochen hat. Im Gegensatz zu dem früheren § 13 hat der Gesetzgeber in § 16 Abs. 1 Satz 1 Buchstabe d die Abwägung selbst vorgenommen, dahin nämlich, daß die Bekanntgabe im Falle des Widerspruchs des Betroffenen nach Aufklärung gemäß § 16 Abs. 1 Satz 2 sowie dem weiter vorauszusetzenden Hinweis auf die Widerspruchsmöglichkeit unterbleiben muß. Im Rahmen einer Präzisierung des § 4 LPG könnte klargestellt werden, ob diese Konsequenz gewünscht ist.

Die Übermittlung personenbezogener Daten an die Presse darf nicht schon dann zugelassen werden, wenn sie der Erfüllung der öffentlichen Aufgabe „dient" (§ 4 Abs. 1 LPG), sondern nur dann, wenn es für die Informationsbedürfnisse der Presse geboten ist und der Verhältnismäßigkeitsgrundsatz be-

achtet wird. Zur näheren Ausgestaltung einer Übermittlungsregelung könnten die in der höchstrichterlichen Rechtsprechung entwickelten Grundsätze herangezogen werden. Daraus läßt sich zur Veröffentlichung personenbezogener Daten durch Presse wie auch Rundfunk u. a. entnehmen, daß diese

- nur im Rahmen einer Güterabwägung von Presse-, Rundfunk- und Meinungsfreiheit einerseits sowie dem allgemeinen Persönlichkeitsrecht andererseits im konkreten Einzelfall bei Beachtung des Verhältnismäßigkeitsgrundsatzes beurteilt werden kann;
- ein gewichtiges Informationsinteresse der Öffentlichkeit gerade an der Personenbezogenheit der Informationen erfordert;
- nicht zulässig ist, wenn das Öffentlichkeitsinteresse auch ohne personenbezogene Daten erfüllt werden kann;
- bei schweren Straftaten Erwachsener auf Grund des von ihnen selbst erregten öffentlichen Interesses erlaubt sein kann, soweit die Veröffentlichung sich in der Regel auf die aktuelle Berichterstattung beschränkt und den Aspekt der Unschuldsvermutung beachtet;
- in Verfahren der Zivil-, Verwaltungs-, Arbeits- und Sozialgerichtsbarkeit im Gegensatz zu Strafverfahren weniger in Betracht kommt;
- bei beruflichen Tätigkeiten mit Öffentlichkeitswirkung ggf. bejaht werden kann (etwa zur Aufklärung gravierender Mißstände);
- bei schweren Eingriffen (Berichte über ehrenrührige Vorgänge) eine vorherige Anhörung des Betroffenen voraussetzt.

Im **Rundfunkrecht** des Landes ist ein Informationsanspruch gegenüber den öffentlichen Stellen bisher gar nicht geregelt. Auch hier empfiehlt sich die Schaffung einer normenklaren Rechtsvorschrift für die Mitteilung personenbezogener Daten an die Medien, soweit nicht – so im Strafverfahrensrecht – bereichspezifische Regelungen anzustreben sind.

Unabhängig von Auskunftsersuchen der Medien erscheinen im übrigen Rechtsvorschriften geboten, welche den öffentlichen Stellen verläßliche, auch den Datenschutz der Bürger beachtende Maßstäbe für eine aktive und regelmäßige Öffentlichkeitsarbeit gegenüber den Medien an die Hand geben. Verwaltungsinterne Richtlinien bisheriger Praxis können die jedenfalls aus datenschutzrechtlicher Sicht erforderliche gesetzliche Grundlage für eine Öffentlichkeitsarbeit, die die Übermittlung personenbezogener Daten beinhaltet, nicht ersetzen. Gleiches gilt für Empfehlungen wie etwa die am 8. März 1988 vom Hauptausschuß des Deutschen Städtetages beschlossenen Leitsätze zur städtischen Presse- und Öffentlichkeitsarbeit.

Schließlich lassen die medienrechtlichen Bestimmungen über das **Gegendarstellungsrecht** eine Aussage darüber vermissen, ob öffentliche Stellen im Rahmen von Gegendarstellungen im Einzelfall auch personenbezogene Daten mitteilen dürfen, sofern dies zur Richtigstellung im überwiegenden Allgemeininteresse erforderlich ist und die Verhältnismäßigkeit gewahrt wird.

5. Rechtsprechung des Bundesverfassungsgerichts zum informationellen Selbstbestimmungsrecht

5.1 Geltungsumfang

Hatte es bei der Interpretation des Volkszählungsurteils nicht an Versuchen gefehlt, den Geltungsumfang des Grundrechts auf informationelle Selbstbestimmung einzuschränken, so ist dem der Erste Senat des Bundesverfassungsgerichts in seinem Beschluß vom 9. März 1988 (NJW 1988, 2031) in begrüßenswerter Deutlichkeit entgegengetreten. Wörtlich heißt es dort zum Selbstbestimmungsrecht:

„In dieses Recht wird nicht nur dann eingegriffen, wenn der Staat vom einzelnen die Bekanntgabe persönlicher Daten verlangt oder diese der automatisierten Datenverarbeitung zuführt. Die Möglichkeiten und Gefahren der automatischen Datenverarbeitung haben zwar die Notwendigkeit eines Schutzes persönlicher Daten deutlicher hervortreten lassen, sind aber nicht Grund und Ursache ihrer Schutzbedürftigkeit. Das Recht auf informationelle Selbstbestimmung schützt vielmehr wegen seiner persönlichkeitsrechtlichen Grundlage generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten und ist nicht auf den jeweiligen Anwendungsbereich der Datenschutzgesetze des Bundes und der Länder oder datenschutzrelevanter gesetzlicher Sonderregelungen beschränkt."

Damit sehe ich mich in meiner Auffassung über die umfassende Geltung des Selbstbestimmungsrechts erneut bestätigt.

5.2 Informationelle Gewaltenteilung

Und noch eine Klarstellung: Im Volkszählungsurteil forderte das Bundesverfassungsgericht die „informationelle Gewaltenteilung" im Blick auf die Trennung der Kommunalstatistik von anderen Aufgabenbereichen der Gemeinden und ihrer Verbände. Die 1. Kammer des Ersten Senats befand mit Beschluß vom 18. Dezember 1987 (NJW 1988, 959), nunmehr ohne Beschränkung auf einzelne Aufgabenbereiche, daß der Grundsatz der informationellen Gewaltenteilung auch innerhalb der Gemeindeverwaltung gelte; aus der Einheit der Gemeindeverwaltung folge keine informationelle Einheit.

5.3 Normenklarheit

Hingegen halte ich den Beschluß der 3. Kammer des Zweiten Senats vom 10. Februar 1988 (DVBl. 1988, 530) zur Sicherheitsüberprüfung von Beamten im Hinblick auf das Gebot der Normenklarheit für problematisch. Nach dem Volkszählungsurteil verlangt dieses Gebot von einer das Selbstbestimmungsrecht einschränkenden gesetzlichen Grundlage, daß sich aus ihr die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben. Die Kammer ist der Ansicht, daß § 55 des Bundesbeamten-

gesetzes (Beratungs- und Gehorsamspflicht) in Ausprägung der hergebrachten Grundsätze des Berufsbeamtentums, insbesondere der Treuepflicht des Beamten gegenüber seinem Dienstherrn, hinreichend deutlich erkennen lasse, daß der Dienstherr von seinen Beamten diejenigen Angaben verlangen könne, die zur Gewährleistung der Sicherheit im Bereich des öffentlichen Dienstes geeignet und erforderlich seien. Es bleibt abzuwarten, ob der Erste Senat des Bundesverfassungsgerichts diese Auffassung teilt.

5.4 „Übergangsbonus"

Zur Frage der Dauer des vom Bundesverfassungsgericht anerkannten „Übergangsbonus" bei Fehlen notwendiger bereichspezifischer Datenschutzvorschriften (vgl. dazu 8. Tätigkeitsbericht, S. 7/8) wird von Verwaltungsgerichten erster Instanz zunehmend angenommen, die Frist sei abgelaufen. Andererseits hält das Oberlandesgericht Frankfurt in seinem Beschluß vom 14. Juli 1988 (NJW 1989, 47) die Speicherung und Aufbewahrung personenbezogener Daten in einer Zentralen Namenskartei der Staatsanwaltschaft übergangsweise noch für zulässig. Der Gesetzgeber befinde sich bezüglich des Schutzes persönlicher Daten in einer schwierigen Anpassungsphase; zudem seien auf dem Gebiet des Strafverfahrensrechts bereits Vorbereitungen zur Gesetzesänderung getroffen worden.

Was die materiellen Voraussetzungen des Übergangsbonus im Datenschutzrecht betrifft, hat sich das Bundesverfassungsgericht (3. Kammer des Zweiten Senats) hierzu zum ersten und, soweit ersichtlich, bisher einzigen Male in seinem Beschluß vom 24. März 1987 (NJW 1988, 405) geäußert. Es lehnte eine Einsichtnahme des Opfers einer Straftat in strafrechtliche Ermittlungsakten bei damaligem Fehlen einer gesetzlichen Grundlage ab. Sie sei im Hinblick auf die Möglichkeit, zivilrechtliche Schadensersatzansprüche effektiv im Zivilprozeß durchzusetzen, von Verfassungs wegen nicht geboten (vgl. jetzt § 406 e StPO).

6. Datenschutz in den Bereichen der Verwaltung

6.1 Einwohnerwesen

6.1.1 Datenübermittlung an politische Parteien

Wiederholt wurde ich auf Grund von Bürgereingaben und Beratungsersuchen von Gemeinden mit der Frage befaßt, inwieweit es zulässig ist, Daten an Parteien außerhalb der Frist in § 35 Abs. 1 des Meldegesetzes für das Land Nordrhein-Westfalen (MG NW) zu übermitteln, wie etwa für Einladungen von Senioren zu einer Kaffeetafel.

Nach § 35 Abs. 1 MG NW darf die Meldebehörde politischen Parteien im Zusammenhang mit Parlaments- und Kommunalwahlen in den sechs der Wahl vorangehenden Monaten Auskunft aus dem Melderegister über Namen, akademische Grade und Anschriften von Wahlberechtigten nach Lebensaltersgruppen erteilen. Diese Vorschrift wurde einerseits geschaffen, damit die Parteien ihre Aufgabe, nach Artikel 21 Abs. 1 Satz 1 des Grundgesetzes bei der politischen Willensbildung des Volkes mitzuwirken, erfüllen können. Die zeitliche Begrenzung der Datenübermittlung soll andererseits die Bürger vor einer Beeinträchtigung ihrer schutzwürdigen Belange schützen.

Außerhalb der Frist in § 35 Abs. 1 MG NW ist die Datenübermittlung an Parteien nach § 34 Abs. 3 MG NW zu beurteilen, wonach die Meldebehörde nichtöffentlichen Stellen eine Melderegisterauskunft über die Vielzahl nicht namentlich bezeichneter Einwohner nur dann erteilen darf, wenn sie im öffentlichen Interesse liegt (vgl. zu § 34 Abs. 3 MG NW auch S. 91/92). Außerdem dürfen nach § 7 Satz 1 MG NW schutzwürdige Belange der Betroffenen durch die Verarbeitung oder sonstige Nutzung personenbezogener Daten nicht beeinträchtigt werden.

Mit Rücksicht darauf, daß die Parteien nach § 35 Abs. 1 MG NW die Möglichkeit haben, in den sechs einer Wahl vorangehenden Monaten Daten von Wahlberechtigten, also auch von Senioren, zu erhalten, ist das öffentliche Interesse an einer Datenübermittlung außerhalb dieses Zeitraumes eng auszulegen. Ein öffentliches Interesse an der Übermittlung von Namen und Anschriften der über 60jährigen Bürger und Bürgerinnen für die Einladung zu einer Kaffeetafel oder der Daten von Neubürgern einer Gemeinde an Parteien außerhalb der genannten Frist vermag ich daher nicht zu erkennen.

Der Innenminister, den ich auf Grund einer Eingabe um Stellungnahme zu der Übermittlung personenbezogener Daten aus dem Melderegister an Parteien gebeten hatte, hat mir mitgeteilt, daß auch er ein öffentliches Interesse an einer Datenübermittlung an Parteien für Kaffeetafeln, Bürgerfeste oder ähnliche Veranstaltungen, denen im übrigen zumindest als Nebenzweck sicherlich auch ein Werbecharakter für die veranstaltende Partei beizumessen sein dürfte, nicht zu erkennen vermag.

6.1.2 Melderegisterauskünfte an Inkassobüros

Ein Inkassobüro hat bei verschiedenen Einwohnermeldeämtern die Erteilung erweiterter Melderegisterauskünfte über den Familienstand zahlreicher Schuldner beantragt. Soweit die Schuldner verheiratet waren, sollte gleichzeitig der Vorname des Ehegatten mitgeteilt werden. Die Einwohnermeldeämter lehnten die Erteilung einer solchen erweiterten Melderegisterauskunft ab.

Soweit ein berechtigtes Interesse glaubhaft gemacht wird, darf die Meldebehörde eine erweiterte Melderegisterauskunft über die in § 34 Abs. 2 Nr. 1 bis 8 MG NW aufgeführten Daten eines einzelnen bestimmten Einwohners erteilen. Zu diesen Daten gehört auch der Familienstand, beschränkt auf die Angabe, ob verheiratet oder nicht. Die Auskunft über den Vornamen des Ehegatten gehört nicht zu diesen Daten.

Wichtigste Voraussetzung für die Erteilung einer erweiterten Melderegisterauskunft ist die Glaubhaftmachung eines berechtigten Interesses. Die Prüfung, ob im Einzelfall die Voraussetzungen vorliegen, muß im Wege der Interessenabwägung zwischen dem Auskunftsinteresse des Auskunftsuchenden und den schutzwürdigen Belangen des Betroffenen erfolgen.

Nicht immer wird ein wirtschaftliches Interesse, zum Beispiel Kaufpreisforderungen einzuziehen, ausreichend sein. Insbesondere kann ein solches Interesse nicht als genügend angesehen werden, wenn der Auskunftsuchende es versäumt, sich die der erweiterten Melderegisterauskunft unterliegenden Daten von seinen Kunden nennen zu lassen, obwohl die Kenntnis dieser Daten nach der Art des Geschäftsbetriebes für die möglicherweise erforderliche Einziehung einer Forderung zweckmäßig erscheint (vgl. OVG Münster, NJW 1971, 1627 u. NJW 1973, 110).

Außerdem hat das Bundesverwaltungsgericht in seinem Urteil vom 22. Dezember 1987 (NJW 1988, 1611) ausgeführt, daß ein berechtigtes Interesse an der Erteilung einer erweiterten Melderegisterauskunft in der Regel nicht vorliegt, wenn sich der Antragsteller die Daten vom Betroffenen nachweisen lassen kann. Die Meldebehörde ist nicht zur Erteilung einer erweiterten Melderegisterauskunft gezwungen, wenn sich der Antragsteller diese Daten innerhalb eines angemessenen Zeitraumes vom Betroffenen geben und nachweisen lassen kann, hierauf aber etwa zur Erleichterung seines Geschäftsbetriebes verzichtet.

Im übrigen reicht nach meiner Auffassung für die Glaubhaftmachung eines berechtigten Interesses an einer Auskunft über den Familienstand der alleinige Hinweis auf eine Gesamtschuldnerhaftung nach § 1357 BGB nicht aus. Nicht jedes Rechtsgeschäft, das ein Ehegatte abschließt, verpflichtet den anderen Ehegatten. § 1357 BGB findet nur auf die Geschäfte zur angemessenen Deckung des Lebensbedarfs der Familie Anwendung. Die Vorschrift gilt auch nicht für Ehegatten, die getrennt leben.

Ich bin davon ausgegangen, daß es sich bei den Anträgen auch um eine Art Datenanforderung „auf Vorrat" handelte und daß nicht in jedem Fall eine sofor-

tige Inanspruchnahme des Mitschuldners beabsichtigt war. Eine Übermittlung auf Vorrat für den Fall, daß die Daten später einmal zur Erledigung der Aufgaben des Inkassobüros gebraucht werden, ist nicht zulässig.

6.2 Bau- und Wohnungswesen

Bürger wenden sich in zunehmendem Maße dagegen, auf Formularen öffentlichen Stellen gegenüber Einwilligungserklärungen für eine nahezu unbeschränkte Datenerhebung bei beliebigen dritten Stellen abzugeben.

Insbesondere im Bereich des Bau- und Wohnungswesens sind für die Gewährung von Zuschüssen jeglicher Art oder für die Überprüfung der Berechtigung erhaltener Zuschüsse oder sonstiger Vergünstigungen **Antragsformulare** auszufüllen. Für die Richtigkeit der gemachten Angaben sind häufig Nachweise erforderlich. In den verwendeten Vordrucken ist zum Teil eine Verpflichtung des Antragstellers oder des Betroffenen enthalten, der Bewilligungsbehörde auf Verlangen Nachweise etwa über die Einkommens- und Vermögensverhältnisse oder über vorhandenes Eigenkapital vorzulegen oder ihr zu gestatten, die für erforderlich gehaltenen Auskünfte bei Kreditinstituten und Behörden, insbesondere bei den Finanzbehörden, über die Leistungsfähigkeit und Zuverlässigkeit einzuholen, sowie die Zustimmung zur Auskunfterteilung durch Behörden oder Dritte zu erteilen.

Wie das Bundesverfassungsgericht im Volkszählungsurteil ausgeführt hat, wäre eine Rechtsordnung, in der Bürger nicht mehr wissen können, wer was wann über sie weiß, mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar (BVerfGE 65, 1, 43). Die Einholung einer Einwilligungserklärung für alle erdenklichen Fälle der Datenerhebung ist wegen fehlender Transparenz für den Betroffenen mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar.

Eine wirksame Einwilligung setzt nach § 4 Satz 2 und 3 DSG NW eine umfassende Aufklärung voraus, die dem Betroffenen eine bewußte und freie Entscheidung über die Preisgabe und Verarbeitung seiner Daten ermöglicht. Weiter ist bei der Datenerhebung nach § 12 DSG NW auch im Falle der Freiwilligkeit die Bestimmung des § 12 Abs. 2 DSG NW zu beachten.

Wird ein Verwaltungsverfahren nur auf Grund der freien Entscheidung des Antragstellers mit dessen ausdrücklicher Einwilligung eingeleitet und hängt die erfolgreiche Durchführung des Verfahrens von der Mitwirkung des Bürgers durch Erteilung von Auskünften und Vorlage von Unterlagen ab, so gebietet das Recht auf informationelle Selbstbestimmung, daß dem Grundsatz der Freiwilligkeit und Einwilligung während des gesamten Verfahrens Rechnung getragen wird.

Der Bürger muß die Möglichkeit haben, durch Antragsrücknahme auf die Gewährung von Zuschüssen zu verzichten, wenn er die Nachteile für größer hält, die ihm durch Erteilung einer bestimmten Auskunft oder Vorlage einer bestimmten Unterlage erwachsen, als die Vorteile, die er durch Gewährung von Zuschüssen erlangen würde.

Es ist daher nicht gerechtfertigt, ohne Kenntnis des Antragstellers und über dessen Kopf hinweg von beliebigen Stellen alle geeignet erscheinenden Auskünfte einzuholen. Der Antragsteller muß vielmehr die erforderlichen Nachweise grundsätzlich selbst erbringen.

Es mag aus datenschutzrechtlicher Sicht zwar ausreichen, daß der Antragsteller darauf hingewiesen wird, welche Informationsflüsse zwischen Behörden oder anderen Stellen bei der Bearbeitung seines Antrags für erforderlich gehalten werden und daher zu erwarten sind, und er dies billigend zur Kenntnis nimmt. Die Wirksamkeit einer solchen Einwilligung ist jedoch von einer vorausgehenden präzisen Unterrichtung abhängig. Pauschale Formulierungen wie die, daß die Bewilligungsbehörde Auskünfte bei Kreditinstituten und Behörden, insbesondere bei den Finanzinstituten und Behörden einholen darf, zeigen dem Antragsteller nicht, wer was wann und bei welcher Gelegenheit über ihn erfährt.

Mangels hinreichender Unterrichtung des Erklärenden und mangels hinreichender Präzision der Erklärung ist eine solche „Einwilligung" unwirksam. Sie rechtfertigt beispielsweise nicht die Durchbrechung des Steuergeheimnisses. Welche Informationsflüsse im Einzelfall erforderlich sind, ergeben sich konkret erst im Laufe eines Verfahrens und können nicht von vornherein genannt werden. Eine pauschale Vorabzustimmung ist jedoch unwirksam. Alle geeignet erscheinenden Auskünfte sollten daher beim Antragsteller selbst eingeholt werden und nur mit dessen Kenntnis und Zustimmung direkt bei Dritten eingeholt werden dürfen, wobei der Antragsteller auf die zu erwartenden negativen Folgen hinzuweisen ist, mit denen er bei Nichterteilung seiner Zustimmung zu rechnen hat.

6.3 Rechtswesen

6.3.1 Auskunftsrechte gegenüber der Staatsanwaltschaft

Auf die Probleme des Bürgers, sein Auskunftsrecht gegenüber der Staatsanwaltschaft durchzusetzen, hatte ich bereits in meinem 8. Tätigkeitsbericht hingewiesen (S. 40/41). In ihrer Stellungnahme zu meinem Tätigkeitsbericht (Drucksache 10/2676, S. 21) weist die Landesregierung hierzu darauf hin, daß der Justizminister für seinen Geschäftsbereich bereits sichergestellt habe, daß Anträge auf Erteilung einer Auskunft durch die Staatsanwaltschaften pragmatisch bearbeitet werden. Es sei somit gewährleistet, daß **jeder** Antrag auf Erteilung einer Auskunft – unabhängig vom Bearbeitungsstand und der Form der Datenverarbeitung in Akten oder in Dateien – an Hand der Umstände des Einzelfalles geprüft werde. Prinzipielle Meinungsunterschiede über die derzeitige Behandlung von Auskunftsersuchen zwischen dem Justizminister und dem Landesbeauftragten bestünden insoweit nicht.

Gleichwohl bestand auch in diesem Berichtszeitraum die Notwendigkeit, die Auskunftsverweigerung durch eine Staatsanwaltschaft zu beanstanden. Die Entscheidung über den Auskunftsantrag des Bürgers entsprach weder den

Erklärungen der Landesregierung, noch trug sie der Neuregelung des Auskunftsrechts der Bürger durch das Gesetz zur Fortentwicklung des Datenschutzes Rechnung. In seiner Stellungnahme, die zeitlich nach Inkrafttreten des neuen Datenschutzgesetzes zu meiner Beanstandung erfolgte, hat der Justizminister das Vorliegen eines Verstoßes gegen Vorschriften über den Datenschutz verneint. Der Justizminister vertritt in diesem Zusammenhang die Auffassung, daß allgemein gehaltene Gesuche um Auskunft die Frage nach Datenspeicherungen im Rahmen etwa schwebender Verfahren einschließen und die Staatsanwaltschaft derartige Auskünfte in aller Regel aus kriminaltaktischen Erwägungen nicht erteilen dürfe, weil sie die ordnungsgemäße Erfüllung staatsanwaltschaftlicher Aufgaben gefährden würde. Diese Erwägungen stünden zur Vermeidung von Gegenschlüssen auch dann einer Auskunftserteilung generell entgegen, wenn wahrheitsgemäß eine Negativauskunft erteilt werden könnte.

In diesem Zusammenhang bat der Justizminister zu bedenken, daß ein Bürger regelmäßig nicht ohne konkreten Anlaß eine Behörde – und schon gar nicht eine Staatsanwaltschaft – um Auskunft über etwa vorhandene, seine Person betreffende Vorgänge bittet. Es liege in der Natur staatsanwaltschaftlicher Akten, daß an ihrem Inhalt vor allem solche Personen ein Interesse haben, die von staatsanwaltschaftlichen Ermittlungen betroffen sind oder sein können.

Nach der Auffassung des Justizministers müßte der Bürger seinen Auskunftsantrag von vornherein beschränken, etwa auf abgeschlossene Verfahren, oder von Anfang an sein besonderes Auskunftsinteresse, etwa an noch nicht abgeschlossenen Verfahren, deutlich machen. Ein allgemein gehaltenes Auskunftsersuchen wäre dagegen stets als ausforschungsverdächtig abzulehnen.

Diese Erwägungen stehen nicht im Einklang mit dem Recht auf informationelle Selbstbestimmung und mit der Neuregelung des Auskunftsrechts der Bürger im Datenschutzgesetz Nordrhein-Westfalen.

Die Landesregierung Nordrhein-Westfalen hat in der Begründung zu § 18 E-DSG NW (Drucksache 10/1565, S. 57) ausgeführt, die Verpflichtung öffentlicher Stellen zur Erteilung von Auskunft und Einsicht sei nunmehr generell anders strukturiert. Die bisherige Regelung, wonach bestimmte Behörden (Verfassungsschutz, Staatsanwaltschaft und Polizei sowie Landesfinanzbehörden) von der Verpflichtung zur Auskunft gänzlich ausgenommen seien (§ 16 Abs. 2 i.V.m. § 15 Abs. 2 Nr. 1 DSG NW a.F), sei mit dem Recht auf informationelle Selbstbestimmung unvereinbar und könne daher nicht mehr aufrechterhalten werden. Grundsätzlich müsse jeder erfahren dürfen, wer was wann und bei welcher Gelegenheit über ihn gespeichert habe. Ausnahmen von diesem Grundsatz seien nur zulässig, wenn die Einzelabwägung ergebe, daß überwiegende Gründe des Gemeinwohls der Auskunftserteilung entgegenstehen.

Danach ist davon auszugehen, daß, soweit das Datenschutzgesetz Nordrhein-Westfalen auf die Staatsanwaltschaft bei Erledigung ihrer Aufgaben An-

wendung findet (§ 2 Abs. 1 Satz 2 DSG NW), dem Bürger auf sein Auskunftsersuchen generell Auskunft erteilt werden **muß.** Lediglich unter den Voraussetzungen des § 18 Abs. 3 DSG NW ist im Einzelfall eine Auskunftsverweigerung möglich. Dabei sind dann aber auch § 18 Abs. 4 und Abs. 6 DSG NW zu beachten.

Außerhalb des Anwendungsbereichs des § 18 DSG NW, etwa bei Auskunft über noch nicht abgeschlossene Verfahren, fehlt es an einer normenklaren gesetzlichen Grundlage für eine entsprechende Einschränkung des Rechts auf informationelle Selbstbestimmung der Bürger. Bis zur Schaffung einer derartigen bereichspezifischen gesetzlichen Regelung, etwa im Rahmen der Novellierung der Strafprozeßordnung, gilt zur Zeit noch der sog. Übergangsbonus nach der Rechtsprechung des Bundesverfassungsgerichts. Insoweit kommt die Verweigerung der Auskunftserteilung gegenüber dem anfragenden Bürger auch derzeit nur im Ausnahmefall in Betracht (vgl. 8. Tätigkeitsbericht, S. 40/41).

In diesem Zusammenhang bleibt darauf hinzuweisen, daß, wenn über den Bürger keine Daten bei der Staatsanwaltschaft gespeichert sind und keine Gründe, die für eine Ausforschung sprechen können, vorliegen, ihm diese Auskunft zu erteilen ist. Dabei kann die Tatsache der Stellung des Auskunftsersuchens für sich allein nicht zur Begründung eines Ausforschungsverdachts ausreichen. Ein Ausforschungsverdacht dürfte im übrigen in der Regel nur hinsichtlich schwebender Verfahren bestehen. Insoweit müßte dem Betroffenen Gelegenheit gegeben werden, sein Auskunftsinteresse näher darzulegen. Überzeugen diese Gründe des Betroffenen nicht, so ist ihm gleichwohl im übrigen Auskunft zu erteilen. Zur Vermeidung von Gegenschlüssen ist die Antwort entsprechend zu beschränken. Das hierbei auftretende Formulierungsproblem ist von den Sicherheitsbehörden in gleichgelagerten Fällen bereits seit Jahren gelöst.

Da der Justizminister meiner Beanstandung wiederum nicht gefolgt ist, ist es Sache der Landesregierung und ggf. des Landtags, den Bürgern des Landes Nordrhein-Westfalen die Ausübung ihres Rechts auf informationelle Selbstbestimmung im Wege der Auskunft auch im Bereich der Staatsanwaltschaft allgemein zu ermöglichen. Die Bürger sollten auch davor geschützt sein, daß sie, wenn sie insoweit von ihren verfassungsmäßigen Rechten Gebrauch machen, sich u. U. der Staatsanwaltschaft gegenüber der Ausforschungsabsicht verdächtig machen, wie die zusätzlichen Erwägungen des Justizministers zeigen.

6.3.2 Strafvollzug

Wie in allen früheren Berichtsjahren waren die Eingaben von Gefangenen auch dieses Mal sehr zahlreich. Sie befaßten sich überwiegend mit der Möglichkeit Gefangener, Kenntnis von personenbezogenen Daten Mitgefangener zu nehmen. So wurde mir wiederholt geschrieben, daß sich diese Möglichkeiten insbesondere beim Einsatz Gefangener im Reinigungsdienst sowie bei der

Akten- und Altpapiervernichtung ergeben. Die Leiter der betreffenden Justizvollzugsanstalten versicherten zwar, daß die Gefangenen weder bei der Papiervernichtung noch bei Reinigungsarbeiten unbeaufsichtigt seien und somit eine unbefugte Kenntnisnahme personenbezogener Daten nicht möglich sei. Nach Auffassung der Gefangenen soll es dagegen relativ einfach sein, die Bediensteten abzulenken oder ihre Aufmerksamkeit zu mindern. Ein Mittel soll sein, die Reinigungsarbeiten besonders langsam durchzuführen. Je länger die Arbeit dauere, um so mehr lasse die Aufmerksamkeit der überwachenden Bediensteten nach.

In einem Fall, bei dem nicht geklärt werden konnte, wie ein Gefangener zwei Hälften eines ausgefüllten Vordrucks an sich gebracht hatte, vermutete dann auch der Leiter der Vollzugsanstalt, daß sich die Vordruckhälften in einem Papierkorb befunden und ein Gefangener sie bei Reinigungsarbeiten trotz Überwachung unbemerkt mitgenommen haben könnte. Gerade weil sich menschliches Versagen nie ganz ausschließen läßt, müssen beim Einsatz Gefangener zu Arbeiten in der Vollzugsanstalt besondere organisatorische Maßnahmen getroffen werden, wie etwa:

- Soweit Gefangene Büroräume reinigen, sollten zuvor Unterlagen mit personenbezogenen Daten verschlossen werden.
- Papierkörbe sollten nicht von Gefangenen geleert werden.
- Keine Postkontrolle, während Gefangene den Raum putzen.
- Keine Beteiligung Gefangener bei der Verteilung der Post.
- Auszüge über vorhandenes Eigengeld oder Hausgeld nur im verschlossenen Umschlag übergeben.
- Durchführung von Zellenräumungen durch Hausarbeiter erst, nachdem die Zelle von einem Bediensteten auf Schriftgut des Gefangenen durchgesehen und dieses von dem Bediensteten eigenhändig verpackt worden ist.
- Gefangenentransportscheine nicht von Gefangenen ausfüllen lassen.
- Gefangene und auch Freigänger nicht mit der Aktenvernichtung beauftragen.
- In dem nach der Allgemeinen Verfügung des Justizministers vom 22. Juli 1975 zu führenden Kontrollbuch für Zustellungen sind etwaige auf demselben Blatt des Kontrollbuchs voraufgehende Eintragungen abzudecken, wenn ein Gefangener den Empfang einer Sendung mit seiner Unterschrift bestätigt.
- Bei der Verwendung von Unterlagen eines Gefangenen für Stellungnahmen in gerichtlichen Verfahren gegen andere Gefangene ist sorgfältig darauf zu achten, daß auf diese Weise Gefangene keine Daten Mitgefangener zur Kenntnis bekommen.

Im Bereich des Strafvollzugs sind jedoch nicht nur die personenbezogenen Daten Gefangener vor der Kenntnisnahme durch Mitgefangene zu schützen.

In einem mir vorgetragenen Fall ging es um den Schutz eines Bediensteten im Justizvollzug: Das Land Nordrhein-Westfalen führte einen Schadensersatzprozeß gegen einen Gefangenen. Dem anwaltlichen Schriftsatz waren Ablichtungen der zum Nachweis der Forderung dienenden Unterlagen beigefügt. Hierbei handelte es sich insbesondere um ärztliche Atteste, Arztrechnungen, Rezepte und Dienstunfähigkeitsbescheinigungen eines Bediensteten. Diese Unterlagen, die auch die Anschrift des Bediensteten enthieten, sollten dem Gefangenen (Beklagten) zugestellt werden.

Der Gefangene hatte zuvor Morddrohungen gegenüber dem Bediensteten geäußert, von deren Ernsthaftigkeit die Justizvollzugsanstalt überzeugt war. Die Anstaltsleitung hatte die Eintragung eines Sperrvermerks im Melderegister des zuständigen Einwohnermeldeamtes beantragt. Eine Eintragung im Telefonbuch war nicht erfolgt. Um so schwerwiegender wäre die Bekanntgabe der Anschrift des Bediensteten an den Gefangenen durch die Zustellung der Unterlagen gewesen.

Durch die Aufmerksamkeit des Leiters der zuständigen Vollzugsanstalt wurden die für den Gefangenen bestimmten Unterlagen nicht an ihn zugestellt, sondern an das Gericht zurückgegeben, damit bestimmte Daten des Bediensteten unkenntlich gemacht wurden. Der Präsident des Vollzugsamts hat diesen Fall zum Anlaß für die Anordnung genommen, künftig in Unterlagen, die zur Weiterleitung an Gerichte und Prozeßgegner bestimmt sind, die Anschriften Bediensteter unkenntlich zu machen.

6.3.3 Rechtspflege und Datenschutz

Nach § 22 Abs. 1 in Verbindung mit § 2 Abs. 1 DSG NW unterliegen die Gerichte meiner Kontrolle nur, soweit sie Verwaltungsaufgaben wahrnehmen. Viele Bürgereingaben betreffen jedoch immer wieder den Bereich der Rechtspflege. Auch soweit meine Zuständigkeit nicht gegeben ist, nehme ich solche Eingaben mitunter zum Anlaß, die jeweilige Stelle auf die Probleme des Bürgers aufmerksam zu machen. Die Anliegen der Bürger nicht nur im Zivil- oder Strafverfahren, sondern auch in Konkursverfahren, Vormundschafts- und Pflegschaftssachen, Erbschaftsangelegenheiten, Zwangsversteigerungsverfahren, Zwangsvollstreckungssachen und auch im Bereich der Tätigkeit des Gerichtsvollziehers zeigen, daß der Umgang der Gerichte mit personenbezogenen Daten nicht immer den Vorstellungen der Betroffenen über den Datenschutz entspricht. In diesen Fällen wurden nach Auffassung der Bürger zu viele personenbezogene Daten an Verfahrensbeteiligte oder ihrer Ansicht nach auch an Unbeteiligte weitergegeben. Die gesetzlichen Vorschriften verpflichten die Gerichte, Verfahrensbeteiligten Gelegenheit zur Stellungnahme zu dem Vorbringen eines Beteiligten zu geben. Dies kann oft nur durch Übersendung von Kopien der Schriftsätze und Anlagen geschehen. Dies rechtfertigt jedoch nicht grundsätzlich die Übersendung von vollständigen Unterlagen, ohne zu prüfen, ob nicht datenschutzrechtliche Belange der Betroffenen durch diese Verfahrensweise beeinträchtigt werden (vgl. insoweit auch oben S. 52/53).

Durch eine Eingabe bin ich auf die Verfahrensweise der Gerichte bei der Zustellung nach § 212 a ZPO aufmerksam gemacht worden. Nach § 212 a ZPO

genügt bei der Zustellung an einen Anwalt, Notar oder Gerichtsvollzieher oder eine Behörde oder Körperschaft des öffentlichen Rechts zum Nachweis der Zustellung das mit Datum und Unterschrift versehene schriftliche Empfangsbekenntnis des Zustellungsempfängers.

Die Gerichte verwenden üblicherweise als Empfangsbekenntnis eine Antwortpostkarte nach einem Vordruck. Auf dieser Postkarte sind Daten wie die kurze Bezeichnung des Schriftstücks, die Namen der Parteien, die Geschäftsnummer und das Gericht sowie die Bezeichnung des Zustellungsempfängers enthalten. Um den Datenschutzbelangen der Betroffenen Rechnung zu tragen, hatte ich vorgeschlagen, jedem Empfangsbekenntnis nach § 212 a ZPO einen adressierten Briefumschlag beizufügen. Zumindest sollte das Empfangsbekenntnis nicht als Antwortpostkarte gestaltet sein.

Der Justizminister hat auf meine Veranlassung die Vordrucke für Antwortpostkarten geändert. Aus Gründen der Haushaltsmittelbewirtschaftung und der Arbeitsökonomie hat er zwar von der vorgeschlagenen Versendung des Empfangsbekenntnisses im verschlossenen Briefumschlag abgesehen. Er hat jedoch den Datenumfang auf der Postkarte auf das bei der förmlichen Postzustellung zugelassene Maß reduziert.

Abgesehen von solchen einer befriedigenden Lösung zugeführten Einzelfällen bedürfen die Verfahrensregelungen aller Gerichtszweige einer Überarbeitung unter Berücksichtigung des Rechts auf informationelle Selbstbestimmung der Verfahrensbeteiligten.

6.4 Polizei

6.4.1 Datenspeicherung über Homosexuelle

In mehreren Bürgereingaben sowie zahlreichen Presseberichten wurde im Zusammenhang mit der Ermittlungstätigkeit der Polizei in einem Mordfall der Verdacht geäußert, die Polizei führe über Homosexuelle sog. Rosa Listen. Nach Einsichtnahme in die Bahnhofsverbotskartei der Bahnpolizei hatte die örtlich zuständige Kreispolizeibehörde (KPB) eine Reihe von Personen vorgeladen, zu denen auf den Karteikarten der Bahnhofsverbotskartei entsprechende Hinweise eingetragen waren.

Wie schon bei früheren Überprüfungen dieser Art (vgl. etwa 2. Tätigkeitsbericht, S. 36), war das Ergebnis meiner Ermittlungen bei der KPB, daß Karteien, Dateien oder sonstige Sammlungen mit Angaben über Sexualverfahren (wie etwa „Rosa Listen") **nicht** geführt werden. Mit dem Innenminister des Landes Nordrhein-Westfalen besteht Übereinstimmung, daß die Führung derartiger Sammlungen durch die Polizei unzulässig wäre.

Darüber hinaus bestanden Zweifel an der Rechtmäßigkeit der Datenerhebung durch Einblicknahme in **sämtliche** Karteikarten der Bahnhofsverbotskartei. Nach dem Ermittlungsansatz der Polizei in dem Mordfall konnte ein Großteil der in der Kartei verzeichneten Personen von vornherein ausgeschieden werden.

Der Bundesbeauftragte für den Datenschutz, dem die Datenschutzkontrolle für die Behörden der Bundesbahn obliegt, hatte im Vorfeld meiner abschließenden Stellungnahme die Gestattung der Einsichtnahme in die gesamte Kartei gegenüber dem Vorstand der Deutschen Bundesbahn beanstandet, weil sie sich nicht auf die von der Kriminalpolizei benötigten Informationen beschränkte. Diese Bewertung hinsichtlich der Einsichtnahme in sämtliche Karteikarten durch Beamte der KPB wird von mir geteilt. Die Einsichtnahme war unzulässig, da sie zur Aufgabenerfüllung der KPB im konkreten Ermittlungsverfahren nicht erforderlich war. Keine datenschutzrechtlichen Bedenken hingegen bestanden gegen die Einsichtnahme in die Karteikarten für diejenigen Personen, die nach dem Ermittlungsansatz der KPB zur Aufklärung des Falles möglicherweise beitragen konnten.

Allgemein läßt sich für die Ermittlungstätigkeit der Polizei im Zusammenhang mit diesem Fall feststellen:

Soweit eine gesetzliche Regelung hierfür fehlt, scheidet bei der Einsichtnahme durch die Polizei in eine Kartei einer anderen Behörde die Durchsicht aller der in dem Karteikasten gesammelten aufbewahrten Karteikarten in der Regel aus. Zulässig ist lediglich die Durchsicht der dieser Sammlung entnommenen Karteikarten der „Treffer" und der eingehender zu prüfenden Zweifelsfälle. Die vorherige Sichtung der gesamten Kartei muß dabei durch Mitarbeiter der karteiführenden Stelle erfolgen. Im Extremfall kann der Umfang der Zweifelsfälle unter Umständen auch die gesamte Kartei umfassen.

Eine Durchsicht dürfte auch dann in Betracht kommen, wenn erkennbar der Ermittlungsansatz der Polizei der karteiführenden Stelle nicht zu vermitteln ist. Eine Entscheidung hierüber sollte auf höherer Ebene und unter Berücksichtigung der Schwere des Delikts getroffen werden.

Nach Ablauf des sog. Übergangsbonus bedarf auch dieses Vorgehen der Polizei einer normenklaren bereichspezifischen Regelung in der Strafprozeßordnung.

6.4.2 Personengebundener Hinweis ANST (Ansteckungsgefahr)

Zur Speicherung personenbezogener AIDS-Daten in polizeilichen Informationssystemen haben die Datenschutzbeauftragten des Bundes und der Länder sowie die Datenschutzkommission des Landes Rheinland-Pfalz bei Gegenstimme des Bayerischen Landesbeauftragten für den Datenschutz am 7. Dezember 1987 in einem Beschluß ihre datenschutzrechtlichen Bedenken geäußert (vgl. Anlage 3, S. 135/136).

Anfang Oktober 1988 hat die ständige Konferenz der Innenminister und -senatoren ein Konzept zur Speicherung von Daten über HIV-Infizierte in Polizeidateien einstimmig verabschiedet, das dem vorgenannten Beschluß der Datenschutzbeauftragten nur teilweise entgegenkommt; so ist u. a. die Speicherung nunmehr in das Ermessen des Bundes oder eines jeden Landes gestellt. Diese Ermessensentscheidung erhöht die Zweifel an der Erforderlichkeit.

Unter Hinweis auf Presseberichte, das Land Niedersachsen habe die Notwendigkeit einer Speicherung für seine Polizei verneint und alle bislang eingespeicherten Daten über HIV-Infizierte gelöscht, habe ich den Innenminister gebeten zu prüfen, ob für Nordrhein-Westfalen eine ähnliche Regelung herbeigeführt werden kann.
Der Innenminister hat durch Erlaß vom 15. November 1988 angeordnet, entsprechende Hinweise nicht mehr zu speichern und die bestehenden Speicherungen unverzüglich zu löschen.

6.4.3 Besuchergruppen in Polizeistationen

Im laufenden Berichtsjahr wurde ich mehrfach darauf aufmerksam gemacht, daß in Polizeileitstellen durch Besuchergruppen der Datenschutz nicht gewährleistet ist. Bei derartigen Besichtigungen geht der normale Dienstbetrieb weiter, so daß Besucher unter Umständen dienstliche Gespräche (z. B. Notrufe, Kfz-Überprüfungen, Personenüberprüfungen) mithören können.

Das Grundrecht auf Datenschutz verbietet den Behörden nicht nur, personenbezogene Daten ohne gesetzliche Grundlage oder Einwilligung des Betroffenen selbst weiterzugeben. Es verpflichtet sie auch, die technischen und organisatorischen Maßnahmen zu treffen, die zum Schutz der Daten gegen unbefugte Kenntnisnahme durch Dritte erforderlich sind. Dementsprechend bestimmt § 10 Abs. 1 Satz 1 DSG NW, daß öffentliche Stellen, die selbst oder im Auftrag einer anderen Stelle personenbezogene Daten verarbeiten, die technischen und organisatorischen Maßnahmen zu treffen haben, die erforderlich sind, um eine den Vorschriften des Datenschutzgesetzes entsprechende Verarbeitung der Daten sicherzustellen. Dazu gehören auch Maßnahmen zum Schutz des Bürgers vor dem Mithören anderer, insbesondere nicht zur Behörde gehörender Personen.

Ein Bürger, der sich beispielsweise unter dem Notruf an die Polizei wendet, dürfte wenig Verständnis dafür haben, daß möglicherweise eine mehr oder weniger große Zahl von Besuchern von seinem Anliegen Kenntnis erhält. Der Weiterverbreitung der durch Mithören erlangten Daten durch Besucher sind keine Grenzen gesetzt.

Soweit technische und organisatorische Maßnahmen zum Schutz vor unbefugtem Mithören nicht nur mit einem Aufwand möglich sind, der nicht in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (§ 10 Abs. 1 Satz 2 DSG NW), habe ich dem Innenminister des Landes empfohlen, durch Erlaß zu regeln, von der Führung von Besuchern oder Besuchergruppen durch Polizeileitstellen während des Dienstbetriebes abzusehen.

Der Innenminister ist meiner Empfehlung gefolgt.

6.4.4 Interne Datenschutzkontrolle

Bei Stellungnahmen von Kreispolizeibehörden (KPB) zu meinen Auskunftsersuchen war aufgefallen, daß insbesondere bei allgemein gehaltenen Ersuchen die Stellungnahmen unkoordiniert von unterschiedlichen Abteilungen oder

Dezernaten erfolgten. Dies hatte Auswirkungen auf die Qualität der Auskünfte und war nach meiner Auffassung auch der Grund für mitunter objektiv falsche Auskünfte. Ich habe deshalb dieses Problem zum Gegenstand von Kontrollbesuchen gemacht und dabei Maßnahmen zur Abhilfe vorgeschlagen.

Nach § 10 Abs. 1 Satz 1 DSG NW haben die KPB die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine den Vorschriften dieses Gesetzes entsprechende Verarbeitung der Daten sicherzustellen. Dazu ist es erforderlich, die Datenverarbeitung in geeigneter Weise zu überwachen, und zwar nach § 10 DSG NW sowohl die Datenverarbeitung in Dateien, als auch die in Akten. Jede KPB ist zur datenschutzrechtlichen Selbstkontrolle verpflichtet (vgl. auch 6. Tätigkeitsbericht, S. 153 bis 155).

Das Fehlen einer für die interne Datenschutzkontrolle zuständigen Stelle kann nach Ergebnissen meiner bisherigen Überprüfungen dazu führen, daß

- ein alle Abteilungen umfassendes Datensicherungskonzept fehlt,
- Einzelkonzepte hausintern nicht abgestimmt entwickelt und isoliert in Kraft gesetzt werden,
- nicht bekannt ist, welche geltenden Hausverfügungen, Dienstanweisungen und Richtlinien es gibt, zu deren Beachtung die Bediensteten der Dienststelle verpflichtet sind,
- keine zeitnahe Überprüfung, Fortschreibung und Bekanntmachung dieser Regelungen stattfindet,
- für eine Kontrolle der Einhaltung dieser Regelungen sich keine Stelle verantwortlich fühlt,
- Widersprüche und Unstimmigkeiten zwischen dem Inhalt der Übersicht (DSG NW a.F) und dem der Anmeldungen zum Dateienregister des Landesbeauftragten für den Datenschutz nicht festgestellt und beseitigt werden,
- durch Beschränkung der Auskunft auf das Vorhandensein oder Nicht-Vorhandensein von Daten in der einzelnen Abteilung unwissentlich dem betroffenen Bürger eine unvollständige oder gar falsche Auskunft über gespeicherte Daten erteilt wird,
- durch Nichtbeteiligung anderer Abteilungen dem Landesbeauftragten für den Datenschutz unwissentlich eine entsprechend unrichtige Auskunft erteilt wird,
- soweit nicht das Landeskriminalamt an die Aussonderungs- und Löschungsfristen erinnert, die notwendige Vernichtung von Unterlagen nach Ablauf der Aufbewahrungsfristen nicht systematisch überwacht wird.

In diesem Zusammenhang habe ich daher empfohlen,

- Auftrag und Befugnisse einer für die interne Kontrolle zuständigen Stelle schriftlich klar zu formulieren und sicherzustellen, daß diese Aufgabe einer fachlich geeigneten Organisationseinheit zugeordnet ist;

- die Verantwortung für das Gestalten des Konzepts der Datensicherung und für dessen Verwirklichung nach Möglichkeit so zuzuordnen, daß eine Interessenkollision ausgeschlossen ist, und die Zuordnung dieser Aufgabe im Geschäftsverteilungsplan unmißverständlich zum Ausdruck zu bringen;
- die hausinternen Dienstanweisungen und Hausverfügungen zum Datenschutz in der Zuständigkeit einer Stelle zu sammeln, auf Vollständigkeit und Richtigkeit zu überprüfen und für eine zeitnahe Fortschreibung Sorge zu tragen, was eine entsprechende Unterrichtungsverpflichtung aller Abteilungen, einschließlich des 14. Kommissariats voraussetzt;
- nach Überprüfung der Anmeldungen zum Dateienregister die erforderlichen Änderungsmeldungen nach § 23 DSG NW und der hierzu noch ergehenden Dateienregisterverordnung vorzunehmen;
- bei Anfragen des Landesbeauftragten für den Datenschutz oder bei Bürgeranfragen alle in Frage kommenden Abteilungen und Dezernate zu beteiligen;
- bei unverhältnismäßig hohem Aufwand die Antwort gegebenenfalls in der Weise einzuschränken, daß ein Hinweis auf § 18 Abs. 2 Satz 2 DSG NW erfolgt, etwa durch die Formulierung: „soweit an Hand Ihrer Angaben überprüfbar".

Im Hinblick auf die besondere Sensitivität der von der Polizei verarbeiteten Daten sollte sichergestellt werden, daß zumindest dieser Datenschutzstandard bei allen Kreispolizeibehörden des Landes Nordrhein-Westfalen realisiert ist.

6.5 Sozialwesen

6.5.1 Mitwirkungspflicht und Amtsermittlung

Nach meinen Feststellungen lassen Sozialleistungsträger häufig die Mitwirkungspflicht des Betroffenen nach §§ 60 ff. des Ersten Buches des Sozialgesetzbuchs (SGB I) außer acht, indem sie sich Informationen über den Betroffenen unmittelbar bei Dritten beschaffen und sich dabei auf den Grundsatz der Amtsermittlung (§§ 20, 21 des Zehnten Buches des Sozialgesetzbuchs – SGB X –) berufen. Diese Verwaltungspraxis gibt Veranlassung, auf das Verhältnis zwischen Mitwirkungspflicht und Amtsermittlungsgrundsatz näher einzugehen.

Nach § 21 SGB X stehen den Sozialleistungsträgern zwar eine Reihe von Möglichkeiten zur Verfügung, Beweise über Sachverhalte zu erheben. Jedoch gewährleistet das Recht auf informationelle Selbstbestimmung die Befugnis des Betroffenen, grundsätzlich selbst über die Preisgabe seiner persönlichen Daten zu bestimmen. Daraus ergibt sich, daß die Wahl behördlicher Informationsbeschaffung nicht mehr völlig frei ist; vielmehr hat die **Mitwirkung** des Betroffenen **Vorrang** vor der Amtsermittlung. Alles, was der Betroffene in den Grenzen seiner Mitwirkungspflicht (§ 65 SGB I) selbst beibringen kann, darf

nach dem Gebot des geringstmöglichen Eingriffs grundsätzlich nur bei ihm beschafft werden. Kommt der Betroffene seiner Mitwirkungspflicht nach §§ 60 ff. SGB I nicht nach, treten die Folgen des § 66 SGB I (Versagung oder Entziehung der Leistung) ein. Angesichts dieser bereichspezifisch geregelten Rechtsfolgen ist ein Rückgriff auf die Amtsermittlungsvorschriften der §§ 20, 21 SGB X nicht zulässig.

Anders sind allerdings die Fälle zu beurteilen, in denen die Rechtsfolgen des § 66 SGB I nicht eintreten können (z. B. bei Rückforderung überzahlter Leistungen) und der Betroffene nicht oder nicht ausreichend mitwirkt, wie auch die Fälle, in denen Anhaltspunkte dafür bestehen, daß der Betroffene unrichtige Angaben gemacht hat. In diesen Fällen muß dem Leistungsträger zwar gestattet sein, nach §§ 20, 21 SGB X von Amts wegen zu ermitteln. Jedoch gebietet der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz auch hier, zunächst den Betroffenen zu befragen.

6.5.2 Amtsermittlung nach § 116 Abs. 2 BSHG

In meinem 7. Tätigkeitsbericht (S. 54 bis 57) habe ich darauf hingewiesen, daß es unzulässig ist, bei **Anfragen über Arbeitsverdienst** von dem Arbeitgeber des Unterhaltspflichtigen mehr Angaben zu verlangen, als in § 116 Abs. 2 des Bundessozialhilfegesetzes (BSHG) genannt sind, wie neuer Arbeitgeber, Krankenkasse, Lohnsteuerermäßigung, Lohnpfändungen oder -abtretungen, Berufstätigkeit des Ehegatten, ggf. dessen Arbeitgeber, zuständige Familienausgleichskasse, Zahlung von Kindergeld für welche Kinder sowie Entlassungsgrund und „auf eigenen Wunsch entlassen".

Leistungsträger vertreten die Auffassung, daß die Erhebung solcher Angaben zwar nicht auf § 116 Abs. 2 BSHG, aber auf §§ 20, 21 SGB X gestützt werden könne. Dieser Auffassung kann ich nicht folgen.

Nach § 116 Abs. 2 BSHG hat der Sozialleistungsträger – als Pendant zur Auskunftspflicht des Arbeitgebers – einen Auskunftsanspruch gegenüber dem Arbeitgeber des Unterhaltspflichtigen, allerdings beschränkt auf die in dieser Vorschrift enumerativ genannten Angaben. Für die Erhebung darüber hinausgehender Angaben fehlt eine Befugnisnorm für den Eingriff in die Grundrechte des Unterhaltspflichtigen, so daß für die Erhebung weiterer Angaben beim Arbeitgeber die Einwilligung des Unterhaltspflichtigen erforderlich ist. Die §§ 20, 21 SGB X scheiden hier als Rechtsgrundlage aus, da § 116 Abs. 2 BSHG als abschließende spezialgesetzliche Regelung den allgemeinen Amtsermittlungsvorschriften vorgeht und diese begrenzt. Auch § 21 Abs. 4 SGB X, der unter bestimmten Voraussetzungen die Finanzbehörden zur Auskunftserteilung verpflichtet, gestattet nur Auskünfte über die Einkommens- und Vermögensverhältnisse des Unterhaltspflichtigen.

6.5.3 Verlangen von Erklärungen Dritter

Durch eine Eingabe wurde mir bekannt, daß das Landesamt für Ausbildungsförderung bei Anträgen auf **Stundung** der Rückzahlung von BAföG-Leistun-

gen Erklärungen von Verwandten, Freunden usw. des Betroffenen darüber verlangte, daß diese nicht zu einer Bürgschaft bereit seien.

Die Gewährung von Leistungen nach dem Bundesausbildungsförderungsgesetz (BAföG) umfaßt nicht nur die Auszahlung, sondern erstreckt sich auch auf die Abwicklung der Rückzahlung von zu Unrecht gewährten BAföG-Leistungen (§ 20 Abs. 1 BAföG). Daraus folgt, daß derjenige, der Stundung der Rückzahlung begehrt, der Mitwirkungspflicht nach § 60 SGB I unterliegt. Dmentsprechend hat er auf Verlangen des zuständigen Leistungsträgers Beweisurkunden vorzulegen (§ 60 Abs. 1 Nr. 3 SGB I). Nach § 59 Abs. 1 Nr. 1 der Landeshaushaltsordnung soll die Stundung in der Regel nur gegen Sicherheitsleistung gewährt werden.

Für die Entscheidung, ob Stundung ausnahmsweise ohne Sicherheitsleistung gewährt werden kann, mag eine Unterrichtung darüber, daß Verwandte und Freunde zu einer Bürgschaft nicht bereit sind, erforderlich sein. Allerdings bedarf es hierzu keiner authentischen Erklärung der Dritten; vielmehr muß im Hinblick darauf, daß der Betroffene gezwungen wäre, seinen Verwandten und Freunden den Bezug von BAföG-Leistungen sowie seine derzeitige Rückzahlungsunfähigkeit zu offenbaren, eine Erklärung des Betroffenen, daß Dritte nicht zu einer Bürgschaft bereit sind, genügen. Auf jeden Fall wäre das Verlangen einer authentischen Erklärung der Dritten nach meiner Auffassung unverhältnismäßig und unter Berücksichtigung des § 65 Abs. 1 Nr. 2 SGB I wegen der damit verbundenen Selbstoffenbarung sensibler Daten dem Betroffenen nicht zumutbar.

Der Auffassung des Landesamtes für Ausbildungsförderung, bei der Stundung handele es sich wegen der bereits eingetretenen Bestandskraft des Erstattungsanspruchs nicht mehr um die Durchführung des Bundesausbildungsförderungsgesetzes, so daß nicht die §§ 60 ff. SGB I, sondern allein § 59 LHO anwendbar sei, kann nicht gefolgt werden. Die Stundung von bestandskräftigen Erstattungsansprüchen darf nicht isoliert betrachtet werden. Sie ist vielmehr als eine Modifikation der Erstattung der gewährten BAföG-Leistungen, und zwar als Rückzahlungsaufschub anzusehen. Es handelt sich dabei also um einen Annex zur Abwicklung der Rückzahlung, der der Aufgabenerfüllung nach dem Sozialgesetzbuch zuzurechnen ist. Die Bedingungen für eine Stundung sind allerdings in der Landeshaushaltsordnung geregelt.

6.5.4 Prüfung von Zuwendungen an freie Träger

Ein Jugendwohlfahrtsausschuß hatte beschlossen, die Gewährung von Zuschüssen für die Beratungs- und Betreuungsarbeit eines freien Trägers davon abhängig zu machen, daß als Verwendungsnachweis dem Jugendamtsleiter oder einem von ihm beauftragten Bediensteten zur Vermeidung einer Mehrfachbetreuung die Namen der betreuten Familien und der jeweilige Betreuungsschwerpunkt mitgeteilt werden. Der freie Träger sah durch diese Offenlegung die für seine Arbeit unerläßliche Vertraulichkeit verletzt.

Zu einer ordnungsgemäßen Haushalts- und Wirtschaftsführung wie auch zu einer nachprüfbaren Rechnungslegung nach den Vorschriften der Gemeindeordnung gehört die Prüfung, ob Zuschüsse zweckentsprechend verwendet worden sind. Zu dieser Feststellung kann es erforderlich sein, personenbezogene Daten anzufordern, wobei jedoch der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz zu beachten ist.

Ich habe Zweifel, ob das Verlangen nach **namentlicher Bekanntgabe** der durch den freien Träger betreuten Familien nicht gegen den Verhältnismäßigkeitsgrundsatz verstößt. Dabei ist zu berücksichtigen, daß es sich bei den angeforderten Daten immerhin um Angaben handelt, die im öffentlichen Bereich dem besonderen Schutz des Sozialgeheimnisses unterliegen. Außerdem ist zu bedenken, daß die Bekanntgabe der Namen an den Leiter des Jugendamtes möglicherweise die Aufgabenerfüllung des freien Trägers beeinträchtigen, wenn nicht sogar längerfristig unmöglich machen würde, da Betroffene, die sich bewußt an nichtstaatliche Stellen wenden, auch erwarten, daß ihre Anonymität gegenüber staatlichen Stellen gewahrt wird.

Einer nicht notwendigen Mehrfachbetreuung könnte etwa dadurch begegnet werden, daß sich die betreuenden Stellen von den Betroffenen bestätigen lassen, von keiner anderen Stelle betreut zu werden, wobei diese Bestätigung nicht dem Jugendamtsleiter zugänglich gemacht werden darf.

Auf meine Empfehlung hat der Jugendwohlfahrtsausschuß einen neuen Beschluß gefaßt, wonach dem Jugendamt mit dem Verwendungsnachweis lediglich die Betreuungsschwerpunkte und die Fallzahlen mitzuteilen sind.

6.5.5 Jugendhilfeplanung

Durch eine Ratsfraktion wurde mir die Fragebogenaktion eines Jugendamtes im Rahmen der Jugendhilfeplanung bekannt. Die Untersuchung hatte das Ziel, durch **Analyse des Freizeitverhaltens** ein umfassendes Bild zur Situation der Jugend zu gewinnen. Der hierfür entwickelte Fragebogen enthielt neben den Angaben über Geschlecht, Alter, Staatsangehörigkeit, Beruf, Schulabschluß, Familienstand, Wohnort (Stadtteil) und Vereinsmitgliedschaft unter anderem Fragen nach Verbindungen oder der Zugehörigkeit zu bestimmten Gruppierungen, wie z. B. Drogenabhängige, Alkoholiker, Straffällige, Neo-Nazis, Hausbesetzer sowie die Frage nach dem Verhältnis zu den Eltern. Die Fragebogen wurden über die Schulen verteilt und sollten ausgefüllt über die Klassensprecher und die Vertrauenslehrer zurückgegeben werden.

Bei dieser Fragebogenaktion handelte es sich um die Erhebung personenbezogener Daten, da Betroffene auf Grund der erhobenen Angaben zumindest mit dem beim Jugendamt bereits vorhandenen Zusatzwissen bestimmbar waren. Gegen diese Befragung bestanden sowohl inhaltlich als auch hinsichtlich des Verfahrens erhebliche datenschutzrechtliche Bedenken. Insbesondere mit den Fragen nach Verbindungen oder der Zugehörigkeit zu den genannten Gruppierungen sowie mit der Frage nach dem Verhältnis zu den Eltern wird in einer nach meiner Auffassung nicht mehr zumutbaren Weise in die Intimsphä-

re der Befragten eingedrungen und zugleich deren Persönlichkeitsrecht verletzt. Die Frage nach der Zugehörigkeit zu bestimmten Gruppierungen stellt überdies eine **Aufforderung zur Selbstbezichtigung** dar, die schlechterdings unzulässig ist. Mit derartigen Fragen wird die vom Bundesverfassungsgericht (vgl. BVerfGE 65, 1, 46) gezogene Grenze für eine zulässige Datenerhebung eindeutig überschritten. Dies gilt unabhängig davon, ob die Befragung auf freiwilliger Grundlage erfolgte. Die Erhebung dieser Daten ist daher unzulässig. Unzulässig erhobene Daten sind zu löschen.

Außerdem wurde durch das vorgesehene Verfahren, die Fragebogen über die Klassensprecher an die Vertrauenslehrer zurückzugeben, diesen Personen die Möglichkeit der Kenntnisnahme von dem Inhalt der Fragebogen eröffnet. Ein solches Verfahren verstößt gegen die aus dem Recht der Befragten auf informationelle Selbstbestimmung folgende Verpflichtung, verfahrensrechtliche Vorkehrungen zum Schutze dieses Grundrechts zu treffen.

Auf meine Empfehlung hat das Jugendamt die Fragebogen ohne Auswertung vernichtet.

6.5.6 Gewährung von Sachleistungen

Presseberichten war zu entnehmen, daß Sozialämter dazu übergegangen seien, einmalige Beihilfen als Sachleistung zu gewähren, indem sie zwecks Kostenersparnis Großhandelsrabatte mit Lieferfirmen aushandeln, dabei als Besteller auftreten und die **Anschrift des Hilfeempfängers als Lieferadresse** angeben. Bei diesem Verfahren offenbaren die Sozialämter gegenüber den Lieferfirmen die Tatsache des Sozialhilfebezuges durch den Hilfeempfänger, ohne daß dies zur Aufgabenerfüllung nach dem Sozialgesetzbuch erforderlich wäre.

Sozialhilfe kann als persönliche Hilfe, als Geldleistung oder als Sachleistung gewährt werden (§ 8 Abs. 1 BSHG). Über Form und Maß der Sozialhilfe entscheidet der Sozialleistungsträger nach pflichtgemäßem Ermessen (§ 4 Abs. 2 BSHG). Dieses dem Sozialleistungsträger eingeräumte Ermessen bei der Wahl der Form der Sozialhilfe ist jedoch nicht frei, sondern an die Zweckbestimmung der Hilfe gebunden. Aufgabe der Sozialhilfe ist es, dem Empfänger der Hilfe die Führung eines Lebens zu ermöglichen, das der Würde des Menschen entspricht (§ 1 Abs. 2 Satz 1 BSHG).

Zur Führung eines menschenwürdigen Lebens gehört, daß dem erwachsenen Menschen die Möglichkeit gelassen wird, im Rahmen der ihm nach dem Gesetz zustehenden Mittel seine Bedarfsdeckung frei zu gestalten. Dem wird der Sozialhilfeträger dadurch gerecht, daß er die Hilfe zum Lebensunterhalt in der ganz überwiegenden Mehrzahl der Fälle, soweit nicht konkrete Anhaltspunkte für eine zweckwidrige Verwendung der bewilligten Hilfe bestehen, in Geld gewährt, das dem Hilfeempfänger im ganzen ausgezahlt wird. Nur so kann der Betroffene selbst frei bestimmen, was und/oder wo er einkauft.

Soweit Leistungsträger statt dessen dazu übergehen, Sachleistungen zu gewähren, indem sie zwecks Kostenersparnis Großhandelsrabatte mit Lieferfir-

men aushandeln, dabei als Besteller auftreten und die Anschrift des Hilfeempfängers als Lieferadresse angeben, läuft ein solches Verfahren der gesetzlich definierten Aufgabe der Sozialhilfe zuwider. Zwar sind die Leistungsträger nach der Gemeindeordnung gehalten, die Haushaltswirtschaft sparsam und wirtschaftlich zu führen. Diese Verpflichtung findet jedoch ihre Grenze an dem im Bundessozialhilfegesetz konkretisierten Verfassungsgebot des Schutzes der Menschenwürde (Artikel 1 Abs. 1 des Grundgesetzes). Zur Erfüllung der genannten gesetzlichen Aufgabe des Leistungsträgers ist es nicht erforderlich, Dritten personenbezogene Daten des Hilfeempfängers zu offenbaren.

Diese gesetzlichen und verfassungsrechtlichen Vorgaben können nicht dadurch umgangen werden, daß dem Betroffenen die Einwilligung in die Weitergabe seiner Anschrift als Lieferadresse abverlangt wird, um statt Geldleistungen Sachleistungen gewähren zu können. Im übrigen bestehen erhebliche Bedenken gegen die Rechtswirksamkeit einer solchen Einwilligung. Eine wirkliche Einwilligung setzt Freiwilligkeit voraus. Daran bestehen hier aber Zweifel, weil sich der Betroffene unter Druck gesetzt fühlen könnte, die Einwilligung zu erteilen. Damit wäre er in seiner Entscheidung nicht mehr frei.

Bedenken bestehen in gleicher Weise gegen die Praxis einiger Sozialämter, den Hilfeempfänger zu einer **Selbstoffenbarung** zu veranlassen, indem sie ihm Berechtigungsscheine mit seinem Namen und dem Sozialamt als Aussteller aushändigen oder dem Leistungsbescheid Kostenübernahmeerklärungen beifügen, damit der Betroffene die Lieferfirma veranlaßt, die Ware bei ihm anzuliefern und die Rechnung an das Sozialamt zu übersenden.

Auch in den Fällen, in denen ausnahmsweise eine Geldleistung wegen Vorliegens besonderer Gründe, wie z. B. wegen der Gefahr einer mißbräuchlichen Verwendung von Sozialleistungen, ausgeschlossen ist und deshalb Sachleistungen in Form von Gutscheinen oder Kostenübernahmeerklärungen gewährt werden, hat der Sozialleistungsträger seine Verpflichtung zur Wahrung des Sozialgeheimnisses zu beachten. Zwar findet eine Offenbarung durch den Leistungsträger nicht statt, da der Gutschein oder die Kostenübernahmeerklärung keinem Dritten, sondern dem Betroffenen selbst ausgehändigt wird. Aus der Verpflichtung des Leistungsträgers zur Wahrung des Sozialgeheimnisses kann jedoch ein Anspruch des Betroffenen hergeleitet werden, die Warengutscheine und die Kostenübernahmeerklärungen so auszustellen, daß das Sozialamt nicht als Aussteller erkennbar ist. Ebensowenig darf der Name des Hilfeempfängers vermerkt sein. Demnach ist festzuhalten, daß bei der Gewährung von Sachleistungen anstelle von Geldleistungen ein Verfahren zu wählen ist, bei dem der Sozialhilfebezug des Betroffenen gegenüber Dritten nicht offenbart werden muß.

6.5.7 Verwendungszweck auf Überweisungsträgern

In meinem 6. Tätigkeitsbericht (S. 69) hatte ich darauf hingewiesen, daß das Verwaltungsgericht Düsseldorf (NJW 1985, 1794) es für unzulässig erachtet hat, bei Zahlungen nach dem Bundessozialhilfegesetz an den Betroffenen auf

Überweisungsträgern außer der Angabe des Empfängers, des Datums des Leistungsbescheides, des Leistungszeitraumes und des anonymisierten Aktenzeichens, in dem die Amtsgliederungsziffer enthalten sein darf, und des Absenders weitere Angaben hinzuzufügen, durch die die Geldleistung als Sozialleistung erkennbar wird. Damit wurde der von mir vertretenen Rechtsauffassung zur Unzulässigkeit der **Angabe des Verwendungszwecks** auf dem Überweisungsträger bei Auszahlung von Sozialleistungen Rechnung getragen, allerdings mit der Einschränkung, daß ich nach wie vor Bedenken gegen die Angabe der Amtsgliederungsziffer habe, da hierdurch Dritten das Amt und damit der Zweck der Leistung bekannt wird.

Der Minister für Arbeit, Gesundheit und Soziales hat im Hinblick auf die Entscheidung des Verwaltungsgerichts Düsseldorf mit Erlaß vom 18. Oktober 1985 gegenüber den Sozialhilfeträgern angeregt, bei der Überweisung von Sozialleistungen auf Bezeichnungen wie Sozialhilfe, Hilfe zum Lebensunterhalt, einmalige Beihilfe, Pflegegeld o. ä. zu verzichten und ein anonymisiertes Aktenzeichen anzugeben.

Dennoch erreichen mich immer wieder Eingaben von Betroffenen, die sich dagegen wehren, daß Sozialleistungsträger den Verwendungszweck wie z. B. „Sozialleistung", „Wohngeld" auf dem Überweisungsträger oder der Postanweisung angeben. In einem Fall war ich sogar gehalten, dieses Verfahren förmlich zu beanstanden.

Die Sozialleistungsträger machen geltend, daß das genannte Urteil des Verwaltungsgerichts Düsseldorf nicht rechtskräftig geworden, sondern vom Berufungsgericht für wirkungslos erklärt worden sei. Dabei wird jedoch übersehen, daß das Urteil lediglich aus verfahrensrechtlichen Gründen nicht rechtskräftig geworden ist. Somit kann es weiterhin zur Stützung meiner Rechtsauffassung herangezogen werden.

Ein Oberstadtdirektor, der an sich bereit war, meiner Auffassung zu folgen, wies mich darauf hin, daß die **Wohngeldstelle** das Zahlungsverfahren über die Oberfinanzkasse abwickele und somit an das vom Minister für Stadtentwicklung, Wohnen und Verkehr eingeführte landeseinheitliche Verfahren gebunden sei. Danach war die Angabe „Wohngeld" auf dem Überweisungsträger vorgesehen. Der Minister für Stadtentwicklung, Wohnen und Verkehr hat nach anfänglichen Zweifeln an der Anwendbarkeit des oben genannten Urteils auf alle Sozialleistungen meinen Bedenken Rechnung getragen und das Landesamt für Datenverarbeitung und Statistik (LDS) um Prüfung gebeten, wie der Verwendungszweck anonymisiert werden kann. Mit dem Vorschlag des LDS, auf dem Überweisungsträger den Begriff „Wohngeld" durch ein der Wohngeldnummer nachgestelltes „W" zu ersetzen, habe ich mich unter der Voraussetzung einverstanden erklärt, daß nur die Wohngeldnummer angegeben wird. Auf das nachgestellte „W" muß verzichtet werden, da es die Art der Leistung erkennbar macht.

6.5.8 Schutz des Sozialgeheimnisses gegenüber Gerichten

Fälle aus der Praxis zeigen immer wieder, daß Gerichte die Tragweite des Sozialdatenschutzes verkennen, indem sie auch bei fehlender gesetzlicher Offenbarungsbefugnis darauf bestehen, daß ihnen Verwaltungsakten für ihre Aufgabenerfüllung übersandt werden. So hatte im Rahmen eines Sorgerechtsverfahrens das zuständige Gericht die persönliche Eignung des Vaters zu prüfen. Dem Gericht lagen Erkenntnisse darüber vor, daß der Betroffene vor etwa 13 Jahren straffällig geworden und ihm deshalb Jugendgerichtshilfe gewährt worden war.

Dem Ersuchen des Gerichts an das Jugendamt auf Übersendung der Jugendgerichtshilfeakte durfte nicht entsprochen werden, weil eine Aufgabe des Jugendamtes nach dem Sozialgesetzbuch, zu deren Erfüllung die Offenbarung der in der Akte festgehaltenen personenbezogenen Daten des Betroffenen erforderlich gewesen sein könnte, hier nicht vorlag. Dabei hat außer acht zu bleiben, daß die Kenntnis des Akteninhalts für das Gericht möglicherweise entscheidungserheblich war. Nach § 35 Abs. 3 SGB I besteht, soweit eine Offenbarung von Sozialdaten nicht zulässig ist, keine Pflicht zur Vorlage von Akten. Damit ist das Sozialgeheimnis, soweit eine gesetzliche Offenbarungsbefugnis (§§ 67 bis 77 SGB X) nicht vorliegt, **gerichtsfest.**

Der Auffassung des Landessozialgerichts Essen (Urteil vom 21. 7. 1982 – L 8 J 18/80 –), § 35 SGB I i.V.m. §§ 67 ff. SGB X regele nur den Schutz der Sozialdaten in Verwaltungsverfahren der Sozialleistungsträger, wie auch der neuerdings von Haus (NJW 1988, 3126 ff.) vertretenen Auffassung, die in den §§ 35 SGB I, 67 ff. SGB X statuierte partielle Informationssperre habe keinen Einfluß auf gerichtliche Sachverhaltsermittlungen, kann nicht gefolgt werden. Der Gesetzgeber hat hier eine abschließende Regelung für die Befugnis zur Offenbarung von Sozialdaten getroffen. Andere Vorschriften, insbesondere des gerichtlichen Verfahrens, greifen daneben nicht durch (vgl. Ausschußbericht, Bundestagsdrucksache 8/4022, S. 84). § 35 Abs. 3 SGB I dient deshalb nur der Klarstellung; er verdeutlicht die Tragweite der Absätze 1 und 2 insbesondere im Hinblick auf das gerichtliche Verfahren (Ausschußbericht a.a.O., S. 96). Den Gerichten bleibt in solchen Fällen nur der Weg, die Einwilligung des Betroffenen in die Aktenübersendung einzuholen (§ 67 SGB X). Entsprechend ist auch im vorliegenden Fall letztlich verfahren worden, wobei das Jugendamt die Akte, soweit sie Angaben über Dritte enthielt, in anonymisierter Form dem Gericht übersandt hat.

6.5.9 Bekanntgabe von Unterhaltsleistungen

Förmlich beanstanden mußte ich, daß ein Sozialamt der Hilfeempfängerin trotz Überleitung des Unterhaltsanspruchs auf sich die Höhe des von ihrem Sohn zu leistenden Unterhaltsbeitrages mitgeteilt hatte. Das Sozialamt war der Ansicht, die Hilfeempfängerin habe Anspruch darauf, die Nettoaufwendungen der Sozialhilfe zu erfahren. Zudem hätten Unterhaltsberechtigte nach den Vorschriften des Bürgerlichen Gesetzbuchs das Recht, Auskünfte über die Einkommens- und Vermögensverhältnisse von Unterhaltspflichtigen zu verlangen.

Die nach den Vorschriften des Bundessozialhilfegesetzes zulässige Überleitung des Unterhaltsanspruchs der Hilfeempfängerin auf das Sozialamt hatte zur Folge, daß der Hilfeempfängerin die Sozialhilfe in ungekürzter Höhe zu gewähren war. Da ihr somit die Sozialhilfe nicht um den Unterhaltsbeitrag des Unterhaltspflichtigen gekürzt wurde, war es auch nicht erforderlich, ihr dessen Höhe mitzuteilen.

Ein gesetzlicher Anspruch der Hilfeempfängerin auf Mitteilung der Nettoaufwendungen der Sozialhilfe bestand nicht. Zwar trifft es zu, daß der Unterhaltsberechtigte nach dem Bürgerlichen Gesetzbuch einen Anspruch auf Auskunft über die Einkommens- und Vermögensverhältnisse des Unterhaltspflichtigen hat. Diesen Auskunftsanspruch zu erfüllen, ist jedoch grundsätzlich nicht Aufgabe des Sozialleistungsträgers nach dem Sozialgesetzbuch.

6.6 Gesundheitswesen

6.6.1 AIDS

Durch Presseberichte wurde mir bekannt, daß die Medizinischen Einrichtungen einer Universität bis Mitte 1987 HIV-Tests bei Patienten und Mitarbeitern ohne deren Einwilligung durchgeführt haben. Außerdem hatte ein Patient einer städtischen Krankenanstalt bei Prüfung der Ergebnisse seiner Blutanalyse festgestellt, daß während seines eintägigen stationären Aufenthalts ohne seine Einwilligung ein AIDS-Test vorgenommen worden war.

Die Verwendung einer Blutprobe zum Zwecke der Durchführung einer **HIV-Untersuchung ohne Einwilligung** des Betroffenen stellt eine Erhebung personenbezogener Daten dar und bedarf als Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen wie auch in sein Grundrecht auf Datenschutz einer gesetzlichen Grundlage. Eine solche war für die Durchführung einer HIV-Untersuchung nicht vorhanden. Auch der mit den Patienten geschlossene Behandlungsvertrag, der lediglich Maßnahmen zum Zwecke der Behandlung zuläßt, rechtfertigte diese Datenerhebung nicht. Sie war somit nur mit ausdrücklicher Einwilligung des Betroffenen zulässig. Daten, deren Erhebung unzulässig war, sind zu löschen. Dies gilt sowohl nach dem zum Zeitpunkt der Datenerhebung geltenden Recht (vgl. 1. Tätigkeitsbericht, S. 20) wie auch nach § 19 Abs. 3 Satz 1 Buchstabe a DSG NW. Auf meine Empfehlung haben die städtischen Krankenanstalten die Angaben über die HIV-Untersuchung in den Patientenunterlagen gelöscht.

Bei den Medizinischen Einrichtungen der Universität wäre eine Löschung angesichts von jährlich 44 000 stationär und etwa 80 000 ambulant behandelten Patienten mit einem unverhältnismäßigen organisatorischen Aufwand verbunden gewesen. Ähnliche Schwierigkeiten bestanden bei der Löschung von HIV-Testergebnissen der Mitarbeiter, weil das nach dem Geburtsdatum aufgebaute Gesamtarchiv wegen der Aufbewahrungsfrist bis zum 70. Lebensjahr der Betroffenen auf etwa 80 000 Akten angewachsen war. Im Hinblick auf diese besonderen Umstände habe ich den Medizinischen Einrichtungen empfohlen,

- Angaben über den HIV-Test in den Krankenakten der Patienten zu löschen, wenn der Patient es verlangt oder wenn seine Krankenakte bei erneuter Behandlung – durch die Medizinischen Einrichtungen der Universität oder eine andere Stelle – beigezogen wird, es sei denn, daß der Patient ein Verbleiben der Angaben in der Akte wünscht;
- Angaben über den HIV-Test in den Gesundheitsakten der noch beschäftigten Mitarbeiter im Hochschulklinikbereich auf Verlangen des Betroffenen, spätestens bei der nächsten arbeitsmedizinischen Vorsorgeuntersuchung zu löschen, es sei denn, daß der Betroffene ein Verbleiben der Angaben in der Akte wünscht;
- Angaben über den HIV-Test in den Gesundheitsakten ehemaliger Mitarbeiter auf Verlangen des Betroffenen oder vor einer erneuten Verwendung oder Weitergabe der Akten zu löschen, es sei denn, daß der Betroffene ein Verbleiben der Angaben in der Akte wünscht.

In einem weiteren Fall bat mich ein Bürger um Hilfe, der sich freiwillig einem HIV-Test (mit negativem Ergebnis) in einer Universitäts-Hautklinik unterzogen hatte. Dabei sei ihm ausdrücklich Anonymität zugesichert worden. Gleichwohl habe ihn die Klinik später zu einem neuerlichen Test aufgefordert. Daraufhin begehrte er die **Löschung** seines Namens und seiner Anschrift in den ärztlichen Unterlagen. Die Klinik bestritt, dem Betroffenen eine über die ärztliche Schweigepflicht hinausgehende Anonymität zugesichert zu haben, und berief sich auf die ärztliche Dokumentationspflicht.

Nach der Rechtsprechung (BGH NJW 1978, 2337) stellt eine ordnungsgemäße Dokumentation über die Behandlung des Patienten nicht, wie früher angenommen wurde, allein eine im Belieben des Arztes stehende Gedächtnisstütze dar, sondern wird dem Patienten als Bestandteil einer sorgfältigen Behandlung vom Arzt geschuldet. Die Dokumentationspflicht wird aus dem Behandlungsvertrag als selbständige vertragliche Nebenpflicht abgeleitet.

Auf der Grundlage dieser Rechtsprechung muß es als zulässig angesehen werden, wenn die Parteien des Behandlungsvertrages nach Abschluß der Behandlung vereinbaren, die Unterlagen zu vernichten. Voraussetzung hierfür wird allerdings sein müssen, daß der Patient auf mögliche Ansprüche aus dem Behandlungsvertrag verzichtet.

Deshalb habe ich dem Betroffenen vorgeschlagen, der Klinik den Abschluß einer Vereinbarung über die Löschung seines Namens und seiner Anschrift in den Aufzeichnungen über seine Untersuchung unter gleichzeitigem Verzicht auf mögliche Ansprüche aus dem Behandlungsvertrag anzubieten. Nachdem der Betroffene auf meinen Vorschlag eingegangen war, habe ich die Klinik darauf hingewiesen, daß sie im Hinblick auf das Recht des Betroffenen auf informationelle Selbstbestimmung gehalten sei, das Angebot des Betroffenen anzunehmen, und ihr empfohlen, nach Abschluß dieser Vereinbarung Namen und Anschrift des Betroffenen in den Klinikunterlagen zu löschen, sofern sie es nicht vorziehe, die Aufzeichnungen über die Untersuchung insgesamt zu vernichten. Die Klinik hat inzwischen die Daten des Betroffenen gelöscht.

6.6.2 Amtsärztliche Untersuchungen im öffentlichen Dienst

Mehrere Eingaben richteten sich gegen den anläßlich der Einstellung in den öffentlichen Dienst des Landes wie auch der kommunalen Gebietskörperschaften bei der amtsärztlichen Untersuchung verwendeten Fragebogen. Mit den darin enthaltenen umfangreichen **„Angaben zur Vorgeschichte"** wird der Betroffene gezwungen, sich gezielt zum Vorliegen bestimmter Krankheiten, auch in seinem engeren Familienkreis, sowie zu jetzigen Beschwerden oder Erkrankungen zu äußern. So soll er z. B. Suchtkrankheiten, Nerven- oder Geisteskrankheiten, auch Selbstmord/-versuche offenbaren. Zur eigenen Vorgeschichte hat er z. B. auch frühere Geschlechtskrankheiten, körperliche/geistige/seelische Behinderungen anzugeben. Hinsichtlich seiner derzeitigen Beschwerden soll der Betroffene Angaben über Stimmungs- und Antriebsschwankungen sowie über die derzeit von ihm eingenommenen Medikamente und die tägliche Menge der konsumierten alkoholischen Getränke und Tabakwaren machen. Außerdem hat der Betroffene seine behandelnden Ärzte (auch für die Vergangenheit) zu benennen.

Der Fragebogen ist Bestandteil des Runderlasses des Ministers für Arbeit, Gesundheit und Soziales vom 05. 08. 1985 (SMBl. 20307), durch den der Runderlaß des Innenministers vom 11. 07. 1966 geändert worden ist. Danach ist der Fragebogen (Anlage 2 des Runderlasses) bei amtsärztlichen Untersuchungen von Landesbediensteten zu verwenden. Für die amtsärztliche Untersuchung von Kommunalbediensteten wird seine Anwendung empfohlen.

Wenngleich sich medizinische Fragen einer datenschutzrechtlichen Beurteilung grundsätzlich entziehen, habe ich dennoch Zweifel, ob derart sensible Angaben, deren Erhebung tief in die Privatsphäre eindringt, für den Betroffenen zumutbar sind und dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz noch entsprechen. Im übrigen werden auch aus ärztlicher Sicht erhebliche Bedenken gegen diese Fragestellungen erhoben (vgl. Rhein. Ärztebl. 1986, 824).

Für bedenklich halte ich im übrigen auch die in der Anlage 2 des Runderlasses enthaltene Erklärung des Betroffenen, durch die er die behandelnden und begutachtenden Ärzte von ihrer Schweigepflicht entbindet und in die leihweise Überlassung vorhandener Unterlagen zur Befundauswertung durch das Gesundheitsamt sowie darin einwilligt, daß das vollständige Gutachten dem Auftraggeber bekanntgegeben werden kann.

Die Entbindung aller in der Anlage 2 des Runderlasses aufgeführten behandelnden und begutachtenden Ärzte von der Schweigepflicht ohne zeitliche Begrenzung und die damit verbundene Möglichkeit, bei allen angegebenen Krankheiten die ärztlichen Unterlagen anzufordern, eröffnet eine nahezu unbegrenzte **Ausforschung** der gesundheitlichen Verhältnisse des Betroffenen, die gemessen an dem Zweck der Untersuchung überzogen ist.

Im übrigen kann hier von einer wirklichen Einwilligung in die Bekanntgabe des vollständigen Gutachtens an den Auftraggeber nicht die Rede sein. Denn Bewerber, die den Amtsarzt nicht von der ärztlichen Schweigepflicht gegen-

über der personalbewirtschaftenden Stelle entbinden, werden im Regelfall nicht eingestellt, wie ich der Antwort der Landesregierung (Drucksache 10/2546) auf die Kleine Anfrage 964 entnommen habe. Eine wirkliche Einwilligung setzt Freiwilligkeit voraus. Der Betroffene muß demnach aus freiem Entschluß, ohne – auch indirekten – Zwang und ohne Rechtsnachteile befürchten zu müssen, die Einwilligung erteilen. Diese Voraussetzungen liegen hier nicht vor.

Vielmehr hat der Bewerber seine gesundheitliche Eignung durch ein Zeugnis des Gesundheitsamtes nachzuweisen. Dementsprechend besteht für ihn die Obliegenheit, einer Bekanntgabe derjenigen personenbezogenen Daten zuzustimmen, deren Kenntnis unter Beachtung des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes für die Entscheidung über seine Einstellung erforderlich ist. Dies kann im Extremfall das gesamte Gutachten sein, allerdings mit Ausnahme der Familienanamnese. Ist der Bewerber mit der Bekanntgabe dieser Daten an die personalbewirtschaftende Stelle nicht einverstanden, versagt er also seine Zustimmung, so muß er damit rechnen, nicht eingestellt zu werden. Hierauf muß der Bewerber hingewiesen werden. Entsprechend sind bei amtsärztlichen Untersuchungen von Bediensteten diese auf die ihnen aus der Verweigerung der Zustimmung entstehenden Rechtsnachteile hinzuweisen.

Nach Nr. 5 des Runderlasses ist das Ergebnis einer angeordneten ärztlichen Untersuchung oder Begutachtung dem Untersuchten von dem Gesundheitsamt nicht bekanntzugeben; der Dienstvorgesetzte des Untersuchten entscheidet, ob und zu welchem Zeitpunkt dem Untersuchten das Ergebnis mitzuteilen ist oder ihm zugänglich gemacht werden kann. Diese Regelung ist mit § 18 DSG NW, wonach der Betroffene grundsätzlich einen Rechtsanspruch auf Auskunft und Akteneinsicht hat, nicht vereinbar.
Ich habe dem Minister für Arbeit, Gesundheit und Soziales empfohlen,

- den Runderlaß vom 11. 07. 1966 unter Berücksichtigung meiner Ausführungen zu überarbeiten;
- den Bewerber darauf hinzuweisen, daß er im Falle der Nichterteilung des Einverständnisses mit der Bekanntgabe des vollständigen Gutachtens an den Auftraggeber damit rechnen muß, nicht eingestellt zu werden;
- den Bediensteten auf die ihm aus der Verweigerung seiner Zustimmung zur Bekanntgabe seiner Daten an die personalbewirtschaftende Stelle entstehenden Rechtsnachteile hinzuweisen.

6.6.3 Fortschreibung von Untersuchungsdaten

In meinem 8. Tätigkeitsbericht (S. 76) habe ich darauf hingewiesen, daß die Praxis der Gesundheitsämter, die über die Vorsorgeuntersuchungen im Kindergarten geführte Karteikarte mit anläßlich der Einschulungs- und der Schulentlassungsuntersuchung erhobenen Daten fortzuschreiben, eine **Zweckentfremdung** darstellt, für die die erforderliche gesetzliche Grundlage derzeit fehlt. Demgegenüber vertritt die Landesregierung in ihrer Stellungnahme zu meinem 8. Tätigkeitsbericht (Drucksache 10/2676, S. 39/40) die Auffassung,

die Vorsorgeuntersuchung im Kindergarten und die Einschulungsuntersuchung dienten demselben Zweck, nämlich etwaige Krankheiten aufzudecken und sie einer Behandlung zuzuführen.

Ich habe daraufhin gegenüber dem Minister für Arbeit, Gesundheit und Soziales förmlich beanstandet, daß er das Recht auf informationelle Selbstbestimmung sowie das Grundrecht auf Datenschutz verletzt, indem er es ablehnt, die Gesundheitsämter darauf hinzuweisen, daß bis zur Schaffung einer entsprechenden gesetzlichen Grundlage die Daten der Vorsorgeuntersuchung im Kindergarten nicht für Zwecke der Einschulungs- und der Schulentlassungsuntersuchung verwendet werden dürfen. Entgegen der Auffassung der Landesregierung dienen die Vorsorgeuntersuchung im Kindergarten und die Untersuchungen im Rahmen der Schulgesundheitspflege nicht demselben Zweck.

Die Vorsorgeuntersuchungen im Kindergarten nach § 12 Abs. 2 des Kindergartengesetzes (KgG) bezwecken den Schutz der Kinder im Kindergarten vor übertragbaren Krankheiten sowie die frühzeitige Erkennung und Behandlung von gesundheitlichen Gefährdungen und Erkrankungen, insbesondere die Früherkennung von Behinderungen (vgl. Künzel/Moskal, Kindergartengesetz Nordrhein-Westfalen, Kommentar, 11. Aufl. Erl. II, III zu § 12). Demgegenüber dient die Einschulungsuntersuchung primär einem anderen Zweck. Nach § 3 Abs. 2 Satz 1 der Verordnung über den Bildungsgang in der Grundschule (AO-GS) entscheidet der Schulleiter auf Grund einer Untersuchung durch den vom Gesundheitsamt bestellten Schularzt über die Aufnahme in die Schule. Die schulärztliche Untersuchung umfaßt die Feststellung des körperlichen Entwicklungsstandes und die Beurteilung der allgemeinen, gesundheitlich bedingten Leistungsfähigkeit einschließlich der Sinnesorgane (§ 3 Abs. 2 Satz 2 AO-GS). Nach § 4 Abs. 1 Satz 1 Buchstabe a AO-GS stellt der Schulleiter auf Grund von § 4 des Schulpflichtgesetzes ein schulpflichtiges Kind für ein Jahr vom Schulbesuch zurück, wenn das Gutachten des Schularztes erhebliche Bedenken gegen die Einschulung geltend macht. Aus diesen Vorschriften ergibt sich, daß die Einschulungsuntersuchung in erster Linie der Feststellung der Schulreife des Kindes, nicht der Erkennung von Krankheiten dient. Entsprechendes gilt für die Schulentlassungsuntersuchung, die, soweit sie überhaupt durchgeführt wird, Aufschluß über die körperliche Berufseignung geben soll.

Die Vorschriften des Gesetzes über die Vereinheitlichung des Gesundheitswesens und die hierzu ergangenen Durchführungsverordnungen können als Rechtsgrundlage für die Fortschreibung der bei der Vorsorgeuntersuchung im Kindergarten erhobenen Daten mit den im Rahmen der Schulgesundheitspflege erhobenen Daten nicht herangezogen werden. Es mag dahinstehen, ob sich aus diesen Vorschriften eine gemeinsame Zweckrichtung ergibt. Jedenfalls enthalten sie keine normenklare Regelung für die Verwendung der Daten.

Auf Nr. 2.6 des Runderlasses des Kultusministers und des Ministers für Arbeit, Gesundheit und Soziales vom 4. April 1975, wonach Untersuchungsbefunde aus vorhergehender ärztlicher Kindergartenbetreuung so weit wie möglich her-

anzuziehen und bei der Beurteilung ergänzend zu berücksichtigen sind, kann die Fortschreibung der anläßlich der Vorsorgeuntersuchung im Kindergarten erhobenen Daten mit anläßlich der Einschulungs- und der Schulentlassungsuntersuchung erhobenen Daten nicht gestützt werden, da Verwaltungsvorschriften keine gesetzliche Grundlage sind.

In seiner Erwiderung hat der Minister für Arbeit, Gesundheit und Soziales die Auffassung vertreten, daß die allgemeinen gesundheits- und jugendpolitischen Zwecke der ärztlichen Untersuchungen in Kindergärten und Schulen nicht unberücksichtigt bleiben dürfen. Dem muß ich entgegenhalten, daß angesichts der vorhandenen normenklaren bereichspezifischen Vorschriften im Kindergartengesetz, in der Verordnung über den Bildungsgang in der Grundschule und im Schulpflichtgesetz nicht auf allgemeine gesundheits- und jugendpolitische Zwecke der ärztlichen Untersuchungen abgehoben werden kann, um damit einen Eingriff in Grundrechte der Betroffenen zu rechtfertigen. Im übrigen ist auf die Unterschiede zwischen den Aufgaben des Gesundheitsamtes und dem Tätigkeitsfeld behandelnder Ärzte hinzuweisen.

6.6.4 Unzulässige Verwendung medizinischer Gutachten

Ein Arzt beschwerte sich darüber, daß die Ärzteversorgung ein von ihr für die Entscheidung über den Antrag des Betroffenen auf Gewährung einer Berufsunfähigkeitsrente eingeholtes medizinisches Gutachten an die Ärztekammer weitergegeben hatte. Die Ärztekammer hatte ihrerseits das Gutachten zwecks Einleitung eines Verfahrens zum Widerruf der Approbation an die zuständige Bezirksregierung weitergeleitet.

Wenngleich es sich bei der Ärzteversorgung um eine Einrichtung der Ärztekammer handelt, so ist für den Austausch personenbezogener Daten zwischen diesen Stellen eine gesetzliche Grundlage erforderlich. Denn aus der Einheit der Verwaltung der Ärztekammer folgt keine informationelle Einheit; der Grundsatz der informationellen Gewaltenteilung gilt auch innerhalb der Ärztekammer (vgl. BVerfG NJW 1988, 959).

Eine gesetzliche Grundlage für die Weitergabe des Gutachtens war hier nicht vorhanden. Die Weitergabe konnte – ungeachtet mangelnder Normenklarheit – weder auf die Vorschriften des Heilberufsgesetzes (HeilberG) noch auf die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen in der damals geltenden Fassung gestützt werden, weil die in § 5 HeilberG genannten Aufgaben nicht solche der Ärzteversorgung sind und § 11 DSG NW nur für die Übermittlung personenbezogener Daten aus Dateien galt.

Da somit das medizinische Gutachten unter Verletzung des informationellen Selbstbestimmungsrechts wie auch des Grundrechts auf Datenschutz an die Ärztekammer weitergegeben worden war, unterlag es dort einem **Verwendungsverbot** mit der Folge, daß die Ärztekammer das Gutachten nicht ihrerseits an die Bezirksregierung hätte weiterleiten dürfen. Überdies konnten auch die Aufgaben der Ärztekammer nach § 5 Abs. 1 Buchstabe a HeilberG die Weitergabe an die Bezirksregierung nicht rechtfertigen. Aus der dort allge-

mein geregelten Unterstützungspflicht ist für den Betroffenen auch nicht andeutungsweise erkennbar, daß ein medizinisches Gutachten, welches für einen ganz bestimmten Zweck, nämlich die Entscheidung über die Gewährung einer Berufsunfähigkeitsrente, eingeholt wurde, für einen anderen Zweck, nämlich die Einleitung eines Verfahrens zum Widerruf der Approbation, verwendet wird.

Da das medizinische Gutachten aus den genannten Gründen auch bei der Bezirksregierung als unberechtigtem Letztempfänger einem Verwertungsverbot unterlag, hatte die Ärzteversorgung sie hierauf hinzuweisen und im Hinblick auf den aus dem Grundrechtsverstoß sich ergebenden **Folgenbeseitigungsanspruch** des Betroffenen das Gutachten von der Bezirksregierung zurückzuverlangen. Dies ist meiner Empfehlung entsprechend geschehen.

6.6.5 Epidemiologische Forschung

Von Epidemiologen wird in der Öffentlichkeit wieder verstärkt der Vorwurf erhoben, der Datenschutz verhindere die Forschung. Ein großer Teil medizinischer Untersuchungen sei heute in der Bundesrepublik Deutschland auf Grund der Datenschutzbestimmungen nicht mehr durchführbar. Damit lebt eine bereits vor Jahren geführte Diskussion über das Spannungsverhältnis zwischen Forschung und Datenschutz wieder auf (vgl. 4. Tätigkeitsbericht, S. 75).

Zwischen Forschungsfreiheit (Artikel 5 Abs. 3 GG) und informationeller Selbstbestimmung (Artikel 2 Abs. 1, Artikel 1 Abs. 1 GG) besteht ein **Zielkonflikt,** der einen Ausgleich im Wege einer Güterabwägung erfordert. Statt der abwegigen Alternative „Datenschutz **oder** Forschung" muß es heißen: Durchführung der Forschung unter Beachtung der Grundsätze und Einzelbedingungen des Datenschutzes. Der Anspruch des einzelnen Betroffenen auf Schutz seiner Individualsphäre gebietet das Einschreiten der Datenschutzbeauftragten, wenn Forschung einseitig zu Lasten der Persönlichkeitsrechte der Patienten betrieben wird. Vor dem Hintergrund moderner Informationstechnologie sollte Datenschutz nicht als Behinderung von Wissenschaft und Forschung, sondern als Instrument gesehen werden, mit dem Informationsflüsse im wohlverstandenen Interesse der Bürger reguliert werden. Der Widerstreit zwischen Forschung und Datenschutz stellt den Verantwortlichen die Aufgabe, einen Weg zu finden, der Forschungsziele nicht beeinträchtigt und gleichzeitig dem berechtigten Verlangen der Betroffenen nach Wahrung ihrer Persönlichkeitsrechte gerecht wird. Der Forschende muß sich bewußt sein, daß auch die Methoden der Informationsbeschaffung und -verarbeitung zu Forschungszwekken den Bedingungen der Eignung, Erforderlichkeit und Verhältnismäßigkeit der Mittel unterworfen sind.

Daraus folgt, daß die Erhebung und Verarbeitung anonymisierter Daten eindeutig den Vorzug gegenüber dem Zugriff auf personenbezogene Daten verdient. Der Zugriff auf personenbezogene Daten ist stets subsidiär. Nach dem Volkszählungsurteil ist sogar bei der Erhebung von Einzelangaben für **statistische** Zwecke zu prüfen, ob das Ziel der Erhebung nicht auch durch eine anonymisierte Ermittlung erreicht werden kann (BVerfGE 65, 1, 48).

Wie die Diskussion auf dem 85. Deutschen Ärztetag 1982 über die Schaffung von Krebsregistern gezeigt hat, ist epidemiologische Forschung bei entsprechender Organisation und Rückfragemöglichkeit durchaus auch mit anonymisierten Daten möglich. Zum Schutz persönlicher Patientendaten seien Anonymisierungs- und Aggregationsmethoden verstärkt weiterzuentwickeln. Auch die Datenschutzbeauftragten des Bundes und der Länder haben an die medizinische Forschung appelliert, stärker als bisher den bereits vorhandenen Forschungsstand zur Anonymisierung personenbezogener Daten zu nutzen und sich vordringlich um die Weiterentwicklung von Anonymisierungs- und Aggregationsmethoden zu bemühen.

Soweit allerdings mit personenbezogenen Patientendaten geforscht wird, darf der Rückgriff auf diese Daten grundsätzlich nicht am Betroffenen vorbei, sondern muß in seiner Kenntnis und mit seiner Einwilligung erfolgen. Keinesfalls darf das Selbstbestimmungsrecht des Betroffenen dadurch unterlaufen werden, daß ihm unter Berufung auf therapeutische Kontraindikation gleichsam das eigene Interesse entgegengehalten wird und deshalb die gebotene Aufklärung unterbleibt. Ausnahmen bedürfen einer bereichspezifischen gesetzlichen Regelung (vgl. oben S. 19/20).

Im übrigen hat sich die Ärzteschaft selbst – ausgehend von der ärztlichen Schweigepflicht – in den Berufsordnungen (BO) dafür entschieden, daß Patientendaten zu Forschungszwecken nur anonymisiert oder mit ausdrücklicher Zustimmung des Betroffenen weitergegeben werden dürfen (§ 2 Abs. 7 BO).

6.7 Personalwesen

6.7.1 Automatisierte Personalverwaltungssysteme

Im Bereich der Landesverwaltung gibt es derzeit im Geschäftsbereich des Kultusministers und des Ministers für Wissenschaft und Forschung automatisierte Personalverwaltungssysteme. Auf die beim Kultusminister geführte **Stellendatei,** die Datei der Amtlichen Schuldaten, die Seminareinweisungsdatei sowie die Datei der Versetzungsbewerber und Rückkehrer aus einer Beurlaubung bin ich ausführlich in meinem 8. Tätigkeitsbericht eingegangen (S. 84 bis 89). Für die Stellendatei und die Datei der Amtlichen Schuldaten bin ich dabei zu dem Ergebnis gelangt, daß eine Speicherung der Namen der Betroffenen in diesen Dateien, soweit der Kultusminister speichernde Stelle und damit „Herr der Daten" sein soll, jedenfalls auf der Grundlage der Generalklausel des § 10 Abs. 1 DSG NW a.F nach meiner Auffassung nicht zulässig ist. Hierzu hat sich auch durch das Datenschutzgesetz Nordrhein-Westfalen vom 15. März 1988 keine Änderung ergeben.

Mit dem beim Minister für Wissenschaft und Forschung geführten **Stelleninformationssystem SIS** habe ich mich im Jahr 1988 befaßt. Der Minister für Wissenschaft und Forschung speichert in dieser Datei für alle Stellen des Einzelplanes 06, also für das gesamte wissenschaftliche wie auch nicht-wissen-

schaftliche Personal der Hochschulen einschließlich der medizinischen Einrichtungen, Daten mit folgenden Angaben: Wertigkeit/Bezeichnung der Stelle; Zuordnung zu Lehreinheiten bzw. Dezernaten, zentralen Einrichtungen, sonstigen Diensten; Art der Inanspruchnahme (planmäßig besetzt, nicht planmäßig besetzt, Art der nicht planmäßigen Besetzung, Vakanz); Dauer der Inanspruchnahme für den derzeitigen Stelleninhaber (bei in Anspruch genommenen Stellen) bzw. Stand der Stellenbesetzung (bei Vakanzen); Aufgabenumschreibung (bei Professoren) bzw. derzeitiger Einsatz im Fachbereich/innerhalb der Lehreinheit (beim übrigen wissenschaftlichen und fachnahen nicht-wissenschaftlichen Personal); Name und Geschlecht des Stelleninhabers; Fakultät oder Fachbereich; Standort und Haushaltsvermerk.

Als gesetzliche Grundlage für das Speichern personenbezogener Daten der Hochschulangehörigen im Stelleninformationssystem SIS kommt nunmehr § 29 Abs. 1 Satz 1 DSG NW in Betracht. Nach dieser Vorschrift dürfen Daten von Bewerbern und Beschäftigten nur verarbeitet werden, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes erforderlich ist, oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht. § 29 Abs. 1 Satz 1 DSG NW enthält selbst keine Aussage zur Art der Datenverarbeitung. Aus dem Gesamtzusammenhang der Vorschrift, insbesondere aus Absatz 4 und Absatz 6, ist jedoch zu ersehen, daß im übrigen § 29 Abs. 1 Satz 1 DSG NW als gesetzliche Grundlage auch für eine automatisierte Verarbeitung personenbezogener Daten von Beschäftigten in Betracht kommt.

Der Einsatz der automatisierten Datenverarbeitung im Personalwesen bringt eine besondere Gefährdung der Persönlichkeitsrechte der Betroffenen mit sich. Denn die Automatisierung bewirkt eine erhöhte Verfügbarkeit und damit Verwertbarkeit der betreffenden Angaben. Angaben über eine bestimmte Person sind im automatisierten Verfahren wesentlich schneller auffindbar und nutzbar als in einer evtl. umfangreichen Akte. Dasselbe gilt auch für die Suche nach den gleichen Angaben bei einer größeren Gruppe von Betroffenen (z. B. bei allen Bediensteten einer Behörde oder des Bereichs, auf den sich das ADV-Verfahren bezieht). Das jeweilige Datum ist also im Hinblick auf die einzelne Person schneller greifbar und mit den entsprechenden Daten einer großen Zahl anderer Bediensteter vergleichbar. Derartige Vergleiche wären, wenn die Daten in Akten gespeichert sind, falls überhaupt, so nur mit einem unverhältnismäßigen Zeitaufwand möglich. Außerdem ist bei bestimmten Daten, etwa bei Leistungs- bzw. Abwesenheitsdaten, die Gefahr eines Kontextverlustes gegeben.

Dieses Gefahrenpotential kann sich je nach der konkreten Art einer automatisierten Personaldatenverarbeitung in unterschiedlicher Weise realisieren. Es läßt sich auch nicht allgemeingültig sagen, daß eine automatisierte Personal-

datenverarbeitung tatsächlich zu einer Beeinträchtigung schutzwürdiger Belange der Betroffenen führen muß. Wegen der bestehenden Gefahrenlage, die verstärkt von dem Betroffenen so empfunden wird, sind jedoch an die Voraussetzungen der Zulässigkeit der Datenverarbeitung in diesen Fällen besonders strenge Maßstäbe anzulegen.

Aus den dargestellten Gründen hat der Gesetzgeber für zwei besonders sensible Bereiche unmittelbar Konsequenzen gezogen: Nach § 29 Abs. 4 DSG NW dürfen die Ergebnisse medizinischer oder psychologischer Untersuchungen und Tests der Beschäftigten automatisiert nur verarbeitet werden, wenn dies dem Schutz der Beschäftigten dient. Nach § 29 Abs. 6 DSG NW dürfen Beurteilungen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen werden. Abgesehen von diesen Sonderfällen ist nach § 29 Abs. 1 DSG NW – ebenso wie nach § 10 Abs. 1 DSG NW a.F. – die Zulässigkeit der automatisierten Personaldatenverarbeitung davon abhängig, ob sie zur rechtmäßigen Aufgabenerfüllung der speichernden Stelle erforderlich ist.

In meiner Kontrollpraxis habe ich zum Begriff der Erforderlichkeit stets darauf hingewiesen, daß es hierfür nicht ausreicht, daß die Datenverarbeitung für die speichernde Stelle vorteilhaft oder zweckmäßig erscheint. Als erforderlich kann eine Datenverarbeitung nur dann angesehen werden, wenn sie wirklich notwendig ist, so daß ohne sie die Aufgaben der datenverarbeitenden Stelle nicht oder nur mangelhaft erfüllt werden könnten. Bei der Prüfung der Erforderlichkeit zur rechtmäßigen Aufgabenerfüllung ist in diesen Fällen aber auch zu beachten, daß sich bei der Übernahme von Daten in ein bestimmtes automatisiertes Verfahren die Frage nach der Verhältnismäßigkeit des Umgangs mit den Daten neu stellt. Gerade bei Personaldaten kann die Speicherung eines Datums in einer Personalakte bzw. in einem Personalbogen zur gesetzlichen Aufgabenerfüllung völlig ausreichend sein. Die Prüfung der Verhältnismäßigkeit bezieht sich demnach auf die Frage, ob das jeweilige automatisierte Verfahren gegenüber der herkömmlichen Verarbeitung der Daten in den Personalakten weitere ADV-spezifische Wirkungen – insbesondere belastender Art für die Betroffenen – auslösen könnte.

Nach der vom Minister für Wissenschaft und Forschung gegebenen Begründung wird die Datenverarbeitung im System SIS für Zwecke der Personalplanung und Hochschulplanung benötigt. Dadurch soll ermöglicht werden, entsprechende Aussagen sowohl für einzelne Lehreinheiten an einzelnen Hochschulen als auch für die Lehreinheiten an allen Hochschulen insgesamt und über die jeweiligen Stellenkategorien ohne Rücksicht auf die Zuordnung zu Lehreinheiten und Hochschulen zu machen. Die Hochschulplanung der neunziger Jahre könne nicht davon ausgehen, daß Innovationen im Hochschulbereich, Umorientierungen zwischen den Fächern und die Inangriffnahme neu hinzukommender Aufgaben durch Vermehrung des Personalbestandes erfüllt werden können. Anders als in der Vergangenheit, wo die Erledigung neuer Aufgaben in der Regel durch Personalzuwächse habe ermöglicht werden können, müsse für die Zukunft daher verstärkt zentral ein optimaler Personalein-

satz sichergestellt werden. Hierzu sei es erforderlich, Stellenpools anzulegen, in die in einzelnen Hochschulen für bestimmte Aufgaben nicht mehr benötigte freie Stellen fallen, um für die Erledigung neuer Aufgaben ggf. auch in anderen Hochschulkapiteln zur Verfügung zu stehen. Auch die zukünftige Stellenbesetzungspolitik müsse sich stärker als in der Vergangenheit daran orientieren, in welchen Zeiträumen Stellen wieder besetzbar würden. Dies gelte nicht nur für Professorenstellen, sondern auch für die Mitarbeiterstellen und für das nicht-wissenschaftliche Personal. Die erhobenen Daten ermöglichten darüber hinaus, die Personalausstattung der einzelnen Lehreinheiten nicht nur quantitativ, sondern strukturell besser zwischen den Hochschulen vergleichen zu können, und böten damit eine wesentliche Grundlage für die Ermittlung von Ausstattungsstandards der einzelnen Fächer unter inhaltlichen, nicht nur quantitativen Gesichtspunkten.

Nach dem bisherigen Stand meiner Überprüfung bin ich bei dieser Begründung davon ausgegangen, daß die Erforderlichkeit für die Speicherung der in SIS gespeicherten personenbezogenen Angaben von Angehörigen der Hochschulen und medizinischen Einrichtungen des Landes Nordrhein-Westfalen für das wissenschaftliche Personal bejaht werden kann. Hinsichtlich dieses Personenkreises ist nach dem derzeitigen Erkenntnisstand auch der Umfang der von den Hochschulen angeforderten und im Stelleninformationssystem SIS gespeicherten Daten als verhältnismäßig anzusehen. Es ist einleuchtend, daß insoweit bei der Planung des Personalbestandes und der Durchführung entsprechender Maßnahmen sowohl haushaltsrechtliche als auch wissenschaftliche, personalwirtschaftliche und personalrechtliche Erfordernisse zu berücksichtigen sind. Dies ist jedoch ohne Kenntnis der im Stelleninformationssystem SIS gespeicherten Daten einschließlich des Namens und Geschlechts der Stelleninhaber nicht möglich. Die damit verbundene Belastung für die Betroffenen erscheint unter Berücksichtigung der möglichen und zugelassenen Auswertungen nicht unverhältnismäßig.

Diese Erwägungen können jedoch nach meiner Auffassung für eine Speicherung personenbezogener Daten des nicht-wissenschaftlichen Personals weder hinsichtlich der Erforderlichkeit noch hinsichtlich der Verhältnismäßigkeit gelten. Soweit für wissenschaftliche und personalwirtschaftliche Planungen im Hochschulbereich Aussagen über die Personalausstattung für einzelne Lehreinheiten erforderlich sind, können diese auf Grund entsprechender Stellenplandaten getroffen werden. Die Kenntnis von Name und Geschlecht der Stelleninhaber ist dafür nicht erforderlich.

Nach § 73 Abs. 3 Nr. 1 des Landespersonalvertretungsgesetzes unterliegt die Einführung, Anwendung, wesentliche Änderung oder wesentliche Erweiterung von automatisierter Verarbeitung personenbezogener Daten der Beschäftigten außerhalb von Besoldungs-, Gehalts-, Lohn- und Versorgungsleistungen der Mitbestimmung des zuständigen Personalrates. Für die Personalvertretung ergibt sich daher im Mitbestimmungsverfahren die Möglichkeit, Vereinbarungen über konkrete Einzelheiten einer beabsichtigten Personaldaten-

verarbeitung mit der Dienststelle zu treffen. Solche Vereinbarungen können insbesondere dazu dienen, das auch unter Heranziehung des Verhältnismäßigkeitsgrundsatzes noch recht globale Kriterium der Erforderlichkeit zur Aufgabenerfüllung der speichernden Stelle einzugrenzen und Maßnahmen zur Wahrung schutzwürdiger Belange der Betroffenen zu treffen. Insbesondere kommen in Betracht Festlegungen auf den Katalog der Daten, die zulässigen Verarbeitungen, insbesondere Auswertungen, Übermittlungen und Verknüpfungen, sowie die notwendigen organisatorischen und technischen Maßnahmen der Datensicherung nach dem jeweiligen Stand der Technik. Darüber hinaus sollte vereinbart werden, wie und unter welchen Voraussetzungen die datenschutzrechtlichen Ansprüche des Betroffenen auf Einsicht, Berichtigung und Löschung geltend gemacht werden können.

Unabhängig von den beim Kultusminister und beim Minister für Wissenschaft und Forschung bestehenden automatisierten Personalverwaltungssystemen führen viele öffentliche Stellen in einzelnen Bereichen des Personalwesens automatisierte Dateien wie Stellendateien, Urlaubs-, Krankheits- oder Abwesenheitsdateien, Verfahren für Organisationsuntersuchungen oder Zeiterfassungssysteme. Derartige Datenspeicherungen bergen bei einer – auch automatisiert herstellbaren – Verknüpfung der einzelnen Systeme die Gefahr der Entstehung eines verfassungsrechtlich sehr bedenklichen **Personalinformationssystems** in sich. Ein solches System, das eine Zusammenfassung von Daten über das Personal aus verschiedenen Anwendungsgebieten (Personalverwaltung im engeren Sinne, Personalfürsorge, Arbeitsplätze, Arbeitsleistung u. a.) und eine Verknüpfung über ein gemeinsames Kennzeichen ermöglicht, würde nicht nur als Kontrollinstrument zur Überwachung des Verhaltens und der Leistung des Personals, sondern auch zur Erstellung und Erfassung von Persönlichkeitsprofilen genutzt werden können. Ebenso kann eine automatisierte Speicherung beispielsweise von Leistungsdaten, die ohne jeden Kontextbezug, also ohne Rücksicht auf die individuelle Situation, in der sie erhoben wurden, gespeichert sind, zur Entstehung von schematisierten Persönlichkeitsprofilen der Beschäftigten führen, die sie unverhältnismäßig belasten können. Solche Besorgnisse sind mir wiederholt von Personalräten mitgeteilt worden.

Ich habe gegen die Zusammenführung von Leistungsdaten mit anderen personenbezogenen Daten, wie Stellenplandaten und Fehlzeitendaten, erhebliche datenschutzrechtliche Bedenken, da eine automatisierte Speicherung, Nutzung und Weitergabe dieser Daten eine nahezu lückenlose Leistungs- und Verhaltenskontrolle – unbegrenzt speicherbar und jederzeit abrufbar – ermöglicht, die nach meiner Auffassung unverhältnismäßig wäre. Wie das Bundesverfassungsgericht in seinem Volkszählungsurteil ausgeführt hat, muß sichergestellt sein, daß der Einzelne unter den Bedingungen einer automatisierten Erhebung und Bearbeitung der seine Person betreffenden Angaben nicht zum bloßen Informationsobjekt wird.

6.7.2 Vorlage von Personalakten beim Amtsarzt

Unsicherheiten hinsichtlich des erforderlichen Umfangs der Datenweitergabe zur Feststellung der Dienstfähigkeit durch einen Amtsarzt führen häufig dazu, daß die vollständige Personalakte übersandt wird. Zur Erstellung eines Gutachtens kann die Kenntnis der in den Personalakten enthaltenen Vorgänge – etwa ein sich über Jahre hinziehendes dienstliches Verhalten – erforderlich sein, die nach Auffassung des Dienstvorgesetzten auf eine mögliche Dienstunfähigkeit des Beamten hindeuten. Dies rechtfertigt jedoch nicht in jedem Fall die Übersendung der vollständigen Personalakte, da diese auch zahlreiche andere, oft sensible Daten enthält, die für die Erstellung des Gutachtens ohne Bedeutung sind; dies gilt vor allem dann, wenn die Angabe der Bedenken des Dienstvorgesetzten ausgereicht hätte.

6.7.3 Datenanforderung durch Aufsichtsbehörden

Ein Ministerium forderte im Hinblick auf eine effiziente Personalplanung eine **Dienstaltersliste** vom Beamten der nachgeordneten Behörden an. Die Dienstaltersliste sollte zusätzlich Auskunft geben über Prüfungsergebnis und Gesamturteil der letzten dienstlichen Beurteilung. Für die Anforderung solcher Listen war seinerzeit eine gesetzliche Grundlage nicht ersichtlich. Da Personaldaten aus Personalakten erhoben wurden und deshalb ihrem Wesen nach geheimzuhalten waren, konnte nur eine bereichspezifische Regelung einen Eingriff in die Persönlichkeitsrechte der Betroffenen rechtfertigen. § 102 des Landesbeamtengesetzes kam als gesetzliche Grundlage nicht in Betracht, weil die Vorschrift für die Betroffenen nicht erkennen läßt, daß ihre in den Personalakten festgehaltenen Daten an die oberste Dienstbehörde weitergegeben werden sollen. Somit war die Anforderung der Dienstaltersliste unzulässig.

Im übrigen waren auch Erhebung und Weitergabe der Daten **aller** in Frage kommenden Beamten der nachgeordneten Behörden für die Auswahl der qualifiziertesten Beamten für das Ministerium nicht erforderlich. Jedenfalls wäre eine generelle Datenerhebung „auf Vorrat" datenschutzrechtlich nicht zulässig.

Auch nach der inzwischen in § 29 DSG NW getroffenen Regelung für die Verarbeitung von Personaldaten wäre die Anforderung einer Dienstaltersliste aus den genannten Gründen unzulässig. Keine durchgreifenden datenschutzrechtlichen Bedenken bestehen gegen die Anforderung von Personaldaten der für die zu besetzende Stelle geeigneten Beschäftigten, wenn die Daten auf den im Einzelfall erforderlichen Umfang beschränkt bleiben. Eine solche Anforderung kann u. U. auch kurzfristig durch telefonischen Anruf bei den nachgeordneten Behörden erfolgen.

6.7.4 Personalnebenakten beim Vorgesetzten

Bei einem Polizeipräsidenten wurden von den Leitern der Abteilungen S und K Durchschriften personalrechtlicher Entscheidungen ihrer Mitarbeiter, wie z. B. Versetzungen, Abordnungen, Beurlaubungen, Nebentätigkeitsgenehmigungen, aber auch Rügen, zur Verfügung gestellt und von diesen in „Sonderakten" aufbewahrt.

Gegen diese Verfahrensweise bestehen erhebliche datenschutzrechtliche Bedenken. Über eine bloße aus dienstlichen Gründen erforderliche Kenntnisnahme von personalrechtlichen Entscheidungen durch Vorgesetzte hinaus dürfen keine Durchschriften personalrechtlicher Entscheidungen an Vorgesetzte weitergegeben werden. Insoweit ist eine gesetzliche Grundlage nicht ersichtlich. Auch § 29 DSG NW enthält keine Regelung über die Führung von **Personalnebenakten.** Nach dem Bericht der interministeriellen Arbeitsgruppe zur strukturellen Fortentwicklung des Personalaktenrechts im öffentlichen Dienst kann die Führung von Personalnebenakten allenfalls notwendig sein, wenn die personalverwaltende Behörde nicht mit der Beschäftigungsbehörde identisch ist oder mehrere personalverwaltende Behörden für den Beschäftigten zuständig sind. Aber auch insoweit bedürfte es nach meiner Auffassung einer gesetzlichen Regelung.

Auf meine Bedenken, die der Innenminister teilt, hat der Regierungspräsident veranlaßt, die bereits gesammelten Durchschriften der personalrechtlichen Entscheidungen zu vernichten und sich künftig auf die Kenntnisnahme von personalrechtlichen Entscheidungen durch Vorgesetzte zu beschränken.

6.7.5 Abschottung der Beihilfestelle

Wegen der besonderen Schutzwürdigkeit der Beihilfedaten der Beschäftigten und ihrer Angehörigen halte ich eine bereichspezifische Regelung zum Umgang mit diesen sensiblen Daten für dringend erforderlich (s. auch oben S. 38 f.). Inzwischen unterstreicht auch der Bericht der interministeriellen Arbeitsgruppe zur strukturellen Fortentwicklung des Personalaktenrechts im öffentlichen Dienst die Notwendigkeit einer ausdrücklichen gesetzlichen Regelung, nach der etwa Beihilfedaten ausschließlich für Beihilfezwecke zu verwenden, Beihilfevorgänge von den übrigen Personalvorgängen getrennt zu bearbeiten und aufzubewahren sowie Verwendung und Weitergabe von Beihilfedaten für andere als für Beihilfezwecke nur in gesetzlichen Ausnahmefällen zulässig sind.

Gegenüber mehreren Stellen mußte ich auf die – schon nach geltendem Recht gebotene – Abschottung der Beihilfestelle von der übrigen Personalverwaltung dringen.

Zu der nach § 13 Abs. 2 Satz 4 der Beihilfenverordnung gebotenen vertraulichen Behandlung der Beihilfeanträge gehört grundsätzlich, daß die Beihilfedaten, die dem Dienstherrn im Rahmen der Beihilfegewährung offenbart werden, nur zum Zwecke der Gewährung von Beihilfen verwandt und nicht auch Personalentscheidungen zugrunde gelegt werden. Der Beihilfeberechtigte darf durch die Art der Organisation des Beihilfewesens weder davon abgehalten werden, zum Arzt zu gehen, noch davon, entstandene Rechnungen zur Beihilfegewährung einzureichen. Daher muß als grundrechtssichernde Schutzvorkehrung die Abschottung der Beihilfestelle von der Personalverwaltung gewährleistet sein.

Die Funktion der Beihilfestelle ist derjenigen einer Betriebskrankenkasse vergleichbar. Diese hat das Sozialgeheimnis nach § 35 Abs. 1 SGB I zu wahren

und darf personenbezogene Daten ihrer Versicherten nur unter den gesetzlichen Voraussetzungen offenbaren. Es ist kein Grund ersichtlich, weshalb der darin zum Ausdruck kommende Grundsatz, daß Daten, die im Zusammenhang mit der Gewährung von Sozialleistungen nach dem Sozialgesetzbuch erhoben und bearbeitet werden, vor dem Arbeitgeber geheimzuhalten sind, nicht auch auf das Beihilfewesen im öffentlichen Dienst übertragen werden kann. Denn auch bei Beihilfen handelt es sich im weiteren Sinne um eine „Sozialleistung" des Dienstherrn für seine Bediensteten.

Schließlich verlangt auch die beamtenrechtliche Fürsorgepflicht des Dienstherrn eine Organisation der Beihilfegewährung, die den Beschäftigten nicht aus Angst davor, daß seine Beihilfedaten an dafür nicht zuständige Mitarbeiter des Dienstherrn gelangen, daran hindert, die ihm zustehenden Beihilfeleistungen in Anspruch zu nehmen. Bei psychiatrischen Behandlungen etwa dürfte dies ganz besonders problematisch sein.

Soweit eine getrennte Bearbeitung der Beihilfevorgänge und der übrigen Personalvorgänge aus innerbehördlichen Gründen auf unüberwindbare Schwierigkeiten stößt, halte ich es für erwägenswert, dem Gebot der getrennten Bearbeitung von Beihilfevorgängen dadurch deutlicher Rechnung zu tragen, daß die Aufgaben der Beihilfegewährung für die Beschäftigten der Landesverwaltung zentral einer Landesbehörde übertragen werden. Es wäre insoweit zu prüfen, ob nicht das Landesamt für Besoldung und Versorgung – wie dies beispielsweise in Baden-Württemberg geschieht – die Beihilfebearbeitung für die Landesverwaltung übernehmen kann.

Sollte eine solche Aufgabenübertragung nicht möglich sein und die Beihilfesachbearbeitung innerhalb der Behörde verbleiben, müßte wenigstens sichergestellt sein, daß außer den für die Beihilfesachbearbeitung unmittelbar verantwortlichen Personen – also Sachbearbeiter und Dezernent/Referent – nur noch der Behördenleiter bzw. dessen ständiger Vertreter die Möglichkeit des Zugriffs auf Beihilfedaten hat. Kann aus organisatorischen Gründen eine solche Trennung nicht vollzogen werden, verlangt das Gebot der getrennten Bearbeitung aber mindestens die Zuordnung der Beihilfesachbearbeitung zu einem anderen Dezernat bzw. einer anderen Gruppe als der für Personalangelegenheiten zuständigen, wenn schon nicht die Zuordnung zu einer anderen Abteilung in Betracht gezogen werden kann.

6.8 Volkszählung 1987

Am Beispiel der Volkszählung 1987 hat sich gezeigt, daß die Empfindsamkeit der Bürger für den korrekten Umgang mit ihren Daten deutlich gewachsen ist. Dem stand nach meinen Feststellungen vielfach eine mangelnde Sensibilität der Verantwortlichen in den Gemeinden für die berechtigten Interessen der Auskunftspflichtigen am Schutz ihrer Daten gegenüber. So habe ich insbesondere in der Erhebungsphase zahlreiche zum Teil gravierende Mängel festgestellt, die das Vertrauen in eine strikte Trennung von statistischer Erhebung und Verwaltungsvollzug erschüttert und die Akzeptanz auch bei Bürgern, die

der Volkszählung überwiegend positiv gegenüberstanden, verringert haben. Andererseits haben sich die Verantwortlichen auf meine Intervention hin bei der Mehrzahl der festgestellten Verstöße einsichtig gezeigt und sind größtenteils meinen Empfehlungen gefolgt. In wenigen, allerdings schwerwiegenden Fällen habe ich jedoch die festgestellten Verstöße förmlich beanstanden müssen. Im Rückblick hätte ich meine in der Phase der Vorbereitung der Volkszählung öffentlich geäußerte Zuversicht über die Gewährleistung des Datenschutzes bei der Durchführung der Volkszählung vor Ort, gemessen an der hier festgestellten Sorglosigkeit, zurückhaltender formuliert.

6.8.1 Abschottung der Erhebungsstellen

Während die festgestellten Mängel im Bereich der räumlichen und organisatorischen Abschottung der Erhebungsstellen von den Verwaltungsstellen rasch – in den meisten Fällen auf telefonische Empfehlung – behoben wurden, stieß ich bei der **personellen Abschottung** der Erhebungsstellen auf Mängel, die zum Teil von den Verantwortlichen keineswegs als solche erkannt und akzeptiert worden sind.

Zentrales Problem der personellen Abschottung war der Einsatz von Beschäftigten aus sog. sensiblen Bereichen der Verwaltung in den Erhebungsstellen sowie später der Einsatz der Beschäftigten der Erhebungsstellen nach Beendigung ihrer dortigen Tätigkeit in sensiblen Bereichen der Verwaltung. In meinem 8. Tätigkeitsbericht (S. 95) hatte ich bereits darauf hingewiesen, daß das Gebot der personellen Abschottung verlangt, in der Erhebungsstelle keine Personen einzusetzen, bei denen die Möglichkeit besteht, daß sie die Erkenntnisse aus der Volkszählung zu Lasten der Auskunftspflichtigen nutzen können. Dem kann nur Rechnung getragen werden, wenn diese Personen von vornherein nicht in derartige Interessenkonflikte gebracht werden. Auf meine entsprechende Empfehlung wandten sich mehrere Gemeinden an ihren kommunalen Spitzenverband, der ebenso wie der Innenminister meine Auffassung nicht teilte. Beide hielten mir entgegen, daß die Regelungen in § 4 Abs. 1 Satz 2 und 3 der Verordnung über die Durchführung des Volkszählungsgesetzes 1987 und die Bestimmung der Erhebungsstellen sowie das in § 9 Abs. 2 des Volkszählungsgesetzes 1987 (VZG) bzw. im Bundesstatisktikgesetz enthaltene Gebot der statistischen Geheimhaltung für die personelle Abschottung ausreichten, und meinten, daß meinen Empfehlungen die Rechtsgrundlage fehle.

Das Bundesverfassungsgericht hat in seinem Beschluß vom 24. September 1987 (NJW 1987, 2805) den Einsatz von Personen in der Erhebungsstelle entsprechend dem Gebot einer personellen Trennung der Erhebungsstelle problematisiert, aber nicht entschieden, weil die Beschwerdeführer nicht geltend gemacht hatten, in der für sie zuständigen Erhebungsstelle seien Personen beschäftigt gewesen, bei denen im Hinblick auf ihre dienstliche Tätigkeit ein Wechsel zwischen Verwaltungsvollzugs- und Erhebungsstellentätigkeit oder aus sonstigen Gründen Interessenkonflikte nicht auszuschließen seien. Gegenüber dem Bundesverfassungsgericht hat der in einem anderen Verfahren

zur Stellungnahme aufgeforderte Bundesbeauftragte für den Datenschutz ausgeführt, daß die Schutznorm des § 9 Abs. 1 Satz 2 VZG den Ausschluß von solchen Mitarbeitern erfordere, bei denen auf Grund ihrer sonstigen Tätigkeit die Gefahr bestehe, daß Erkenntnisse aus der Volkszählung in Verwaltungsentscheidungen, die auskunftspflichtige Bürger belasten, einfließen könnten. Diese Auffassung hat er dem Bundesminister des Innern mitgeteilt, der ebenso wie das Statistische Bundesamt seine Auffassung ausdrücklich bestätigt hat. Das Statistische Bundesamt hat die Statistischen Landesämter auf diese gemeinsame Rechtsauffassung hingewiesen und die große Bedeutung der vom Volkszählungsgesetz geforderten personellen Voraussetzungen in den Erhebungsstellen für das Gelingen der Zählung betont.

Ich sehe daher keine Veranlassung, von meiner bisher vertretenen Auffassung abzuweichen, und habe sowohl den Einsatz von Mitarbeitern aus sensiblen Bereichen der Verwaltung in den Erhebungsstellen als auch eine anschließende Verwendung der Mitarbeiter der Erhebungsstelle in Bereichen der Verwaltung beanstandet, wenn Interessenkonflikte zu besorgen waren. Im Hinblick darauf, daß die gleiche Problemsituation bei der Einrichtung der Statistikdienststellen im Rahmen des § 14 Abs. 1 Satz 3 VZG i.V.m. § 32 Abs. 2 DSG NW besteht, bleibt diese Frage über die Volkszählung hinaus von besonderer Bedeutung.

6.8.2 Einsatz der Automatisierten Datenverarbeitung

Besonderes Augenmerk galt dem Einsatz der **Automatisierten Datenverarbeitung,** insbesondere bei der Rücklaufkontrolle in den Erhebungsstellen, weil hier das Risiko einer Durchbrechung des verfassungsrechtlichen Gebots der strikten Trennung von Statistik und Verwaltung erheblich größer war. Deshalb habe ich besondere Vorkehrungen zum Schutz des Statistikgeheimnisses und strenge Abschottungsmaßnahmen gefordert. Meiner Empfehlung im 8. Tätigkeitsbericht (S. 94/95) ist der Innenminister gefolgt. In seinem Runderlaß vom 10. 04. 1987 zum Einsatz der Automatisierten Datenverarbeitung bei der Vorbereitung und Durchführung der Volkszählung 1987 (MBl. NW. 1987, S. 572) hat er einen Katalog von organisatorischen und technischen Vorkehrungen festgelegt.

6.8.3 Durchführung der Erhebung

Ich habe mich immer wieder mit Beschwerden von Auskunftspflichtigen beschäftigen müssen, deren Angaben nicht bei ihnen selbst, sondern bei Dritten, wie z. B. bei in der Wohnung des Auskunftspflichtigen angetroffenen Verwandten oder Freunden erhoben wurden, ohne daß der Auskunftspflichtige Kenntnis davon hatte oder damit einverstanden war. In den meisten Fällen handelte es sich um Personen, die ihren zweiten Wohnsitz noch im Hause der Eltern hatten. Diese Vorfälle zeigen, daß die Zähler über ihr eng begrenztes Fragerecht nach § 10 Abs. 7 i.V.m. § 13 Abs. 5 VZG nur unzureichend belehrt worden waren.

Mehrfach haben sich erstaunte Bürger an mich gewandt, die von der Erhebungsstelle Unterlagen erhielten, die schon von anderen Auskunftspflichtigen ausgefüllt und deren Eintragungen nur unzureichend ausradiert worden waren. Es wurden aber auch ausgefüllte Erhebungsvordrucke mit unvollständig beantworteten Fragen versehentlich an andere Auskunftspflichtige zur Ergänzung zurückgesandt. Hier führte mangelnde Sorgfalt zur Verletzung des Statistikgeheimnisses.

Nicht mehr nur mangelnde Sorgfalt, sondern in hohem Maße mangelnde Sensibilität spiegeln die Art und Weise der Durchführung der Erhebung in manchen Heimen und Anstalten wider. Von Erhebungsstellenleitern wurde oft verkannt, daß in den Heimen und Anstalten jede Einschaltung der Heim- oder Anstaltsleitung für die Bewohner eine bedrückende Situation auslösen konnte, in der sie sich bevormundet oder regelrecht unter Druck gesetzt fühlten.

So wurden in Schwesternwohnheimen die Erhebungsunterlagen durch den Leiter des Wohnheims – zum Teil bereits halb ausgefüllt – mit der Bemerkung ausgehändigt, die Erhebungsvordrucke seien zu ergänzen und an ihn wieder zurückzugeben. Der Leiter eines Altersheimes hatte die Erhebungsbogen der Heimbewohner gleich selbst ausgefüllt. In einer Landesklinik wurde die vom Gesetzgeber vorgesehene hilfsweise Verpflichtung des Leiters der Klinik zur Auskunft der Einfachheit halber von vornherein in Anspruch genommen; die auskunftspflichtigen Patienten merkten auch hier von der Volkszählung überhaupt nichts.

Noch problematischer ging es in zwei Justizvollzugsanstalten zu, in denen Justizvollzugsbeamte zu Zählern bestellt wurden, die die Erhebungsunterlagen an die Strafgefangenen austeilten und die ausgefüllten Bogen offen an sich zurückgeben ließen. Verständlicherweise gewannen die Strafgefangenen dabei den Eindruck, daß die Anstaltsleitung eine Durchsicht oder Kontrolle der ausgefüllten Erhebungsbogen vornehmen würde.

Diese Fälle zeigen, wie wenig Gespür manche Verantwortliche dafür hatten, daß mit der Auskunftspflicht der Bürger selbstverständlich das Recht korrespondiert, in erster Linie selbst über die Erteilung der Auskunft zu entscheiden. Hierzu gehört auch das Recht, zwischen mündlicher oder schriftlicher Beantwortung zu wählen. Ich habe in den mir bekanntgewordenen Fällen vielfach die Wiederholung der Volkszählung mit den zur Wahrung des Statistikgeheimnisses erforderlichen Vorkehrungen empfohlen.

Spektakulär war der Fund von zur Vernichtung vorgesehenen Unterlagen mit personenbezogenen Daten von Auskunftspflichtigen in einem ungesicherten Müllcontainer, der im Hof einer Erhebungsstelle stand. Hier war versäumt worden, die Unterlagen sofort nach Aussonderung zu vernichten, wie es die Wahrung des Statistikgeheimnisses geboten hätte. Unmittelbar nach dem Vorfall wurde der Erhebungsstelle ein Reißwolf zur Verfügung gestellt.

Die Erhebungsstelle einer größeren Stadt hat offenbar in einer Telefonaktion Bürger, die bisher ihre Auskunftspflicht noch nicht erfüllt hatten, zur telefoni-

schen Beantwortung der Fragen aus dem Personen- und Wohnungsbogen angehalten. Die Erhebungsstelle berief sich darauf, daß die Auskunftspflichtigen ihre Einwilligung zur **fernmündlichen Erhebung** ihrer Daten erteilt hätten. Gleichwohl war diese Verfahrensweise nach meiner Auffassung unzulässig, und zwar unabhängig davon, daß mindestens in einem Fall Zweifel an der Einholung der Einwilligung bestanden.

Eine telefonische Erhebung aller Angaben in den Erhebungsbogen kann weder auf das Volkszählungsgesetz noch auf die Verordnung über die Durchführung des Volkszählungsgesetzes 1987 und die Bestimmung der Erhebungsstellen gestützt werden. Im Rahmen der gesetzlichen Regelungen hat der Auskunftspflichtige die Möglichkeit, seiner Auskunftspflicht entweder durch mündliche Beantwortung der Fragen gegenüber dem Zähler oder durch schriftliche Beantwortung nachzukommen. Er kann wählen, ob er die Fragen gemeinsam mit anderen Haushaltsmitgliedern oder für sich alleine beantworten will. Schließlich steht es dem Auskunftspflichtigen frei, ob er dem Zähler die Vor- und Familiennamen der übrigen Haushaltsmitglieder sowie den Vor- und Familiennamen des Wohnungsinhabers mündlich oder schriftlich mitteilt. Bei diesen abschließenden Verfahrensregelungen zur Durchführung der Erhebung handelt es sich um zwingendes Recht, das nicht zur Disposition der Beteiligten steht.

Zudem widerspricht eine vollständige telefonische Erhebung der Absicht des Gesetzgebers, die lückenlose und richtige Zählung durch Begehung des Gemeindegebiets sicherzustellen und Gefährdungen zu vermeiden, wie sie durch eine fernmündliche Befragung entstehen können. Neben der Gefahr von Fehlinterpretationen würde der Auskunftspflichtige von vornherein auf die Interviewmethode festgelegt, die durch das Volkszählungsgesetz nicht gedeckt ist.

Eine telefonische Erhebung ist nach meiner Auffassung auch dann unzulässig, wenn der Auskunftspflichtige eingewilligt hat. In diesen Fällen besteht insbesondere die Gefahr, daß der angerufene Auskunftspflichtige auch zu Angaben über weitere Haushaltsmitglieder befragt wird. Dadurch würde das persönliche Auskunftsrecht jedes einzelnen Haushaltsmitgliedes verletzt.

Im übrigen sieht auch die Durchführungsverordnung eine telefonische Erhebung nicht vor. Vielmehr hat die Erhebungsstelle wiederholt nicht erreichte Auskunftspflichtige **schriftlich** an die Erfüllung der Auskunftspflicht zu erinnern. Auskunftspflichtigen, die die Angaben verweigern, hat sie schriftlich die Rechtslage zu erläutern und sie durch Heranziehungsbescheid nochmals zur Erfüllung der Auskunftspflicht aufzufordern. Unvollständig ausgefüllte Erhebungsvordrucke sollen möglichst durch Nachfrage beim Auskunftspflichtigen ergänzt werden; endgültig nicht oder unvollständig ausgefüllte Erhebungsvordrucke sind von der Erhebungsstelle mit den aus dem Melderegister übermittelten Daten zu ergänzen. Damit hat der Verordnungsgeber das Erhebungsverfahren abschließend geregelt und bewußt auf weitere Möglichkeiten zur Optimierung des Volkszählungsergebnisses verzichtet.

Da der Oberstadtdirektor seine Verfahrensweise dennoch für zulässig hielt und sich dabei auf die Auffassung des Landesamtes für Datenverarbeitung und Statistik berief, mußte ich die telefonische Erhebung sämtlicher Angaben zur Volkszählung durch Mitarbeiter der Erhebungsstelle förmlich beanstanden. Ich habe empfohlen, telefonische Erhebungen zu unterlassen, wenn damit erstmals und vollständig die Angaben beim Auskunftspflichtigen erhoben werden sollen, und die auf diese Weise ausgefüllten Erhebungsvordrucke zu vernichten. Weder der Innenminister noch das Landesamt für Datenverarbeitung und Statistik haben zu dieser Beanstandung Stellung genommen.

6.8.4 Verfremdung der Erhebungsmerkmale

Das Gebot der Anonymisierung der Volkszählungsdaten verlangt nicht nur eine Vernichtung der Erhebungsunterlagen (wie Haushaltsmantelbogen und Personenbogen), sondern auch die Löschung der laufenden Nummern und Ordnungsnummern, die auch ohne Speicherung der Hilfsmerkmale den Personenbezug ermöglichen. Hierzu ist die Verfremdung der vor den einzelnen Datensätzen stehenden laufenden Nummern und Ordnungsnummern erforderlich.

Das vom Landesamt für Datenverarbeitung und Statistik vorgelegte Verfremdungsprogramm wurde geprüft. Gegen das beabsichtigte Verfahren zur Anonymisierung der Erhebungsmerkmale durch Vorgabe einer festen Startzahl habe ich Bedenken erhoben. Ich habe das Landesamt für Datenverarbeitung und Statistik darauf hingewiesen, daß das Verfremdungsprogramm eine ausreichende Anonymisierung nur dann sicherstellt, wenn

- die Startzahl nicht vorgegeben, sondern maschinell eine Zufallsstartzahl erzeugt wird,

- die Vergabe der Zufallsstartzahl bei jedem Lauf neu erzeugt wird, wobei der Umfang der in einen Lauf einbezogenen Datensätze entsprechend klein sein muß,

- die Zufallsstartzahl weder angezeigt noch ausgedruckt wird bzw. werden kann und nicht länger als bis zum Programmende gespeichert wird,

- sichergestellt wird, daß möglichst wenige Mitarbeiter den Verfremdungsalgorithmus kennen.

Außerdem habe ich gebeten zu prüfen, ob nicht mit einem mehrstelligen Algorithmus die Nummer der Regionalliste und die Nummer des Gebäudes als Ganzes verschlüsselt werden können. Die hierarchische Struktur würde dann erhalten bleiben, ohne daß die Untergliederung der Regionallistennummer ein zusätzliches Reidentifizierungsrisiko bildet.

6.8.5 Vernichtung der Erhebungsunterlagen

Maßgebliche Vorgabe ist das in § 15 Abs. 2 VZG geregelte Vernichtungsgebot zum „frühestmöglichen" Zeitpunkt. Das Bundesverfassungsgericht hat in seinem Verschluß vom 24. September 1987 (NJW 1987, 2805) festgestellt, daß die Statistischen Landesämter gehalten seien, für jede der Erhebungsunterlagen den jeweils frühestmöglichen Zeitpunkt zu ermitteln und die Vernichtung oder Löschung zu diesem Zeitpunkt vorzunehmen. Art und Geschwindigkeit der Aufbereitung und ihrer Organisation bildeten keine verbindlichen, etwa die Gerichte bindenden tatsächlichen Vorgaben der Statistischen Landesämter, sondern hätten sich ihrerseits am **Gebot frühestmöglicher Vernichtung** und Löschung zu orientieren. Daraus ergibt sich eindeutig, daß es auf keinen Fall in Betracht kommt, alle Erhebungspapiere bis zu dem gesetzlich zugelassenen spätesten Zeitpunkt – zwei Wochen nach Feststellung der amtlichen Bevölkerungszahl des Landes – aufzubewahren.

Nicht zuletzt im Hinblick auf die vom Bundesverfassungsgericht insoweit besonders betonte Kontrollaufgabe der Datenschutzbeauftragten ist es notwendig, Zeitpunkte für die Vernichtung der Erhebungsunterlagen jeweils für jede der Erhebungsunterlagen (Organisationspapiere, Namens- und Adreßlisten, Namensteil der Regionalliste, Haushaltsmantelbogen, Wohnungs- und Personenbogen, Arbeitsstättenbogen) verbindlich zu benennen. Es bestehen erhebliche datenschutzrechtliche Bedenken, wenn die Erhebungsunterlagen über den Abschluß der maschinellen Plausibilitätskontrollen hinaus bis zur „rechtskräftigen" Feststellung der amtlichen Einwohnerzahl aufbewahrt und erst dann vernichtet werden. Auch das Ziel, einen möglichst hohen Grad an Genauigkeit der Ergebnisse der Volkszählung zu erreichen, rechtfertigt es nicht, den Vernichtungszeitpunkt so weit hinauszuschieben, bis er mit dem gesetzlich vorgeschriebenen spätesten Zeitpunkt zusammenfällt.

Ein abschließender Bericht des Landesamtes für Datenverarbeitung und Statistik stand am Ende des Berichtszeitraums noch aus.

6.8.6 Datenübermittlung an die Gemeinden (GV)

Nachdem der Landesgesetzgeber in § 32 DSG NW die gesetzliche Voraussetzung für eine Übermittlung von Einzelangaben aus der Volkszählung zu ausschließlich statistischen Zwecken geschaffen hat, richten Gemeinden, die bisher keine Statistikämter hatten, entsprechend § 32 Abs. 2 DSG NW **Statistikdienststellen** ein. Bei der Einrichtung der Statistikdienststellen sind besondere Anforderungen an die räumliche, organisatorische und personelle Abschottung von anderen Verwaltungsstellen zu erfüllen.

Ich halte es für erforderlich, daß die notwendigen organisatorischen und technischen Vorkehrungen in einer Dienstanweisung erfaßt werden, deren Einhaltung durch eine unabhängige interne Kontrolle – etwa durch das Rechnungsprüfungsamt – überwacht wird.

Außerdem sind auch hier Regelungen zu treffen, die eine Interessenkollision für die in der Statistikdienststelle eingesetzten Mitarbeiter, ein kurzfristig

wiederholtes Auswechseln der Mitarbeiter und eine unmittelbare Abfrage von statistischen Ergebnissen durch andere Verwaltungsstellen bei den Mitarbeitern verhindern. Eine Interessenkollision ist dann zu befürchten, wenn Mitarbeiter vor ihrem Einsatz in der Statistikdienststelle oder unmittelbar nach Beendigung ihrer Tätigkeit in der Statistikdienststelle in sensiblen Bereichen des Verwaltungsvollzuges (beispielsweise Einwohnermeldeamt, Sozialamt) eingesetzt waren oder eingesetzt werden sollen. Es besteht dann die Besorgnis, daß Erkenntnisse aus ihrer Tätigkeit in der Statistikdienststelle zu Lasten eines Auskunftspflichtigen verwandt werden. Das Gebot der Abschottung entsprechend § 14 Abs. 1 Satz 3 VZG i.V.m. § 32 Abs. 2 DSG NW verlangt nach meiner Auffassung Vorkehrungen, die eine derartige Interessenkollision von vornherein ausschließen.

Weitere besondere Anordnungen sind vorzusehen, wenn zur Unterstützung der Statistikdienststelle die Automatisierte Datenverarbeitung eingesetzt wird; hierbei kann der Runderlaß des Innenministers vom 10. 04. 1987 (s. o. S. 82) in den Ziffern 3 bis 6 entsprechende Anhaltspunkte geben.

Bei der Weitergabe statistischer Ergebnisse an die anderen Verwaltungsstellen muß besonders geregelt sein, bis zu welcher statistischen Einheit die aggregierten Daten weitergegeben werden dürfen, um eine Reidentifizierung der betroffenen Bürger – auch mit Zusatzwissen – auszuschließen. Der Leiter der Statistikdienststelle muß hierfür das notwendige Fachwissen haben.

6.9 Schule

6.9.1 Schüler- und Elterndaten

Daß der Datenschutz auch bei der Datenverarbeitung an den Schulen gewährleistet sein muß, ist heute anerkannt. In den vorangegangenen Tätigkeitsberichten habe ich zu zahlreichen Einzelfragen Stellung genommen, die an mich herangetragen worden sind oder auf die ich bei Kontrollbesuchen gestoßen bin. Dabei war ich stets bemüht, bei der notwendigen Durchsetzung datenschutzrechtlicher Bestimmungen die Belange der Praxis mit zu berücksichtigen. Die zunehmende Zahl von Eingaben aus dem schulischen Bereich macht deutlich, daß sich bei Schülern, Lehrern und Eltern ein ausgeprägtes Datenschutzbewußtsein entwickelt hat.

Mit seinem Runderlaß vom 10. März 1983 – Verwaltungsvorschriften (VVzASchO) zu § 5 Abs. 4 der Allgemeinen Schulordnung – **Richtlinien zum Schülerstammblatt** und zum sonstigen Datenbestand in der Schule – hat der Kultusminister für die Verarbeitung von Schülerdaten grundlegende Datenschutzregelungen getroffen. An der ursprünglichen Fassung dieser Vorschriften und an der Änderung durch den Runderlaß vom 29. Juli 1986 bin ich beteiligt gewesen. Die Verwaltungsvorschriften haben sich in der Praxis bewährt. Sie können allerdings auf Dauer die in diesem Bereich erforderliche gesetzliche Regelung nicht ersetzen (vgl. oben S. 39/40).

Durch Änderungserlaß vom 1. Juni 1988 hat der Kultusminister eine vorläufige Anpassung der Richtlinien zum Schülerstammblatt an die durch das Inkrafttreten des neuen Datenschutzgesetzes Nordrhein-Westfalen veränderte Lage vorgenommen. Hierbei ist jedoch im wesentlichen nur eine Anpassung im Wortlaut erfolgt. Grundlegende Änderungen der Rechtslage, die das neue Datenschutzgesetz mit sich gebracht hat, sind bisher nicht ausreichend berücksichtigt. Ich halte es daher für erforderlich, daß kurzfristig eine weitere Überarbeitung der VVzAschO erfolgt. Dies gilt insbesondere für die Vorschriften über die Übermittlung oder Weitergabe von Daten und über die Datenverarbeitung durch den kommunalen Schulträger (Nr. 4 und Nr. 5 VVzAschO).

Der zulässige Inhalt von **Klassenbüchern** wird ebenfalls durch die Richtlinien festgelegt. Auch hierzu habe ich in der Vergangenheit wiederholt Stellung genommen. Ergänzungen der Richtlinien, die aus rechtlichen Gründen sowie aus Notwendigkeiten der Praxis erforderlich geworden sind, hat der Kultusminister durch Runderlaß vom 29. Juli 1986 festgelegt. Danach können die Anschriften und Telefonnummern der Erziehungsberechtigten in das Klassenbuch aufgenommen werden, wenn diese nicht widersprochen haben. Dagegen ist die Liste der schriftlichen Arbeiten und von deren Ergebnissen nicht mehr im Klassenbuch, sondern als gesonderte Unterlage zu führen. Die Eintragung eines Tadels in das Klassenbuch war bereits in der ursprünglichen Fassung der Richtlinien nicht vorgesehen und ist daher wegen ihrer abschließenden Natur nicht zulässig.

Nach dem Runderlaß vom 29. Juli 1986 enthalten die VVzAschO nunmehr auch die notwendige Regelung, daß im Bereich der berufsbildenden Schulen personenbezogene Daten an die **Arbeitgeber und Ausbildungsbetriebe** übermittelt werden dürfen, wenn dies zur rechtmäßigen Erfüllung der Aufgaben der Schule oder der durch Rechtsvorschrift festgelegten Verpflichtungen des Arbeitgebers oder Ausbildungsbetriebes erforderlich ist. Dieser Informationsaustausch entspricht dem dualen System der Berufsausbildung (§ 1 Abs. 5 des Berufsbildungsgesetzes), nach welchem Ausbildungsbetrieb und Schule gemeinsam für den Ausbildungserfolg verantwortlich sind; er ist nach § 16 Abs. 1 Satz 1 Buchstabe a DSG NW zulässig. In der Praxis ergeben sich jedoch immer wieder Unklarheiten, in welchem Umfang derartige Datenübermittlungen zulässig sind: etwa ob bereits Mißerfolge bei einzelnen Aufgaben oder gelegentlich auftretende Verspätungen in der Schule dem Ausbildungsbetrieb mitgeteilt werden dürfen oder ob – was nach meiner Auffassung zutreffend ist – solche Mitteilungen erst erfolgen dürfen, wenn ein wesentliches Abfallen der Leistungen eines Schülers festzustellen ist.

Soweit ersichtlich, ist diese Frage weder in einer Schulordnung noch in Erlassen des Kultusministers oder sonstigen Verwaltungsvorschriften geregelt. Es entspricht nach meiner Auffassung jedoch einem Bedürfnis der Praxis, und gleichzeitig würde es der Klarstellung der Zulässigkeit derartiger Übermittlungen nach § 16 Abs. 1 Satz 1 Buchstgabe a DSG NW dienen, wenn durch entsprechende Vorschriften nähere Vorgaben für den Informationsaustausch zwischen Schule und Ausbildungsbetrieb gegeben würden.

Nach der gegenwärtigen Fassung der VVzAschO ist eine Übermittlung von Daten ehemaliger Schüler an einen Mitschüler, der ein **Klassentreffen** organisieren will, nicht zulässig. Die Richtlinien zum Schülerstammblatt und zum sonstigen Datenbestand in der Schule sind in dieser Frage enger als die Rechtslage. Denn bereits nach dem bis zum April 1988 geltenden Recht habe ich die Auffassung vertreten, daß die Schule derartigen Übermittlungswünschen in der Regel entsprechen kann. Nunmehr richtet sich die Zulässigkeit dieser Übermittlung nach § 16 Abs. 1 Satz 1 Buchstabe d DSG NW, wobei die Betroffenen nach Satz 2 vor der Übermittlung zu unterrichten sind und dieser widersprechen können. Ich hätte keine datenschutzrechtlichen Bedenken, wenn die VVzAschO zu dieser Frage ergänzt würden, so daß eine Berücksichtigung des in der Praxis nicht seltenen Wunsches zur Übermittlung von Adressen ehemaliger Schüler zum Zweck der Organisation von Klassentreffen möglich wird.

6.9.2 Generelles Schulinformationssystem

Von der gemeinsamen kommunalen Datenverarbeitungszentrale Emscher/Lippe ist unter der Bezeichnung GESI ein Datenverarbeitungssystem entwikkelt worden, das als „Generelles Schulinformationssystem" bezeichnet wird. Hierauf bezogen sich auch im Berichtszeitraum mehrere Eingaben.

GESI wird von den betreffenden Städten zur Erfüllung der ihnen als Schulträger obliegenden Aufgaben angewandt und kann von den Schulen zur automatisierten Verarbeitung bestimmter Angaben aus den Schülerstammblättern sowie für Zwecke der unteren Schulaufsichtsbehörde mitgenutzt werden.

Nach § 2 des Schulverwaltungsgesetzes (SchVG) sind die Gemeinden als Schulträger für die Errichtung, Organisation und Verwaltungsführung der Schulen verantwortlich. Sie beschließen über die Errichtung, Änderung und Auflösung öffentlicher Schulen (§§ 8, 10 SchVG) und sind verpflichtet, zur Sicherung eines gleichmäßigen Schulangebots für ihren Bereich einen Schulentwicklungsplan aufzustellen und fortzuschreiben (§10 b SchVG).

Nach den Vorschriften des Schulfinanzgesetzes sind die Gemeinden zur Tragung der Sachausgaben (Aufwendungen für Bau, Erhaltung und Einrichtung) der öffentlichen Schulen verpflichtet; zu den Sachausgaben gehören auch die Schülerfahrkosten. Darüber hinaus unterstützen die Gemeinden die in ihrer Trägerschaft stehenden Schulen bei der Schulanmeldung sowie bei der Überwachung der Schulpflicht nach den §§ 10 bis 20 des Schulpflichtgesetzes.

GESI dient einer rationelleren Abwicklung der im Rahmen dieser gesetzlichen Aufgaben anfallenden Verwaltungstätigkeiten. Seine Programmziele sind insbesondere

- Bereitstellung von Planungs- und Organisationsdaten für die Schulentwicklung und Schulorganisation,
- Unterstützung bei der Schulpflichtüberwachung,
- Rationalisierung der Verwaltungsarbeit in den Schulen und in der Schulverwaltung.

GESI enthält die zur Erfüllung dieser gesetzlichen Aufgaben erforderlichen personenbezogenen Angaben von Schülern. Diese Daten, die der Schulträger auf Grund der genannten gesetzlichen Vorschriften erheben und weiterverarbeiten darf, entsprechen einem Teil des erheblich umfangreicheren Datenkataloges der Anlage I bis III der Richtlinien zum Schülerstammblatt und zum sonstigen Datenbestand in der Schule.

Eine Erweiterung der Nutzung des Generellen Schulinformationssystems GESI wird durch den Umstand ermöglicht, daß diejenigen Schülderdaten, die der Schulträger zur Erfüllung seiner Aufgaben aus eigenem Recht verarbeiten darf, auch Bestandteil des von der Schule zu führenden Schülerstammblattes sind. Dieser gemeinsame Grunddatenbestand wird von dem Schulträger als Schülerindividualdatei für eigene Zwecke verarbeitet. Auf Grund der Kongruenz der Daten bietet der Schulträger den Schulen an, diese Daten als Teil des von ihnen zu führenden Schülerstammblattes in dem Informationssystem GESI zu verarbeiten. Diejenigen Schulen, die von dem Service-Angebot des Schulträgers Gebrauch machen, bleiben Herr der Daten; der Schulträger verarbeitet die Daten insoweit in ihrem Auftrag. Die Verarbeitung von Daten des Schülerstammblattes in kommunalen ADV-Anlagen ist nach Nr. 2.5 i. V. m. Nr. 6.1 VVzASchO zulässig.

GESI bietet für die Schulen die Möglichkeit, sich im Rahmen der Auftragsdatenverarbeitung Organisationsmittel wie Schülerlisten, Adreßaufkleber, vorbereitete Zeugnisformulare erstellen zu lassen.

Die übrigen Daten des Schülerstammblattes der Schulen dürfen allerdings nicht in GESI, sondern nur an der Schule selbst gespeichert werden. Dies kann in herkömmlicher Weise oder in schuleigenen Anlagen (Nr. 2.5 VVzA-SchO) geschehen.

Eine von mir bei einem Schulträger vorgenommene Überprüfung der in GESI enthaltenen Einzeldaten hat ergeben, daß die Angabe der **Krankenkasse** des Schülers gespeichert wird. Dieses Datum ist jedoch weder im Datenkatalog der Anlage I bis III der Richtlinien zum Schülerstammblatt enthalten, noch ist seine Kenntnis für die Erfüllung von Aufgaben des Schulträgers erforderlich.

In dem erwähnten Fall enthielt GESI für die berufsbildenden Schulen zudem auch die Angaben von Name, Anschrift und Telefonnummer des Ausbildungsbetriebes, obwohl diese Daten für die Aufgabenerfüllung des Schulträgers nicht erforderlich sind. Dieser Umstand war in der historischen Entwicklung des Informationssystems bei dem Schulträger begründet. Ich habe dazu empfohlen, diese Angaben aus dem in GESI gemeinsam geführten Datenbestand herauszunehmen. Sie sind dann, wie auch die übrigen in dem Datenkatalog der Anlage I bis III der Richtlinien zum Schülerstammblatt aufgeführten Daten, in Dateien der Schulen zu führen.

Im übrigen habe ich gegen eine gemeinsame Verarbeitung der im Datenkatalog von GESI gespeicherten Daten für Aufgaben des Schulträgers und der Schulen keine datenschutzrechtlichen Bedenken. Allerdings muß durch die

Konfiguration der beim Schulträger und bei den Schulen eingesetzten ADV-Anlagen und die angewandte Software sichergestellt sein, daß der Schulträger nicht auf die bei den Schulen geführten schulinternen Dateien (z.B. Leistungsdateien, Stundenplandateien) zugreifen kann. Dieser Gefahr ist insbesondere bei dem Bestehen einer On-line-Verbindung zwischen Datenverarbeitungsanlagen der Schulen und des Schulträgers durch programmtechnische Maßnahmen vorzubeugen.

Die wenig glückliche Bezeichnung „Generelles Schulinformationssystem" mag dazu beigetragen haben, den Eindruck entstehen zu lassen, durch GESI könne der Schulträger auf die Schülerstammblattdaten der angeschlossenen Schulen zugreifen. Tatsächlich jedoch sollte lediglich das ursprünglich als „Gelsenkirchener Schulinformationssystem" entwickelte Datenverarbeitungssystem den hieraus abgeleiteten Kurznamen GESI auch nach der Übernahme durch andere Städte beibehalten. Im Interesse von mehr Transparenz bei der Verarbeitung personenbezogener Daten wäre es zu begrüßen, wenn diejenigen Schulträger, die GESI benutzen, die Schulen und auch die Lehrerschaft über die Möglichkeiten und Beschränkungen des Systems weitergehend als bisher unterrichten würden.

6.9.3 Weitergabe von Elterndaten an politische Parteien

Im Zusammenhang mit einer Elternbefragung zur Feststellung des Bedürfnisses für eine Gesamtschule nach § 10 Abs. 2 und 4 des Schulverwaltungsgesetzes habe ich bislang eine Weitergabe von Elternadressen an politische Parteien und örtliche Initiativen als datenschutzrechtlich zulässig angesehen. Das Inkrafttreten des neuen Datenschutzgesezes sowie weitere Bürgereingaben zu dieser Frage haben mich jedoch zur Überprüfung der zuletzt in meinem 7. Tätigkeitsbericht (S. 117/118) dargelegten Auffassung veranlaßt.

Die Zulässigkeit der Übermittlung dieser Daten ist nunmehr nach § 16 Abs. 1 Satz 1 Buchstabe d und Satz 2 DSG NW zu beurteilen, soweit die Elternadressen aus Unterlagen des Schulverwaltungsamtes oder Schulamtes stammen. Danach ist eine Übermittlung zulässig, wenn sie im öffentlichen Interesse liegt oder hierfür ein berechtigtes Interesse geltend gemacht wird und der Betroffene in diesen Fällen der Datenübermittlung nicht widersprochen hat. Ein **berechtigtes** Interesse der jeweiligen politischen Partei oder örtlichen Initiative ist hierbei in aller Regel anzuerkennen. Der Betroffene ist über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten, den Verwendungszweck wie auch über sein Widerspruchsrecht in geeigneter Weise zu unterrichten. Werden die Elternadressen dagegen dem Melderegister entnommen, so ist eine Übermittlung nach § 34 Abs. 3 Satz 1 des Meldegesetzes für das Land Nordrhein-Westfalen (MG NW) nur zulässig, soweit eine derartige Gruppenauskunft im **öffentlichen** Interesse liegt. Dies habe ich bisher bejaht. Allerdings haben betroffene Bürger gegen diese Auslegung zunehmend Einwendungen vorgebracht. Die Betroffenen weisen darauf hin, daß die politischen Parteien und örtlichen Initiativen auch ohne direkte Anschreiben an die Eltern in der Lage seien, ihre politische Auffassung gegenüber den in Betracht kom-

menden Eltern zu verdeutlichen: etwa durch Flugblätter, Anzeigen oder Kundgebungen. Es bestehen daher Zweifel, ob in derartigen Fällen das Vorliegen eines öffentlichen Interesses noch anzunehmen ist.

Nach § 7 Satz 1 und 2 MG NW dürfen schutzwürdige Belange der Betroffenen durch die Verarbeitung oder sonstige Nutzung personenbezogener Daten der Meldebehörde nicht beeinträchtigt werden. Schutzwürdige Belange werden insbesondere beeinträchtigt, wenn die Verarbeitung oder sonstige Nutzung, gemessen an ihrer Eignung und ihrer Erforderlichkeit zu dem vorgesehenen Zweck, den Betroffenen unverhältnismäßig belastet.

Im Hinblick darauf, daß Eltern die Bekanntgabe ihrer Daten an politische Parteien und örtliche Initiativen sowie deren briefliche Kontaktaufnahmen als unerwünschtes Eindringen in ihre Privatsphäre betrachtet haben, kann bei einer Interessenabwägung ein Zurücktreten ihrer schutzwürdigen Belange nicht länger als gerechtfertigt angesehen werden.

Im Ergebnis halte ich daher meine Auffassung nicht länger aufrecht, daß Melderegisterauskünfte auf Grund von § 34 Abs. 3 MG NW an politische Parteien und örtliche Initiativen im Zusammenhang mit einer Elternbefragung zur Feststellung des Bedürfnisses für eine Gesamtschule nach § 10 Abs. 2 und 4 SchVG zulässig sind.

6.9.4 Lehrerdaten

Immer wieder betreffen Eingaben die Frage, in welchem Umfang ein **Schulleiter** personenbezogene Daten der an seiner Schule eingesetzten Lehrer erheben und festhalten darf und wann eine Löschung dieser Daten zu erfolgen hat.

Nach § 29 Abs. 1 Satz 1 DSG NW dürfen Daten von Beschäftigten nur verarbeitet werden, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht. Erforderlich sind insbesondere solche Angaben, die zur Wahrnehmung der in § 20 Abs. 2 des Schulverwaltungsgesetzes (SchVG) festgelegten Aufgaben eines Schulleiters als Leiter der Schule und Vorgesetzter aller an der Schule tätigen Personen benötigt werden. Zu diesen Aufgaben gehören beispielsweise die Erstellung von Stunden- und Vertretungsplänen. In der „Dienstanweisung für automatisierte Verarbeitung von personenbezogenen Daten in der Schule" (RdErl. vom 15. 09. 1988 – GABl. NW. S. 442 –) hat der Kultusminister einen verbindlichen Katalog von Daten und Verwendungszwecken festgelegt, der für die automatisierte Verarbeitung von personenbezogenen Lehrerdaten für Schulleiteraufgaben eine abschließende Regelung bedeutet.

Für Lehrerdaten, die in herkömmlicher Form gespeichert werden – etwa in Akten oder Bögen – gibt es bisher keine solche verbindliche Festlegung. Es muß daher jeweils im Einzelfall entschieden werden, ob und wie lange die Kenntnis

einzelner Daten für die Aufgaben eines Schulleiters erforderlich ist. Wie immer ist auch in diesem Zusammenhang an die Erforderlichkeit ein strenger Maßstab anzulegen. Dabei ist zu berücksichtigen, daß der Schulleiter nicht Dienstvorgesetzter der an seiner Schule tätigen Lehrer und nicht personalaktenführende Stelle ist. Hierdurch ergeben sich dem Umfang nach Grenzen für ein Festhalten von Lehrerdaten durch den Schulleiter. Eine Datensammlung, die den Umfang einer „zweiten Personalakte" erreicht, ist daher nicht zulässig. Auch gegen ein zeitlich unbegrenztes Festhalten von Daten bestehen datenschutzrechtliche Bedenken. Wegen der grundsätzlichen Bedeutung der Angelegenheit habe ich den Kultusminister um Prüfung gebeten, ob eine verbindliche Festlegung der Datenverarbeitung personenbezogener Lehrerdaten für Schulleiteraufgaben – einschließlich der Speicherungsdauer – auch für das Verarbeiten dieser Daten in Akten oder anderen Unterlagen getroffen werden kann.

Zur Übermittlung von Lehrerdaten an den **Schulträger** habe ich in meinen früheren Tätigkeitsberichten darauf hingewiesen, daß die Übersendung von Durchschriften der vollständigen Erhebungsbögen SCD 021, LID 121, UVD 221 und KLD 321 nicht zulässig ist (vgl. 8. Tätigkeitsbericht, S. 89/90). Die Landesregierung hat hierzu in ihrer Stellungnahme erklärt, der Kultusminister werde meine Empfehlung folgen, und die vollständigen Erhebungsbögen würden in Zukunft den Schulträgern nicht mehr zugeleitet. In der Zwischenzeit sind die Bögen SCD 021, UVD 221 und KLD 321 so umgestaltet worden, daß eine Übermittlung personenbezogener Lehrerdaten entfällt. Von dem Bogen LID 121 erhält der Schulträger in Zukunft keine Durchschrift mehr. Diese Änderung des Verfahrens wird leider erst für die Oktoberstatistik 1989 wirksam.

Die Zahl der Eingaben, die sich gegen die Übermittlung personenbezogener Daten von Lehrern an den Schulträger im Rahmen seiner Beteiligung bei der Anstellung, Beförderung und Versetzung gemäß § 23 SchVG richtet, ist derzeit rückläufig. Ich führe dies auch darauf zurück, daß der Kultusminister durch Runderlaß vom 24. Februar 1987 (GABl. NW. S. 113, BASS 21-01 Nr. 1) Verwaltungsvorschriften zur Anwendung des § 23 SchVG erlassen und dabei auch die Übermittlung von Personalangaben an den Schulträger neu geregelt hat. Das Festhalten und Aufbewahren dieser Lehrerdaten nach Abschluß des Beteiligungsverfahrens, etwa in einer „Schulträgerakte", ist allerdings nicht zulässig, weil § 23 SchVG dafür keine gesetzliche Grundlage sein kann. Auch hierauf habe ich bereits früher hingewiesen (8. Tätigkeitsbericht, S. 90/91). Diese Auffassung wird auch vom Kultusminister geteilt. Um in der Praxis solche unzulässigen Datensammlungen zu verhindern, halte ich es für erforderlich, durch eine Änderung der Verwaltungsvorschriften zur Anwendung des § 23 SchVG vorzusehen, daß die von dem Schulträger in diesem Verfahren benötigten Lehrerdaten von der Schulaufsichtsbehörde nur unter der Auflage mitgeteilt werden, die Daten nach Abschluß des Verfahrens zurückzugeben oder zu vernichten.

Nicht selten beklagen sich Lehrer über den Mißstand, daß bei der **Besetzung von Schulleiterstellen** nicht nur ihre Namen, sondern vielfach auch sehr weitgehende Einzelheiten zum Besetzungsverfahren in der **örtlichen Presse** mitgeteilt werden. Hierbei wird häufig die Vermutung geäußert, von seiten des Schulträgers wären entsprechende Informationen an die Presse weitergegeben worden. Dies wäre datenschutzrechtlich unzulässig. Zwar sind nach § 4 Abs. 1 des Landespressegesetzes (LPG) die Behörden verpflichtet, den Vertretern der Presse die zur Erfüllung ihrer Aufgaben dienenden Auskünfte zu erteilen. In den hier genannten Fällen bestünde ein solcher Anspruch jedoch nicht, da Personaldaten grundsätzlich geheimzuhalten sind (§ 4 Abs. 2 Nr. 2 LPG) und darüber hinaus die Auskunft ein schutzwürdiges privates Interesse verletzen würde (§ 4 Abs. 2 Nr. 3 LPG).

Die Befürchtung einer unzulässigen Weitergabe von Lehrerdaten durch öffentliche Stellen wurde im Berichtszeitraum erneut im Zusammenhang mit der Herausgabe des **Philologen-Jahrbuchs** (Kunzes Kalender) geäußert. Hierauf bezog sich auch die Kleine Anfrage 1391, die von der Landesregierung am 26. Oktober 1988 beantwortet wurde (Drucksache 10/3727). Eine Übermittlung von Lehrerdaten an den Herausgeber des Jahrbuchs ist nur mit schriftlicher Einwilligung des Betroffenen zulässig. Der Kultusminister hat darauf bereits mit Runderlaß vom 13. August 1980 hingewiesen. Dem Erfordernis einer schriftlichen Einwilligung durch den Betroffenen genügt es nicht, wenn ein „Vertrauenslehrer" dem Herausgeber des Philologen-Jahrbuchs eine Liste mit den Daten der an seiner Schule tätigen Kollegen übermittelt und dazu schriftlich versichert, die Einwilligung des Betroffenen zur Übermittlung und Aufnahme der Daten in das Philologen-Jahrbuch liege vor. Eine schriftliche Bestätigung einer dritten Person darüber, daß ein Lehrer ihr gegenüber die Einwilligung mündlich erteilt habe, kann die geforderte eigene Erklärung der Einwilligung durch den Betroffenen nicht ersetzen.

Die Datenerhebung des Herausgebers im Kollegenkreis durch Vertrauenslehrer unterliegt jedoch nicht meiner Kontrolle, da es sich hierbei nicht um öffentliche Stellen des Landes handelt. Den durch unzulässige Veröffentlichungen ihrer Daten betroffenen Lehrkräften ist zu empfehlen, gegebenenfalls den Philologenverband Nordrhein-Westfalen, Am Ringofen 10, 4030 Ratingen 4, darauf hinzuweisen, daß ihre Daten ohne gültige Einwilligung in das Philologen-Jahrbuch aufgenommen worden sind und darauf zu dringen, daß diese in der nächsten Ausgabe nicht mehr aufgenommen werden. Ebenso besteht die Möglichkeit, sich an die für die Überwachung des Datenschutzes im nicht-öffentlichen Bereich örtlich zuständige Aufsichtsbehörde nach § 30 Abs. 1 BDSG zu wenden. Im Falle des Philologenverbandes Nordrhein-Westfalen, Ratingen, ist dies der Regierungspräsident Köln, Zeughausstraße 4–8, 5000 Köln 1.

6.10 Umweltdaten

Bei öffentlichen Stellen im Lande Nordrhein-Westfalen werden seit langem für vielfältige Aufgaben im großen Umfang „Umweltdaten" gesammelt und in Kartierungen, Dateien oder besonderen Verzeichnissen zusammengestellt. In diesem Zusammenhang werden zunehmend Datenschutzfragen an mich herangetragen.

In der Antwort der Landesregierung auf die Kleine Anfrage 109 (Drucksache 10/574) werden über 70 Sammlungssysteme zu Umweltdaten angegeben, die bei Landesbehörden oder Kommunalbehörden geführt werden. Dabei handelt es sich allerdings nicht in allen Fällen um personenbezogene Daten im Sinne von § 3 Abs. 1 DSG NW. So wird z. B. das bei der Landesanstalt für Immissionsschutz geführte Immissionskataster in einem Raster von 8 × 8 km geführt, für andere Kataster, etwa das Emmissionskataster oder den Luftreinhalteplan, ist ein Raster von 1 × 1 km vorgesehen. Es ist davon auszugehen, daß derart **großräumige Angaben** nicht als Aussagen zu einzelnen Grundstükken anzusehen sind.

Darüber hinaus muß auch bei Umweltdaten, die eindeutig auf ein einzelnes Grundstück beziehbar sind, nach dem Schutzzweck des Datenschutzgesetzes geprüft werden, inwieweit es gerechtfertigt ist, sie als personenbezogene Daten im Sinne von § 3 Abs. 1 DSG NW anzusehen. Hierfür reicht der rechtstheoretische Ansatz, nach dem alle Angaben bezüglich eines Grundstückes eine Aussage über die sachlichen Verhältnisse des Grundstückseigentümers darstellen, nach meiner Auffassung nicht aus. Als Beispiel hierfür sei auf das Biotopkataster verwiesen, das nach näherer Maßgabe des Runderlasses des Ministers für Umwelt, Raumordnung und Landwirtschaft vom 6. März 1986 bei der Landesanstalt für Ökologie, Landschaftsentwicklung und Forstplanung Nordrhein-Westfalen geführt wird. Die erfaßten Biotope werden in Karten im Maßstab 1:25 000 und in ergänzenden Biotopkatasterblättern dokumentiert. Neben statistischen Angaben zur jeweiligen Fläche enthält jedes Biotopkatasterblatt eine Beschreibung des Gebietes, Angaben zu den bekannten Tier- und Pflanzenvorkommen sowie über Wert, Gefährdung und Vorschläge für die Maßnahmen zur Sicherung und Pflege. Bei diesen Angaben handelt es sich um eine Beschreibung von **Naturgegebenheiten,** die nicht an Grundstücksgrenzen gebunden sind und Veränderungen in zeitlicher und räumlicher Hinsicht unterliegen. Es dürfte verfehlt sein, derartige naturgegebene Angaben als personenbezogene Daten den Regeln des Datenschutzes zu unterwerfen. Sonst müßten Kartierungen, wie etwa die Geologische Karte Nordrhein-Westfalen, die Angaben enthält über die Beschaffenheit der an der Erdoberfläche anstehenden Gesteinsfolgen, Vorkommen und Nutzungsmöglichkeit von Rohstoffen, Böden und Grundwasser, u. U. ebenfalls als personenbezogene Aussagen angesehen werden.

Angaben über **Altlasten** sind dagegen, sofern sie parzellenscharf einem Grundstück zugeordnet werden können, Angaben über sachliche Verhältnisse des Eigentümers und damit personenbezogene Daten, wenn der Grundstückseigentümer eine natürliche Person ist. Die Unterscheidung zu den vorerwähnten, durch die Natur vorgegebenen Beschaffenheiten eines Grundstücks ergibt sich u. a. aus der Überlegung, daß Altlasten aus Handlungen oder Unterlassungen des Grundstückseigentümers oder seiner Rechtsvorgänger resultieren.

Die Frage, an wen unter welchen Voraussetzungen welche Daten aus den bei Verwaltungsbehörden geführten Umweltdaten-Sammlungssystemen bekannt-

gegeben werden dürfen, führt in der Praxis immer wieder zu Schwierigkeiten. Zum Teil fehlen gesetzliche Grundlagen für die Bekanntgabe personenbezogener Daten, zum Teil sind sie unterschiedlich ausgestaltet. Die Freie und Hansestadt Hamburg hat daher im April 1987 im Bundesrat den Entwurf eines Umweltdatenauskunftsgesetzes eingebracht (Bundesratsdrucksache 172/87). Damit sollte ein gesetzlich verankerter Anspruch der Bürger gegenüber der Umweltverwaltung geschaffen werden, Auskunft über bestimmte Umweltdaten zu erhalten, sowie der Verwaltung das Recht eingeräumt werden, diese Daten von sich aus zu veröffentlichen. Ein ähnliches Ziel verfolgt der von den GRÜNEN im November 1987 im Bundestag eingebrachte Entwurf eines Gesetzes über das Einsichtsrecht in Umweltakten (Bundestagsdrucksache 11/1152).

Derartige Initiativen greifen einen Trend auf, der im Ausland in einer Diskussion um **Aktenöffentlichkeit** bereits seit längerer Zeit deutlich hervorgetreten ist und z. B. im amerikanischen „freedom of information act" von 1967 zu gesetzgeberischen Konsequenzen geführt hat. Der Bundesrat hat die Gesetzesinitiative der Stadt Hamburg hauptsächlich aus Gründen der fehlenden Gesetzgebungszuständigkeit des Bundes abgelehnt. Die zuständigen Ausschüsse haben jedoch in der Begründung der entsprechenden Beschlußempfehlung anerkannt, daß die Information der breiten Öffentlichkeit über Umweltdaten eine entscheidende Voraussetzung für wirksamen Umweltschutz ist, und haben darauf hingewiesen, daß bereits auf Grund von Rechtsvorschriften vielfältige Informationsrechte der betroffenen Bürger und der Öffentlichkeit bestehen. Diese Informationsrechte seien vorrangig zu erfüllen. Etwa vorhandene Regelungslücken seien spezialgesetzlich zu schließen.

Verständlicherweise werden datenschutzrechtliche Hindernisse beim Zugang zu Umweltdaten nicht gerade erfreut zur Kenntnis genommen. So wird auch in der Kleinen Anfrage 109 (Drucksache 10/574) ausgeführt, es erweise sich bei der Unterstützung des Verfassungsauftrages aus Artikel 29 a der Landesverfassung, die natürlichen Lebensgrundlagen zu schützen, als hinderlich, wenn die zuständigen Stellen des Landes unter Berufung auf den Datenschutz die Bekanntgabe von Umweltdaten über Betriebe ablehnten, die Schadstoffbelastungen der natürlichen Lebensgrundlagen bewirken.

Eingriffe in das Recht auf informationelle Selbstbestimmung sowie in das Grundrecht auf Datenschutz können jedoch nicht unmittelbar auf Artikel 29 a gestützt werden. Artikel 29 a, der im Jahre 1985 in die Verfassung des Landes Nordrhein-Westfalen eingefügt worden ist, stellt die natürlichen Lebensgrundlagen und die Umwelt unter den Schutz des Landes, der Gemeinden und der Gemeindeverbände. Die Vorschrift enthält eine Staatszielbestimmung und ist insbesondere bei der Ermessensausübung von Gesetzgebung und Verwaltung von Bedeutung. Subjektiv-öffentliche Rechte des einzelnen werden durch die Vorschrift nicht begründet. Das **Staatsziel Umweltschutz** kann jedoch ein überwiegendes Allgemeininteresse begründen, das Voraussetzung für die Zulässigkeit von Grundrechtseingriffen durch den Gesetzgeber ist.

Ich habe daher nach sorgfältiger Prüfung keine datenschutzrechtlichen Bedenken dagegen erhoben, daß die Landesregierung in dem Gesetzentwurf zur Änderung des Landeswassergesetzes – LWG – vom 3. Dezember 1987 (Drucksache 10/2661) nunmehr durch eine Änderung des § 160 Abs. 1 LWG für jeden Bürger ein freies Einsichtsrecht in die **Wasserbücher** einräumen will. Nach der bisherigen Fassung der Vorschrift ist hierfür ein berechtigtes Interesse erforderlich. In den Ländern Bremen, Hamburg und Hessen ist eine entsprechende Öffnung der Wasserbücher bereits beschlossen worden. Nach der Begründung zum Gesetzentwurf der Landesregierung wird damit dem allgemeinen Bedürfnis nach größerer Publizität des Wasserbuches Rechnung getragen und allen, die an wasserwirtschaftlichen Fragestellungen interessiert sind, eine umfassende Information ermöglicht. Das Interesse der von der Eintragung Betroffenen an der Geheimhaltung bestimmter Unterlagen bleibt durch Absatz 2 der Vorschrift weiterhin geschützt. Danach ist die Einsicht in solche Unterlagen, die Mitteilungen über geheimzuhaltende Betriebseinrichtungen oder Betriebsweisen enthalten, nur nach Zustimmung dessen gestattet, der an der Geheimhaltung ein berechtigtes Interesse hat.

Als ich in meinem 8. Tätigkeitsbericht (S. 124/125) zu der Frage Stellung genommen habe, ob Karten oder Verzeichnisse über Altlasten der Öffentlichkeit zugänglich gemacht werden dürfen, gab es dafür noch keine gesetzliche Grundlage. Im **Abfallgesetz** für das Land Nordrhein-Westfalen vom 21. Juni 1988 – LAbfG – (GV. NW. S. 250) sind nunmehr gesetzliche Regelungen über das Erheben und Speichern von Angaben über Altablagerungen und Altstandorte sowie über die Auskunftserteilung aus den Altlastenkatastern geschaffen worden. Nach § 32 Abs. 1 LAbfG sind die katasterführenden Behörden befugt, anderen Behörden und Einrichtungen des Landes sowie den Gemeinden und Gemeindeverbänden Daten, Tatsachen und Erkenntnisse über Altablagerungen und Altstandorte mitzuteilen, soweit dies zur Wahrnehmung der diesen Stellen auf den Gebieten der Gefahrenermittlung, Gefahrenabwehr, Überwachung oder Planung obliegenden Aufgaben erforderlich ist. Auf Verlangen teilen die katasterführenden Behörden ihnen vorliegende Daten, Tatsachen und Erkenntnisse den Eigentümern und Nutzungsberechtigten mit; sie können auch Dritte unterrichten, soweit diese ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten darlegen. Soweit jedoch Behörden oder andere Stellen Erkenntnisse über Altablagerungen und Altstandorte der Öffentlichkeit zugänglich machen, darf nach Absatz 2 der Vorschrift die Bekanntgabe keine Angaben enthalten, die einen Bezug auf eine bestimmte oder bestimmbare natürliche Person zulassen. Dies gilt nicht, wenn solche Angaben offenkundig sind oder ihre Bekanntgabe zur Abwehr von Gefahren oder aus anderen überwiegenden Gründen des Gemeinwohls erforderlich ist.

Zur Frage der Bekanntgabe von **Angaben über Altlasten** bin ich im Berichtszeitraum von mehreren Gebietskörperschaften um eine Stellungnahme dazu gebeten worden, ob eine Karte oder ein Verzeichnis über Altlasten im Rat oder in dem für diese Fragen zuständigen Umweltausschuß **in öffentlicher Sitzung** behandelt werden darf.

Gesetzliche Grundlage für die Bekanntgabe der Daten an Rats- und Ausschußmitglieder ist im vorliegenden Fall § 14 Abs. 5 i.V.m. § 14 Abs. 1 DSG NW. Die Weitergabe personenbezogener Daten innerhalb einer öffentlichen Stelle – hier: zwischen der Verwaltung und dem Rat bzw. dem Ausschuß – ist danach zulässig, wenn sie zur rechtmäßigen Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist und keine unzulässige Zweckentfremdung der Daten vorliegt. Es ist davon auszugehen, daß der Rat bzw. der zuständige Ausschuß nach den Vorschriften der Gemeindeordnung und der ergänzenden Satzung für die Behandlung von Fragen, die mit Altlasten zusammenhängen, zuständig ist (§§ 28, 41 Abs. 1 und § 41 Abs. 2 Satz 1 der Gemeindeordnung – GO –). Da in diesem Fall die Kenntnis der Daten zur Erfüllung der Aufgaben des Rates bzw. des Ausschusses erforderlich ist, dürfen den Rats- bzw. Ausschußmitgliedern die entsprechenden Daten bekanntgegeben werden.

Soweit die Beratung in öffentlicher Sitzung erfolgen soll, kommen als gesetzliche Grundlage für diese Erweiterung der Bekanntgabe die Vorschriften des § 33 Abs. 2 und § 42 Abs. 2 Satz 1 GO in Betracht. Nach diesen Vorschriften sind die Sitzungen des Rates und seiner Ausschüsse öffentlich. Durch die Geschäftsordnung kann für Angelegenheiten einer bestimmten Art, auf Antrag eines Rats- oder Ausschußmitgliedes oder auf Vorschlag des Gemeindedirektors für einzelne Angelegenheiten die Öffentlichkeit ausgeschlossen werden.

Sitzungen, bei denen in den Anspruch eines Betroffenen auf Schutz seiner personenbezogenen Daten eingegriffen wird, dürfen nach Artikel 4 Abs. 2 der Landesverfassung nur dann öffentlich abgehalten werden, wenn wegen der Bedeutung der Angelegenheit oder im Hinblick auf ihre öffentliche Erörterung ein überwiegendes Interesse der Allgemeinheit an der Behandlung in öffentlicher Sitzung besteht.

Gesichtspunkte, aus denen bei der Behandlung von Angaben über Altlasten in öffentlicher Sitzung eine Beeinträchtigung schutzwürdiger Belange Betroffener folgen kann, können sehr unterschiedlich gelagert sein. Daher muß nach meiner Auffassung zur Beantwortung der Frage, ob das Allgemeininteresse einer öffentlichen Behandlung überwiegt, jeweils eine Einzelfallprüfung stattfinden. Dabei ist als grundsätzliche Vorgabe gemäß Artikel 29 a der Landesverfassung davon auszugehen, daß den Fragen des Umweltschutzes eine hohe Priorität zukommt. Im Einzelfall können jedoch konkrete schutzwürdige Belange eines Betroffenen höher einzuschätzen sein als das Öffentlichkeitsinteresse. In diesen Fällen dürfen die Angaben nur in nicht-öffentlicher Sitzung behandelt werden. Auch der Minister für Umwelt, Raumordnung und Landwirtschaft, den ich in diesem Zusammenhang um eine Stellungnahme gebeten habe, geht davon aus, daß Angaben über Altlasten in öffentlicher Sitzung behandelt werden können, wenn nicht im Einzelfall die Rücksichtnahme auf konkret vorliegende schutzwürdige Belange den Ausschluß der Öffentlichkeit gebieten. Die Vorschrift des § 32 Abs. 2 LAbfG habe insoweit keine andere Regelung getroffen.

Nach dieser Auslegung führt die Vorschrift des § 32 Abs. 2 LAbfG nicht zwangsläufig zu einem Verbot, solche Angaben in öffentlicher Sitzung kommunaler Gremien zu behandeln. Allerdings könnte gegen die Vorschriften der Gemeindeordnung über die Öffentlichkeit vorgebracht werden, daß diese keine dem Gebot der Normenklarheit entsprechende Aussage über die Bekanntgabe personenbezogener Daten treffen, und darüber hinaus, daß auch im Hinblick auf den Verhältnismäßigkeitsgrundsatz in der Gemeindeordnung keine näheren Vorgaben für die Frage des Ausschlusses der Öffentlichkeit bei vorgesehener Behandlung personenbezogener Informationen gegeben werden. Wie auch dieses Beispiel zeigt, empfiehlt es sich, daß der Gesetzgeber insoweit eine entsprechende Änderung der Gemeindeordnung vornimmt (vgl. auch oben S. 14/15).

6.11 Verkehr

6.11.1 Gesundheitsangaben für die Fahrerlaubnis

Wegen der besonderen Gefahren, die von Kraftfahrzeugen ausgehen, hat die Frage der gesundheitlichen Eignung von Fahrzeugführern naturgemäß eine große Bedeutung. Alle Bewerber um eine Fahrerlaubnis haben sich daher einem Sehtest zu unterziehen und die darüber erteilte Sehtestbescheinigung mit den Antragsunterlagen einzureichen (§§ 8 Abs. 2 Nr. 3, 9 a StVZO). Bewerber um eine Fahrerlaubnis der Klasse 2 haben sich einer ärztlichen Untersuchung ihres Gesundheitszustandes zu unterziehen und darüber eine Bescheinigung beizubringen (§§ 8 Abs. 2 Nr. 4, 9 c StVZO).

Für die Beantragung einer Fahrerlaubnis der Klassen 3 und 1 ist dagegen nach der derzeit geltenden gesetzlichen Regelung nicht ausdrücklich vorgeschrieben, daß der Antragsteller ein ärztliches Zeugnis oder ähnliche Unterlagen zum Nachweis seiner gesundheitlichen Eignung vorlegen muß. Die Fahrerlaubnisbehörden verlangen in diesen Fällen jedoch als Anlage zum Antrag auf Erteilung einer Fahrerlaubnis die Ausfüllung eines Gesundheitsfragebogens. Darin werden neben Fragen zum Hör- und Sehvermögen auch eingehende Fragen etwa über das Fehlen von Gliedmaßen, zu Leiden an inneren Organen, Krankheiten des Gehirns und Nervensystems, zum Vorliegen von Suchtkrankheiten und zur Durchführung von Entziehungsmaßnahmen gestellt. Hierzu werde ich immer wieder um Prüfung gebeten, ob der Straßenverkehrsbehörde derartige Fragen, „die nur ein Arzt stellen dürfe", erlaubt seien. Dazu habe ich bereits in meinem 7. Tätigkeitsbericht (S. 132) dargelegt, daß im Antragsverfahren auf Erteilung einer Fahrerlaubnis dem Antragsteller Fragen gestellt werden dürfen, soweit diese für die Beurteilung seiner Eignung zum Führen von Kraftfahrzeugen erheblich und für den Betroffenen nicht unzumutbar sind. Eine Verpflichtung des Antragstellers zur Beantwortung der Fragen über seinen Gesundheitszustand besteht nicht.

Allerdings muß er bei Nichtbeantwortung damit rechnen, daß die Behörde die Vorlage anderer geeigneter Unterlagen verlangt, die eine Prüfung der Kraftfahrtauglichkeit ermöglichen. In Betracht kommt in solchen Fällen dann ins-

besondere ein ärztliches (oder nach Wahl des Betroffenen amtsärztliches) Zeugnis, in dem bescheinigt wird, daß der Antragsteller geistig und körperlich uneingeschränkt oder nur eingeschränkt zum Führen von Kraftfahrzeugen geeignet ist und ggf., welche Einschränkung vorliegt.

Zwar besteht für die Klassen 3 und 1 keine ausdrücklich normierte Verpflichtung zur Beibringung einer solchen Bescheinigung über den Gesundheitszustand. Andererseits hat die Straßenverkehrsbehörde insoweit eine Ermittlungspflicht, und der Antragsteller soll nach § 26 Abs. 2 des Verwaltungsverfahrensgesetzes bei der Ermittlung des Sachverhalts mitwirken. Dennoch bleibt die Frage, ob die Straßenverkehrsbehörde jemanden, der sich weigert, den Gesundheitsfragebogen auszufüllen und auch nicht bereit ist, eine ärztliche Bescheinigung über seinen Gesundheitszustand vorzulegen, allein deshalb als ungeeignet zum Führen von Kraftfahrzeugen ansehen und ihm die beantragte Fahrerlaubnis versagen darf. Im Interesse der Rechtssicherheit erscheint mir hier eine gesetzliche Regelung geboten.

6.11.2 Frühere Straftaten

Bei der Entscheidung über die Neuerteilung einer Fahrerlaubnis nach vorangegangener Entziehung werden von der Straßenverkehrsbehörde oftmals Straftaten berücksichtigt, die schon sehr lange Zeit zurückliegen und im Bundeszentralregister bereits getilgt sind. Dies ruft immer wieder den Unwillen der Betroffenen hervor, die eine solche Praxis für datenschutzrechtlich unzulässig erachten und sich bei mir beschweren.

Nach § 51 Abs. 1 des Bundeszentralregistergesetzes (BZRG) darf eine Verurteilung wegen einer Straftat nach Tilgung in dem Register dem Betroffenen im Rechtsverkehr grundsätzlich nicht mehr vorgehalten und nicht mehr zu seinem Nachteil verwertet werden. Eine Ausnahme von dem Verwertungsverbot gilt allerdings bei Verfahren, die die Erteilung einer Fahrerlaubnis zum Gegenstand haben, wenn die Verurteilung wegen dieser Tat in das Verkehrszentralregister einzutragen war (§ 52 Abs. 2 BZRG). Nach dieser Rechtslage kann die Verwertung früherer Straftaten auch nach Tilgung dieser Delikte im Bundeszentralregister und im Verkehrszentralregister in Fahrerlaubnisangelegenheiten grundsätzlich nicht beanstandet werden.

Die gegenwärtige Rechtslage nach § 52 Abs. 2 BZRG wird jedoch nicht nur von den Betroffenen als unbefriedigend angesehen, weil sie dem Bewährungsgrundsatz in keiner Weise Rechnung trägt. Auch der Bundesminister für Verkehr hat in einem Schreiben gegenüber dem Bundesbeauftragten für den Datenschutz eingeräumt, daß die derzeitige Gesetzeslage in der Praxis zu Ergebnissen führen kann, die für den Betroffenen nur schwer verständlich sind. Die Datenschutzbeauftragten des Bundes und der Länder haben sich daher schon seit längerem dafür eingesetzt, daß eine frühere Tat in einem Verfahren auf Erteilung oder Entziehung einer Fahrerlaubnis nur berücksichtigt werden darf, solange die Verurteilung wegen dieser Tat im Verkehrszentralregister eingetragen ist. Damit würde eine angemessene Begrenzung der Verwertbarkeit

früherer Straftaten erreicht. Deswegen begrüße ich, daß der Bundesminister der Justiz dieser Empfehlung in seinen Vorschlägen zur Änderung des Bundeszentralregistergesetzes durch folgende Neufassung des § 52 Abs. 2 BZRG wie folgt Rechnung getragen hat:

„(2) Abweichend von § 51 Abs. 1 darf eine frühere Tat ferner in einem Verfahren berücksichtigt werden, das die Erteilung oder Entziehung einer Fahrerlaubnis zum Gegenstand hat, solange die Verurteilung wegen dieser Tat im Verkehrszentralregister eingetragen ist."

6.11.3 Halterauskünfte

In mehreren Bürgereingaben bin ich darauf aufmerksam gemacht worden, daß für **Sozialämter** ein On-line-Zugriff auf das örtliche Fahrzeugregister eingerichtet worden war. Zur Begründung dieser Zugriffsmöglichkeit wurde darauf hingewiesen, das Sozialamt benötige zur Überprüfung der Vermögensverhältnisse von Antragstellern Angaben darüber, ob diese Halter eines Kraftfahrzeuges seien. Auch wenn man von der Richtigkeit dieser Begründung ausgeht, ist eine solche Nutzung der Halterdaten nicht zulässig. Wie auch in der Begründung (Bundestagsdrucksache 10/4737) des Gesetzes zur Änderung des Straßenverkehrsgesetzes vom 28. Januar 1987 (BGBl. I S. 486) unter Hinweis auf das Volkszählungsurteil deutlich hervorgehoben wird, kommt es für die Zulässigkeit einer Nutzung der in den Fahrzeugregistern gespeicherten Daten grundsätzlich auf die Zweckbestimmung dieser Daten an. Nutzungen außerhalb des eigentlichen Registerzwecks sind nur für die im Straßenverkehrsgesetz (StVG) ausdrücklich genannten staatlichen Aufgaben unter den insoweit näher angegebenen Voraussetzungen als Ausnahmen zulässig. Eine Nutzung durch das Sozialamt zur Überprüfung der Bedürftigkeit ist dabei jedoch nicht vorgesehen (§§ 35, 36 StVG).

Als unzulässig erwies sich aus den gleichen Gründen das von einem **Kurort** angewandte Verfahren: Die Gemeinde ließ die Halter von Kraftfahrzeugen ermitteln, für die ein längerer Aufenthalt in der Gemeinde festgestellt wurde. Anschließend wurden diejenigen Halter, für die keine Kurbeitragsabgabe gezahlt worden war, angeschrieben und um Auskünfte über die Dauer des Aufenthalts, die Zahl der Begleitpersonen sowie um nachträgliche Entrichtung der insgesamt fälligen Kurbeitragsabgabe gebeten.

Der in der Praxis häufigste Fall der Auskunfterteilung für **private Zwecke** ist die einfache Registerauskunft nach § 39 Abs. 1 StVG. Danach sind durch die Zulassungsstelle unter anderem Name und Anschrift des Halters zu übermitteln, wenn der Empfänger unter Angabe des betreffenden Kennzeichens darlegt, daß er die Daten zur Geltendmachung von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt. Hierzu rechnen nicht nur Ansprüche aus Unfällen, sondern auch solche auf Grund von Besitz- oder Eigentumsbeeinträchtigungen (§ 1004 BGB), die sich durch abgestellte Fahrzeuge ergeben.

Für die Zulässigkeit einfacher Registerauskünfte ist es ausreichend, daß auf Grund der vom Datenempfänger dargelegten Sachlage Rechtsansprüche im Zusammenhang mit der Teilnahme am Straßenverkehr möglich sind. Es ist nicht Aufgabe der Zulassungsstelle, im Streitfalle der Entscheidung der dazu berufenen Gerichte vorzugreifen.

Die Erteilung von Halterauskünften für private Zwecke auf **telefonische Anfragen** muß im Regelfall als unzulässig angesehen werden. Denn wie bei allen telefonischen Anfragen, besteht auch hier vor allem die Gefahr, daß die Identität des Anfragenden in vielen Fällen nicht zweifelsfrei festgestellt werden kann. Dann darf auf eine telefonische Anfrage keine Registerauskunft erteilt werden. Datenschutzrechtliche Bedenken wegen der zweifelhaften Identität des Anfragenden entfallen jedoch, wenn dieser dem Gesprächspartner persönlich bekannt ist. Darüber hinaus ist es jedenfalls zum Teil möglich, durch entsprechende organisatorische oder auch technische Maßnahmen das mit einer telefonischen Anfrage verbundene Risiko der zweifelhaften Identität des Gesprächspartners auszugleichen; z. B. durch Rückrufverfahren, durch die Verwendung von Code-Wörtern oder ähnlichen Maßnahmen. Aber auch in den Fällen, in denen die Identität des Anfragenden keinem Zweifel unterliegt, wird es in der Regel durch ein telefonisches Auskunftsersuchen nicht möglich sein, bei der Zulassungsstelle die Überzeugung zu vermitteln, daß die erbetenen Daten wirklich nur zur Verfolgung von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr und nicht zu anderen Zwecken benötigt werden.

In jedem Fall halte ich es für erforderlich, daß bei der Zulassungsstelle über erteilte Halterauskünfte **Aufzeichnungen** geführt werden. Daraus müssen zum jeweiligen Kfz-Kennzeichen mindestens das Datum der Auskunftserteilung, der Anlaß und der Empfänger ersichtlich sein. Denn ohne derartige Aufzeichnungen ist eine nachträgliche Prüfung der Einhaltung der Zulässigkeitsvoraussetzungen weder durch die speichernde Stelle noch durch den Landesbeauftragten für den Datenschutz möglich. Die Aufzeichnungen sind außerdem erforderlich, um dem Betroffenen auf seinen Antrag Auskunft über den Empfänger einer Datenübermittlung nach § 18 Abs. 1 Satz 1 Nr. 3 DSG NW zu erteilen.

7. Organisatorische und technische Maßnahmen

7.1 Organisation der Datensicherung

7.1.1 Aufgaben für eine Datenzentrale bei dezentraler DV

In einer zunehmenden Zahl von Fällen wird die automatisierte Datenverarbeitung dezentralisiert. Automatisierte Datenverarbeitung ist heute nicht mehr allein den großen Rechenzentren vorbehalten. Zahlreiche öffentliche Stellen, deren Datenverarbeitung bisher einem großen Rechenzentrum übertragen war, stehen vor der Frage, ob sie diese Arbeiten ganz oder teilweise auf eine eigene Datenverarbeitungsanlage übernehmen sollten.

Die Vorzüge der selbständigen Arbeit werden dabei im allgemeinen zurückhaltend beurteilt. Die Schwierigkeiten können von dem, der seine eigene automatisierte Datenverarbeitung plant, häufig nur vermutet werden. Über einige der Schwierigkeiten wird unten (S. 109 bis 112) berichtet.

Mit besonderem Bedauern sehe ich die Gefahr, daß die über Jahre aufgebaute Leistungskraft **großer Datenverarbeitungszentralen** möglicherweise zerfällt und nicht für die Zukunft genutzt wird. Der Betrieb eines Rechenzentrums, der vielleicht jetzt reduziert oder gar eingestellt werden soll, ist ja nicht die einzige Aufgabe der Datenzentrale. Die übrigen Aufgaben, zu denen insbesondere Entwicklung und organisatorische Beratung gehören, können aber die meisten der Stellen, die heute die Selbständigkeit vorziehen, kaum eigenverantwortlich wahrnehmen. Immer wieder rege ich daher die Datenzentralen und die zur selbständigen Datenverarbeitung entschlossenen öffentlichen Stellen an zu prüfen, ob auch bei der Dezentralisierung einige Funktionen zentral erhalten und eventuell sogar ausgebaut werden sollten.

Im Bereich einer von mir kontrollierten kommunalen Datenzentrale hat in den letzten Jahren die dezentrale Datenverarbeitung an Bedeutung gewonnen. Alle Städte und Gemeinden des Kreises verfügen über eigene Datenverarbeitungsanlagen. Während des Kontrollbesuchs wurde erörtert, welche Aufgaben sich für die Datenzentrale nach der Dezentralisierung der Datenverarbeitung ergeben könnten. Schwerpunkte derartiger Aufgaben können insbesondere die Entwicklung von Programmen, die Beratung in Fragen der Datenverarbeitung und der Datensicherheit sowie die Unterstützung bei internen Kontrollen sein. Auf die Möglichkeit, diese Aufgaben auch bei dezentralisierter Datenverarbeitung weiter der Datenzentrale zu übertragen, wurde bereits in meinem siebten (S. 183) und achten Tätigkeitsbericht (S. 166) hingewiesen.

Bei den Erörterungen mit der kommunalen Datenzentrale standen Fragen der **Entwicklung von Anwendungsprogrammen** im Vordergrund. Auf dezentral eingesetzten Datenverarbeitungsanlagen werden im allgemeinen Fremdprogramme verwendet. Fast immer wird allerdings die Frage aufgeworfen, ob es

zweckmäßig und für die dezentral arbeitende Stelle möglich ist, einzelne Programme selbst zu entwickeln oder die Fremdprogramme selbst so zu ändern, daß sie den eigenen Anforderungen besser angepaßt sind.

Bei den Plänen und Entscheidungen, Programme selbst zu entwickeln oder zu ändern, werden oft die eigenen Möglichkeiten überschätzt und die bestehenden Schwierigkeiten unterschätzt. Zwar sind die Kosten der Datenverarbeitungsanlagen in den letzten Jahren stark gesunken; mit einem weiteren Sinken ist auch in der Zukunft zu rechnen. Nicht entsprechend verringert haben sich aber Schwierigkeit und Kosten der Entwicklung von Programmen. Gerade deshalb werden dezentral eingesetzte Datenverarbeitungsanlagen im allgemeinen mit Fremdprogrammen betrieben.

In manchen Fällen hat der Hersteller des Programms bereits gewisse Möglichkeiten zur Anpassung an den jeweiligen Einsatzfall vorgesehen. Ein solches Programm kann dann durch Eingabe von Parametern den Wünschen des Anwenders angepaßt werden. Jedes darüber hinausgehende Eingreifen des Anwenders in die Programmlogik sollte aber unterbleiben. Schon die geringste zusätzliche Änderung führt dazu, daß das Programm neu getestet und freigegeben werden muß.

Die dezentral arbeitende Stelle übernimmt mit einer solchen Änderung eine Verantwortung, die sie nur selten tragen kann. Dem Bearbeiter fehlen die für die Änderung notwendigen Kenntnisse des Gesamtprogramms. Der zuständige Vorgesetzte ist im allgemeinen weder in der Lage, Schwierigkeitsgrad und Verantwortbarkeit der Änderung zu beurteilen, noch kann er die durchzuführenden Arbeiten fachlich beaufsichtigen.

Die Entwicklung eigener Programme bei einer dezentral arbeitenden Stelle ist dann ähnlich zu beurteilen, wenn durch die Programme wesentliche Dateien geändert werden können. Auch in diesem Fall kann der zuständige Vorgesetzte das damit verbundene Risiko im allgemeinen nicht überblicken und die Entwicklung nicht fachlich beaufsichtigen. Insbesondere sollten Dateien, die von Fremdprogrammen verwaltet werden, keinesfalls von eigenen Programmen geändert werden dürfen.

Naheliegend wäre es, wenn auch in Zukunft Entwicklungsarbeiten weitgehend oder ausschließlich von der Datenzentrale durchgeführt würden. Es ist davon auszugehen, daß die zentrale Entwicklung von Programmen jetzt und in absehbarer Zukunft einer eventuellen dezentralen Entwicklung unter dem Gesichtspunkt der Datensicherheit weit überlegen ist.

Die Erfahrung hat darüber hinaus gezeigt, daß jede Übernahme von Fremdprogrammen zu einer gewissen Abhängigkeit von deren Lieferfirma führt. Es ist zu fragen, ob nicht auch nach einer Dezentralisierung der Datenverarbeitung die Anwendungsprogramme wie bisher von öffentlichen Stellen bereitgestellt werden sollten. Die heutigen Datenzentralen könnten dabei eine wichtige Rolle spielen.

7.1.2 Interne Kontrolle

Auf einem wichtigen Gebiet beobachte ich, wie meine Empfehlungen aufgegriffen und in die organisatorische Wirklichkeit umgesetzt werden. In jedem der bisherigen Tätigkeitsberichte wurde auf die Notwendigkeit **interner Kontrollen** hingewiesen. Es ist notwendig, nachträglich zu überprüfen, ob geltende Vorschriften und gegebene Anweisungen eingehalten wurden. Dazu sollte eine interne Kontrollinstanz institutionalisiert werden, die fachlich kompetent ist und eine hinreichende Unabhängigkeit besitzt. Ohne geeignete Kontrollen kann die Datensicherheit im allgemeinen nicht angemessen gewährleistet werden. Zwei Beispiele sollen zeigen, wie meine Empfehlungen in die Verwaltungspraxis umgesetzt werden.

Anläßlich eines Kontrollbesuchs bei einer großen Stadt konnte ich mich davon überzeugen, daß das Rechnungsprüfungsamt dieser Stadt auch interne Kontrollen der Datensicherheit wahrnimmt. Das Rechnungsprüfungsamt führt unter anderem Prüfungen unter dem Gesichtspunkt der Datensicherheit durch.

Ich habe es begrüßt, daß die Kontrolle der Datensicherheit durch das Rechnungsprüfungsamt der Stadt wahrgenommen wird. Allerdings habe ich zusätzlich empfohlen, dem Rechnungsprüfungsamt die Aufgabe der internen Kontrolle durch schriftlichen Auftrag ausdrücklich zu übertragen. Darüber hinaus habe ich angeregt, die Rechnunsprüfungsordnung durch den Rat der Stadt entsprechend zu ergänzen. Im Hinblick auf den Einsatz der automatisierten Datenverarbeitung könnte die Rechnungsprüfungsordnung um die Aufgabe der Prüfung der organisatorischen und technischen Maßnahmen zum Sicherstellen einer den Vorschriften und Weisungen entsprechenden Verarbeitung und zum Verhindern von Verlust, unzulässiger Verarbeitung oder Kenntnisnahme von Daten ergänzt werden.

Im Anschluß an einen vor einigen Jahren durchgeführten Kontrollbesuch bei einem als Zweckverband organisierten Krankenhaus hatte ich empfohlen, eine interne Kontrollinstanz zu institutionalisieren und darüber hinaus festzulegen, daß in größeren Zeitabständen überprüft werden solle, ob die zum Datenschutz getroffenen Maßnahmen noch angemessen und ausreichend sind. Inzwischen wurde das Rechnungsprüfungsamt des Kreises, der einer der Träger des Zweckverbandes ist, zur internen Kontrollinstanz für den Datenschutz bestimmt. Auch wurde festgelegt, daß das Rechnungsprüfungsamt mindestens einmal im Jahr zu prüfen hat, ob die zum Datenschutz getroffenen Maßnahmen noch angemessen und ausreichend sind. Dadurch soll sichergestellt werden, daß die organisatorisch-technischen Maßnahmen zum Datenschutz dem jeweils aktuellen Stand entsprechen.

7.1.3 Verbindlichkeit von Dienstanweisungen

Eine Dienstanweisung soll das Verhalten der Mitarbeiter verbindlich regeln. Ein Abweichen von der Dienstanweisung sollte besonderer Zustimmung bedürfen, die im allgemeinen der Leitung der öffentlichen Stelle vorbehalten ist. Insbesondere sollte keine Unklarheit darüber bestehen, ob der Mitarbeiter im

Einzelfall eine Regelung zu befolgen hat oder nicht. Leider wird, wie die folgenden Beispiele zeigen, immer wieder gegen diese elementare Regel verstoßen.

In einer bei einem Kontrollbesuch vorgelegten Dienstanweisung ist unter anderem festgelegt: „Es ist im Einzelfall zu entscheiden, ob und in welchem Umfang eine Maßnahme umgesetzt werden muß." In einer anderen Dienstanweisung, die Vorschriften zur Datenverarbeitung im Auftrag enthält, wird festgelegt, daß „in Ausnahmefällen mit dem Auftraggeber eine im einzelnen von dem (in) dieser Dienstanweisung beschriebenen Verfahren abweichende Regelung vereinbart werden" kann. Beide Dienstanweisungen enthalten keine Aussage darüber, wer befugt ist, über Abweichungen von der Dienstanweisung zu entscheiden.

Ein anderes Beispiel betrifft Regelungen für die Arbeit mit dezentral aufgestellten Datenverarbeitungsanlagen. Zur Arbeit mit diesen Geräten war ein Handbuch entwickelt und an die dezentralen Stellen verteilt worden. Weder aus dem Schreiben, mit dem das Handbuch versandt worden war, noch aus dem Handbuch selbst konnte entnommen werden, wie die Angaben des Handbuchs verstanden werden sollten. Nach dem Text des Handbuchs konnte es sich bei den Angaben in diesem Handbuch um Bedienungshinweise für die automatisierte Datenverarbeitung, um Empfehlungen für deren Einsatz oder auch um Weisungen handeln.

Im Gespräch stellte sich heraus, daß die Ausführungen eines Kapitels des Handbuchs als Empfehlungen zu verstehen sein sollten. Im übrigen sollte das Handbuch eine Weisung darstellen.

Durch die in den Beispielen dargestellten Unklarheiten bezüglich der Verbindlichkeit vorliegender Unterlagen ist die Datensicherheit beeinträchtigt. Der Mitarbeiter muß zweifelsfrei erkennen können, ob eine Unterlage eine für ihn verbindliche Weisung enthält. Sollte es notwendig sein vorzusehen, daß im Einzelfall von der getroffenen Weisung abgewichen werden kann, muß festgelegt sein, wer über das Abweichen entscheiden darf.

7.2 Datensicherheit bei kleineren DV-Anlagen

7.2.1 Beschluß der Konferenz der Datenschutzbeauftragten

Beim Einsatz kleinerer Datenverarbeitungsanlagen, vor allem von persönlichen Computern (PC), bereitet das Gewährleisten der **Datensicherheit** und der **Ordnungsmäßigkeit der Datenverarbeitung** besondere Probleme. Im Hinblick auf diese Probleme haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Konferenz am 10./11. Oktober 1988 Empfehlungen an die Anwender und Hersteller ausgesprochen (Anlage 4, S. 137/138).

Die Anwender werden insbesondere auf die Notwendigkeit hingewiesen, vor jeder Entscheidung, ob für die Arbeiten eines Aufgabengebiets ein PC oder eine sonstige kleinere Datenverarbeitungsanlage eingesetzt werden kann, zu prüfen, ob die dabei erzielbare Datensicherheit ausreichend ist. Sofern die

Datensicherheit mit den verfügbaren Maßnahmen nicht in dem erforderlichen Umfang gewährleistet werden kann, muß auf den Einsatz des PC oder der kleineren Datenverarbeitungsanlage verzichtet werden. Die Hersteller von Hard- und Software werden aufgefordert, für kleinere Datenverarbeitungsanlagen einschließlich der persönlichen Computer Verfahren zu entwickeln und bereitzustellen, die einen Betrieb dieser Geräte mit einem Maß an Datensicherheit ermöglichen, das demjenigen großer Rechenzentren entspricht. Öffentliche Stellen sollten vor der Bestellung einer kleineren Datenverarbeitungsanlage klären, ob für diese Anlage ein entsprechendes Verfahren verfügbar ist. Ist das nicht der Fall, sollte der Hersteller auf den bestehenden Bedarf hingewiesen werden.

In den vergangenen Jahrzehnten wurden Organisationsformen und Verfahren entwickelt, die es in **großen Rechenzentren** ermöglichen, die Datenverarbeitung zuverlässig abzuwickeln. Für große Rechenzentren sind heute die zur Datensicherung erforderlichen Hilfsmittel verfügbar. Große Rechenzentren können in einem der jeweiligen Aufgabenstellung angemessenen Umfang sicherstellen, daß die Datenverarbeitung entsprechend den geltenden Vorschriften und Weisungen erfolgt. Der Datensicherheit dienen dabei vor allem

- eine den Anforderungen angepaßte Strukturierung der Organisation mit geeigneten Funktionstrennungen,
- automatisierte Aufzeichnungen und Sicherungen der Datenverarbeitungsanlage,
- die detaillierte Regelung des Arbeitsablaufs durch eine Dienstanweisung und
- eine institutionalisierte Kontrolle der Arbeitsdurchführung, die den jeweiligen Erfordernissen angepaßt ist.

Bezüglich der Arbeit großer Rechenzentren ist unbestritten, daß ein sicherer Betrieb ohne strukturierte Organisation und ohne geeignete Funktionstrennungen nicht möglich ist. Daher ist es bedenklich, wenn heute in zunehmender Zahl kleinere Datenverarbeitungsanlagen installiert werden, bei denen wegen der geringen Mitarbeiterzahl keine hinreichende Strukturierung der Organisation verwirklicht werden kann. Es erhebt sich in diesen Fällen die Frage, ob die speichernden Stellen in angemessenem Umfang in der Lage sind, eine den Vorschriften und Weisungen entsprechende Verarbeitung der Daten sicherzustellen.

Kleinere Datenverarbeitungsanlagen werden fast immer so eingesetzt, daß von einer organisatorischen Strukturierung des Rechenzentrums, wie sie bei großen Rechenzentren selbstverständlich ist, nicht mehr die Rede sein kann. Selbst die organisatorische Trennung von Programmierung, Maschinenbedienung (Rechenzentrum) und Anwenderbereich wird teilweise aufgehoben. Zum Überwachen und Prüfen der automatisierten Arbeitsdurchführung fehlen der datenverarbeitenden Stelle im allgemeinen die fachlichen Voraussetzungen.

Zwar gibt es häufig noch eine Funktion, die man organisatorisch als Rechenzentrum bezeichnen könnte. Diese Rechenzentrumsfunktion wird aber nur von wenigen Mitarbeitern oder einem einzigen Mitarbeiter wahrgenommen. Möglicherweise ist dieser einzige Mitarbeiter sogar nur während eines sehr kurzen Teils seiner Arbeitszeit für die Maschinenbedienung und im übrigen innerhalb des Anwenderbereichs tätig. Vielleicht sind ihm auch gleichzeitig Programmieraufgaben zur selbständigen Erledigung übertragen. Zur Vertretung des Maschinenbedieners werden häufig Mitarbeiter aus dem Anwenderbereich vorgesehen.

Eine interne Überwachung und Prüfung der Arbeitsdurchführung ist in vielen Fällen nicht institutionalisiert, weil kein Mitarbeiter mit der dafür erforderlichen Fachkunde verfügbar ist. Häufig ist selbst der Vorgesetzte des Maschinenbedieners zu einer Beurteilung der Arbeit seines Mitarbeiters, soweit diese die Durchführung der automatisierten Datenverarbeitung betrifft, nicht in der Lage.

Bei dem Einsatz eines persönlichen Computers, der dem Benutzer während der Benutzung alleine zur Verfügung steht, kann sogar nicht mehr von einer organisatorisch abgrenzbaren Rechenzentrumsfunktion gesprochen werden. Der Benutzer ist Anwender und Maschinenbediener in einer Person. In vielen Fällen liegt bei ihm auch die Aufgabe des Programmierens.

Wegen dieser personellen Situation lassen sich wesentliche Maßnahmen zur Datensicherung, die bei großen Rechenzentren heute als selbstverständlich und unverzichtbar angesehen werden, bei Einsatz kleinerer Datenverarbeitungsanlagen nicht verwirklichen. Funktionstrennungen und eine den Anforderungen der Datensicherheit entsprechend strukturierte Organisation bedürfen einer hinreichenden Mitarbeiterzahl. Falls nur wenige Mitarbeiter die Aufgaben des Rechenzentrums wahrnehmen, ist eine Strukturierung der Organisation im allgemeinen praktisch nicht möglich. Bei Einsatz eines einzigen Mitarbeiters gibt es keine Strukturierung der Organisation.

Dadurch ist die Datensicherheit beim Betrieb kleinerer Datenverarbeitungsanlagen und insbesondere auch beim Einsatz eines PC, der seinem Benutzer während der Benutzung alleine zur Verfügung steht, beeinträchtigt. Diese Beeinträchtigung ist im allgemeinen so stark, daß sie bei einem großen Rechenzentrum – jedenfalls für die Verarbeitung personenbezogener Daten nach verbindlich vorgegebener Verarbeitungslogik – als nicht hinnehmbar angesehen würde.

Es gibt Wege, die Datensicherheit beim Einsatz kleinerer Datenverarbeitungsanlagen in angemessenem Umfang zu verbessern. Dazu müßten allerdings von den Herstellern systemtechnische Voraussetzungen entwickelt und bereitgestellt werden. Erste Lösungen sind am Markt bereits als Angebote für Kreditinstitute erhältlich und unter anderem in Geldausgabeautomaten eingesetzt.

7.2.2 Programmviren

Seit einigen Jahren wird die Gefahr gesehen, Programme durch sogenannte Programmviren zu schädigen. Ein Programmvirus ist ein Programm, das sich selbsttätig in andere Programme kopiert und zu einem späteren Zeitpunkt

durch einen äußeren Auslöser, etwa ein Tagesdatum, veranlaßt wird, „infizierte“ Programme am ordnungsgemäßen Ablauf zu hindern. Die in dem oben wiedergegebenen Beschluß der Datenschutzbeauftragten des Bundes und der Länder (Anlage 4) geforderten Maßnahmen wären auch gegen Programmviren wirksam.

Die Hersteller werden unter anderem aufgefordert, Verfahren bereitzustellen, die gewährleisten, daß Programme ausschließlich in der freigegebenen Fassung zum Ablauf kommen. Ein solches Verfahren würde erkennen lassen, wenn ein Virus in ein Programm eingebracht wird. Ein Kopieren des Virus in andere Programme, das heißt das „Vermehren“ des Virus, könnte dann verhindert werden. Auch wird das Risiko, als Verursacher erkannt zu werden, für denjenigen, der das Virus in die Datenverarbeitungsanlage einbringt, sehr hoch, wenn das Virus bereits nach kurzer Zeit entdeckt wird. Das Einbringen eines Virus ist bisher vor allem deshalb mit geringer Gefahr für den Verursacher verbunden, weil dieser festlegen kann, daß dessen schädigende Wirkung erst später – eventuell erst nach Monaten – eintritt. Ein Aufklären ist dann fast unmöglich.

7.2.3 Feststellungen bei Kontrollbesuchen

– Schwierigkeiten beim Einsatz eines PC oder einer sonstigen kleineren Datenverarbeitungsanlage zeigen sich bei fast jedem Kontrollbesuch. Bedenklich ist es insbesondere, wenn meinen Mitarbeitern Fragen deshalb nicht beantwortet werden können, weil **Fremdprogramme** eingesetzt werden, deren Inhalt der speichernden Stelle selbst nicht bis in letzte Details bekannt ist.

  In meinem 8. Tätigkeitsbericht (S. 167) wird das Beispiel einer Stadt geschildert, die im Rahmen eines regelmäßigen Änderungsdienstes Daten des Einwohnerwesens an die evangelische und die katholische Kirche übermittelt. Während des Kontrollbesuchs konnte die Stadt die Frage nach dem für die Übermittlung geltenden Datensatzaufbau nicht beantworten. Es konnte nicht geklärt werden, welche Daten unter welchen Voraussetzungen übermittelt werden.

  In der jetzt vorliegenden schriftlichen Stellungnahme weist die Stadt darauf hin, daß sie Fremdprogramme einsetze, für die eine ausreichende Dokumentation nicht mitgeliefert worden sei. Eine Nachdokumentation sei nicht mehr möglich. Die Programme würden vielmehr durch ein neues Verfahren abgelöst.

  Bei einer anderen Stadt erwies sich bereits der Versuch, die Übereinstimmung zwischen der Anmeldung zu den Registern der Dateien und der bei der Stadt geführten Datei zu prüfen, als schwierig, weil die Stadt nicht über eine Datensatzbeschreibung verfügte. Als Ersatz für die Datensatzbeschreibung mußte in diesem Fall die Beschreibung der Eingabebildschirme aus der Anwendungsdokumentation herangezogen werden.

Ein umfangreiches Programm einer anderen öffentliche Stelle war von einer privaten Programmierfirma entwickelt worden. Zum Zeitpunkt des Kontrollbesuchs war das Programm allerdings bereits uneingeschränkt übernommen, und die öffentliche Stelle war auch für die Wartung des Programms zuständig.

Als Dokumentation verfügte die öffentliche Stelle nur über drei Unterlagen. Es lag eine vorläufige Verfahrensbeschreibung vor. Als Beschreibung über den Aufbau des Programms gab es eine Zusammenstellung im Umfang von etwa acht DIN A 4 Seiten, die im wesentlichen die Bezeichnungen der Einzelprogramme enthielt, aus denen das Programm aufgebaut war. Aussagen über die Logik dieser Einzelprogramme und über die Struktur des Programms konnten dieser Beschreibung nicht entnommen werden. Dazu gab es lediglich eine Liste der Programmanweisungen. Das Programm war in der Programmiersprache C programmiert worden.

In jedem der als Beispiele geschilderten Fälle mußte ich darauf hinweisen, daß eine aussagekräftige Dokumentation der eingesetzten Programme für die Datensicherheit unerläßlich ist. Die dazu erforderlichen Maßnahmen sollten unverzüglich getroffen werden.

– In einem kontrollierten Rechenzentrum aus dem Bereich der Sozialversicherung wird ein Informationssystem für die angeschlossenen Krankenkassen betrieben. Über angeschlossene Datenendgeräte können die Krankenkassen auf ihre Daten zugreifen.

  Nach der Dienstanweisung ist die Datenverarbeitungsanlage arbeitstäglich regelmäßig von 8.00 Uhr bis 16.00 Uhr vorrangig für den Dialogverkehr und von 16.00 Uhr bis 8.00 Uhr vorrangig für den Batchbetrieb zur Verfügung zu stellen. Auf Rückfrage bestätigte das Rechenzentrum, mit dieser Regelung werde festgelegt, daß die Datenverarbeitungsanlage, auf der das Informationssystem betrieben wird, arbeitstäglich durchgehend in Betrieb ist. **Außerhalb der Arbeitszeit** der Maschinenbediener können Arbeiten ablaufen, deren Abwicklung im bedienerlosen Verkehr möglich ist.

  Während der Zeit des bedienerlosen Verkehrs sind auch die Dialogprogramme nutzbar. Die Datenendgeräte der angeschlossenen Krankenkassen könnten im bedienerlosen Verkehr in gleicher Weise wie während der normalen Dienststunden genutzt werden. Der Betrieb der Datenverarbeitungsanlage außerhalb der Dienststunden ist daher nur dann unbedenklich, wenn sichergestellt ist, daß weder durch Einwirkung auf die Datenverarbeitungsanlage noch über die angeschlossenen Datenendgeräte unbefugte Zugriffe zu den gespeicherten Daten erfolgen können.

  Von den Krankenkassen kann allerdings nur dann erwartet werden, daß sie die für die Datensicherheit außerhalb der Dienstzeit erforderlichen Maßnahmen treffen, wenn ihnen bekannt ist, daß die angeschlossenen Datenendgeräte außerhalb der Dienstzeit in gleicher Weise wie während der Dienstzeit genutzt werden können. Bei dem Kontrollbesuch bei einer angeschlos-

senen Krankenkasse wurde festgestellt, daß dieser nicht bekannt war, daß mit den angeschlossenen Datenendgeräten außerhalb der Dienstzeit ein normaler Dialogbetrieb möglich ist. Der Krankenkasse war daher auch nicht bewußt, daß außerhalb der Dienstzeit Maßnahmen erforderlich sind, um die unbefugte Nutzung der Datenendgeräte sicherzustellen.

Ich habe dem Rechenzentrum empfohlen, alle angeschlossenen Krankenkassen darüber zu informieren, in welchem Umfang eine Nutzung der angeschlossenen Datenendgeräte außerhalb der Dienstzeit möglich ist, und darauf hinzuweisen, daß die Datenendgeräte wegen der Möglichkeit dieser Nutzung auch außerhalb der Dienstzeit gesichert sein müssen.

– Während eines Kontrollbesuchs wurde berichtet, daß ein Ausfall des eingesetzten Systems zur automatisierten Vorgangsverwaltung eine ernste Beeinträchtigung der Möglichkeit bedeuten würde, die übertragenen Aufgaben wahrzunehmen. Für die Bedienung der Datenverarbeitungsanlage sind nur drei Mitarbeiter der kontrollierten Stelle ausgebildet. Es ist zwar unwahrscheinlich, aber nicht völlig auszuschließen, daß diese drei Mitarbeiter gleichzeitig nicht zur Verfügung stehen. Im Hinblick auf die ernsten Folgen eines Ausfalls der automatisierten Vorgangsverwaltung ist es daher angemessen, auch für eine derartige **Ausnahmesituation** Vorsorge zu treffen.

  Dazu sollte festgelegt werden, welche Voraussetzungen erfüllt sein müssen, damit die Datenverarbeitungsanlage durch fachkundige Dritte in Betrieb genommen werden kann. In der Dienstanweisung sollte dann vorgeschrieben werden, daß diese Voraussetzungen ständig zu erfüllen sind. Zu den Aufgaben der internen Kontrolle sollte es gehören zu überprüfen, ob die entsprechenden Regelungen der Dienstanweisung eingehalten werden.

– Es ist üblich, Anwendungsprogramme in einer Sprache zu formulieren, die den Bedürfnissen des Programmierers entgegenkommt. Das dabei entstehende Quellprogramm kann im allgemeinen nicht direkt in der Datenverarbeitungsanlage ablaufen. Es wird vielmehr in einem Zwischenschritt durch ein Übersetzungsprogramm übersetzt. Das Ergebnis dieses Übersetzungsvorgangs ist ein Programm in Maschinensprache. Dieses Maschinenprogramm wird von der Datenverarbeitungsanlage verstanden und kann daher in der Anlage zum Ablauf kommen.

  Aufgabe des Programmierers ist es, ein fehlerfreies Quellprogramm zu erstellen. In großen Rechenzentren ist es Aufgabe der Arbeitsvorbereitung, das zu dem freigegebenen Quellprogramm gehörende Maschinenprogramm nach der Programmfreigabe in der Datei der freigegebenen Maschinenprogramme zu speichern. Diese Datei steht für die Arbeiten der Maschinenbedienung zur Verfügung. Die Programmierer dürfen auf diese Datei keinen Zugriff haben.

  Die Tatsache, daß es ein für die direkte Steuerung des Ablaufs der Datenverarbeitungsanlage ungeeignetes Quellprogramm und ein davon verschiedenes Maschinenprogramm gibt, das dem Programmierer nicht zu-

gänglich ist, bildet eine wesentliche Stütze der Datensicherung in großen Rechenzentren. Mit Hilfe der zwischengeschalteten Arbeitsvorbereitung ist es möglich, eine wirksame **Funktionstrennung** zwischen Programmierung und Maschinenbedienung zu verwirklichen. Manipulationen an freigegebenen und insbesondere an ablauffähigen Programmen werden dadurch wesentlich erschwert.

Bei Einsatz kleinerer Datenverarbeitungsanlagen kann eine Funktionstrennung in ähnlicher Weise verwirklicht werden. Zwar verfügt die Organisationseinheit, bei der die kleinere Anlage aufgestellt ist, wegen der geringen Zahl der bei der automatisierten Datenverarbeitung tätigen Mitarbeiter im allgemeinen nicht selbst über eine Arbeitsvorbereitung. Falls die Programmierung ausschließlich außerhalb dieser Organisationseinheit erfolgt, läßt sich aber sicherstellen, daß die Maschinenbediener der kleineren Anlage nur über die Maschinenprogramme und nicht über Quellprogramme verfügen. Die Quellprogramme sollten sich ausschließlich bei der entwickelnden Stelle befinden. Damit ist den Maschinenbedienern eine Manipulation der Programme erschwert.

Abweichend von der hier beschriebenen üblichen Arbeitsorganisation kommen in der Datenverarbeitungsanlage einer kontrollierten Volkshochschule keine durch Übersetzung entstandenen Maschinenprogramme zum Ablauf. Der Ablauf der Datenverarbeitungsanlage wird vielmehr direkt durch die vom Programmierer erstellten Quellprogramme gesteuert. Jede einzelne Anweisung eines Quellprogramms wird durch ein allgemeines **Interpretationsprogramm** während des Ablaufs des Quellprogramms in der Datenverarbeitungsanlage interpretiert. Die Volkshochschule muß daher zur Steuerung ihrer Datenverarbeitungsanlage über die Quellprogramme verfügen, obgleich sie ihre Programme weder selbst entwickelt hat noch wartet. Die Datensicherheit ist dadurch beeinträchtigt.

Während des Kontrollbesuchs wurde besprochen, daß die Volkshochschule bei dem Hersteller ihrer Datenverarbeitungsanlage klären sollte, ob für die bei ihr eingesetzten Programme auch ein Übersetzer verfügbar ist. In diesem Fall sollte auf das interpretative Arbeiten verzichtet werden. Der Volkshochschule sollten dann nur die übersetzten Maschinenprogramme zur Verfügung stehen. Darüber hinaus sollte die Volkshochschule im Rahmen einer langfristigen Planung anstreben, eine Programmiersprache zu verwenden, bei der ein interpretatives Arbeiten in der Datenverarbeitungsanlage nicht vorgesehen ist.

– Eine kontrollierte große Behörde setzt ein **anwenderorientiertes Recherchesystem** ein. Darunter wird ein Programmsystem verstanden, das ein einfaches Erstellen von Programmen zur Dateiführung und -auswertung für unterschiedliche Anwendungsfälle ermöglicht. Das eingesetzte Programmsystem ist als ein Instrument in der Hand des Anwenders gedacht. Im Rahmen des Kontrollbesuchs wurden grundsätzliche Fragen des Einsatzes eines derartigen Programmsystems erörtert. Programme für einzelne Anwendungsfälle des Programmsystems werden im folgenden als Regelungen bezeichnet.

Wesentliche Zielsetzung bei der Entwicklung des Programmsystems war es, den Arbeitsaufwand für das Erstellen von Regelungen gering zu halten. Gering ist allerdings nicht nur der Aufwand, um eine Regelung zu erstellen. Auch das Ändern von Regelungen durch den Anwender ist ohne Schwierigkeiten möglich. Wegen dieser Eigenart des Programmsystems besteht für die kontrollierte Behörde nur eine geringe Möglichkeit sicherzustellen, daß bei der Arbeit mit diesem Programmsystem eine verbindlich vorgeschriebene Verarbeitungslogik eingehalten wird. Jeder Mitarbeiter ist grundsätzlich in der Lage, Regelungen wieder zu ändern, die er selbst oder ein anderer Mitarbeiter zu einem früheren Zeitpunkt vorgegeben hat.

Unter diesen Umständen ist es nicht überraschend, daß bisher auf die Freigabe von Regelungen verzichtet wurde. Eine Freigabe hätte aber jedenfalls immer dann erfolgen müssen, wenn Regelungen für Verarbeitungen mit verbindlicher Verarbeitungslogik erstellt wurden, denn Regelungen entsprechen Anwendungsprogrammen. Anwendungsprogramme bedürfen aber der Freigabe, falls ihre Verarbeitungslogik verbindlich ist.

Diese Art des Einsatzes des Programmsystems ist unbedenklich, falls nicht eine verbindliche Verarbeitungslogik den Inhalt der Regelungen vorschreibt. Ein solcher unbedenklicher Einsatz liegt vor, wenn einem einzelnen Mitarbeiter die Bearbeitung einer Aufgabe als Gesamtaufgabe übertragen ist und wenn dieser Mitarbeiter dabei selbst darüber entscheidet, welche Daten er mit welcher Logik verarbeiten will. Falls dieser Mitarbeiter das Programmsystem einsetzt, gibt es für ihn keine verbindlich vorgeschriebene Verarbeitungslogik, die in den von ihm aufzustellenden Regelungen verwirklicht sein muß.

Bedenken gegen einen Verzicht auf die Freigabe von Regelungen müssen immer dann erhoben werden, wenn die Verarbeitungslogik verbindlich ist. Eine Verbindlichkeit der Verarbeitungslogik ist im allgemeinen bereits dann anzunehmen, wenn dieselben Regelungen von einer Gruppe von Mitarbeitern als zutreffend unterstellt werden. Eine solche Situation besteht, wenn sich eine Gruppe von Mitarbeitern auf einen bestimmten Aufbau der Datei, mit der sie arbeitet, und auf eine bestimmte Verarbeitungslogik beim Arbeiten mit dieser Datei verläßt.

Dadurch, daß es dem Anwender leicht möglich ist, Regelungen zu ändern, ist die Datensicherheit bei der Arbeit mit verbindlicher Verarbeitungslogik beeinträchtigt. Die kontrollierte Behörde sollte daher jeden Einzelfall mit verbindlicher Verarbeitungslogik daraufhin überprüfen, ob die bei Verwendung des Programmsystems erreichbare Sicherheit für diesen Einsatzfall angemessen ist. Falls die Datensicherheit nicht angemessen ist, sollte der Einsatzfall auf andere Weise bearbeitet werden.

– Abschließend soll eine positive Feststellung vermerkt werden. Auf Schwierigkeiten, die Datensicherheit beim Einsatz eines PC zu gewährleisten, wurde bereits hingewiesen (oben S. 106 bis 108). Zusätzliche Bedenken sind angebracht, wenn ein Mitarbeiter seinen **privateigenen PC** für dienstliche Zwecke einsetzt. Maßnahmen, die in einem solchen Fall erforderlich sind,

werden in meinem 8. Tätigkeitsbericht (S. 175) angegeben. Da diese Maßnahmen die bestehenden Bedenken nur mindern, nicht aber beseitigen können, begrüße ich es ausdrücklich, daß der Innenminister für den Bereich der Polizei durch Erlaß angeordnet hat, daß keine privaten Computer für dienstliche Zwecke genutzt werden dürfen.

7.3 On-line-Zugriffe

– Bei On-line-Zugriffen ist das Authentifizieren dessen, der einen Zugriff auf die Daten beabsichtigt, eine der zentralen Aufgaben der Datensicherung. Ein weit verbreitetes Verfahren, das den Zugriff über Datenendgeräte sichern soll, ist der Paßwortschutz. Allerdings haben die Erfahrungen bei Kontrollbesuchen gezeigt, daß der Paßwortschutz im allgemeinen nur unzulänglich verwirklicht ist und dann einen unzureichenden Schutz bietet.

  In mehreren Tätigkeitsberichten habe ich bereits vorgeschlagen, maschinenlesbare Ausweise und insbesondere **Chipkarten** zur Zugriffssicherung einzusetzen. Bei einer Reihe von Kontakten versuchte ich, die Hersteller von Datenverarbeitungsanlagen zu einer entsprechenden Erweiterung ihres Angebots zu veranlassen. Ein bekannter Hersteller hat mir inzwischen zugesagt, er werde bald für sein gesamtes Produktspektrum eine Zugriffssicherung mit Hilfe von Chipkarten anbieten. Ich würde es begrüßen, wenn öffentliche Stellen in Nordrhein-Westfalen bei entsprechenden Anfragen an Hersteller immer auch nach der Möglichkeit des Einsatzes von Chipkarten zur Zugriffssicherung fragen würden. Sobald bessere technische Möglichkeiten bestehen, sollte diesen gegenüber dem Paßwortschutz der Vorzug gegeben werden.

– Von den an die Datenverarbeitungsanlage eines kontrollierten Rechenzentrums angeschlossenen Datenendgeräten können **Arbeitsaufträge** zur Verarbeitung personenbezogener Daten **durch Datenfernübertragung** erteilt werden. Dabei gibt der Auftraggeber seinen Namen und seine Benutzerkennung an.

  Da die Benutzererkennung keine vertrauliche Angabe ist, kann nicht davon ausgegangen werden, daß sich der Auftraggeber durch diese Angaben gegenüber der Datenverarbeitungsanlage authentifiziert hat. Eine Authentifizierung des Auftraggebers muß aber Voraussetzung dafür sein, daß die Datenverarbeitungsanlage einen Arbeitsauftrag zur Verarbeitung personenbezogener Daten annimmt. Ich habe daher empfohlen, die Annahme von Arbeitsaufträgen durch Datenfernübertragung zur Verarbeitung personenbezogener Daten von der Eingabe des Paßwortes des Auftraggebers abhängig zu machen, solange kein sichereres Verfahren zur Authentifizierung verfügbar ist.

– Während des Kontrollbesuchs bei einer Stadt wurde berichtet, daß **Fernwartung und Ferndiagnose** jeweils durch einen Anruf des Herstellers eingeleitet werden. Der anrufende Mitarbeiter des Herstellers teilt dabei mit, daß Fernwartung oder Ferndiagnose beabsichtigt sei; ein Mitarbeiter der

Stadt stellt daraufhin über einen Akustikkoppler die Verbindung zur Datenverarbeitungsanlage der Stadt her. Der anrufende Mitarbeiter des Herstellers ist den Mitarbeitern der Stadt nicht bekannt. Ein Mißbrauch kann daher nicht ausgeschlossen werden.

Ich habe empfohlen, die Datensicherheit durch eine Änderung des Ablaufs zu verbessern. Die Stadt sollte sich von dem Hersteller ihrer Datenverarbeitungsanlage die Telefonnummer der für die Durchführung der Fernwartung zuständigen Stelle geben lassen. Wenn der Hersteller durch Telefonanruf die Absicht äußert, eine Fernwartung oder Ferndiagnose zu beginnen, sollte sich die Stadt zunächst durch Rückruf unter Verwendung der bei ihr notierten Telefonnummer davon überzeugen, daß es wirklich der Hersteller ist, der angerufen hat. Die Verbindung zur Datenverarbeitungsanlage der Stadt sollte erst nach diesem Rückruf hergestellt werden. Ein entsprechender Ablauf sollte durch Dienstanweisung vorgeschrieben werden.

– Eine vergleichbare Situation entsteht, wenn eine Datenverarbeitungsanlage durch automatisches Anwählen Kontakt zu einer anderen Datenverarbeitungsanlage aufnimmt. Eine solche automatische Kontaktaufnahme geschieht sehr häufig und ist Stand der Technik. Selbstverständlich ist es dabei erforderlich, daß die anrufende Datenverarbeitungsanlage authentifiziert wird. Im allgemeinen sendet diese dazu eine Kennung an die angerufene Anlage.

  Als Sicherung gegen einen möglichen Mißbrauch wurde in meinem vierten (S. 163) und sechsten Tätigkeitsbericht (S. 173) empfohlen, die angerufene Datenverarbeitungsanlage solle die Verbindung nach der Kontaktaufnahme abbrechen, sobald sich die anrufende Anlage zu erkennen gegeben hat. Dann solle die angerufene Anlage von sich aus die anrufende Anlage unter einer Telefonnummer anwählen, die sie aus ihrem Speicher entnimmt.

  Die mit diesem Verfahren erreichte Sicherheit schien sehr hoch zu sein, da durch das **automatische Rückwählen** der Anschluß, der die Verbindung aufnehmen wollte, unmanipulierbar authentifiziert zu sein schien. Inzwischen sind mir aber Tatsachen bekanntgeworden, nach denen die Sicherheit dieses Verfahrens wesentlich geringer ist. Bisher ging ich von der als selbstverständlich unterstellten Annahme aus, daß eine Verbindung immer dann umgehend zusammenbricht, wenn einer der Teilnehmer die Verbindung abbricht. Diese Annahme ist aber nicht zutreffend.

  Nach einer Auskunft des Fernmeldetechnischen Zentralamtes ist von folgendem auszugehen: Wenn ein Anrufer A einen Teilnehmer B angerufen hat, und nur B legt auf, so dauert es je nach eingesetzter Vermittlungstechnik zwischen 6 und 166 Sekunden, bis das von der B zugehörigen Vermittlungsstelle erzeugte Signal bei der A-Vermittlungseinrichtung ausgewertet ist und von dort aus die Verbindung gelöst wird. Versucht B neu zu wählen, während die Verbindung noch nicht gelöst ist, so bleibt er mit A verbunden. Das könnte B zwar am Fehlen von Wählton und Freizeichen erkennen, wenn B diese Signale auswertet; B könnte aber insoweit von A getäuscht werden.

Mit Sicherheit neu wählen kann B also entweder nach 166 Sekunden oder auf einer wirklich freien Leitung. Die notwendige Wartezeit im Nahdienst und bei digitaler Vermittlung liegt im Durchschnitt bei 12 Sekunden. B kann aber nicht wissen, von wem oder von wo er angerufen wurde.

Die angestrebte Sicherheit ist daher nur erreichbar, indem B über eine Leitung zurückruft, die nicht mit derjenigen identisch ist, über die A angerufen hat. Die Sicherheit wird erhöht, wenn B für den Rückruf eine Leitung nutzt, die von der Post als ausschließlich von B abgehend geschaltet ist. Grundsätzlich möglich ist es selbstverständlich auch, die Anlage B erst mit einer Verzögerung von mehr als 166 Sekunden rückwählen zu lassen. Da die genannten Zeitangaben für den Bereich der Deutschen Bundespost gelten, ist dann allerdings immer noch offen, ob bei einem mißbräuchlichen Anruf aus dem Ausland die Verbindung bereits gelöst ist, wenn B mit dem Rückwählen beginnt.

Öffentliche Stellen, deren Datenverarbeitungsanlage über Wählanschluß angerufen werden kann, sollten die Sicherheit unter den hier angeführten Gesichtspunkten überprüfen.

7.4 Speichern von Angaben zur Benutzeridentifizierung

Mit Hilfe archivierter Systemnachrichten ist es möglich, die Aktivitäten eines Datenverarbeitungssystems für einen vergangenen Zeitraum zu rekonstruieren. Bei der Aufklärung eventueller Unregelmäßigkeiten besteht an dieser Möglichkeit besonderes Interesse. Systemnachrichten, die auf Magnetband aufgezeichnet und daher maschinell auswertbar sind, können eine wesentliche Hilfe bei der Aufklärungsarbeit bedeuten. Wünschenswert ist es daher, die Systemnachrichten auf maschinenlesbarem Datenträger zu archivieren. Eine Aufbewahrung aller archivierten Systemnachrichten für fünf Jahre wäre angemessen.

Bei einem Kontrollbesuch bei einer Datenverarbeitungszentrale wurde festgestellt, daß bei bestimmten Systemaufzeichnungen die Parameter, mit denen eine unmittelbare Benutzeridentifizierung möglich ist (z. B. Benutzerkennung), nicht in der Protokollierung festgehalten werden. Damit ist die Möglichkeit, diese Protokolle für die Aufklärung eventueller Unregelmäßigkeiten zu verwenden, erheblich beeinträchtigt. Während des Kontrollbesuchs wurde berichtet, der Verzicht auf die Protokollierung von Parametern, mit denen eine unmittelbare Benutzeridentifizierung möglich ist, gehe auf **Bedenken des Personalrats** zurück. Über den Umfang derartiger Protokollierungen werde mit dem Personalrat verhandelt.

Soweit eine Protokollierung für Zwecke der Datensicherung erfolgt, ist die Verpflichtung zu einer derartigen Protokollierung in § 10 DSG NW geregelt. Nach § 10 Abs. 1 DSG NW haben öffentliche Stellen, die selbst oder im Auftrag einer anderen öffentlichen Stelle personenbezogene Daten verarbeiten, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine den Vorschriften dieses Gesetzes entsprechende Verarbeitung der Daten

sicherzustellen. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Werden personenbezogene Daten automatisiert verarbeitet, sind nach § 10 Abs. 2 DSG NW unter anderem Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten geeignet sind,

(3.) die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten zu verhindern (Speicherkontrolle),

(4.) zu verhindern, daß Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten benutzt werden können (Benutzerkontrolle),

(5.) zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die zu ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle) und

(10.) die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

Die **Protokollierung von Systemnachrichten** einschließlich der jeweiligen Benutzeridentifizierung dient der Datensicherheit. Das Wissen der Mitarbeiter um bestehende Aufzeichnungen und damit um die Möglichkeit umfassender nachträglicher Aufklärung trägt wesentlich dazu bei, bereits auf den Versuch des Mißbrauchs eines Datenverarbeitungssystems zu verzichten. Wegen der Möglichkeit der Aufklärung eventueller – auch länger zurückliegender – Unregelmäßigkeiten ist die Protokollierung sogar eine der wesentlichen präventiven Maßnahmen. Die Aufzeichnung von Systemnachrichten einschließlich der Benutzeridentifizierung gehört zu den Maßnahmen der Speicherkontrolle, Benutzerkontrolle, Zugriffskontrolle und Organisationskontrolle.

Das Datenschutzgesetz Nordrhein-Westfalen enthält mehrere Vorschriften, die gewährleisten, daß Systemnachrichten, soweit sie personenbezogen aufgezeichnet sind, nicht mißbräuchlich verwandt werden dürfen und in besonderer Weise zu sichern sind. Nach § 29 Abs. 5 DSG NW dürfen Daten der Beschäftigten, soweit sie im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach § 10 Abs. 2 DSG NW gespeichert werden, nicht zu Zwecken der Verhaltens- oder Leistungskontrolle genutzt werden. Darüber hinaus schreibt § 19 Abs. 2 Satz 1 Buchst. d DSG NW vor, daß personenbezogene Daten zu sperren sind, wenn sie nur zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind.

Bei den gespeicherten Systemnachrichten handelt es sich im allgemeinen um automatisierte Dateien. Nach § 19 Abs. 2 Satz 3 DSG NW ist bei automatisierten Dateien die Sperrung grundsätzlich durch technische Maßnahmen sicherzustellen. Diese Vorschrift bedeutet einen zusätzlichen Schutz für derartige Dateien.

Die Möglichkeit der Verwendung der mit Benutzeridentifizierung gespeicherten Systemnachrichten regelt § 19 Abs. 2 Satz 4 DSG NW. Danach dürfen gesperrte Daten über die Speicherung hinaus nicht mehr weiterverarbeitet werden, es sei denn, daß dies zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich ist oder der Betroffene eingewilligt hat.

Systemnachrichten, die mit Personenbezug gespeichert werden, sind wegen der genannten Regelungen des Datenschutzgesetzes Nordrhein-Westfalen in besonderer Weise zu sichern. Die mißbräuchliche Verarbeitung derartiger Aufzeichnungen wird bei Einhaltung dieser Vorschriften verhindert. Ich gehe daher davon aus, daß durch die Regelungen des Datenschutzgesetzes Nordrhein-Westfalen den berechtigten Wünschen des Personalrats weitgehend entsprochen wird und daß daher eine Zustimmung des Personalrats zur Speicherung der Benutzeridentifizierung als Bestandteil von Systemnachrichten erreicht werden kann.

Ich habe empfohlen, soweit das Datenverarbeitungssystem die entsprechenden Möglichkeiten bietet, Systemnachrichten einschließlich der Parameter, die eine unmittelbare Benutzeridentifizierung ermöglichen, aufzuzeichnen und zu archivieren, diese Systemnachrichten zu sperren, soweit die gespeicherten Daten personenbezogen sind, und bei automatisierten Dateien die Sperrung durch technische Maßnahmen sicherzustellen.

7.5 Verarbeitung von Daten im Auftrag

– Kontrollbesuche bei einem Verband im Bereich der Sozialversicherung und einem seiner Mitglieder ergaben, daß Unklarheiten über den **Begriff der Datenverarbeitung im Auftrag** bestehen. Bei dem Verband ist eine Datenverarbeitungsanlage aufgestellt, die von den Mitgliedern dieses Verbandes genutzt wird. Nach Ansicht der Beteiligten verarbeiten die einzelnen Mitglieder ihre Daten selbst auf der bei dem Verband aufgestellten Datenverarbeitungsanlage.

  Die Beteiligten gehen davon aus, daß die Arbeit des Verbandes für die Mitglieder nicht als Datenverarbeitung im Auftrag anzusehen ist. Eine Auftragskontrolle nach Nr. 8 der Anlage zu § 6 Abs. 1 Satz 1 BDSG wurde daher bisher nicht durch das kontrollierte Mitglied wahrgenommen. Nach dem Inhalt des abgeschlossenen Vertrages und entsprechend der Praxis der Zusammenarbeit zwischen dem Verband und dem Mitglied verarbeitet aber der Verband die Daten des Mitglieds in dessen Auftrag.

  Bei der Datenverarbeitung im Auftrag kommt es auf die tatsächlichen Verhältnisse an und nicht auf die Rechtsnatur des Auftragsverhältnisses (vgl. Dammann in Simitis/Dammann/Mallmann/Reh, Kommentar zum Bundesdatenschutzgesetz, 3. Auflage (1981), Rdnr. 3 zu § 8). Für die Wertung, ob Datenverarbeitung im Auftrag vorliegt oder nicht, sind folgende Kriterien maßgebend, die bei Datenverarbeitung im Auftrag gleichzeitig erfüllt sein müssen:

- Gegenstand des Auftrags muß es sein, personenbezogene Daten zu verarbeiten (Dammann, Rdnr. 4 zu § 8).
- Mit dem Auftragsverhältnis darf keine Verlagerung der fachlichen Verantwortung verbunden sein. Das Auftragsverhältnis muß sich vielmehr auf die technische Durchführung im Rahmen der Datenverarbeitung beschränken (vgl. Dammann, Rdnr. 3 zu § 8; Ordemann-Schomerus, Bundesdatenschutzgesetz, 3. Auflage (1982), Erl. 1 zu § 8; von der Groeben in Ruckriegel/von der Groeben/Hunsche, Datenschutz und Datenverarbeitung in Nordrhein-Westfalen (1979), Anm. 3 zu § 7 DSG NW).
- Der Auftragnehmer muß bei wenigstens einer der Phasen der Datenverarbeitung unterstützend tätig werden (vgl. Dammann, Rdnr. 4 zu § 8).
- Es muß grundsätzlich möglich sein, daß der Auftragnehmer im Ablauf der Datenverarbeitung Daten zur Kenntnis nimmt oder auf ihren Inhalt einwirkt (vgl. Dammann, Rdnr. 4 zu § 8).

Bereits aus verschiedenen Regelungen des Vertrages des Verbandes mit dem Mitglied ergeben sich Hinweise darauf, daß der Verband die Daten des Mitglieds in dessen Auftrag verarbeitet. So wird unter anderem festgelegt, daß der Verband eine ordnungsgemäße Datenverarbeitung sicherstellt. Der Verband hat also die für eine ordnungsgemäße Datenverarbeitung notwendigen Maßnahmen zu treffen und die erforderlichen Arbeiten zu verrichten.

In der Praxis ist der Verband für die Arbeit der Datenverarbeitungsanlage voll verantwortlich.

- Der Verband ist für die Arbeit der Maschinenbediener nicht nur disziplinar, sondern auch fachlich verantwortlich. Die Fachaufsicht über die Arbeit der Maschinenbediener wird von den als Vorgesetzte zuständigen Mitarbeitern des Verbandes wahrgenommen.
- Der Verband hat die volle Verfügungsgewalt über das Rechenzentrum.
- Der Verband ist für die Datensicherheit des Rechenzentrums verantwortlich.
- Der Verband entscheidet über die im Rechenzentrum durchzuführenden Arbeiten.
- Der Verband entscheidet über den Zugang zum Rechenzentrum.

Dem Verband wurde nur die technische Durchführung der Datenverarbeitung übertragen. Bei ihm liegt keine fachliche Verantwortung für die verarbeiteten Daten.

- Das Mitglied ist speichernde Stelle und damit Herr der Daten.
- Die Verarbeitung der Daten erfolgt ausschließlich auf Weisung des Mitglieds.

Aus dem Inhalt des Vertrages und aus der Praxis der Arbeitsdurchführung ergibt sich, daß der Verband die Daten des Mitglieds in dessen Auftrag verarbei-

tet. In dem Vertrag sollte daher zum Ausdruck gebracht werden, daß es sich bei der vertragsgemäßen Arbeit des Verbandes um Datenverarbeitung im Auftrag handelt.

– Der Verband hat darüber hinaus **als Auftragnehmer** die bei ihm gespeicherten **Daten gegen unbefugte Zugriffe** zu **sichern.** Insbesondere muß er sicherstellen, daß auf die Daten eines Mitglieds nicht unbefugt von anderen Mitgliedern zugegriffen werden kann. So muß sich ein Mitglied zum Beispiel darauf verlassen können, daß ein Zugriff auf seine Daten von einem bei einem anderen Mitglied stehenden Datenendgerät ausgeschlossen ist. Im Hinblick auf Feststellungen, die ich auch bei anderen Kontrollbesuchen machte, erscheint es mir notwendig, darauf hinzuweisen, daß es dazu nicht ausreicht, den Mitgliedern einen nur beschränkt sicheren Paßwortschutz zur Verfügung zu stellen. Durch das Datenverarbeitungssystem müssen vielmehr Sicherungen bereitgestellt werden, die gewährleisten, daß unbefugte Zugriffe Dritter auf gespeicherte Daten einer speichernden Stelle ausgeschlossen sind.

  Nach § 6 Abs. 1 Satz 1 BDSG hat derjenige, der im Rahmen des § 1 Abs. 2 oder im Auftrag der dort genannten Personen oder Stellen personenbezogene Daten verarbeitet, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen zu gewährleisten. Werden personenbezogene Daten automatisch verarbeitet, sind nach der Anlage zu § 6 Abs. 1 Satz 1 BDSG zur Ausführung der Vorschriften dieses Gesetzes Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind, die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle; Nr. 3 der Anlage) und zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten durch selbsttätige Einrichtungen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (Zugriffskontrolle; Nr. 5 der Anlage).

  Als Auftragnehmer der Mitglieder hat der Verband daher unter anderem sicherzustellen, daß auf Daten eines Mitglieds nur von den Datenendgeräten dieses Mitglieds zugegriffen werden kann. Dieser Anforderung genügte das kontrollierte System nicht. So ermöglicht ein bestimmtes Programm es unter anderem, von den Datenendgeräten eines Mitglieds auf die Daten eines anderen Mitglieds zuzugreifen. Um sicherzustellen, daß jedes Mitglied dennoch nur auf seine eigenen Daten zugreifen kann, erhält jedes Mitglied für die Nutzung dieses Programms ein eigenes Paßwort. Nur unter Benutzung des für dieses Programm vergebenen besonderen Paßworts eines Mitglieds ist es möglich, mit dem Programm auf die Daten dieses Mitglieds zuzugreifen. Das Paßwort ermöglicht allerdings auch von den Datenendgeräten jedes anderen an die Datenverarbeitungsanlage angeschlossenen Mitglieds einen entsprechenden Zugriff.

Der Verband konnte keinen Grund nennen, warum es erforderlich sein könnte, das Datenendgerät eines Mitglieds zu nutzen, um mit dem Programm auf die Daten eines anderen Mitglieds zuzugreifen. Eine derartige Möglichkeit sollte daher nicht bestehen. Die Tatsache, daß das jeweilige Paßwort durch den Verband nur dem berechtigten Mitglied mitgeteilt wird, stellt keinen hinreichenden Schutz dar. Die Erfahrung hat gezeigt, daß ein Paßwortschutz häufig nicht als zuverlässige Sicherung angesehen werden kann.

Die Sicherung durch die Datenverarbeitungsanlage muß so konzipiert sein, daß es keine Möglichkeit gibt, von einem Datenendgerät eines Mitglieds eine Transaktion zu veranlassen, die zur unzulässigen Verarbeitung oder Kenntnisnahme von personenbezogenen Daten eines anderen Mitglieds führt. Es sollte sichergestellt sein, daß die Auswirkungen von Handlungen am Datenendgerät eines Mitglieds ausschließlich Daten dieses Mitglieds oder allgemein verfügbare Daten betreffen können. Ich habe empfohlen zu veranlassen, daß das Informationssystem baldmöglichst entsprechend geändert wird.

7.6 Datenübermittlung im Rahmen der Wartung

An mich war die Frage gerichtet worden, ob es zulässig sei, ein beschädigtes Gerät mit Festplatte, auf der personenbezogene Daten aufgezeichnet sind, im Ausland warten zu lassen, ohne daß die aufgezeichneten Daten vorher gelöscht wurden. Diese Frage wurde während des Kontrollbesuchs bei einem Verband aus dem Bereich der Sozialversicherung erörtert.

7.6.1 Zugriffsberechtigung des Wartungspersonals

Aufgabe der Wartung ist es, dem Betreiber eine funktionsfähige Datenverarbeitungsanlage zur Verfügung zu stellen. Gegenstand von Wartungsverträgen ist das Erhalten oder Wiederherstellen der Funktionsfähigkeit einer Datenverarbeitungsanlage, daran angeschlossener Geräte und bei bestimmten Wartungsverträgen auch spezieller Programme. Zu den Aufgaben der Wartung gehört in keinem Fall eine der Phasen der Datenverarbeitung. Wartung ist daher entgegen einer gelegentlich vertretenen Ansicht keine Datenverarbeitung im Aufgrag (oben S. 118 bis 120).

Soweit im Rahmen der Wartung ein Zugriff auf personenbezogene Daten erfolgt, werden diese an Dritte übermittelt (offenbart). Hierfür ist eine gesetzliche Grundlage erforderlich. Als gesetzliche Grundlage für die Offenbarung personenbezogener Daten, die dem Sozialgeheimnis (§ 35 SGB I) unterliegen, an die Herstellerfirma im Rahmen der Anlagenwartung kommt nur die erste Alternative des § 69 Abs. 1 Nr. 1 SGB X in Betracht. Hiernach ist eine Offenbarung personenbezogener Daten zulässig, soweit sie erforderlich ist für die Erfüllung einer gesetzlichen Aufgabe nach diesem Gesetzbuch durch eine in § 35 SGB I genannte Stelle. Es ist davon auszugehen, daß diese Voraussetzung nur selten erfüllt ist. Darüber hinaus ist eine mögliche zusätzliche Einschränkung der Offenbarung nach § 76 SGB X zu beachten.

Soweit personenbezogene Daten nicht dem Sozialgeheimnis unterliegen, kommt als gesetzliche Grundlage für die Übermittlung personenbezogener Daten an die Herstellerfirma im Rahmen der Anlagenwartung nur § 16 Abs. 1 Satz 1 Buchstaben a oder b DSG NW in Betracht. Hiernach ist die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs zulässig, wenn

a) sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelten Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen des § 13 Abs. 1 vorliegen oder

b) die Voraussetzungen des § 13 Abs. 2 Satz 1 Buchstaben a, b, d oder f vorliegen.

Nach § 13 Abs. 1 Satz 2 DSG NW dürfen die Daten nur für Zwecke weiterverarbeitet werden, für die sie erhoben worden sind. Diese Voraussetzung wird bei einer Übermittlung personenbezogener Daten an die Herstellerfirma im Rahmen der Anlagenwartung nicht erfüllt. § 16 Abs. 1 Satz 1 Buchstabe a DSG NW scheidet daher als gesetzliche Grundlage für eine derartige Übermittlung aus.

Für die Zulässigkeit der Übermittlung personenbezogener Daten an die Herstellerfirma im Rahmen der Anlagenwartung kommt von den in § 16 Abs. 1 Satz 1 Buchstabe b DSG NW genannten Voraussetzungen in der Regel nur § 13 Abs. 2 Satz 1 Buchstabe a DSG NW in Betracht. Sollen hiernach personenbezogene Daten zu Zwecken weiterverarbeitet werden, für die sie nicht erhoben oder erstmals gespeichert worden sind, ist dies nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder die Wahrnehmung einer durch Gesetz oder Rechtsverordnung zugewiesenen einzelnen Aufgabe die Verarbeitung dieser Daten zwingend voraussetzt. Eine Rechtsvorschrift im Sinne der ersten Alternative ist nicht vorhanden. Eine Übermittlung im Rahmen der Wartung ist daher nur zulässig, wenn die Wahrnehmung einer durch Gesetz oder Rechtsverordnung zugewiesenen einzelnen Aufgabe die Verarbeitung dieser Daten zwingend voraussetzt. Es ist davon auszugehen, daß diese Voraussetzung allenfalls selten erfüllt ist. Im Falle einer Übermittlung ist darüber hinaus zu beachten, daß der Empfänger die übermittelten Daten nur für die Zwecke verarbeiten darf, zu denen sie ihm übermittelt wurden (§ 16 Abs. 2 DSG NW).

7.6.2 Daten auf beschädigten Festplatten

Magnetplatten, die an den Hersteller zurückgehen und damit den Bereich der Verfügungsgewalt eines Rechenzentrums verlassen, dürfen keine personenbezogenen Daten mehr enthalten. Sie sind daher vor der Herausgabe zu löschen. Bei beschädigten Geräten mit Festplatten ist dem Anwender ein Löschen meist nicht mehr möglich. In diesem Fall besteht die Gefahr, daß Magnetplatten mit personenbezogenen Daten zur Wartung bei dem Hersteller ungelöscht das Rechenzentrum verlassen. Ein großes Rechenzentrum hat mich darauf hingewiesen, es könne nicht ausgeschlossen werden, daß Geräte mit Festplatten von dem Hersteller zur Wartung in das Ausland transportiert werden.

Bezüglich der Zulässigkeit der Weitergabe personenbezogener Daten auf einer ungelöschten Festplatte, die dem Hersteller zur Wartung übergeben wird, habe ich darauf hingewiesen, daß es durch geeignete Vertragsgestaltung und Arbeitsdurchführung im allgemeinen möglich ist, das Löschen der Daten auf einer Festplatte nicht im Rahmen der Wartung, sondern vorab als **Datenverarbeitung im Auftrag** durchführen zu lassen. Dazu müßte das Löschen von der Wartung vertraglich getrennt werden und vor Beginn der Wartung abgeschlossen sein.

Handelt es sich um **Sozialdaten,** so ist nach § 80 Abs. 2 SGB X eine Auftragserteilung nur zulässig, wenn der Datenschutz beim Auftragnehmer nach der Art der zu verarbeitenden Daten den Anforderungen genügt, die für den Auftraggeber gelten (Satz 1). Der Auftraggeber ist verpflichtet, erforderlichenfalls Weisungen zur Ergänzung der beim Auftragnehmer vorhandenen technischen und organisatorischen Maßnahmen (§ 6 Abs. 1 des Bundesdatenschutzgesetzes) zu erteilen (Satz 2). Wird der Auftrag an eine nicht-öffentliche Stelle erteilt, so hat sich der Auftragnehmer vorher schriftlich bestimmten Kontrollen durch den Auftraggeber zu unterwerfen; der Auftraggeber muß jederzeit berechtigt sein, mit Mitteln des § 30 Abs. 2 und 3 BDSG die Einhaltung der Vorschriften über den Datenschutz sowie seiner ergänzenden Weisungen zu den technischen und organisatorischen Maßnahmen zu überwachen (§ 80 Abs. 2 Satz 3 SGB X). Im übrigen ist nach § 80 Abs. 5 SGB X eine Datenverarbeitung im Auftrag durch eine nicht-öffentliche Stelle nur zulässig, wenn anders Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der automatischen Datenverarbeitung erheblich kostengünstiger besorgt werden können. Darüber hinaus ist in jedem Falle einer Offenbarung personenbezogener Daten die Zweckbindung und die Geheimhaltungspflicht des Empfängers nach § 78 SGB X zu beachten.

Falls das Löschen einer dem Hersteller übergebenen Festplatte durch eine Stelle außerhalb des Geltungsbereichs des Sozialgesetzbuchs erfolgt, ist zusätzlich § 77 SGB X zu beachten. Danach ist eine Offenbarung personenbezogener Daten gegenüber Personen oder Stellen außerhalb des Geltungsbereichs dieses Gesetzbuchs nicht zulässig, soweit Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Es wird kaum möglich sein, eine Beeinträchtigung schutzwürdiger Belange des Betroffenen auszuschließen. Ein Löschen außerhalb des Geltungsbereichs des Sozialgesetzbuchs ist daher im allgemeinen unzulässig.

Soweit die auf der Festplatte gespeicherten **Daten nicht** dem **Sozialgeheimnis** unterliegen und das Löschen als Datenverarbeitung im Auftrag innerhalb des Geltungsbereichs des Grundgesetzes erfolgt, gelten die an den Hersteller weitergegebenen Daten nicht als übermittelt, da der Auftragnehmer nach § 3 Abs. 3 DSG NW nicht Dritter ist. In diesen Fällen hat der Auftraggeber jedoch die Regelungen des § 11 Abs. 1 und 3 DSG NW über die Verarbeitung personenbezogener Daten im Auftrag zu beachten. Darüber hinaus hat er die Verpflichtung zur Auftragskontrolle nach § 10 Abs. 2 Nr. 8 DSG NW. Hinweise zur Wahrnehmung der Auftragskontrolle für diesen Fall enthält mein 3. Tätigkeitsbericht (S. 131/132).

Falls das Löschen einer dem Hersteller übergebenen Festplatte durch eine Stelle außerhalb des Geltungsbereichs des Grundgesetzes erfolgt, ist diese Stelle auch bei Datenverarbeitung im Auftrag Dritter (§ 3 Abs. 3 DSG NW). Die weitergegebenen Daten sind in diesem Fall auch dann übermittelt, wenn das Löschen als Datenverarbeitung im Auftrag durchgeführt wird (§ 3 Abs. 2 Nr. 4 DSG NW).

Die übermittelnde Stelle muß sich vergewissern, ob § 17 DSG NW die Übermittlung erlaubt. Dies wird selten der Fall sein, da der Datenschutzstandard in der Bundesrepublik ein vergleichsweise hohes Niveau hat. Dies gilt insbesondere auch für das neue Datenschutzgesetz Nordrhein-Westfalen, das differenzierte Bestimmungen in Ausprägung des Grundsatzes der Zweckbindung enthält. Nach Artikel 5 des Übereinkommens der Mitgliedstaaten des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (BGBl. II 1985, S. 539) dürfen zwar gespeicherte Daten nicht so verwendet werden, daß es mit den festgelegten und rechtmäßigen Zwecken unvereinbar ist. Jedoch bedarf das Übereinkommen der Umsetzung durch die Vertragsstaaten in nationales Recht.

Zusammenfassend ist festzustellen, daß der **Transport** eines Gerätes, auf dessen Festplatte personenbezogene Daten gespeichert sind, zum Löschen oder zur Wartung **in das Ausland** in den praktisch denkbaren Fällen **unzulässig** ist. Die gespeicherten Daten müssen daher im Inland gelöscht werden. Ein Übermitteln oder Offenbaren der Daten im Rahmen der Anlagenwartung ist aber auch im Inland im allgemeinen unzulässig. Gespeicherte personenbezogene Daten müssen daher vor der Übergabe eines Gerätes zur Wartung in die alleinige Verfügungsgewalt des Herstellers gelöscht werden. Das Löschen kann bei geeigneter Vertragsgestaltung und Arbeitsdurchführung durch den Hersteller als Datenverarbeitung im Auftrag innerhalb des Geltungsbereichs des Grundgesetzes und damit ohne Übermittlung der personenbezogenen Daten erfolgen. Die öffentliche Stelle bleibt in diesem Fall als speichernde Stelle für die Sicherheit der Daten bis zu deren Löschung verantwortlich.

Öffentliche Stellen in Nordrhein-Westfalen, die über eine Datenverarbeitungsanlage mit angeschlossener Festplatte verfügen, auf der personenbezogene Daten gespeichert sind, sollten den Hersteller ihrer Datenverarbeitungsanlage über diese Rechtslage in Kenntnis setzen. Es sollte rechtzeitig Vorsorge getroffen werden, daß eine defekte Festplatte als Datenverarbeitung im Auftrag innerhalb der Bundesrepublik gelöscht werden und die öffentliche Stelle die Auftragskontrolle wahrnehmen kann.

7.7 Sicherungsmaßnahmen bei Besucherverkehr

Immer häufiger werden in Bürgereingaben Sicherungsmaßnahmen öffentlicher Stellen im Hinblick auf den Besucherverkehr gefordert. Im Vordergrund stehen dabei Bedenken, das Gespräch mit dem Sachbearbeiter könne unbefugt von Dritten mitgehört werden, und die Sorge, Akten der öffentlichen Stelle seien nicht ständig unter Aufsicht und könnten daher unbefugt eingesehen werden.

Schwierigkeiten dieser Art entstehen insbesondere in Großraumbüros mit Besucherverkehr. Aber auch der Arbeitsraum mit mehreren Arbeitsplätzen, die Theke für den Kontakt zum Bürger, die Nachbarschaft von Wartezone und Arbeitsplatz oder Theke und auch die offene Tür zum Nachbarraum können die Vertraulichkeit in unzulässiger Weise beeinträchtigen. Zwei Beispiele sollen veranschaulichen, welche Schwierigkeiten auftreten und wie Möglichkeiten zur Lösung gesucht werden können.

7.7.1 Vertraulichkeit von Gesprächen

Die Ämter einer kontrollierten Stadt sind in **Großraumbüros** untergebracht. Im Hinblick auf die aus Artikel 4 Abs. 2 der Landesverfassung folgende Verpflichtung, personenbezogene Daten gegen unbefugte Kenntnisnahme durch Dritte zu schützen, wie auch auf die aus § 35 Abs. 1 Satz 1 SGB I sich ergebende Verpflichtung der Leistungsträger zur Wahrung des Sozialgeheimnisses muß in einem Großraumbüro besondere Sorgfalt darauf verwandt werden zu verhindern, daß Gespräche am Arbeitsplatz eines Sachbearbeiters von Unbefugten mitgehört werden können.

In jedem Großraumbüro muß darauf geachtet werden, alle Arbeitsplätze akustisch hinreichend gegeneinander zu isolieren. In Großraumbüros ohne Publikumsverkehr soll die gegenseitige Störung vermieden werden. In Großraumbüros mit Publikumsverkehr ist es insbesondere erforderlich, durch hinreichende akustische Isolierung der Arbeitsplätze die Vertraulichkeit der Gespräche zu gewährleisten. Nach meinen Erfahrungen ist es auch in einem Großraumbüro mit starkem Publikumsverkehr möglich, dieser Anforderung zu genügen.

Durch die Unterbringung der Ämter in Großraumbüros soll bei der kontrollierten Stadt dem einzelnen Bürger ein leichterer Zugang zu allen Sachbearbeitern ermöglicht werden. Abgesehen von wenigen Ausnahmen verzichtet die Stadt darauf, Arbeitsplätze durch Türen gegen wartende Bürger abzuschirmen. Mit häufigem Bürgerkontakt ist daher an zahlreichen Arbeitsplätzen zu rechnen. In vielen Bereichen des Großraumbüros muß auch mit der Anwesenheit von Bürgern gerechnet werden, die nur den Arbeitsplatz des für sie zuständigen Sachbearbeiters suchen. Unter diesen Umständen ist eine gute akustische Isolierung der Arbeitsplätze von besonderer Bedeutung.

Bei der Begehung der Großraumbüros der Stadt wurde allerdings ausnahmslos festgestellt, daß ein Mithören der an einem Arbeitsplatz geführten Gespräche noch über gewisse Entfernungen möglich ist. Die Vertraulichkeit von Gesprächen an den Arbeitsplätzen ist dadurch deutlich beeinträchtigt. Die Situation ist nicht in allen Ämtern gleich. Zu den bestehenden Unterschieden trägt sicher auch die unterschiedliche Stärke des von der Klimaanlage stammenden Hintergrundgeräuschs bei, das zu einer gewissen akustischen Isolierung der einzelnen Arbeitsplätze führt.

Eine Reihe möglicher Maßnahmen wurde erörtert:

- Von anderen Großraumbüros ist bekannt, daß es möglich ist, eine bessere **Schalldämpfung** zu verwirklichen. Durch Teppichboden, Zwischenwände

und geeignete Deckenverkleidung wird bei den Großraumbüros der Stadt zwar bereits die Schallübertragung verringert. Ich gehe aber davon aus, daß es möglich ist, die Schalldämpfung durch geeignete ergänzende Maßnahmen weiter zu verbessern.

Während des Kontrollbesuchs wurde besprochen, daß sich die Stadt zu dieser Frage von einer geeigneten Firma oder einem Ingenieurbüro fachlich beraten lassen will.

– Als Beitrag zur akustischen Isolierung sollten alle Arbeitsplätze einen hinreichenden räumlichen Abstand voneinander haben. Die **Anordnung der Arbeitsplätze** in den Großräumen der Stadt entspricht bereits in gewissem Umfang dieser Forderung. Durch aufgelockerte Anordnung der Schreibtische wird im allgemeinen der Abstand zwischen den einzelnen Arbeitsplätzen sichergestellt.

Allerdings wurden auch Ausnahmen von der aufgelockerten Anordnung festgestellt. So sind die Arbeitsplätze des Einwohnermeldeamtes zum Teil unmittelbar einander benachbart angeordnet. Während des Kontrollbesuchs wurde besprochen, daß hier Änderungen erfolgen sollten.

In allen Ämtern wurde jeweils im Fensterbereich eine besondere Häufung von Arbeitsplätzen angetroffen. Im Fensterbereich war daher der Abstand zwischen den einzelnen Arbeitsplätzen geringer. Dadurch verringerte sich allerdings auch die Zahl der Arbeitsplätze, die noch außerhalb des Fensterbereichs unterzubringen waren, und es wurde möglich, bei der Anordnung dieser Arbeitsplätze größere Abstände einzuhalten.

Während des Kontrollbesuchs wurde besprochen, daß überprüft werden sollte, ob im Fensterbereich Arbeitsplätze mit stärkerem Bürgerkontakt einander benachbart sind. Zwischen derartigen Arbeitsplätzen sollten möglichst Arbeitsplätze ohne Bürgerkontakt angeordnet werden. Bei geringem Besucherverkehr könnte durch Dienstanweisung festgelegt werden, daß eine Beratung von zwei Parteien an benachbarten Beratungsplätzen nur dann stattfinden darf, wenn beide Parteien eingewilligt haben.

– Die Möglichkeit, Arbeitsplätze mit stärkerem Bürgerkontakt dadurch gegeneinander zu isolieren, daß andere Arbeitsplätze dazwischen angeordnet werden, gilt selbstverständlich nicht nur für den Fensterbereich. Eine entsprechend geänderte Anordnung der Schreibtische wurde während des Kontrollbesuchs am Beispiel der Wohngeldstelle erörtert. Die Stadt sollte unter diesem Gesichtspunkt die Anordnung aller Arbeitsplätze überprüfen.

– Unabhängig von Maßnahmen zur akustischen Isolierung in den Großraumbüros und von einer zweckmäßigeren Anordnung der Arbeitsplätze wäre es eine wichtige Maßnahme im Sinne des Datenschutzes, wenn die Unterredung mit dem Sachbearbeiter in besonderen Fällen oder auf Wunsch des Bürgers in einem **Besprechungszimmer** stattfinden könnte. Grundsätzlich besteht diese Möglichkeit bereits. Ausdrückliche Nachfrage während des Kontrollbesuchs bei einzelnen Ämtern ergab allerdings, daß davon nur

in seltenen Ausnahmefällen und nur auf Initiative des Sachbearbeiters Gebrauch gemacht wird. Erschwerend ist, daß die Besprechungszimmer nur in einem anderen Stockwerk zur Verfügung stehen.

Die Stadt berichtete während des Kontrollbesuchs, es sei vorgesehen, in den beiden Stockwerken, in denen sich die Großraumbüros befinden, jeweils einige abgetrennte Besprechungszimmer zu schaffen. Danach sei die Möglichkeit deutlich verbessert, das Gespräch mit dem Sachbearbeiter auf Wunsch in einem Besprechungszimmer zu führen.

Es wurde besprochen, daß der Bürger in geeigneter Weise auf diese Möglichkeit aufmerksam gemacht werden sollte. Als Hinweise könnten etwa Schilder in den Wartezonen oder auf den Schreibtischen der Sachbearbeiter dienen.

7.7.2 Sichern von Akten

Die Begehung der Großraumbüros der Stadt (oben S. 125) ergab, daß die Arbeitsplätze durch zahlreiche Stellwände gegeneinander abgegrenzt sind. In einer Reihe von Fällen ist die Abgrenzung sogar so weitgehend, daß Einzelräume entstanden sind. Die Folge waren besondere Probleme für das sichere **Aufbewahren der Akten** der Sachbearbeiter.

In jedem Bürogebäude müssen Maßnahmen getroffen werden, die sicherstellen, daß Akten nicht in die Hände Unbefugter gelangen können. Falls in einem Bürogebäude Einzelbüros für jeweils einen oder mehrere Mitarbeiter vorgesehen sind, kann nicht zweifelhaft sein, welche Maßnahmen zu treffen sind. Ein Arbeitsraum, in dem sich kein befugter Mitarbeiter aufhält, muß verschlossen sein. Wer als letzter seinen Arbeitsraum verläßt, hat diesen daher zu verschließen.

Falls die Reinigung eines Arbeitsraums in Abwesenheit der in dem Raum tätigen Mitarbeiter erfolgt oder erfolgen kann, muß entweder für eine ständige Aufsicht gesorgt oder es muß sichergestellt werden, daß sich sämtliche Akten mit personenbezogenen Daten in sicher verschlossenen Schränken befinden. Falls die Reinigung außerhalb der Dienstzeit ohne ständige Aufsicht erfolgt, sind daher alle Akten mit personenbezogenen Daten nach Dienstschluß in verschlossenen Schränken aufzubewahren.

Im allgemeinen ist ein Großraumbüro während der Dienstzeit ständig besetzt. Man könnte daher zunächst von der Vorstellung ausgehen, jeder Arbeitsplatz befinde sich ständig unter Beobachtung anderer Mitarbeiter. Selbst bei starkem Publikumsverkehr sei daher während der Dienstzeit ein Verschließen der an einem Arbeitsplatz liegenden Akten nicht erforderlich.

Eine solche Aussage würde selbst für ein Großraumbüro ohne Trennwände zwischen den einzelnen Arbeitsplätzen nur sehr eingeschränkt gelten. Ein in dem Großraum tätiger Mitarbeiter wird nur die in nächster Nähe liegenden Arbeitsplätze so weitgehend beobachten, daß Kenntnisnahme oder Entwendung von Akten durch Dritte ausgeschlossen werden kann.

Die Situation wird darüber hinaus geändert, falls innerhalb des Großraums dem einzelnen Mitarbeiter durch Stellwände die Beobachtung anderer Arbeitsplätze verwehrt ist. Zweifellos liegt es im Sinne des Datenschutzes, wenn der Bürger, der zu einem sensiblen Thema eine Unterredung mit einem Sachbearbeiter führt, keinen Sichtkontakt zu anderen Bürgern oder anderen Sachbearbeitern befürchten muß. Bezüglich der Sicherheit von Akten an einem Arbeitsplatz darf aber nicht übersehen werden, daß ein Großraum durch das Aufstellen von Stellwänden in isolierte Bereiche aufgeteilt wird. Diese isolierten Bereiche sind insoweit wie getrennte Räume anzusehen, als sie aus anderen Bereichen nicht eingesehen werden können. Eine Überwachung eines durch Stellwände abgetrennten Raums durch einen Nachbarraum scheidet in diesen Fällen praktisch aus.

Hätte ein durch Stellwände geschaffener abgetrennter Raum mit einem oder mehreren Arbeitsplätzen eine Tür, müßte diese verschlossen werden, sobald der Raum von dem letzten Mitarbeiter verlassen wird. Ein Verschließen des Raums ist aber nicht möglich. Der Mitarbeiter, der als letzter den Raum verläßt, kann keine geeignete Maßnahme zur Sicherung eventuell auf den Schreibtischen anderer Mitarbeiter liegender Akten treffen.

Zur Sicherung der Akten ist es daher erforderlich, daß jeder Mitarbeiter, der seinen Arbeitsplatz verläßt, entweder

- alle Akten mit personenbezogenen Daten verschließt oder
- sicherstellt, daß sich in demselben Raum ein anderer Mitarbeiter befindet, der den Arbeitsplatz für die Zeit der Abwesenheit unter ständiger Beobachtung hat.

Durch **Dienstanweisung** muß den Mitarbeitern daher ein entsprechendes Verhalten vorgeschrieben werden. Die Sicherheit der Akten hängt in diesem Fall weitgehend davon ab, ob die Dienstanweisung ausnahmslos befolgt wird.

7.7.3 Selbstkontrolle der öffentlichen Stelle

Nach aller Erfahrung wird ein den Anforderungen der Datensicherheit entsprechendes Verhalten der Mitarbeiter nicht bereits dadurch erreicht, daß dieses Verhalten durch Dienstanweisung vorgeschrieben wird. Es muß vielmehr durch ergänzende Maßnahmen sichergestellt werden, daß sich die Mitarbeiter entsprechend dieser Dienstanweisung verhalten.

Jedenfalls ist es Aufgabe des Vorgesetzten zu kontrollieren, ob die Dienstanweisung eingehalten wird. Eine Dienstanweisung zur Datensicherung enthält allerdings häufig Regeln, die im Einzelfall als kleinlich erscheinen, obgleich ihre Notwendigkeit für jeden einsehbar sein sollte. Manchem Vorgesetzten fällt es schwer, auch in derartigen Fällen das Einhalten der Dienstanweisung durchzusetzen.

Falls es für die Sicherheit von großer Bedeutung ist, daß entsprechend der Dienstanweisung verfahren wird, sollte sich daher die Leitung der öffentlichen Stelle diese Forderung erkennbar zu eigen machen. Sie sollte einen Mitarbei-

ter damit beauftragten zu kontrollieren, ob die Dienstanweisung eingehalten wird. Dieser Mitarbeiter sollte in unregelmäßigen Abständen kontrollieren, ob entsprechend den gegebenen Anweisungen verfahren wird. Berichte über die Ergebnisse der Kontrollen sollten der Leitung vorgelegt werden.

Kriterien dafür, ob eine solche **Institutionalisierung der Kontrolle** angemessen ist, sind vor allem die Empfindlichkeit der zu sichernden Daten und eine allgemeine Abschätzung der bestehenden Gefährdung. Im Hinblick auf die Stärke des Besucherverkehrs und die Möglichkeit des einzelnen Besuchers, die Arbeitsplätze weitgehend ungehindert zu erreichen, ist es nach diesen Kriterien bei dem Beispiel des Großraumbüros, in dem die Akten der Sachbearbeiter zu sichern sind (oben S. 127/128), angemessen, eine Kontrolle zu institutionalisieren. Ich habe daher eine entsprechende Empfehlung ausgesprochen.

Düsseldorf, den 13. März 1989

Maier-Bode

Anlage 1 (zu 4.1.4)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 6. Juni 1988

zum Entwurf eines Gesetzes zur Strukturreform im Gesundheitswesen (Gesundheits-Reformgesetz – GRG)

Die Konferenz der Datenschutzbeauftragten stellt fest, daß es in Verhandlungen zwischen dem Bundesbeauftragten für den Datenschutz und dem Bundesminister für Arbeit und Sozialordnung gelungen ist, eine Reihe von Forderungen des Datenschutzes im Regierungsentwurf gegenüber den Vorentwürfen zu verwirklichen.

Gleichwohl halten die Datenschutzbeauftragten eine Verbesserung des Persönlichkeitsschutzes der Krankenversicherten im weiteren Gesetzgebungsverfahren vor allem in den folgenden Punkten für notwendig:

1. **Erfassung medizinischer Daten und Grundsatz des geringstmöglichen Eingriffs**

   Die im Zusammenhang mit Leistungen der gesetzlichen Krankenversicherung vorgesehene automatisierte Verarbeitung von Daten der Versicherten, Ärzte und Zahnärzte darf der Gesetzgeber wegen des damit verbundenen gravierenden Eingriffs in das Selbstbestimmungsrecht der Versicherten nur zulassen, wenn damit tatsächlich auch die erklärten Ziele des Gesetzgebungsvorhabens gefördert, namentlich ein wesentlicher Beitrag zur Kostendämpfung geleistet werden kann, und sich dies nicht auch durch weniger einschneidende Maßnahmen erreichen läßt. So würde es für die Erstellung von Statistiken, die für die Bewertung und Beeinflussung des Leistungsgeschehens wichtig sind, genügen, einen anonymisierten Transparenzbestand zu bilden. Darüber hinaus wäre zu fragen, ob es nicht ausreicht, statt der vorgesehenen versichertenbezogenen umfassenden Datenspeicherung nur die rechtlichen und organisatorischen Voraussetzungen zur Überprüfung von Einzelfällen festzulegen.

2. **Festlegung des Verwendungszwecks personenbezogener Daten**

   Gegen die Nutzung personenbezogener Daten, soweit sie für die Überprüfung der Abrechnung medizinischer Leistungen und zur Kontrolle der Wirtschaftlichkeit erforderlich ist, bestehen keine grundsätzlichen Bedenken. Nach der Rechtsprechung des Bundesverfassungsgerichts muß der Verwendungszweck erhobener Daten vom Gesetzgeber normenklar festgelegt werden. Für Kassenärztliche Vereinigungen und für den Medizinischen Dienst fehlt es im Gesetzentwurf an einer Festlegung des Verwendungszwecks. Der Gesetzentwurf stellt außerdem nicht sicher, daß Daten der Krankenkassen nur für deren Zwecke verwendet werden. Eine Verwendung

medizinischer Daten über den eigentlichen Aufgabenbereich der Krankenkassen, der Kassenärztlichen Vereinigungen und des Medizinischen Dienstes hinaus darf wegen der besonderen Sensibilität der Daten nur für eng umschriebene Ausnahmefälle zugelassen werden. Die allgemeinen Offenbarungsvorschriften des SGB X lassen eine zu weitgehende Nutzung durch Dritte zu.

Dies gilt um so mehr, als die im Entwurf bereits einbezogene technische Entwicklung (maschinenlesbare Datenträger, Krankenversicherungskarte) immer mehr dazu führen wird, daß die versicherungsbezogenen Krankheitsdaten in maschinenlesbarer Form und damit vielfältig verwertbar vorliegen werden.

Die Konferenz begrüßt die Verbesserungsvorschläge der Ausschüsse des Bundesrates.

3. Vereinbarungen der Verbände

Der Gesetzentwurf überläßt die Regelung der Abrechnung der kassenärztlichen Versorgung einschließlich der dafür erforderlichen Datenübermittlung den Vereinbarungen der Verbände der Krankenkassen und Kassenärztlichen Vereinigungen. Verschiedene Vereinbarungen greifen nachhaltig in das informationelle Selbstbestimmungsrecht der Versicherten ein, ohne daß diese – insbesondere als Pflichtversicherte – eine Wahlmöglichkeit hätten. Das betrifft z. B. Festlegungen über den Inhalt von Rezepten und Krankenscheinen, die Einbeziehung Dritter zu Prüfzwecken, Meldung von Behinderungen an die Krankenkassen.

Da der Gesetzgeber nach der Rechtsprechung des Bundesverfassungsgerichts alles Wesentliche selbst regeln muß, reicht es nicht aus, die Regelungsbefugnis an die Verbände zu delegieren. Vielmehr müßte der Umfang der Eingriffe in das informationelle Selbstbestimmungsrecht und der Mindestinhalt der datenschutzrechtlichen Regelungen konkreter als bisher gesetzlich festgelegt werden. Das gilt auch für die Voraussetzungen zur Einführung maschinenlesbarer Krankenversicherungskarten. Darüber hinaus wäre klarzustellen, daß die Verarbeitung und Nutzung personenbezogener Daten für andere als die im Gesetz genannten Fälle nicht durch Vereinbarung vorgesehen werden kann. Der Gesetzgeber sollte überdies ein Verfahren vorsehen, in dem die Wahrung der Rechte der Patienten bei Erlaß solcher Vereinbarungen überprüft wird (z. B. Genehmigungsvorbehalt; eine Genehmigung dürfte nur erteilt werden, wenn in den Vereinbarungen die Forderungen des Datenschutzes der Versicherten angemessen berücksichtigt sind).

Der Inhalt der Vereinbarungen ist dem Betroffenen auf Verlangen zugänglich zu machen.

4. Medizinischer Dienst

Im Hinblick auf die Schutzwürdigkeit der beim Medizinischen Dienst anfallenden Krankheitsdaten sind gesetzliche Regelungen erforderlich über

– Art und Umfang der zu verarbeitenden Daten

- Zweckbestimmung und Verwendungsmöglichkeit (etwa im Bereich des Sozialmedizinischen Dienstes der Rentenversicherungsträger)
- Vermeidung einer med. Zentraldatei
- Informationsrechte der Betroffenen
- Einschränkung der Offenbarungsbefugnisse gegenüber Dritten
- Löschungszeitpunkte.

Die Konferenz begrüßt auch hier die in diese Richtung zielenden Vorschläge der Ausschüsse des Bundesrates.

5. **Auskunftsanspruch**

Wegen der zentralen Bedeutung des Auskunftsanspruchs ist im Gesetzestext deutlich klarzustellen, daß auf Verlangen des Versicherten Auskunft über Leistungen und Kosten sowie nach Maßgabe des § 83 SGB X auch über die Diagnose zu erteilen ist. Der Auskunftsanspruch darf nicht durch Satzung beschränkt werden. Der Anspruch muß auch gegenüber dem Medizinischen Dienst bestehen.

6. **Aufbewahrungsfristen**

Der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz gebietet, die Speicherungsdauer personenbezogener Daten auf das erforderliche Maß zu begrenzen. Hierzu sind konkret bestimmte Aufbewahrungsfristen unerläßlich.

Im Gesetzentwurf ist bisher nur bei den Krankenkassen eine nach Jahren festgelegte Frist für die Aufbewahrung von Daten über Leistungsvoraussetzungen (z. B. Art der Erkrankung, Arbeitsunfähigkeitszeiten) vorgesehen. Die Speicherungsdauer für andere Daten bei Krankenkassen und Kassenärztlichen Vereinigungen (z. B. verordnete Medikamente, ärztliche Leistungen, Überweisungen, Abrechnungsunterlagen) ist im Gesetzentwurf nicht konkret befristet. Nach dem Grundsatz der Normenklarheit und dem Wesentlichkeitsgebot des Bundesverfassungsgerichts hat der Gesetzgeber hier selbst eine bestimmte Aufbewahrungsfrist festzulegen.

Die Konferenz begrüßt auch hier die in diese Richtung zielenden Vorschläge der Ausschüsse des Bundesrates. Sie weist jedoch darauf hin, daß die Aufbewahrungsfrist jeweils am Tage der jeweiligen Leistungsgewährung beginnen muß.

7. **Zentrale Krankheitsdatei der Unfallversicherungsträger**

Der Gesetzentwurf räumt den Unfallversicherungsträgern die Möglichkeit ein, eine zentrale Krankheitsdatei einzurichten.

Angesichts der schon früher diskutierten vielfältigen datenschutzrechtlichen Probleme zentraler Krankheits- und Gefährdungsregister muß der Gesetzgeber jedoch gleichzeitig mit der Erlaubnis zur Einrichtung dafür

sorgen, daß für solche Register ausreichende rechtliche und organisatorische Schutzvorkehrungen wirksam werden. Vorzusehen ist insbesondere eine Einwilligung des Betroffenen in die Speicherung seiner Daten.

Sicherzustellen ist ferner:

- die Verantwortlichkeit für die gespeicherten Daten (speichernde Stelle)
- Art und Umfang der zu speichernden Daten
- die konkrete Zweckbestimmung der Daten in dem betreffenden Register
- Zugriffsrechte.

Sicherzustellen ist schließlich, daß die Patientendaten nicht aus dem durch § 35 SGB I geschützten Bereich (Sozialgeheimnis) herausgelöst werden.

Anlage 2 (zu 4.3.4)

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. März 1988

zur polizeilichen Datenverarbeitung bis zum Erlaß bereichsspezifischer gesetzlicher Regelungen

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 14./15. 3. 1988 in Mainz.

Eines der dringendsten datenschutzrechtlichen Anliegen ist die Schaffung bereichsspezifischer Grundlagen für die Datenverarbeitung der Sicherheitsbehörden. Dies gilt ebenso für die Nachrichtendienste. Schon seit Jahren haben die Datenschutzbeauftragten entsprechende Forderungen erhoben. Spätestens seit dem „Volkszählungsurteil" des Bundesverfassungsgerichts vom 15. 12. 1983 ist das gesetzliche Regelungsdefizit offenbar. So hat der Bayerische Verfassungsgerichtshof in einer Entscheidung vom 9. 7. 1985 bezogen auf die polizeiliche Datenverarbeitung hervorgehoben, es sei geboten, daß der Gesetzgeber die Materie regele, die bisher Gegenstand der „Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen (KpS)" ist.

Mit der Erhebung, Speicherung und Weitergabe personenbezogener Daten greift die Polizei in die Grundrechte der Betroffenen ein, ohne daß dafür immer die verfassungsrechtlich gebotenen gesetzlichen Grundlagen vorhanden sind. So haben schon einige Gerichte die polizeiliche Datenverarbeitung zum Zwecke vorbeugender Straftatenbekämpfung bis zum Erlaß bereichsspezifischer gesetzlicher Grundlagen für unzulässig erklärt. Gleichwohl kommen die gesetzgeberischen Initiativen zur Behebung dieses Zustandes nur äußerst schleppend voran.

Allerdings hat das Bundesverfassungsgericht dem Gesetzgeber in der Vergangenheit Übergangsfristen zur Beseitigung von Regelungsdefiziten zugebilligt, wenn damit eine sonst eintretende Funktionsunfähigkeit staatlicher Einrichtungen vermieden werden kann, die der verfassungsmäßigen Ordnung noch ferner stünde als der bisherige Zustand.

Dabei ist auf folgendes hinzuweisen:

1. Übergangsfristen können ihrer Natur nach nicht unbegrenzt in Anspruch genommen werden. Das Bundesverfassungsgericht hat ausdrücklich darauf hingewiesen, daß sie dann nicht mehr anerkannt werden können, wenn der Gesetzgeber eine Neuregelung ungebührlich verzögert.

2. Während der Übergangsfrist reduziert sich die Befugnis zu Eingriffen auf das, was für die geordnete Weiterführung eines „funktionsfähigen Betriebes" unerläßlich ist. Es ist mithin unzulässig und mit den vom Bundesverfassungsgericht festgestellten reduzierten Befugnissen unvereinbar, bereits bestehende Datenverarbeitungsabläufe noch auszuweiten, etwa durch den Aufbau neuer Datenbanken oder die Ausschöpfung neuer technischer Möglichkeiten, soweit die Eingriffe in die Rechte der Betroffenen damit eine neue Qualität erreichen.

3. Besondere Zurückhaltung hat sich die Polizei dort aufzuerlegen, wo Eingriffe in das informationelle Selbstbestimmungsrecht noch weitere Grundrechte betreffen.

   3.1 Die Feststellungen von Personalien, damit verbundene Datenabgleiche und Speicherungen sowie Film- und Videoaufnahmen sind anläßlich von öffentlichen Versammlungen während der Übergangszeit nur dann als zulässig anzusehen, wenn Anhaltspunkte dafür vorliegen, daß strafbare Handlungen begangen werden.

   3.2 Die Nutzung technischer Hilfsmittel zur verdeckten Datenerhebung durch Lauschangriffe in Wohnungen muß grundsätzlich ausgeschlossen sein.

4. Der Einsatz von verdeckten Ermittlern und V-Leuten sowie langfristige Observationen und polizeiliche Beobachtung dürfen nur zugelassen werden, wenn konkrete Anhaltspunkte für bestimmte schwere Straftaten bestehen. Es muß festgelegt werden, wer diese Maßnahmen anordnen darf, wie die anfallenden Erkenntnisse verwertet werden dürfen und wann die Betroffenen zu unterrichten sind.

5. Im Hinblick auf die von den Verfassungsgerichten für die Übergangszeit geforderte Beschränkung auf das, was für die geordnete Weiterführung eines „funktionsfähigen Betriebes" unerläßlich ist, erinnern die Datenschutzbeauftragten an ihre früheren Beschlüsse zur polizeilichen Datenverarbeitung. Danach sind künftig insbesondere folgende Datenverarbeitungsvorgänge zu unterlassen:

   - Speicherung diskriminierender personenbezogener Hinweise in polizeilichen Informationssystemen;
   - Speicherung (ehemals) verdächtiger Personen zu Zwecken vorbeugender Straftatenbekämpfung ohne verantwortbare kriminologische Prognose;

- Speicherung von Daten über Personen, bei denen eine Anklageerhebung mangels öffentlichen Interesses abgelehnt wurde;
- Speicherung von Daten über Kinder, die der Begehung einer Straftat verdächtigt werden;
- Weitergabe von Informationen, die mit speziellen polizeilichen Befugnissen erhoben wurden, an andere als Polizeidienststellen.

Anlage 3 (zu 6.4.2)

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. Dezember 1987

zur Speicherung personenbezogener Aids-Daten in polizeilichen Informationssystemen

In zwei gemeinsamen Sitzungen von Arbeitsgruppen der ständigen Konferenz der Innenminister und -senatoren sowie der Datenschutzbeauftragten des Bundes und der Länder wurde das Problem der Speicherung von personenbezogenen Aids-Hinweisen in polizeilichen Informationssystemen erörtert. Nach eingehender Beratung der Ergebnisse dieser Gespräche faßten die Datenschutzbeauftragten des Bundes und der Länder sowie die Datenschutzkommission des Landes Rheinland-Pfalz bei Gegenstimme des Bayerischen Landesbeauftragten für den Datenschutz folgenden Beschluß:

I.

Die Speicherung von HIV-Hinweisen soll die Eigensicherung von Polizeibeamten und evtl. auch den Schutz von Personen in Polizeigewahrsam gewährleisten, die mit HIV-Infizierten in Kontakt kommen. Die Datenschutzbeauftragten verkennen nicht, daß Polizeibeamte bei der Berufsausübung spezifischen Gefahren ausgesetzt sind und die notwendigen Maßnahmen ergriffen werden müssen. Insbesondere ein direkter Blutkontakt oder eine Verletzung mit infizierten Injektionskanülen bei Kontakten mit Drogenabhängigen stellen eine solche spezifische Gefährdung dar. Dem Anspruch der Polizeibeamten auf einen weitestgehenden Schutz vor einer Infektion, die zu einer tödlichen Erkrankung führen kann, steht der Anspruch der Betroffenen gegenüber, daß Datenspeicherungen nur dann vorgenommen werden, wenn diese geeignet sind, die Gefährdung wirksam zu verringern, und sie dadurch nicht unverhältnismäßig belastet werden. Hierbei ist auch zu berücksichtigen, daß eine automatisierte Speicherung von medizinischen Daten eine schwerwiegende Beeinträchtigung für die Betroffenen darstellt. Ebenso sind auch die gravierenden sozialen Folgen für diesen Personenkreis zu bedenken, wenn die gespeicherten Daten an Dritte gelangen.

II.

Sowohl medizinische Experten als auch Fachleute aus dem Sicherheitsbereich und dem Gesundheitswesen haben wiederholt Zweifel daran geäußert, daß durch die Speicherung von Informationen über HIV-Infizierte in polizeilichen Informationssystemen die Gefährdung von Polizeibeamten abgewendet werden kann. Hierfür werden folgende Gründe vorgebracht: In vielen Situationen, wie z. B. bei der Hilfeleistung für verletzte Unfallopfer, der Festnahme unbekannter Personen oder auch der plötzlichen Konfrontation mit Straftätern oder Störern sei eine vorherige Überprüfung vorhandener Dateibestände ohnehin nicht möglich. Hinzu komme, daß der Polizei immer nur ein sehr geringer Teil der Infizierten bekannt sein werde, so daß die Polizei in jedem Fall und auch ohne besondere Hinweise Schutzmaßnahmen treffen müsse.

Angesichts dieser Zweifel, die von den Datenschutzbeauftragten geteilt werden, kann die Speicherung – wenn überhaupt – nur unter sehr eingeschränkten Voraussetzungen hingenommen werden. Möglich erscheint dies allenfalls für Situationen, in denen es mit hoher Wahrscheinlichkeit zu gewaltsamen Auseinandersetzungen mit infizierten Personen kommt. Keinesfalls darf eine „Aids-Datei" entstehen. Im übrigen wäre mindestens folgendes zu beachten:

1. Die Speicherung von HIV-Hinweisen im Datenfeld der „personengebundenen Hinweise" im bundesweiten Inpol-System und in vergleichbaren Landessystemen muß eingestellt werden, da diese Hinweise bei sämtlichen Abfragen erscheinen.

2. HIV-Hinweise dürfen allenfalls in solche Dateien aufgenommen werden, in denen sie als Grundlage für die Eigensicherung bei polizeilichem Einschreiten tatsächlich in Betracht kommen.

3. Die Speicherung von HIV-Hinweisen aufgrund von Verdächtigungen und ungeprüften Informationen verbietet sich in jedem Fall. Kommt die Information vom Betroffenen selbst, müßte dieser über die Tatsache und die Bedeutung der Speicherung aufgeklärt werden. Im übrigen kommt nur die Speicherung von ärztlich gesicherten Informationen in Betracht, die die Polizei rechtmäßig erlangt hat.

4. Auf die gespeicherten Daten darf nur ein besonders dazu befugter Benutzerkreis zugreifen, und dies nur zu Zwecken der Eigensicherung. Die Weitergabe an andere Stellen ist nur in besonders festzulegenden Fällen zulässig.

5. Es muß in jedem Fall erkennbar sein, wer wann den HIV-Hinweis in das System eingespeichert hat und hierfür verantwortlich ist, da nur so die Speicherungspraxis überprüft werden kann und notwendige Berichtigungen ermöglich werden.

Anlage 4 (zu 7.2.1)

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 10. Oktober 1988

zur Datensicherheit beim Einsatz kleinerer Datenverarbeitungsanlagen

Beim Einsatz kleinerer Datenverarbeitungsanlagen, vor allem von persönlichen Computern (PC), bereiten die Datensicherheit und die Ordnungsmäßigkeit der Verarbeitung personenbezogener Daten besondere Probleme. Im Hinblick auf diese Probleme geben die Datenschutzbeauftragten des Bundes und der Länder folgende Empfehlungen:

1. Vor jeder Entscheidung, ob für die Arbeiten eines Aufgabengebiets ein PC oder eine sonstige kleinere Datenverarbeitungsanlage eingesetzt werden kann, muß geprüft werden, ob die dabei erzielbare Datensicherheit ausreichend ist. Bei dieser Prüfung müssen insbesondere die Empfindlichkeit der Daten und der Grad der Verbindlichkeit der Verarbeitungslogik berücksichtigt werden. Die Verarbeitung personenbezogener Daten mit einem automatisierten Verfahren, das keine angemessene Datensicherheit bietet, verstößt gegen die Datenschutzgesetze.

2. Eine speichernde Stelle hat auch bei der Verarbeitung personenbezogener Daten auf einem PC oder einer sonstigen kleineren Datenverarbeitungsanlage die technischen und organisatorischen Maßnahmen zu treffen, die je nach Art der zu schützenden Daten geeignet sind, die Datensicherheit zu gewährleisten. Sofern die Datensicherheit mit den verfügbaren Maßnahmen nicht in dem erforderlichen Umfang gewährleistet werden kann, muß auf den Einsatz des PC oder der kleineren Datenverarbeitungsanlage verzichtet werden.

   Um die Datensicherheit zu gewährleisten, sind insbesondere die dem neuesten Stand entsprechenden technischen Maßnahmen zu treffen. Weisungen sollten schriftlich erfolgen und in einer Dienstanweisung zusammengefaßt werden. Durch Kontrollen der Arbeitsdurchführung ist sicherzustellen, daß alle Vorschriften und Weisungen befolgt werden.

3. Die Hersteller von Hard- und Software werden aufgefordert, für kleinere Datenverarbeitungsanlagen einschließlich der persönlichen Computer Verfahren zu entwickeln und bereitzustellen, die einen Betrieb dieser Geräte mit einem Maß an Datensicherheit ermöglichen, das demjenigen großer Rechenzentren entspricht. Vor allem müssen Hilfsmittel verfügbar gemacht werden, die es einer datenverarbeitenden Stelle ermöglichen,

   – ohne organisatorisch strukturiertes Rechenzentrum und damit auch ohne Funktionstrennungen bei der Arbeitsabwicklung,

   – ohne organisatorische Trennung zwischen Anwendung und Durchführung der automatisierten Datenverarbeitung und

– trotz Verzichts auf Detailkenntnisse der automatisierten Datenverarbeitung bei Vorgesetzten und der für die Revision zuständigen Organisationseinheit

sicherzustellen, daß bei der Verarbeitung auf der eingesetzten Datenverarbeitungsanlage eine verbindlich vorgeschriebene Verarbeitungslogik eingehalten wird. Dazu ist es unter anderem erforderlich, Verfahren bereitzustellen, die gewährleisten, daß Programme ausschließlich in der freigegebenen Fassung zum Ablauf kommen. Systemprogramme und Anwendungsprogramme könnten dazu mit einem geeigneten kryptografischen Verfahren versiegelt werden, wodurch Manipulationen erkennbar würden.

Für persönliche Computer und sonstige kleinere Datenverarbeitungsanlagen sollten zur Datensicherheit Systemprogramme und systemnahe Programme mit einem an der Ausstattung großer Anlagen orientierten Leistungsumfang zur Verfügung gestellt werden. Wesentliche der Datensicherheit dienende Komponenten sollten in das Betriebssystem integriert werden, um Manipulationen und Umgehungsmöglichkeiten zu erschweren.

Stichwortverzeichnis