Der Landesbeauftragte für den Datenschutz Nordrhein-Westfalen

12. Tätigkeitsbericht

NRW.

Zwölfter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Nordrhein-Westfalen

für die Zeit vom 1. Januar 1993
bis zum 31. Dezember 1994

Herausgeber: Der Landesbeauftragte
für den Datenschutz Nordrhein-Westfalen
Reichsstraße 43, 40217 Düsseldorf
ISSN 0179-2431
Druck: Neusser Druckerei und Verlag GmbH

Gedruckt auf chlorfrei gebleichtem Papier

Gliederung

Anlagen

1. Vorbemerkung

Zeichen grundlegenden Wandels finden wir derzeit überall - auch im Datenschutz. Das gilt für die technisch-organisatorischen Veränderungen ebenso wie für die Rechtsentwicklung, nicht zuletzt auch für den Stellenwert des Datenschutzes in der Gesellschaft.

Als vor 16 Jahren das Recht auf den Schutz der personenbezogenen Daten in die Verfassung des Landes Nordrhein-Westfalen aufgenommen wurde und das erste Datenschutzgesetz dieses Landes in Kraft trat, waren es die großen Datenverarbeitungszentralen, welche die Besorgnis auslösten, daß mit einer Speicherung unüberschaubarer Datenmengen und den Möglichkeiten ihrer schnellen Verknüpfung und Abrufbarkeit der „gläserne Bürger" geschaffen würde. Die Entwicklung verlief dann aber in ganz andere Richtungen. Automatisierte Datenverarbeitung (ADV) ist heute alltäglich geworden nicht nur in der gewerblichen Wirtschaft und in der öffentlichen Verwaltung, sondern auch im privaten Bereich. Sie begegnet uns in Gestalt von Arbeitsplatzrechnern, tragbaren Laptops, prozessorgestützten Chipkarten, Mobiltelefonen und anderen Geräten. Die Informations- und Kommunikationstechnik ermöglicht in immer weitergehenden Varianten die Vernetzung, Verbreitung und Darstellung von Daten mit hoher Geschwindigkeit über beliebige Entfernungen. Dafür hat sich bereits der Begriff Datenautobahnen eingebürgert.

Die ADV ist uns nicht mehr fremd und unheimlich. Sie erscheint uns als beherrschbare und zukunftsorientierte Technologie. Ihre Gefahren sind nicht unmittelbar wahrnehmbar. Allerdings haben in jüngster Zeit die Erörterung und Erprobung von Datenverarbeitungstechniken via Weltraumsatellit zur Überwachung landwirtschaftlicher Betriebe (vgl. unten S.115/116) und zur Erhebung von Mautgebühren der Autofahrer (vgl. unten S.117 bis 119) die Datenschutzdiskussion wieder belebt. Hier ist offensichtlich, welch immense und tiefgreifende Eingriffe in das Persönlichkeitsrecht in Betracht kommen. Mindestens ebenso viel Aufmerksamkeit muß aber beispielsweise der zunehmend propagierten multifunktionalen Chipkarte zugewendet werden. Sie kann eine Fülle von personenbezogenen Daten enthalten, deren Inhalt, Umfang und Weiterverarbeitungsmöglichkeiten durch Dritte der Betroffene nicht zuverlässig übersehen und bestimmen kann. Wichtig erscheint mir ebenso, neben den Chancen auch die Risiken der modernen Gentechnologie in Bezug auf die informationelle Selbstbestimmung zu erkennen und daraus Folgerungen zu ziehen (vgl. unten S.16 bis 18).

Das Bundesverfassungsgericht hat in dem sog. Volkszählungsurteil (BVerfGE 65, 1), das vor nunmehr elf Jahren ergangen ist, für besondere Rechtsgebiete, in denen die allgemeinen Datenschutzgesetze nicht ausreichen, bereichspezifische Regelungen gefordert. Nach wie vor bestehen hier noch erhebliche Lücken, namentlich im Justizbereich. Es sind jedoch in den vergangenen zwei Jahren sowohl auf Bundesebene als auch in der Gesetzgebung des Landes Nordrhein-Westfalen zahlreiche Rechtsvorschriften erlassen worden, die spezielle Gebiete nunmehr datenschutzrechtlich regeln.

Der Intention des Bundesverfassungsgerichts, mit den bereichspezifischen Regelungen Rechtssicherheit zu schaffen und Freiräume für die Betroffenen zu wahren, wurde dabei leider vielfach nicht gefolgt. Besonders im Ausländerwesen, in der Verbrechensbekämpfung und im Sozialleistungsbereich wurden Vorschriften erlassen, die darauf ausgerichtet sind, das informationelle Selbstbestimmungsrecht der Betroffenen, auch zahlreicher unbeteiligter Dritter, zugunsten erweiterter Überwachungsbefugnisse des Staates ganz erheblich einzuschränken.

Die Öffnung der Grenzen, der Zustrom vieler Menschen in unser Land, neue Formen der Kriminalität, die Sorge um den Arbeitsplatz und die Finanznot der öffentlichen Hände stehen heute thematisch im Vordergrund und lassen die Sicherstellung von Menschen- und Freiheitsrechten im Gemeinschaftsleben als nachrangige Frage erscheinen. Daraus erklärt sich auch, daß aus dem politischen, dem administrativen und dem journalistischen Raum wiederholt Aufforderungen zur Verminderung des Datenschutzes laut werden. Besonders bedauerlich ist in diesem Zusammenhang, daß die Bemühungen um die Aufnahme einer speziellen Grundrechtsnorm über den Datenschutz in das Grundgesetz im parlamentarischen Raum vorerst gescheitert sind. Es bedarf in der Gegenwart wieder verstärkt des eindringlichen Hinweises, daß die Wahrung des informationellen Selbstbestimmungsrechtes Grundvoraussetzung eines demokratischen und geistig-schöpferischen Zusammenlebens in der staatlichen Gemeinschaft ist.

Das Bauwerk Datenschutz ist in Deutschland relativ komfortabel ausgestaltet. Es hat aber immer noch empfindliche undichte Stellen. In den letzten beiden Jahren wurde das Bauwerk beachtlich weiterentwickelt, teilweise muß diese Entwicklung aber leider als Rückbau bezeichnet werden. Der Landesbeauftragte für den Datenschutz hat daher heute nicht nur die Aufgabe, auf die Einhaltung der Datenschutzregelungen zu achten und Verbesserungsvorschläge zu machen, es geht auch um die Erhaltung der Substanz. Hierzu ist es notwendig, daß er sowohl bei rechtlichen als auch bei technisch-organisatorischen Vorhaben, die datenschutzrelevant sind, frühzeitig informiert und gehört wird.

Der nachfolgende Bericht gibt nach einer allgemeinen Darstellung meiner Tätigkeitsschwerpunkte einen Überblick über Entwicklungen auf dem Gebiet der Gesetzgebung des Bundes und des Landes Nordrhein-Westfalen. Sodann wird über Fragen des grenzüberschreitenden Datenschutzes informiert. Schließlich enthält der Bericht wieder für die einzelnen Fachbereiche und den technisch-organisatorischen Bereich die Beschreibung und Bewertung von Einzelfragen, an denen sich die Vielfalt der Datenschutzproblematik zeigt.

Den Mitarbeiterinnen und Mitarbeitern meiner Dienststelle danke ich für die engagierte, kompetente, zuverlässige Zusammenarbeit und die sachkundigen Beiträge zur Gestaltung dieses Berichts.

2. Allgemeines

2.1 Beratung und Kontrolle

Grundlage meiner Beratungs- und Kontrolltätigkeit bildeten wie in den früheren Jahren vor allem die **Eingaben** der Bürgerinnen und Bürger und die **Beratungsersuchen** der öffentlichen Stellen. Dabei ergab sich wieder eine breite thematische Streuung. Neben den Schwerpunktbereichen Meldewesen, Polizei, Justiz, Sozialwesen und Schule beschäftigten mich eine Reihe von Datenschutzproblemen im Zusammenhang mit der Durchführung von Wahlen. Dabei ist zu berücksichtigen, daß in Nordrhein-Westfalen im Jahre 1994 drei allgemeine Wahlen stattgefunden haben und eine vierte, die Landtagswahl, im Mai 1995 bevorsteht. Zugenommen haben in letzter Zeit die Eingaben aus den Bereichen Steuern und andere Abgaben sowie aus dem Personalwesen.

Die Hinweise der Bürgerinnen und Bürger und die Anfragen der öffentlichen Stellen lassen wegen ihres Praxisbezugs am deutlichsten erkennen, wo Regelungsdefizite vorhanden sind oder Mängel im Vollzug auftreten. Darüber hinaus habe ich aber auch von Amts wegen Überprüfungen vorgenommen. Hierzu habe ich u. a. **Kontroll- und Informationsbesuche** durchgeführt in zwei Ministerien, einer Landwirtschaftskammer, dem Landesversicherungsamt Nordrhein-Westfalen, der Kammerleitstelle für Gewerbesteuermeßbeträge, einer Allgemeinen Ortskrankenkasse, mehreren Polizeibehörden, einer Justizvollzugsanstalt, einem Versorgungsamt, Schulämtern, einem Staatlichen Gewerbeaufsichtsamt, einem Kommunalen Rechenzentrum, mehreren Sparkassen und einer Vielzahl unterschiedlicher kommunaler Ämter und Einrichtungen. Die Gespräche anläßlich dieser Besuche sind durchweg aufgeschlossen und mit Verständnisbereitschaft geführt worden. Nach den Kontrollbesuchen habe ich den betroffenen Stellen detaillierte Prüfungsberichte zur Stellungnahme zugesandt.

Erheblichen Umfang nahm auch meine Beratungstätigkeit bei der Vorbereitung von datenschutzbezogenen Rechts- und Verwaltungsvorschriften und von größeren Datenverarbeitungsvorhaben ein. Besonders gilt dies für den Bereich der **Gesetzgebung** in Bund und Land. Hierzu habe ich eine Reihe von Vorlagen an den Landtag gerichtet und Stellungnahmen gegenüber den fachlich zuständigen obersten Landesbehörden abgegeben. Näheres ist im 3. Abschnitt dieses Tätigkeitsberichts dargestellt.

Im Berichtszeitraum hatte ich auch gegenüber dem Bundesverfassungsgericht zu einer **Verfassungsbeschwerde** Stellung zu nehmen. Abzuwägen war hier das informationelle Selbstbestimmungsrecht des im Grundbuch Eingetragenen gegenüber dem Recht eines Pressevertreters auf Grundbucheinsicht. Das Verfahren wurde im Berichtszeitraum nicht abgeschlossen.

Besondere Fragestellungen ergaben sich im Zusammenhang mit der **Privatisierung** öffentlicher Aufgaben. Die Folgerungen, die aus den damit verbun-

denen Organisationsveränderungen für den Datenschutz zu ziehen sind, werden mich in Zukunft vermehrt beschäftigen.

Insgesamt hat sich die Beachtung des Datenschutzes in der behördlichen Praxis weiter verfestigt, von allfälligen Ausnahmen abgesehen. Bei festgestellten Datenschutzverstößen haben die beteiligten öffentlichen Stellen in aller Regel meine **Empfehlungen** angenommen und zumindest eine Behebung der Mängel in der Zukunft in Aussicht gestellt, so daß ich meist von **Beanstandungen** absehen konnte. Gleichwohl war es notwendig, im Berichtszeitraum insgesamt 28 förmliche Beanstandungen auszusprechen. Zwölf dieser Beanstandungen betrafen die Preisgabe von personenbezogenen Daten aus dem Bereich der Justiz an Dritte zu Forschungszwecken. Hier bestand eine grundsätzliche Meinungsverschiedenheit zwischen dem Justizministerium des Landes Nordrhein-Westfalen und mir über die anzuwendenden Rechtsgrundlagen und zur Auslegung des § 28 DSG NW. Es ist zu hoffen, daß durch die kürzlich erfolgte Novellierung des § 28 DSG NW eine datenschutzkonforme Praxis einvernehmlich erzielt werden kann. Einzelheiten hierzu sind unten (S.22/23) dargestellt.

Die übrigen 16 Beanstandungen betrafen folgende Fälle:

- übermäßige Datenerhebung für eine Entscheidung über Haupt- und Nebenwohnung,
- Fortschreibung des Melderegisters im Widerspruch zu gerichtlichen Entscheidungen,
- fehlende Dokumentation über einfache Melderegisterauskünfte,
- unzulässige Datenübermittlung durch gemeindliche Vollstreckungsbeamte an Dritte,
- Verweigerung der Einsicht in Unterlagen des Justizministeriums im Zusammenhang mit einer Petition,
- Dauer der Speicherung von Daten Unschuldiger im Bereich der Staatsanwaltschaft,
- unzulässige Auskünfte an die Presse durch ein Gericht,
- automatisierter Datenabgleich zwischen Sozialamt und Straßenverkehrsamt,
- Abgleich der Sozialhilfeempfänger-Dateien der kreisangehörigen Gemeinden mit der Kraftfahrzeughalter-Datei des Kreises,
- Übermittlung der Namen und Anschriften sämtlicher Blindengeldempfänger an ein privates Forschungsinstitut,
- Übersendung eines Arztbriefes mit Operationsberichten an sämtliche vorbehandelnden Ärzte,

- Weiterleitung von Amtsarztgutachten durch den Personaldezernenten einer Bezirksregierung an den Medizinaldezernenten,
- unzulässige Datenerhebung in einem Bewerbungsfragebogen,
- unzulässige Verwendung von auf Arbeitszeitkarten festgehaltenen Daten über Fehlzeiten für dienstliche Beurteilungen im Justizvollzugsbereich,
- Dokumentation der erteilten Halterauskünfte an Personen und Stellen außerhalb des öffentlichen Bereichs (durch die Kfz-Zulassungsstelle),
- Erstellung einer Liste mit Namen, Anschriften und Telefonnummern der Lehrerinnen und Lehrer einer Hauptschule zur Verteilung an alle Mitglieder des Kollegiums.

Datenschutz ist nicht nur Sache der jeweils handelnden öffentlichen Stellen. Auch die **Aufsichtsbehörden** haben darüber zu wachen, daß die datenschutzrechtlichen Vorschriften eingehalten werden. Deswegen werden im Falle von Beanstandungen bei Kommunen, im Hochschulbereich oder bei sonstigen Körperschaften, Anstalten oder Stiftungen des öffentlichen Rechts die zuständigen Aufsichtsbehörden unterrichtet (§ 24 Abs. 1 Satz 2 DSG NW). Ich hatte leider in einigen Fällen Veranlassung, die Aufsichtsbehörde darauf hinzuweisen, daß sie eine solche Unterrichtung nicht einfach nur zu den Akten zu nehmen hat, sondern der Angelegenheit nachzugehen gehalten ist und mich im Rahmen der vorgeschriebenen Zusammenarbeit von sich aus über das Ergebnis unterrichten sollte.

2.2 Öffentlichkeitsarbeit

Zur Durchsetzung des Datenschutzes gehört Aufklärung. Datenschutzverletzungen kann so vorbeugend begegnet werden. Deswegen habe ich im Berichtszeitraum auf eine gezielte Öffentlichkeitsarbeit wieder besonders Gewicht gelegt, soweit dies angesichts der Vielschichtigkeit und Schwierigkeit der Materie mit den begrenzten Möglichkeiten meiner Dienststelle umsetzbar war.

Die von mir bereits seit einer Reihe von Jahren herausgegebenen Organisationshilfen zur Datensicherung in unterschiedlichen Bereichen (z. B. Zentralisierte ADV, PC, Netze, Unterlagenvernichtung) sollen die öffentlichen Stellen beim Untersuchen und Gestalten der Datensicherheit unterstützen. Sie geben ausführliche Hinweise, welche Sachverhalte regelungsbedürftig sind, und bieten Anregungen für die Art der Regelung. Die große Zahl der Anforderungen, die mich laufend erreichten, bestätigte mir, daß die Organisationshilfen als für die Praxis hilfreiche Werkzeuge angenommen worden sind. Häufig wurde auch der Wunsch geäußert, über eine Zusammenstellung aller Organisationshilfen zu verfügen. Um diesem Wunsch zu entsprechen, habe ich alle bisher erschienenen Organisationshilfen in einem „Sammelheft Organisationshilfen" zusammengefaßt.

Ähnlich bewährt hat sich die Herausgabe eines „Leitfadens Datenschutz - Einwohnermeldebereich -", der allen mit dem Einwohnerwesen befaßten öffentlichen Stellen in Nordrhein-Westfalen eine praktische Arbeitshilfe im Interesse des Datenschutzes bietet. Durch systematische Gliederung und ein ausführliches Stichwortverzeichnis ist das Auffinden der Problemhinweise und Lösungsmöglichkeiten erleichtert.

Eine häufig angeforderte Broschüre ist das im Berichtszeitraum von mir neu herausgebrachte Heft „Datenschutzgesetz", das in handlicher Ausgabe u. a. Gesetzestext und Übersichten über die Organisation des Datenschutzes in Nordrhein-Westfalen und die Datenschutzkontrollinstanzen enthält. Dieses Heft und die vom Bundesbeauftragten für den Datenschutz in Zusammenarbeit mit den Landesbeauftragten im Jahre 1993 herausgebrachte Informationsbroschüre „Der Bürger und seine Daten" erfahren eine starke Nachfrage, und es freut mich über die jeweiligen Anfragenden zu hören, wer sich mit datenschutzrechtlichen Problematiken befaßt. Dies sind zunehmend auch Schülerinnen und Schüler, die sich in Facharbeiten und Referaten mit datenschutzrechtlichen Fragen auseinandersetzen.

Als weitere Möglichkeit der Öffentlichkeitsarbeit wurden in meinem Haus Kolloquien angeboten für bestimmte Personenkreise. Die Veranstaltungen zielten auf die die Teilnehmer speziell interessierenden datenschutzrechtlichen Fragen ab. Bereits die erste Veranstaltung mit Teilnehmern aus dem Kreis der Oberfinanzdirektionen erwies sich als für beide Seiten fruchtbar. Nicht nur der rege Austausch über die speziellen datenschutzrechtlichen Fragen läßt in meinen Augen solche Veranstaltungen als sehr sinnvoll erscheinen. Zwar wurde der Teilnehmerkreis überschaubar gehalten, um die Effektivität des Informationsaustausches nicht zu gefährden. Ich denke aber trotzdem, daß durch die Teilnehmer ein entsprechender „Vervielfältigungseffekt" in der heimischen Behörde erzielt wird, indem dort über das Kolloquium berichtet wird. Eine weitere Veranstaltung dieser Art wurde mit einem Teilnehmerkreis aus dem Bereich der Justiz durchgeführt. Auch hier war das Interesse an der Erörterung datenschutzrechtlicher Fragen groß, und ich wurde schon gebeten, weitere ähnliche Veranstaltungen durchzuführen.

Es erreichten mich auch zahlreiche Anfragen zur Teilnahme an auswärtigen Fortbildungsseminaren, Gesprächsrunden oder Vortragsveranstaltungen. Solchen Wünschen bin ich im Rahmen der personellen Möglichkeiten meiner Dienststelle nachgekommen. Allerdings sind mir hier durch die ständige Arbeitsbelastung meiner Mitarbeiterinnen und Mitarbeiter gewisse Grenzen gesetzt.

Fortgesetzt hat sich auch das Interesse von Fernsehen, Rundfunk und Presse an aktuellen Themen zum Datenschutz. Hierzu haben Vertreter meiner Dienststelle und ich des öfteren in Gesprächen und Interviews Stellung genommen, wodurch ein breiteres Publikum informiert wurde.

Schließlich ist Teil meiner Öffentlichkeitsarbeit auch der vorliegende Tätig - keitsbericht, der außer den Mitgliedern des Landtags und der Landesregie-

rung u. a. auch den öffentlichen Stellen im Lande und der Presse zur Kenntnis gebracht wird.

2.3 Zusammenarbeit im Datenschutz

Die **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** trat im Berichtszeitraum viermal zusammen. In den dabei gefaßten Beschlüssen und Entschließungen äußerte sich die Konferenz u. a. zu folgenden Themen:

- der EG-Richtlinie vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt,
- den regelmäßigen Datenübermittlungen an die öffentlich-rechtlichen Rundfunkanstalten und die Gebühreneinzugszentrale (GEZ),
- der Gewährleistung des Datenschutzes bei der Mobilkommunikation,
- dem Integrierten Verwaltungs- und Kontrollsystem (InVeKoS),
- dem Datenschutz bei der Privatisierung der Deutschen Bundespost Telekom und bei der europaweiten Liberalisierung des Telefonnetzes und anderer Telekommunikationsdienste,
- den kartengestützten Zahlungssystemen im Öffentlichen Nahverkehr,
- der Gefährdung der Vertraulichkeit der Funkkommunikation von Sicherheitsbehörden und Rettungsdiensten,
- den Chipkarten im Gesundheitswesen,
- der Informationsverarbeitung im Strafverfahren,
- dem Abbau des Sozialdatenschutzes,
- dem Gesetzentwurf der Bundesregierung zur Neuordnung des Postwesens und der Telekommunikation,
- dem Ausländerzentralregister,
- der EG-Statistikverordnung,
- den fehlenden bereichspezifischen gesetzlichen Regelungen bei der Justiz,
- Art. 12 Verbrechensbekämpfungsgesetz zur Trennung von Polizei und Nachrichtendiensten,
- Europol,
- dem EG-Richtlinienentwurf zum Datenschutz im ISDN und in Mobilfunknetzen.

Zur Vorbereitung ihrer Sitzungen hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder Arbeitskreise eingerichtet. Die Arbeitskreise Steuerverwaltung und Statistik haben wiederholt unter meinem Vor-

sitz getagt. Der Arbeitskreis Steuerverwaltung befaßte sich mit der Planung einer bundesweiten Automation der Besteuerungsverfahren, der Zulässigkeit einer Verarbeitung von Steuerdaten im Auftrag durch Private sowie mit Eintragungen auf der Lohnsteuerkarte. Schwerpunktmäßig befaßte sich der Arbeitskreis Statistik mit datenschutzrechtlichen Problemen bei Statistikvorhaben im Bereich der Europäischen Union und der Bundesgesetzgebung zum Mikrozensusgesetz und zum Bevölkerungsstatistikgesetz sowie Regelungsdefiziten bei der Sozialhilfe- und der Justizvollzugsstatistik.

Die 15. und 16. **Internationale Konferenz** der Datenschutzbeauftragten tagte im September 1993 in Manchester und im September 1994 in Den Haag. Sie befaßte sich mit der fortschreitenden Notwendigkeit einer Abstimmung der nationalen Datenschutzregelungen mit dem Ziel, gemeinsame Grundsätze für den grenzüberschreitenden Verkehr mit personenbezogenen Daten zu erreichen. Diese Notwendigkeit wird durch die weltweite Entwicklung neuer Informations- und Kommunikationstechniken verstärkt.

Zusätzlich hat sich im Mai 1994 eine Konferenz der **Datenschutzkontrollinstitutionen der Europäischen Union** konstituiert und erste Beratungen aufgenommen. Dabei hat sie gemeinsam interessierende aktuelle Themen, insbesondere die EG-Datenschutzrichtlinie (unten S. 31) behandelt. Sollte diese Richtlinie bald verabschiedet werden, könnte sie die Rolle eines Leitbildes im gesamten internationalen Rahmen übernehmen.

3. Datenschutzgesetzgebung

Das Datenschutzrecht hat sich im Berichtszeitraum in einer Reihe von Spezialgebieten weiter entwickelt. Damit wurde dem Erfordernis nachgekommen, für besondere Rechtsgebiete, in denen die allgemeine Datenschutzgesetzgebung keine normenklaren und vor allem auch dem Verhältnismäßigkeitsgrundsatz entsprechenden Regelungen bietet, bereichspezifische Vorschriften zu schaffen. Leider hat sich dabei teilweise die Tendenz fortgesetzt, das informationelle Selbstbestimmungsrecht des einzelnen zugunsten von vielfältigen Eingriffsbefugnissen der öffentlichen Stellen weiter einzuschränken. In einigen wichtigen Bereichen, vor allem auf dem Gebiet der Justiz, fehlt es bis heute an dringend erforderlichen bereichspezifischen Datenschutzregelungen.

Die nachfolgende Darstellung gibt einen Überblick über wichtige Neuregelungen und noch anstehenden Handlungsbedarf.

3.1 Bundesbereich

3.1.1 Ausländerzentralregistergesetz

Das Ausländerzentralregister ist für die ausländischen Mitbürgerinnen und Mitbürger von besonderer datenschutzrechtlicher Bedeutung, weil es eine umfassende Registrierung ihrer personenbezogenen Daten an einer Stelle mit umfassenden Zugriffsrechten ganz verschiedener öffentlicher Stellen zuläßt. Zum Entwurf dieses Gesetzes habe ich gegenüber dem Innenministerium des Landes Nordrhein-Westfalen Stellung genommen und als nach meiner Auffassung schwerwiegendsten Mangel herausgestellt, daß das Ausländerzentralregister sich nicht auf die Aufgabenstellung eines zentralen Informations- und Kommunikationssystems für die mit der Durchführung ausländer- oder asylrechtlicher Vorschriften betrauten Behörden beschränken, sondern zu einem automatisierten Verbundsystem zwischen Ausländerbehörden, Polizei, Staatsanwaltschaft und Verfassungsschutz ausgebaut werden soll. Diese Ausweitung erscheint mit Rücksicht auf die bisherige Praxis nicht erforderlich und schwächt die datenschutzrechtliche Position der Ausländerinnen und Ausländer in besonderer Weise. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 9./10. März 1994 einen Beschluß zum Ausländerzentralregister gefaßt und ihre Bedenken dargelegt (vgl. Anlage 1, S. 170/171). Zwischenzeitlich ist das Ausländerzentralregistergesetz - weitgehend dem Entwurf entsprechend - in Kraft getreten (Gesetz vom 2. September 1994, BGBl. I S. 2265).

Nunmehr liegt auch der Entwurf einer Verordnung zur Durchführung des Ausländerzentralregistergesetzes vor. Hierzu habe ich gegenüber dem Innenministerium des Landes Nordrhein-Westfalen ebenfalls Stellung genommen.

Dabei habe ich mich auf Grund der mir gesetzten kurzen Frist auf einige wesentliche Punkte beschränkt. So ist m. E. die Regelung, daß der Betroffene

nach Maßgabe des Ausländerzentralregistergesetzes jederzeit Auskunft über die zu seiner Person im Register gespeicherten Daten verlangen kann, lückenhaft. Die Entscheidung über eine Auskunftsverweigerung dürfte in der Regel nur die zuständige Behörde selbst, nicht aber die Registerbehörde treffen können. Weiter sollte in der Verordnung klargestellt werden, daß die Bezeichnung und Anschrift der zuständigen Stelle dem Auskunftsuchenden bekanntgegeben werden.

Herausgestellt werden sollte auch, daß bei einem Datenbestand zu einer Person, der von mehreren zuständigen öffentlichen Stellen angeliefert ist, die Auskunftsverweigerung sich jeweils nur auf den Teil des Datenbestandes bezieht, der von der gefährdeten Stelle angeliefert worden ist.

Das Innenministerium hat meine Stellungnahme dem Bundesministerium des Innern zugesandt und angeregt, meine Vorschläge zu berücksichtigen. Ein Ergebnis liegt bisher noch nicht vor.

3.1.2 Verbrechensbekämpfungsgesetz

Ein unter Datenschutzgesichtspunkten wichtiges Gesetz ist das Verbrechensbekämpfungsgesetz vom 28. Oktober 1994 (BGBl. I S. 3186). Es regelt insbesondere auch im Bereich der Strafprozeßordnung ein beschleunigtes Verfahren und vor allem im Achten Buch der Strafprozeßordnung ein länderübergreifendes staatsanwaltliches Verfahrensregister. Außerdem wird das Gesetz zu Artikel 10 Grundgesetz geändert.

Besonderes Gewicht hat die neue Regelung über bestimmte Formen der Zusammenarbeit zwischen dem Bundesnachrichtendienst und der Polizei, durch welche die bisherige Beschränkung des Bundesnachrichtendienstes auf die Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung sind, aufgegeben worden ist.

Zur Beratung und Entscheidung im Vermittlungsausschuß über das Verbrechensbekämpfungsgesetz am 23.9.1994 habe ich gegenüber dem Justizministerium und dem Innenministerium des Landes Nordrhein-Westfalen Stellung genommen und auf erhebliche datenschutzrechtliche Bedenken hingewiesen. Mit der erwähnten Regelung, die dem Bundesnachrichtendienst neue Befugnisse im Zusammenhang mit der Strafverfolgung einräumt, wird ein entscheidender Schritt in Richtung auf eine nach meiner Auffassung verfassungswidrige Aufhebung des Trennungsgebots getan. Die Strafverfolgung durch die Polizei und die Nachrichtensammlung durch Geheimdienste sind im demokratischen Verfassungsstaat prinzipiell unterschiedliche Aufgaben und müssen es bleiben. Die Risiken für die rechtsstaatliche Transparenz und die gerichtliche Überprüfbarkeit von Strafverfahren sind bei Zulassung der Datenauswertung durch Nachrichtendienste für die Kriminalitätsbekämpfung unübersehbar.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 26./27. September 1994 einen Beschluß zum Verbrechensbekämpfungs-

gesetz gefaßt. Danach müssen geheimdienstliche Informationsmacht und polizeiliche Exekutivbefugnisse strikt getrennt bleiben (vgl. Anlage 2, S.171).

3.1.3 Strafverfahrensänderungsgesetz

Das Gesetz über die Organisierte Kriminalität und das Verbrechensbekämpfungsgesetz haben zwar einige Bereiche des Strafverfahrens neu geregelt. Es fehlt aber immer noch eine umfassende Anpassung des Strafverfahrensrechts an die Anforderungen des Volkszählungsurteils, das vor nunmehr elf Jahren ergangen ist. Der vom Bundesrat am 14.10.1994 beschlossene Entwurf eines Strafverfahrensänderungsgesetzes 1994 (StVÄG 1994) - Bundesratsdrucksache 620/94 - ist sicherlich auch darauf zurückzuführen, daß es bisher an einer Regelungsinitiative des Bundes fehlt. Aber auch dieser Entwurf enthält gravierende Mängel. Er fällt weit hinter den Standard der allgemeinen Datenschutzgesetze und sogar der Polizeigesetze der Länder zurück.

Nach dem Entwurf müssen Verdächtige ebenso wie Verbrechensopfer und Tatzeugen damit rechnen, daß Daten über ihre Person aus Strafakten nicht nur an andere Rechtspflegeorgane, sondern an beliebig viele andere Behörden weitergegeben werden. Auch private Personen und Unternehmen, etwa Versicherungen, legitimiert ein nicht näher definiertes „berechtigtes Interesse" zur Auskunft aus oder zur Einsicht in Strafakten. Der Entwurf mißachtet die besondere Schutzwürdigkeit des Inhalts von Strafakten; deren Informationen werden teilweise unter Zeugniszwang ermittelt und stammen vielfach aus der Intimsphäre der Betroffenen. Justizdateien werden abweichend vom allgemeinen Datenschutzrecht nicht regelmäßig auf nicht mehr benötigte Angaben hin überprüft; gelöscht wird vielmehr, wenn überhaupt, nur nach dem Zufallsprinzip aus Anlaß einer Einzelfallbearbeitung.

Abschließend bleibt festzuhalten, daß der Entwurf eines Strafverfahrensänderungsgesetzes 1994 den datenschutzrechtlichen Anforderungen nicht hinreichend gerecht wird. Die wiederholt geäußerten schwerwiegenden Datenschutzbedenken lassen sich nur ausräumen, wenn Verarbeitungsbedingungen und Datenflüsse präzise geregelt und strikt auf die Zwecke des Strafverfahrens begrenzt werden. Inzwischen hat die Bundesregierung angekündigt, einen eigenen Entwurf auf den Weg zu bringen.

3.1.4 Bundeskriminalamtgesetz

Zu dem vom Bundesministerium des Innern vorgelegten Entwurf eines Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz - BKAG), Stand: 15.12.1993, habe ich gegenüber dem Innenministerium des Landes Nordrhein-Westfalen Stellung genommen. Es war festzustellen, daß generalklauselartige Eingriffsbefugnisse und allgemein gehaltene Rechtsverordnungsermächtigungen weit davon entfernt waren, den Anforderungen des Bundesverfassungsgerichts an normenklare gesetzliche Grundlagen zu genügen. Darüber hinaus waren Eingriffe in Landesgesetzgebungs-

kompetenzen durch Zentralisierung polizeilicher Datenverarbeitung vorgesehen. Dazu war ein Übergang der Kontrollzuständigkeit für die Datenverarbeitung der Länderpolizeien beim Bundeskriminalamt von den Landesbeauftragten auf den Bundesbeauftragten für den Datenschutz beabsichtigt. Auch das Innenministerium des Landes Nordrhein-Westfalen hat sich weitgehend gegen diesen Entwurf ausgesprochen.

Die Bundesregierung hat nunmehr einen (neuen) Gesetzentwurf vorgelegt, der eingehend zu beraten sein wird.

3.1.5 Justizmitteilungsgesetz

Bereits in meinem 9. Tätigkeitsbericht (S. 21) habe ich das Justizmitteilungsgesetz als vordringliches Gesetzgebungsvorhaben bewertet. Bedauerlicherweise ist auch in der vergangenen Legislaturperiode ein entsprechender Regierungsentwurf durch den Deutschen Bundestag nicht verabschiedet worden. Es ist beabsichtigt, den Entwurf in überarbeiteter Fassung, d. h. vor allem unter Berücksichtigung der kritischen Stellungnahme des Bundesrates (Beschluß vom 15.5.1992 - Bundesratsdrucksache 206/92 -), erneut einzubringen.

Obwohl die Justizministerkonferenz sich mit diesem Thema wegen der besonderen Bedeutung der Materie mehrfach beschäftigt hat, hat es keine Fortschritte in der Sache gegeben. So hat sogar der nordrhein-westfälische Justizminister in einem Aufsatz „Die unendliche Geschichte des Justizmitteilungsgesetzes" (DVBl. 1993, 1229 bis 1234) die Thematik kritisch aufgegriffen. Eigene Maßnahmen, wie etwa eine Bundesratsinitiative, hat allerdings die Landesregierung auch nicht ergriffen.

3.1.6 Insolvenzordnung

Durch die Insolvenzordnung vom 5. Oktober 1994 (BGBl. I S. 2866) sind im wesentlichen das bisherige Konkurs- und Vergleichsrecht sowie die in den neuen Ländern fortgeltende Gesamtvollstreckungsordnung abgelöst worden. Das neue Gesetz enthält, wie ich bereits im Laufe der Beratungen des Gesetzentwurfs in einer Stellungnahme dargelegt habe, datenschutzrechtliche Mängel, die nach meiner Ansicht bei der künftigen Anwendung des Gesetzes Schwierigkeiten mit sich bringen werden.

So ist die Regelung über die Auskunftspflicht im Eröffnungsverfahren nicht normenklar. Es handelt sich um eine Generalklausel, die den Umfang der anzugebenden Daten auch nicht annähernd erkennen läßt. Der Umfang der Datenerhebung liegt ansonsten weitgehend im Belieben des Gerichts. Eine Verpflichtung zur Abwägung mit den schutzwürdigen Belangen des Betroffenen ist nicht erkennbar.

Der Schutz von Unterlagen mit personenbezogenen Daten, die nicht zur Insolvenzmasse gehören, ist nicht hinreichend geregelt, so etwa privater Schriftverkehr auf der Festplatte oder auf Disketten eines Personalcomputers.

Die Gefahren, die in diesem Zusammenhang für den Schuldner bestehen, habe ich in meinem 10. Tätigkeitsbericht (S. 57/58) dargestellt.

3.1.7 Schuldnerverzeichnis

Mit dem Gesetz zur Änderung von Vorschriften über das Schuldnerverzeichnis vom 15. Juli 1994 (BGBl. I S. 1566) sind in die Zivilprozeßordnung (§§ 915 bis 915 h ZPO) endlich Vorschriften aufgenommen worden, die die Verarbeitung personenbezogener Daten im Zusammenhang mit Eintragungen in das Schuldnerverzeichnis transparenter als bisher aufzeigen. Die Möglichkeiten, datenschutzfreundliche Regelungen in Abwägung mit den schutzwürdigen Informationsinteressen zu schaffen, sind nicht ausgeschöpft worden. Eine Wiederholung der Problemfälle aus der Vergangenheit ist deshalb nicht zuverlässig ausgeschlossen.

Es ist nicht gelungen, durch die Rechtsverordnung nach § 915 h ZPO, die Verordnung über das Schuldnerverzeichnis (Schuldnerverzeichnisverordnung - SchuVVO) vom 15. Dezember 1994 (BGBl. I S. 3822), alle Datenschutzdefizite auszugleichen. Zu den Entwürfen dieser Verordnung hatte ich schriftlich und mündlich ausführlich Stellung genommen und konkrete Änderungsvorschläge unterbreitet.

3.1.8 Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms

Das am 1.7.1993 in Kraft getretene Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms - FKPG (BGBl. I S. 944) strebt u. a. eine Entlastung der öffentlichen Haushalte an, indem es die Möglichkeit schafft, durch automatisierte Datenabgleiche der Träger der Sozialhilfe mit den Trägern der Renten-, Unfall- und Arbeitslosenversicherung sowie der Sozialhilfeträger untereinander dem vermuteten Mißbrauch bei der Inanspruchnahme von Sozialleistungen zu begegnen.

Damit wird ein Überprüfungsverfahren legalisiert, das in Abkehr von der bislang gesetzlich normierten Einzelfallprüfung auf Grund konkreter Anhaltspunkte zu einer Art „Rasterfahndung" führt, mit der einer Vielzahl von Empfängern von Leistungen nach dem BSHG und/oder dem AFG von vornherein Mißbrauchsverhalten unterstellt wird.

Der vorgesehene Datenabgleich greift in einer mit dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz nur schwer zu vereinbarenden Weise in das informationelle Selbstbestimmungsrecht der Betroffenen ein. Dies wiederum läßt befürchten, daß es zu einem empfindlichen Verlust des Vertrauens der Betroffenen in die Gewährleistung des Sozialgeheimnisses durch die Sozialleistungsverwaltung kommt.

Im einzelnen gibt das Gesetz den Sozialhilfeträgern folgende Überprüfungsmöglichkeiten an die Hand:

- § 117 Abs. 1 BSHG gestattet dem Träger der Sozialhilfe, regelmäßig im Wege des automatisierten Datenabgleichs zu überprüfen, ob und welche Leistungen von der Bundesanstalt für Arbeit sowie von den Trägern der gesetzlichen Renten- oder Unfallversicherung bezogen werden bzw. ob mit dem Leistungsbezug Zeiten einer Versicherungspflicht oder einer geringfügigen Beschäftigung zusammentreffen.

  Das Nähere über das Verfahren ist einer Regelung durch Rechtsverordnung vorbehalten, bis zu deren Schaffung ein derartiger Abgleich nicht zulässig ist.

- § 117 Abs. 2 BSHG gestattet den automatisierten Datenabgleich der Sozialhilfeträger untereinander, sobald die auch hier erforderliche Rechtsverordnung ergangen ist.

- § 117 Abs. 3 BSHG gestattet den Sozialhilfeträgern, zur Vermeidung rechtswidriger Inanspruchnahme von Sozialleistungen bei anderen Stellen ihrer Verwaltung, z. B. bei der Kfz-Zulassungsstelle, im Einzelfall Daten zu überprüfen.

Mit diesen Regelungen hat sich der Gesetzgeber über die Bedenken der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Stellungnahme vom 15. April 1993 (s. Anlage 3, S. 172 bis 174) hinweggesetzt.

3.1.9 Zweites Gesetz zur Änderung des Sozialgesetzbuchs

Durch das Zweite Gesetz zur Änderung des Sozialgesetzbuchs - 2. SGBÄndG vom 13. Juni 1994 (BGBl. I S. 1229) haben die Vorschriften über den Schutz der Sozialdaten eine Reihe von begrifflichen, aber auch inhaltlich bedeutsamen Änderungen erfahren. Dabei übernimmt das Gesetz für die Fachbegriffe weitestgehend die Legaldefinitionen des Bundesdatenschutzgesetzes. Auf diese Weise wurde ein in sich geschlossener Gesetzestext ohne lästige Verweisungen geschaffen. Leider sind in die Neuregelung auch Vorschriften aufgenommen worden, die die Persönlichkeitsrechte der Betroffenen stärker als bisher einschränken.

- Das Sozialgeheimnis umfaßt nicht nur - wie bisher - den Schutz der Sozialdaten vor unbefugten Offenbarungen (jetzt: Übermittlungen), sondern auch das Verbot unbefugter Erhebung, Speicherung, Veränderung und Nutzung.

- Der Sozialdatenschutz Verstorbener ist jetzt ausdrücklich geregelt.

- „Übermitteln" im Sinne des Sozialgesetzbuchs ist nunmehr - über den Wortlaut des Bundesdatenschutzgesetzes hinaus - auch das Bekanntgeben nicht gespeicherter Sozialdaten. Damit werden - in Übereinstimmung mit dem früheren Offenbarungsbegriff - auch Daten geschützt, die ausschließlich im Gedächtnis festgehalten sind.

- Die Weitergabe innerhalb der speichernden Stelle wird dem „Nutzen" zugeordnet, obwohl sie ihrem Wesen nach ein Übermittlungsvorgang ist.

- Die Definition der speichernden Stelle bei Leistungsträgern orientiert sich nur, soweit es sich dabei um eine Gebietskörperschaft handelt, an dem im Datenschutzrecht geltenden funktionalen Stellenbegriff. Ansonsten ist der Leistungsträger (z. B. LVA) insgesamt speichernde Stelle.

- Der im allgemeinen Datenschutzrecht wie auch bisher im Sozialgesetzbuch geltende Grundsatz der Datenerhebung beim Betroffenen wird zwar formal beibehalten, aber so vielfältig durchbrochen, daß die Datenerhebung ohne Kenntnis und Mitwirkung des Betroffenen faktisch zur Regel wird. Überdies ist die im Gesetzentwurf zunächst vorgesehene Verpflichtung der erhebenden Stelle, den Betroffenen in geeigneter Form schriftlich auf die Erhebungsmöglichkeiten hinzuweisen, auf Empfehlung des Vermittlungsausschusses entfallen: eine Mißachtung des Transparenzgebots.

- Entgegen einer Forderung der Datenschutzbeauftragten, dem bislang schon großzügigen Datenaustausch innerhalb des Sozialleistungsbereichs durch Zweckbindung engere Grenzen zu ziehen, hat der Gesetzgeber die Zweckbindung bei der Erhebung, Nutzung und Übermittlung von Sozialdaten weiter gelockert mit der Folge, daß zwischen den Sozialleistungsträgern ein beinahe ungehinderter Austausch von Sozialdaten erlaubt ist.

- Die bislang bestehende generelle Zulässigkeit der Datenübermittlung im Wege der Amtshilfe wird beschränkt auf die Übermittlung für Aufgaben der Polizeibehörden, der Staatsanwaltschaften und Gerichte, der Behörden der Gefahrenabwehr, der Justizvollzugsanstalten und zur Durchsetzung von öffentlich-rechtlichen Ansprüchen ab 1 000,-- DM.

- Im Gesetz ist klargestellt, daß eine Übermittlung auch im Rahmen einer zulässigen Zweckänderung erfolgen darf und für die Aufgabenerfüllung der abgebenden wie der empfangenden Stelle zulässig ist.

- Die Krankenkassen sind befugt, einem Arbeitgeber das Bestehen einer Fortsetzungserkrankung - allerdings ohne Diagnosedaten - mitzuteilen.

- Die Übermittlung von Sozialdaten zur Durchführung eines Strafverfahrens ist, soweit erforderlich uneingeschränkt, nicht nur wegen eines Verbrechens, sondern auch „wegen einer sonstigen Straftat von erheblicher Bedeutung" zulässig. Hier ist auf einen Katalog von Straftatbeständen bewußt verzichtet worden, weil für die Erheblichkeit von Straftaten auch andere Kriterien (z. B. Schadenshöhe) ausschlaggebend sind. Bedenklich bleibt, daß es sich im Ergebnis um eine nicht normenklare Regelung handelt.

  Die speichernde Stelle ist verpflichtet, den Betroffenen zu Beginn des Verwaltungsverfahrens in allgemeiner Form schriftlich darauf hinzuweisen, daß er der Übermittlung von Daten, die dem Patientengeheimnis unterliegen, widersprechen kann.

- Die Zweckbindung von Sozialdaten ist zugunsten der Gerichte, Staatsanwaltschaften, Polizeibehörden und Behörden der Gefahrenabwehr gelokkert worden.
- Die Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz besteht mit Ausnahme der Sozialversicherungsträger und ihrer Verbände nicht für öffentliche Stellen der Länder, also z. B. nicht für Gemeinden und Gemeindeverbände, soweit sie Leistungsträger sind (Sozialamt, Jugendamt, Wohngeldstelle). Dies ist ein bedauerlicher Rückschritt gegenüber dem bisherigen Recht.

3.1.10 Bundeskrebsregistergesetz

Am 1. Januar 1995 ist das bis zum 31. Dezember 1999 befristete Gesetz über Krebsregister (Krebsregistergesetz - KRG - BGBl. I 1994 S. 3351) in Kraft getreten. Das Gesetz hat zum Ziel, für das gesamte Gebiet der Bundesrepublik Deutschland bevölkerungsbezogene Krebsregister einzurichten und zu führen. Durch ein Netz von epidemiologischen Krebsregistern auf Landesebene nach einheitlichen Vorgaben sollen flächendeckend Daten für die epidemiologische Forschung zur Bekämpfung von Krebserkrankungen gewonnen werden.

Wenn das Gesetz auch nicht - wie das nordrhein-westfälische Gesundheitsdatenschutzgesetz - von der Einwilligungslösung ausgeht, sondern die Widerspruchslösung vorsieht, so sehe ich dennoch das Persönlichkeitsrecht des Krebspatienten hinreichend gewahrt, weil der Patient bei der Unterrichtung über die beabsichtigte oder erfolgte Meldung auf sein Widerspruchsrecht hinzuweisen ist und durch seinen Widerspruch die Meldung verhindern oder (im Wege der Löschung) rückgängig machen kann. Hinzu kommt die den Persönlichkeitsschutz garantierende konsequente Trennung zwischen Vertrauens- und Registerstelle als Kernstück des Gesetzes.

Nennenswerte Auswirkungen dieses Gesetzes auf das in Nordrhein-Westfalen bereits bestehende Krebsregister dürften sich wegen der zahlreichen Öffnungsklauseln, die abweichende Regelungen durch Landesgesetz zulassen, nicht ergeben.

3.1.11 Arbeitsschutzrahmengesetz

Zu einem vom Bundesministerium für Arbeit und Sozialordnung vorgelegten Referentenentwurf eines Gesetzes über Sicherheit und Gesundheitsschutz bei der Arbeit (Arbeitsschutzrahmengesetz - ASRG) habe ich mich gegenüber der Landesregierung geäußert. Das Gesetz soll der Umsetzung aktueller EG-Richtlinien zur Durchführung von Maßnahmen zur Verbesserung der Sicherheit und des Gesundheitsschutzes bei der Arbeit dienen und zahlreiche Vorschriften u. a. der Gewerbeordnung, des Ersten Buches des Sozialgesetzbuchs, der Reichsversicherungsordnung, des Arbeitnehmerüberlassungsgesetzes, des Bundesberggesetzes, des Gesetzes über Betriebsärzte,

Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit sowie der Arbeitsstättenverordnung ändern bzw. ersetzen.

Zu Kernpunkten des Gesetzentwurfs habe ich Anregungen gegeben und insbesondere im Anschluß an meine Ausführungen zur Frage „Genomanalyse und informationelle Selbstbestimmung" in meinem 10. Tätigkeitsbericht (S. 89, 173 bis 176) schwerwiegende datenschutzrechtliche Bedenken geäußert:

Die im Gesetzentwurf vorgesehenen genomanalytischen Untersuchungen haben gegenüber sonstigen Vorsorgeuntersuchungen deshalb eine besondere Qualität, weil das genetische Merkmal vererblich ist, die Gefahr einer sozialen Selektion („erbschwache" und „erbstarke" Arbeitnehmer) besteht und ein gesichertes wissenschaftliches Fundament für derartige Untersuchungen ausweislich der Gesetzesbegründung nicht erkennbar ist.

Die mit genomanalytischen Untersuchungen verbundenen Datenerhebungen müssen allein deshalb als unverhältnismäßige Beeinträchtigung des Persönlichkeitsrechts der Betroffenen angesehen werden, weil diese hierbei als Versuchspersonen in die Durchführung wissenschaftlich nicht abgesicherter Untersuchungen eingebunden werden können, ohne hierüber definitiv unterrichtet zu sein, geschweige denn, solchen Untersuchungen zugestimmt zu haben.

Unabhängig hiervon können genomanalytische Untersuchungen nach meiner Auffassung nur in Erwägung gezogen werden, wenn sie zum Schutz von Beschäftigten unabdingbar geboten sind. Zunächst müssen die objektiven Arbeitsbedingungen so gestaltet werden, daß gesundheitlich oder infolge genetischer Veranlagung gefährdete Arbeitnehmer nicht erkranken (Vorrang des objektiven Arbeitsschutzes). Erst wenn nach vollständiger Ausschöpfung dieser Möglichkeiten nur mit Hilfe gesetzlich festzulegender genomanalytischer Untersuchungen eine erbliche Veranlagung festgestellt werden kann, die bei gegenwärtig nicht zu beseitigenden Gesundheitsgefahren am Arbeitsplatz die Gefahr einer schweren bleibenden Schädigung von Arbeitnehmern mit sich bringt, können aus meiner Sicht derartige Untersuchungen zu Zwekken der arbeitsmedizinischen Vorsorge in Betracht kommen.

Es bedarf daher für alle Untersuchungen (d. h. nicht nur Erst-, sondern auch Folgeuntersuchungen) und die hierbei angewandten genomanalytischen Untersuchungsmethoden einer ausdrücklichen gesetzlichen Zulassung. Tarifvertragliche Regelungen, Dienst- oder Betriebsvereinbarungen reichen als Grundlage derartiger Untersuchungen nicht aus. Die gesetzliche Regelung kann allenfalls durch Rechtsverordnungen ausgefüllt werden, in denen neben den Tätigkeiten, bei denen im Falle bestimmter Erbmerkmale schwere Schädigungen zu erwarten sind, auf jeden Fall die wissenschaftlich abgesicherten Untersuchungsverfahren zu bestimmen sind.

Daneben bedarf es der umfassenden Aufklärung der Beschäftigten, die sich auf die mit der Arbeit verbundenen Gefährdungen, die Untersuchungen, die

möglichen Erkenntnisse und deren Verwendung sowie auf die Freiwilligkeit der Untersuchungen erstrecken muß. Wegen der Tragweite des Eingriffs in das Persönlichkeitsrecht muß sichergestellt sein, daß die Einwilligung auch noch nach Vorliegen des Untersuchungsergebnisses gegeben ist.

Ferner habe ich sowohl präzisierende als auch einschränkende Regelungen zu etwaigen genomanalytischen Untersuchungen bei Erst- und Folgeuntersuchungen sowie zur Sicherung der Entscheidungsfreiheit der Beschäftigten und außerdem die gesetzliche Verankerung eines Benachteiligungsverbots im Falle einer verweigerten Einwilligung in derartige Untersuchungen gefordert.

3.1.12 Mikrozensusgesetz

In der vergangenen Legislaturperiode des Deutschen Bundestages hat der Interministerielle Ausschuß für Koordinierung und Rationalisierung der Statistik einen Arbeitsentwurf zur Novellierung des Mikrozensusgesetzes erstellt, worüber mich der Bundesbeauftragte für den Datenschutz unterrichtet hat. Im Hinblick auf die in diesem Arbeitsentwurf enthaltenen deutlichen Tendenzen zu einem datenschutzrechtlichen Rückschritt habe ich dem Innenministerium des Landes Nordrhein-Westfalen meine Bedenken im einzelnen dargelegt.

Der Arbeitsentwurf sieht hinsichtlich einiger Erhebungsmerkmale für den ab 1996 vorgesehenen Mikrozensus eine weitgehende Einführung bzw. Wiedereinführung der Auskunftspflicht vor. Während lediglich bei den Fragen nach der Gesundheit/Behinderteneigenschaft auch weiterhin auf die Auskunft verzichtet werden soll, ist bei allen anderen, nach dem Mikrozensusgesetz 1991 freiwillig zu beantwortenden Fragen die Verankerung einer Auskunftspflicht beabsichtigt, für die einleuchtende Gründe nicht ersichtlich sind. Es besteht daher besonderer Anlaß, angesichts der beabsichtigten Ausweitung der Auskunftspflicht an die im Volkszählungsurteil des Bundesverfassungsgerichts enthaltene Aufforderung an den Gesetzgeber zu erinnern, wonach dieser sich vor künftigen Entscheidungen für eine Erhebung im Hinblick auf die sich stetig weiterentwickelnden Methoden der amtlichen Statistik und der Sozialforschung erneut mit dem dann erreichten Stand der Methodendiskussion auseinanderzusetzen hat, um festzustellen, ob und in welchem Umfang die herkömmlichen Methoden der Informationserhebung und -verarbeitung beibehalten werden können (BVerfGE 65, 1, 55).

In diesem Zusammenhang halte ich es auch für bedenklich, daß künftig die Erhebung einer Vielzahl von Erhebungsmerkmalen und Fragen häufiger und bei mehr Bürgern erfolgen soll, wodurch diese einer zusätzlichen Belastung ausgesetzt werden. Nach den im Volkszählungsurteil aufgestellten Maßstäben wäre es angezeigt, vor derartigen Überlegungen zunächst die Gründe für den Mehrbedarf an Informationen über die Bürger nachvollziehbar darzulegen.

3.1.13 Bevölkerungsstatistikgesetz

Nachdem mir bekanntgeworden war, daß die Novellierung des im Kern aus dem Jahre 1957 stammenden Bevölkerungsstatistikgesetzes in der vergangenen Legislaturperiode des Deutschen Bundestages nicht mehr weiter verfolgt werden sollte, habe ich mich gegenüber der Landesregierung für einen Fortgang der Beratungen dieses Gesetzes, das in seiner gegenwärtigen Fassung in mehrfacher Hinsicht erheblichen verfassungsrechtlichen Bedenken begegnet, eingesetzt. Meine Bedenken richten sich insbesondere dagegen, daß die geltende gesetzliche Regelung mehrere in ihrer Erforderlichkeit zweifelhafte Erhebungsmerkmale vorsieht, die bisherige Auskunftspflicht und die Art der Datenerhebung nicht verfassungskonform ist sowie die verfassungsrechtlich nicht länger hinnehmbaren Regelungen im Bevölkerungsstatistikgesetz darüber hinaus wegen Ablaufs des zugebilligten Übergangsbonus Eingriffe in das Recht auf informationelle Selbstbestimmung nicht mehr zulassen dürften.

- Zweifel an der Erforderlichkeit bestehen z. B. hinsichtlich der Erhebungsmerkmale: Totgeburten, rechtskräftige Urteile in Ehesachen, rechtliche Zugehörigkeit oder Nichtzugehörigkeit zu einer Kirche, Religionsgesellschaft oder Weltanschauungsgemeinschaft. Zudem dringen einzelne Fragen (wie etwa diejenigen nach ehelicher, nichtehelicher Geburt und nach der Zahl der lebend- oder totgeborenen Kinder) tief in den von der Verfassung geschützten, auch für die amtliche Statistik unzugänglichen Intimbereich der Person ein.

- Die im Bevölkerungsstatistikgesetz geregelte Auskunftspflicht sowie die Art der Datenerhebung können auch deshalb kaum noch als verfassungskonform angesehen werden, weil sowohl die (überwiegend) sekundärstatistischen als auch die primärstatistischen Datenerhebungen in Teilen keine klare Trennung von Statistik und Verwaltungsvollzug aufweisen. Sekundärstatistische Datenerhebungen müssen ihre Grenzen am Bestand der Verwaltungsdaten finden. Für das Verwaltungshandeln selbst nicht benötigte Daten dürfen von der Verwaltung für Zwecke der Bevölkerungsstatistik nicht beim Betroffenen und erst recht nicht mit Auskunftspflicht erhoben werden. Gravierend fällt bei der im Bevölkerungsstatistikgesetz nicht vorhandenen Trennung zwischen Statistik und Verwaltungsvollzug ins Gewicht, daß das Gesetz selbst die Erhebungsmerkmale nicht getrennt von den Hilfsmerkmalen ausweist.

- Die Durchführung der Bevölkerungsstatistik kann mehr als elf Jahre nach Verkündung des Volkszählungsurteils weder auf das damit unvereinbare Bevölkerungsstatistikgesetz von 1957 noch etwa auf einen sog. Übergangsbonus gestützt werden. Nach der Rechtsprechung des Bundesverfassungsgerichts steht dem Gesetzgeber als Übergangsbonus nur ein begrenzter Zeitraum zur Verfügung, um die bereichspezifischen Statistikgesetze verfassungskonform zu novellieren. Wenngleich die Feststellung, wann die Übergangszeit für den Gesetzgeber zur Erfüllung des Verfas-

sungsauftrags zum Schutz des informationellen Selbstbestimmungsrechts beendet ist, wegen verschiedener zu beachtender Faktoren nicht schematisch getroffen werden kann, so muß hier die dem Gesetzgeber zuzubilligende zeitliche Toleranzgrenze im Hinblick auf die schwerwiegenden verfassungsrechtlichen Mängel des geltenden Gesetzes, durch die der legislatorische Handlungsbedarf inzwischen unabweislich geworden ist, als überschritten angesehen werden.

3.1.14 Abgabenordnung

Die notwendige Ergänzung der Abgabenordnung um bereichspezifische Datenschutzvorschriften wird von den Datenschutzbeauftragten des Bundes und der Länder seit geraumer Zeit gefordert. Ihre Umsetzung ist kurz vor dem Ziel gescheitert, obwohl ein beachtlicher, mit etlichen Stellungnahmen und Anregungen der Datenschutzbeauftragten begleiteter Gesetzentwurf zur Änderung der Abgabenordnung vom Bundesministerium der Finanzen erarbeitet worden war. Im Februar 1994 hat das Bundesministerium erklärt, daß nach Verabschiedung des Mißbrauchsbekämpfungs- und Steuerbereinigungsgesetzes, in das eine kleine Auswahl auch datenschutzrelevanter Änderungen der Abgabenordnung aus dem Gesetzentwurf übernommen worden war, z. Z. kein Handlungsbedarf mehr in datenschutzrechtlicher Hinsicht bestünde. Diese Auffassung hätten die für Fragen der Abgabenordnung zuständigen Vertreter der obersten Finanzbehörden der Länder vertreten. Die Absicht des Bundesministeriums der Finanzen, auch in absehbarer Zeit eine Änderung der Abgabenordnung auf dem Gebiet des Datenschutzes nicht vorzuschlagen, besteht nach meinem Erkenntnisstand fort.

In ihrer Stellungnahme zu meinem 11. Tätigkeitsbericht (zu Nr. 5.15.1) hat die Landesregierung ausdrücklich darauf hingewiesen, daß sie sich dagegen ausgesprochen habe, die Überarbeitung anderer datenschutzrechtlicher Bestimmungen der Abgabenordnung, wie sie im Gesetzentwurf zur Änderung der Abgabenordnung 1994 vorgesehen war, nicht weiter zu verfolgen. Ich halte es nach wie vor für dringend geboten, die Abgabenordnung entsprechend den datenschutzrechtlichen Anforderungen, wie sie das Bundesverfassungsgericht an eine gesetzliche Ermächtigung für Eingriffe in das informationelle Selbstbestimmungsrecht gestellt hat, zu überarbeiten. In diesem Zusammenhang sei nur beispielhaft erwähnt, daß mit der Einfügung des § 88 a (Sammlung von geschützten Daten) in die Abgabenordnung immer noch keine normenklare gesetzliche Ermächtigung zur Einrichtung einer bundesweit geführten Fahndungsdatei geschaffen ist, also wie bisher unzulässigerweise Fahndungsdaten an die Informationszentrale für den Steuerfahndungsdienst in Wiesbaden übermittelt und von dort abgefragt werden.

3.1.15 Gewerbeordnung

Mit dem Gesetz zur Änderung der Gewerbeordnung (GewO) und sonstiger gewerberechtlicher Vorschriften vom 23. November 1994 (BGBl. I S. 3475)

sind vorrangig datenschutzrechtlich relevante Vorschriften entsprechend den verfassungsrechtlichen Anforderungen bundeseinheitlich geschaffen.

Bei der Bewertung des Gesetzentwurfs habe ich bereits in meinem 11. Tätigkeitsbericht (S. 117) deutlich gemacht, daß die Zielvorstellung einer datenschutzgerechten Ausgestaltung der gewerberechtlichen Vorschriften im allgemeinen erreicht wird. Allerdings ist in der Frage der Übermittlung personenbezogener Daten aus der Gewerbeanzeige an Stellen außerhalb des öffentlichen Bereichs eine Verschlechterung eingetreten. Während früher die Übermittlung von Namen, betrieblicher Anschrift und angezeigter Tätigkeit bei einem Widerspruch des Betroffenen unterbleiben mußte, ist diese Bestimmungsmöglichkeit entfallen.

Kernvorschrift der neuen Regelung ist die als Generalnorm ausgestaltete Vorschrift des § 11 GewO. Sie regelt die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten in sämtlichen Abschnitten gewerberechtlicher Verfahren. Mit der neu gefaßten Vorschrift des § 14 GewO über die Anzeigepflicht von Gewerbebetrieben wird nunmehr auch die Unterrichtung anderer Behörden und Stellen auf eine ausreichende gesetzliche Grundlage gestellt.

3.1.16 Handwerksordnung

Eine weitere Anpassung des Wirtschaftsrechts an die datenschutzrechtlichen Vorgaben erfolgte für den Bereich der Handwerksorganisationen. Nachdem das Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern einige datenschutzrechtliche Neuerungen erfahren hat, gelten nunmehr im Handwerksrecht mit der Novelle der Handwerksordnung vom 20. Dezember 1993 (BGBl. I S. 2256) bereichspezifische Datenschutzregelungen für den Umgang mit personenbezogenen Wirtschaftsdaten. Die Regelungen zur Erhebung und Übermittlung sollen einen bundeseinheitlichen Datenschutzstandard sicherstellen. Im einzelnen sind Regelungen im Zusammenhang mit der Führung der Handwerksrolle und dem Verzeichnis der Berufsausbildungsverhältnisse sowie beitragsrelevante Vorschriften geschaffen worden. Es bleibt abzuwarten, ob das angestrebte ausgewogene Verhältnis zwischen den praktischen Bedürfnissen der Handwerksorganisation und den berechtigten Belangen der Betroffenen erreicht wird.

3.1.17 Umweltinformationsgesetz

Mit Inkrafttreten des Umweltinformationsgesetzes (UIG) vom 8. Juli 1994 (BGBl. I S. 1490) ist die Richtlinie 90/313/EWG des Rates vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt umgesetzt worden. Der grundsätzliche Informationsanspruch findet seine Beschränkung u. a. in § 8 des Gesetzes. Danach besteht kein Anspruch, wenn durch das Bekanntwerden der Informationen personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt würden. Vor der Entscheidung über die Offenbarung der so geschützten Informatio-

nen sind die Betroffenen anzuhören. Es bleibt abzuwarten, welche Probleme sich bei der Anwendung dieser Vorschrift in der Praxis ergeben.

3.2 Landesbereich

3.2.1 Datenschutzgesetz Nordrhein-Westfalen

Mit dem Gesetz zur Änderung des Datenschutzgesetzes Nordrhein-Westfalen und anderer Gesetze vom 22. November 1994 (GV. NW. S. 1064) wurden im DSG NW die Forschungsklausel in § 28 novelliert und redaktionelle Anpassungen an das zwischenzeitlich neugefaßte Bundesdatenschutzgesetz vorgenommen.

Mit der Novellierung des § 28 DSG NW wird in den Fällen, in denen eine Einwilligung Betroffener zur Verarbeitung ihrer personenbezogenen Daten im Rahmen von Forschungsvorhaben nicht vorliegt, eine Regelung geschaffen, die unter Wahrung datenschutzrechtlicher Belange eine wissenschaftsfreundlichere Handhabung gegenüber der bisherigen Rechtslage ermöglicht. Im 9. Tätigkeitsbericht (S. 17 bis 20) hatte ich auf die Probleme in der Praxis der öffentlichen Stellen bei der Datenverarbeitung für wissenschaftliche Zwekke hingewiesen und auf Fragen der Auslegung und Anwendung des § 28 DSG NW bei einer Datenverarbeitung ohne Einwilligung der Betroffenen aufmerksam gemacht.

Im Berichtszeitraum wurde ich insbesondere durch das Justizministerium des Landes Nordrhein-Westfalen oder dessen nachgeordnetem Bereich vermehrt über geplante oder bereits durchgeführte Forschungsvorhaben und die damit in Verbindung stehende Preisgabe von personenbezogenen Daten aus Justizunterlagen an die Forscher unterrichtet. Wie die Überprüfung dieser Fälle zeigte, hat die Auslegung der Ausnahmeklausel, daß „durch das Einholen der Einwilligung der Forschungszwecke gefährdet würde" (§ 28 Abs. 2 Buchstabe c DSG NW a. F.), zunehmend dazu geführt, daß unter Umgehung des Selbstbestimmungsrechts Betroffener und ihres Rechts, eine Verarbeitung ihrer Daten auch zu verweigern, von vornherein von einer Einholung der Einwilligung generell abgesehen wurde und somit großzügig bei Forschungsvorhaben die Preisgabe personenbezogener Daten aus Justizunterlagen zugelassen wurde ohne überhaupt auch nur den Versuch zu unternehmen, Einwilligungen in die Datenverarbeitung einzuholen.

Im Zuständigkeitsbereich des Justizministeriums mußte ich bei Forschungsvorhaben zwölf förmliche Beanstandungen nach § 24 DSG NW vornehmen. Die Beanstandungen machten das Problem fehlender bereichspezifischer Rechtsgrundlagen insbesondere in der Strafprozeßordnung deutlich. Da mit dem nicht verabschiedeten Strafverfahrensänderungsgesetz 1994 bereichspezifische Regelungen in der Strafprozeßordnung weiter auf sich warten lassen, Regelungen für das Zivil- und andere gerichtliche Verfahren ebenfalls fehlen, war nachdrücklich die Stellungnahme der Landesregierung zum 9. Tätigkeitsbericht (Drucksache 10/5055, S. 19) in Erinnerung zu rufen. In allen Fällen, in denen ich eine Beanstandung ausgesprochen habe, beruft

sich das Justizministerium auf die direkte Anwendbarkeit des § 28 DSG NW. Nach meiner Auffassung können die Regelungen des § 28 DSG NW allenfalls im Zusammenhang mit der Rechtsprechung des Bundesverfassungsgerichts zum sog. „Übergangsbonus" als Mindestmaßstab zur Prüfung der Rechtmäßigkeit eines Forschungsvorhabens herangezogen werden. Unter Geltung des § 28 DSG NW a. F. führte dies aber im Ergebnis zu keiner anderen datenschutzrechtlichen Bewertung.

Die Neufassung des § 28 DSG NW läßt nunmehr eine Verarbeitung personenbezogener Daten ohne Einwilligung für Forschungsvorhaben zu, wenn diese Daten zur Durchführung des Vorhabens erforderlich sind, der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann und das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen erheblich überwiegt. Damit ist nach meiner Bewertung eine handhabbare normenklare Regelung geschaffen worden, die die in den letzten Jahren gewonnenen praktischen Erfahrungen aufgreift und sich an die neuere Datenschutzgesetzgebung in anderen Ländern und an das Bundesdatenschutzgesetz angleicht. Es bleibt abzuwarten, ob für die Übergangszeit bis zur Schaffung bereichspezifischer Regelungen vor allem im Bereich des Justizministeriums bei der Durchführung von Forschungsvorhaben unter Beachtung zumindest der Festlegungen im geänderten § 28 DSG NW eine datenschutzkonforme Praxis Platz greift.

3.2.2 Gemeindeordnung

Mit dem Gesetz zur Änderung der Kommunalverfassung vom 14. Juli 1994 (GV. NW. S. 666) hat der Landesgesetzgeber u. a. eine Neufassung der Gemeindeordnung, eine Neufassung der Kreisordnung, eine Änderung der Landschaftsverbandsordnung und eine Änderung des Gesetzes über den Kommunalverband Ruhrgebiet beschlossen. Der von mir im Rahmen der Beratungen des Gesetzentwurfs aufgezeigte Regelungsbedarf in datenschutzrechtlicher Hinsicht (vgl. hierzu auch 11. Tätigkeitsbericht, S. 29/30) hat bisher zu wenig Berücksichtigung gefunden. Hierzu habe ich auch gegenüber dem Landtag eine eingehende Stellungnahme abgegeben (Vorlage 11/2088).

Einzuräumen ist, daß die Regelungsschwerpunkte des Gesetzes auf anderen Gebieten lagen. Es bedarf jedoch einer kritischen Beobachtung, wie die künftige Handhabung der neuen Gemeindeordnung angesichts der bestehenden Regelungsdefizite auf datenschutzrechtlichem Gebiet erfolgt. Dies müßte ggf. zu gesetzgeberischen Konsequenzen führen.

Zudem ist eine Chance vertan worden, in Nordrhein-Westfalen in kommunalverfassungsrechtlichen Vorschriften Datenschutzrecht zu verankern, das für die anderen Bundesländer als Beispielsregelung hätte dienen können.

3.2.3 Meldegesetz

In meinem 11. Tätigkeitsbericht (S. 18) habe ich auf die Notwendigkeit einer klarstellenden Regelung im Melderechtsrahmengesetz (MRRG) hingewiesen, daß die Übermittlung von Wählerdaten an politische Parteien nicht alle wahlberechtigten Bürgerinnen und Bürger umfassen dürfe, sondern, wie es der Wortlaut der Vorschrift nach meiner Auffassung schon immer verlangte, lediglich einzelne Wählergruppen. Der Bundesgesetzgeber hat zwischenzeitlich durch das Erste Gesetz zur Änderung des Melderechtsrahmengesetzes vom 24. Juni 1994 (BGBl. I S. 1430) § 22 MRRG entsprechend klarstellend geändert.

Das Innenministerium des Landes Nordrhein-Westfalen hat diese Umsetzung in das entsprechende Landesrecht bisher nicht eingeleitet. Vielmehr ist durch Erlaß an die Regierungspräsidenten, Oberstadtdirektoren und Oberkreisdirektoren vom 25.3.1994 - I B 1 /41.521 - darauf verwiesen worden, daß mit der Verabschiedung einer Novelle des Meldegesetzes NW (MG NW) in dieser Legislaturperiode nicht mehr zu rechnen sei. Bezogen auf die Gruppenauskünfte an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen bedeute dies, daß die mit dem Ersten Gesetz zur Änderung des Melderechtsrahmengesetzes getroffenen Beschränkungen auf bestimmte Altersgruppen für die bevorstehenden Wahlen bis dahin keine Anwendung fänden und somit im Rahmen des § 35 Abs. 1 Satz 1 MG NW bis auf weiteres Auskünfte über alle Wahlberechtigten erteilt werden könnten.

Mit einem solchen Erlaß wird die gesetzliche Vorgabe des Bundesgesetzgebers, die Datenschutzbelangen dient, ausdrücklich nicht befolgt. Das ist mit dem Recht auf informationelle Selbstbestimmung nicht zu vereinbaren.

3.2.4 Meldedatenübermittlungsverordnung

In meinem 10. Tätigkeitsbericht (S. 37/38) habe ich auf die Problematik des § 9 a der Verordnung über die Zulassung der regelmäßigen Datenübermittlung von Meldebehörden an andere Behörden oder sonstige öffentliche Stellen (MeldDÜV NW), eingefügt durch Verordnung vom 6. August 1986 (GV. NW. S. 594), hingewiesen. Inzwischen hat auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 26./27. Oktober 1993 zur regelmäßigen Datenübermittlung an die öffentlich-rechtlichen Rundfunkanstalten und die Gebühreneinzugszentrale (GEZ) kritisch Stellung genommen und sich bereit erklärt, an geeigneten und verfassungskonformen Lösungen der Landesregierungen zur Sicherung des Gebührenaufkommens der Rundfunkanstalten mitzuwirken (vgl. Anlage 4, S. 174).

Zu einer solchen Mitwirkung sind die Datenschutzbeauftragten des Bundes und der Länder bisher nicht aufgefordert worden.

Bürgereingaben entnehme ich zudem, daß unabhängig von den offenen Rechtsfragen für die Betroffenen schon viel erreicht wäre, wenn sie durch Nachweis einer Anmeldung bei der GEZ bei der Gemeinde erreichen könnten, daß diese die unnötige Datenübermittlung ihrer Daten unterläßt. Bisher lehnen die Gemeinden dies unter Hinweis auf die stringente Regelung des § 9 a MeldDÜV NW ab.

3.2.5 Katasterdatenübermittlungsverordnung

Das Innenministerium des Landes Nordrhein-Westfalen hatte mich zum Entwurf einer Verordnung über die Zulassung automatisierter Abrufverfahren und regelmäßiger Übermittlung von Daten des Liegenschaftskatasters um Stellungnahme gebeten. In der daraufhin überarbeiteten Fassung sind fast alle meine Anregungen und Bedenken berücksichtigt worden. Insbesondere ist zu begrüßen, daß in § 2 die zum Abruf bereitgehaltenen Datenarten enumerativ aufgezählt sind.

Inzwischen ist die Katasterdatenübermittlungsverordnung vom 17. Oktober 1994 (GV. NW. 1995 S. 51) mit diesem Inhalt in Kraft getreten.

3.2.6 Polizeigesetz

Den Arbeitsgrundlagen für die Polizei, seien es gesetzliche Grundlagen oder Verwaltungsvorschriften, war im Berichtszeitraum besondere Aufmerksamkeit zu widmen. Im Zuge der Diskussion um die Verbesserung der Bekämpfungsmöglichkeiten der Organisierten Kriminalität hatte ich Veranlassung, zu dem letztlich abgelehnten Gesetzentwurf der Fraktion der CDU (Drucksache 11/4682) zur Änderung des Polizeigesetzes Nordrhein-Westfalen gegenüber dem Innenausschuß des Landtags Stellung zu nehmen (Vorlage 11/1854). Der Gesetzentwurf sah eine Ermächtigung zur elektronischen Überwachung der Wohnungen durch die Polizei vor. Zu der grundsätzlichen Problematik habe ich in meinem 11. Tätigkeitsbericht (S. 31) Stellung genommen. Der hierzu gefaßte Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 ist mit dem weiteren Beschluß vom 26./27. September 1994 bekräftigt worden (vgl. Anlage 5, S. 175/176). Es war zusätzlich darauf hinzuweisen, daß für den präventiv polizeilichen Bereich der vorbeugenden Straftatenbekämpfung kaum vorstellbar ist, welche Tatsachen im Vorfeld strafbarer Handlungen die Annahme hinreichend konkret rechtfertigen könnten, daß eine Person eine Straftat von erheblicher Bedeutung begehen wird und weiteres polizeiliches Vorgehen nur durch die Gewinnung von Erkenntnissen aus Abhörmaßnahmen in Wohnungen möglich ist.

3.2.7 Polizei-Datenübermittlungsverordnung

Grenzüberschreitender Datenverkehr im präventiv polizeilichen Bereich war bisher gemäß § 28 des Polizeigesetzes des Landes Nordrhein-Westfalen (PolG NW) auf Einzelfälle der Datenübermittlung in das, nicht nur bildlich

gesehen, vor der Haustür liegende Ausland beschränkt. Um dem für die tägliche, über den Einzelfall hinausgehende Polizeiarbeit festzustellenden Regelungsdefizit zu begegnen, hatte ich daher nach einem Informationsbesuch bei einem Polizeipräsidenten in Grenznähe die Inhalte einer nach § 27 Abs. 2 PolG NW möglichen Rechtsverordnung zum Gegenstand eines Meinungsaustausches mit dem Innenministerium des Landes Nordrhein-Westfalen gemacht.

In die neue Verordnung über die Zulassung der Datenübermittlung von der Polizei an ausländische Polizeibehörden (PolDÜV NW) vom 22. Oktober 1994 (GV. NW. S. 958) sind erfreulicherweise auch meine Anregungen eingeflossen. Allerdings bestehen Zweifel an der Notwendigkeit der Einbeziehung des Landeskriminalamts in den Regelungsbereich der Verordnung (§ 3 PolDÜV NW). Dies wird zu gegebener Zeit zu überprüfen sein.

3.2.8 Verfassungsschutzgesetz

Es ist zu begrüßen, daß nunmehr auch die Datenverarbeitung des Verfassungsschutzes des Landes Nordrhein-Westfalen auf eine neue gesetzliche Grundlage gestellt worden ist (Verfassungsschutzgesetz Nordrhein-Westfalen - VSG NW - vom 20.12.1994, GV. NW. 1995 S. 28).

Meine im 10. Tätigkeitsbericht (S. 74) geäußerte Hoffnung, daß die dem Datenschutz gegenüber aufgeschlossene Haltung und Praxis der Verfassungsschutzbehörde auch Eingang in das (neue) VSG NW finden würde, hat sich zwar leider nicht in dem von mir angestrebten Umfang erfüllt. Es bleibt aber festzustellen, daß mir mehrfach Gelegenheit gegeben wurde, die Datenschutzerfordernisse an ein bürgerfreundliches Verfassungsschutzgesetz im Vorfeld und bei den parlamentarischen Beratungen darzulegen; hierzu beziehe ich mich u. a. auf meine Vorlage 11/1896. Das hat letztlich auch zu einigen wichtigen Verbesserungen in dem inzwischen verabschiedeten Gesetz geführt.

3.2.9 Sicherheitsüberprüfungsgesetz

Die Landesregierung hatte im Berichtszeitraum das Vorhaben, die Sicherheitsüberprüfungen von Bediensteten öffentlicher Stellen und den Sabotageschutz auf eine gesetzliche Grundlage zu stellen, durch Einbringung des Entwurfs eines Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Landes Nordrhein-Westfalen (Drucksache 11/7943) einen entscheidenden Schritt vorangebracht. Über die Notwendigkeit der Schaffung solcher Rechtsgrundlagen bestand Einigkeit (vgl. zuletzt 11. Tätigkeitsbericht, S. 53/54).

In einer Stellungnahme zu dem Gesetzentwurf (Vorlage 11/3501) habe ich dargelegt, daß er in mehrfacher Hinsicht datenschutzrechtliche Regelungsdefizite enthielt. Zudem wich der Entwurf in wesentlichen Punkten von datenschutzrechtlich deutlich positiver zu bewertenden Regelungen des entsprechenden Bundesgesetzes ab. Auch wenn die Sicherheitsüberprüfungen die

Einwilligung der betroffenen Personen voraussetzen, muß dabei bedacht werden, daß für viele Betroffene diese Einwilligung über die Gewinnung eines Arbeitsplatzes oder doch wenigstens über die beruflichen Chancen entscheidet.

Meine Anregungen wurden in der parlamentarischen Beratung in den wesentlichen Punkten aufgegriffen. Das Gesetz ist inzwischen verabschiedet worden.

3.2.10 Gesundheitsdatenschutzgesetz

Am 23. Februar 1994 ist das Gesundheitsdatenschutzgesetz - GDSG NW - (GV. NW. S. 84) in Kraft getreten. Damit ist endlich eine bereichspezifische gesetzliche Grundlage für die Datenverarbeitung im Gesundheitswesen geschaffen. Zu begrüßen ist insbesondere, daß sich die neuen Regelungen auch auf die in privater Trägerschaft geführten Krankenhäuser erstrecken. Im Hinblick darauf, daß die Kirchen und Religionsgemeinschaften für ihre Krankenhäuser den Zielen dieses Gesetzes entsprechende Regelungen treffen (§ 2 Abs. 3), besteht nunmehr im gesamten Krankenhausbereich ein einheitlicher Datenschutzstandard.

An den Beratungen zu diesem Gesetz bin ich frühzeitig und wiederholt von dem zuständigen Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen beteiligt worden. Dabei konnte ich zwar eine Reihe von Verbesserungen erreichen, habe mich aber wegen einzelner noch offener Fragen an den Landtag gewandt (Vorlage 11/2449). Meinen dabei geäußerten Bedenken gegen die mit der informationellen Gewaltenteilung unvereinbare Regelung, wonach die Weitergabe von Patientendaten an mit der Behandlung und den sonstigen Tätigkeiten unmittelbar befaßte Organisationseinheiten innerhalb der Einrichtung nicht als Übermittlung gilt, hat der Landtag durch folgende Ergänzung Rechnung getragen:

„Wenn mehrere Ärzte, Ärztinnen, Zahnärzte und Zahnärztinnen gleichzeitig oder nacheinander denselben Patienten untersuchen oder behandeln, so sind sie untereinander von der Schweigepflicht insoweit befreit, als das Einverständnis des Patienten vorliegt oder anzunehmen ist."

In anderen mir wesentlichen Punkten wurden meine Bedenken und Anregungen nicht berücksichtigt. Dies gilt für

- das Absehen von einer Regelung zur Mikroverfilmung;
- die der höchstrichterlichen Rechtsprechung zuwiderlaufende Beschränkung des Akteneinsichtsrechts der Personen, für die Maßnahmen auf Grund des Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (PsychKG) getroffen werden;
- die Anwesenheit Dritter bei der ärztlichen oder zahnärztlichen Untersuchung von Kindergarten- und Schulkindern.

3.2.11 Sechstes Gesetz zur Änderung dienstrechtlicher Vorschriften

Das Sechste Gesetz zur Änderung dienstrechtlicher Vorschriften (GV. NW. S. 468) ist am 1.8.1993 in Kraft getreten. Zu begrüßen ist, daß damit nunmehr ein einheitliches Personalaktenrecht für die Beamten aller Dienstherren in Nordrhein-Westfalen gilt. Das Gesetz sieht detaillierte normenklare Regelungen für die Führung der Personalakten in folgenden Bereichen vor:

- Pflicht zur Führung von Personalakten,
- Begriff, Inhalt und Gliederung der Personalakten (Grund-, Teil- und Nebenakten); Prüfungs-, Sicherheits- und Kindergeldakten; Beihilfeakten,
- Anhörungsrecht,
- Einsicht in die Personalakte,
- Weitergabe der Personalakte sowie Auskünfte daraus an Dritte,
- Entfernung von Vorgängen aus der Personalakte,
- Verarbeitung von Personalaktendaten in Dateien,
- Aufbewahrung von Personalakten.

Zu der von mir vorgeschlagenen Ergänzung des § 45 Abs. 1 LBG verweise ich auf das nunmehr geltende Gesundheitsdatenschutzgesetz - GDSG NW -, das in § 24 Abs. 3 eine entsprechende Regelung trifft.

3.2.12 Landespersonalvertretungsgesetz

Mit dem Dritten Gesetz zur Änderung des Personalvertretungsgesetzes für das Land Nordrhein-Westfalen (LPVG) vom 27. September 1994 (GV. NW. S. 846) ist eine umfangreiche Novellierung der personalvertretungsrechtlichen Vorschriften erfolgt. Hierbei wurden jedoch die in meinem 11. Tätigkeitsbericht (S. 75/76) wiedergegebenen Anregungen nicht berücksichtigt.

Statt der von mir geforderten Erläuterung des Begriffs der „Sammlungen von Personaldaten" ist § 65 Abs. 3 Satz 1 dahingehend ergänzt worden, daß listenmäßig aufgeführte Personaldaten, die regelmäßig Entscheidungsgrundlage in beteiligungspflichtigen Angelegenheiten sind, vom Personalrat auch ohne Zustimmung des Beschäftigten eingesehen werden können, wobei sich aus der Gesetzesbegründung ergibt, welche Daten hierunter fallen. Damit ist die Legitimation für einen weiteren Eingriff in die Persönlichkeitsrechte der Beschäftigten geschaffen worden, der allerdings im Hinblick auf die dem Personalrat obliegenden Aufgaben vertretbar erscheint.

Die in § 65 Abs. 4 angefügte Regelung, wonach die Einhaltung des Datenschutzes dem Personalrat obliegt, genügt nicht meiner Anregung, normenklare und abschließende bereichspezifische, den Umgang mit personenbezogenen Daten durch den Personalrat regelnde Vorschriften zu schaffen. Dies räumt auch die Landesregierung ein, indem sie derartige Regelungen aus Zeitgründen für eine spätere Novellierung zurückgestellt hat.

Ihre - bisher nicht realisierte - Absicht, die erforderlichen Regelungen zunächst in Verwaltungsvorschriften zu treffen, kann an der Notwendigkeit einer alsbaldigen gesetzlichen Normierung nichts ändern.

3.2.13 Schulverwaltungsgesetz

Mit der Änderung des Schulverwaltungsgesetzes - durch Gesetz zur Änderung schulrechtlicher Vorschriften vom 17. Mai 1994 (GV. NW. S. 243) - sind grundlegende bereichspezifische Vorschriften über den Datenschutz in den Schulen geschaffen worden. Bei der Erarbeitung des Gesetzentwurfs hatte ich nicht nur ausreichend Gelegenheit, meine Bedenken und Anregungen zu äußern, sondern fand sie auch im wesentlichen im Gesetz berücksichtigt.

Die in das Schulverwaltungsgesetz eingefügten Vorschriften bilden die gesetzliche Grundlage für die Verarbeitung der Daten der Schülerinnen und Schüler (§ 19), der Lehrkräfte, Lehramtsanwärter und Studienreferendare (§ 19 a) sowie für die zu erlassenden Rechtsverordnungen (§ 19 b Abs. 3). Zu dem Entwurf einer Schülerdatenschutzverordnung habe ich bereits Stellung genommen. Unter den noch ausstehenden Rechtsverordnungen halte ich die Rechtsverordnung zur Verarbeitung der Lehrerdaten für vordringlich, wenn die vorgesehene automatisierte Datenübermittlung im März 1995 (vgl. Antwort der Landesregierung auf die Kleine Anfrage Nr. 2728, Drucksache 11/7807) realisiert werden soll, da ohne diese Rechtsverordnung automatisierte Verfahren zur Übermittlung der Daten der Lehrer an die Schulaufsichtsbehörden nicht eingerichtet werden dürfen.

Die im Gesetz festgelegten Regelungen lassen erwarten, daß eine den Anforderungen des Datenschutzes entsprechende Verarbeitung der personenbezogenen Daten im Schulbereich erfolgt. Das Gesetz enthält zwar keine abschließenden und erschöpfenden Regelungen für alle denkbaren Fragestellungen, es hat sich vielmehr auf wesentliche Grundsätze beschränkt und dort Einzelregelungen getroffen, wo Entscheidungen des Gesetzgebers notwendig waren, wie z. B. das ausdrückliche Verbot einer automatisierten Verarbeitung von Verhaltensdaten und Gesundheitsdaten der Schülerinnen und Schüler. Die weitere notwendige Konkretisierung muß allerdings in den zu erlassenden Rechtsverordnungen realisiert werden. In dem Entwurf einer Schülerdatenschutzverordnung ist dies im wesentlichen geschehen. Die Regelungen dieser Verordnung enthalten für den Schulalltag keine Überraschungen, da sie überwiegend aus den bestehenden Verwaltungsvorschriften übernommen wurden. Allerdings sieht die Schülerdatenschutzverordnung ein Kuriosum namens Schulchronik vor, das ohne jede nähere, abgrenzende Zweckbestimmung zu immensen Datenfriedhöfen an den Schulen führen wird.

Anläßlich verschiedener Gespräche und Überprüfungen an Schulen habe ich feststellen müssen, daß die datenschutzrechtlichen Ergänzungen des Schulverwaltungsgesetzes nur wenigen Schulleitern und Lehrern bekannt sind.

Hier bedarf es auch im Rahmen der Lehrerfortbildung spezieller Fortbildungsangebote vordringlich im Aufgabenfeld „Schulleitung".

3.2.14 Sonderschulentwicklungsgesetz

Zum Ende des Berichtszeitraumes wurde noch der Entwurf eines Gesetzes zur Weiterentwicklung der sonderpädagogischen Förderung (Sonderschulentwicklungsgesetz - SoSchEntwG, Drucksache 11/7186) sowie der Entwurf der Verordnung über die Feststellung des sonderpädagogischen Förderbedarfs und die Entscheidung über den schulischen Förderort (VO-SF) vorgelegt. Damit wird einer langjährigen Forderung nach einer bereichspezifischen datenschutzrechtlichen Rechtsgrundlage für die Durchführung von Sonderschulaufnahmeverfahren (vgl. 11. Tätigkeitsbericht, S. 98) entsprochen.

Während das Sonderschulentwicklungsgesetz als datenschutzrechtlich relevante Regelung nur die Ermächtigung für die Verordnung enthält, bestimmt der Verordnungsentwurf die speziellen Verfahrensregelungen. Neben einer ausführlichen Definition der einzelnen Behinderungsarten und der unterschiedlichen hierauf bezogenen Förderungsschwerpunkte wird klarer als durch die bisherige Erlaßregelung herausgestellt, daß die Schulaufsichtsbehörden Herr der Verfahren sind. Die Schulen melden im wesentlichen nur noch das Verfahren nach vorheriger Information der Erziehungsberechtigten bei der zuständigen Schulaufsichtsbehörde an. Bisher wurde die Feststellung des sonderpädagogischen Förderungsbedarfs wesentlich durch die Sonderschule bestimmt (vgl. Nr. 3.4 des Runderlasses des Kultusministeriums vom 23.10.1984 zum Sonderschul-Aufnahmeverfahren). Es fehlt aber in § 13 der Verordnung die eindeutige Festlegung, daß die Unterlagen des Verfahrens bei der Schulaufsichtsbehörde bleiben und von ihr nur die für die sonderpädagogische Förderung unbedingt notwendigen Daten an die aufnehmende Schule übermittelt werden. Bei meinen Besuchen in einzelnen Schulämtern habe ich nämlich festgestellt, daß die gesamte Akte über das Sonderschulaufnahmeverfahren an die aufnehmende Schule übersandt wird. Diese Verfahrensweise verstößt gegen den Datenschutz.

4. Grenzüberschreitender Datenverkehr

4.1 EG-Datenschutzrichtlinie

Die Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) konnte im Berichtszeitraum noch nicht verabschiedet werden. Die Beratungen wurden in der zweiten Jahreshälfte 1994 während der deutschen EG-Präsidentschaft intensiviert. Nach nunmehr fünfjähriger Behandlung hat der Rat für Wirtschafts- und Finanzfragen einen Gemeinsamen Standpunkt zu der EG-Datenschutzrichtlinie beschlossen.

Die derzeitige Fassung sieht eine Terminregelung zur Frage der Umsetzung der Richtlinie in nationales Recht vor im Sinne einer Übergangsmaßnahme. Dies bedeutet ein schrittweises Umsetzen der Richtlinie in nationales Recht. Den Mitgliedstaaten wird eine dreijährige Frist eingeräumt, staatliche Vorschriften zur Durchführung der Richtlinie zu erlassen.

Im übrigen ist an der Zielsetzung festgehalten worden, die Aufrechterhaltung eines höheren nationalen Datenschutzstandards zu ermöglichen. Den nationalen Spielraum so groß wie möglich zu erhalten, wurde nach wie vor als Vorgabe beibehalten.

Es bleibt zu hoffen, daß zumindest im Jahre 1995 die Richtlinie verabschiedet wird und so die Hemmnisse für die konsequente Errichtung eines Binnenmarktes abgebaut werden.

4.2 Grenzüberschreitender Datenverkehr in einzelnen Bereichen

4.2.1 Europol

Durch den Wegfall der nationalen Binnengrenzen im Bereich der Europäischen Union (EU) rückt die Frage der grenzüberschreitenden polizeilichen Zusammenarbeit auch aus dem Blickwinkel des Datenschutzes mehr und mehr in den Vordergrund.

Die mit dem Europäischen Kriminalamt Europol geschaffene zentrale Polizeieinrichtung, die ich bereits in meinem 11. Tätigkeitsbericht (S. 16) vorgestellt habe, wirft nach wie vor eine Reihe datenschutzrechtlicher Fragen im Hinblick auf die Nutzung der zur Verfügung stehenden Informationen auf. Die derzeit an Stelle einer umfassenden Konvention der EU-Staaten für Europol vorgesehene Übergangslösung mit dem Austausch von Verbindungsbeamten aus allen EU-Staaten birgt selbst nach Meinung des Innenministeriums des Landes Nordrhein-Westfalen die Gefahr, daß Daten nach Zugriff auf die nationalen Informationssysteme ohne ausreichende Prüfung

weitergegeben werden. Insbesondere dieser Aspekt wird bei der weiteren Entwicklung von Europol zu beachten sein.

Inzwischen hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf ihrer Sitzung am 26./27. September 1994 datenschutzrechtliche Anforderungen an ein Übereinkommen der Mitgliedstaaten der EU über die Errichtung von Europol gestellt. Danach wird davon ausgegangen, daß bei den Verhandlungen mindestens folgende Punkte berücksichtigt werden:

„- Das Übereinkommen muß der verfassungsrechtlichen Kompetenzverteilung in Bund und Ländern für die Polizei entsprechen. Die materielle Verantwortung für die Datenverarbeitung muß, soweit die Daten von Landesbehörden erhoben worden sind, weiterhin bei den Ländern liegen. Davon bleiben die Zuständigkeiten und die dazugehörigen Befugnisse des BKA als nationale Stelle für den Informationsverkehr mit Europol unberührt.

- Die Regelungen zur Verarbeitung personenbezogener Daten müssen präzise sein und dem Grundsatz der Verhältnismäßigkeit entsprechen. Beispielsweise erfüllen die in den bisherigen Entwürfen vorgesehenen Befugnisse zur europaweiten Speicherung von Daten unbeteiligter Personen diese Voraussetzungen nicht.

Die Datenschutzbeauftragten erwarten, daß die deutsche Seite eine Klarstellung über die Verantwortung der Länder, zum Beispiel durch eine Protokollerklärung zum Europol-Übereinkommen, trifft."

Dabei gehe ich davon aus, daß im dritten Satz des ersten Spiegelstrichs die Zuständigkeiten und Befugnisse des BKA nach geltender Verfassungs- und Rechtslage gemeint sind. Dies bedeutet, daß - wie in den beiden vorangehenden Sätzen inhaltlich ausgeführt - weder durch die beabsichtigte Konvention noch durch die Art ihrer Ausführung die Datenherrschaft der Länder und damit die entsprechenden Regelungen in den Landespolizeigesetzen eingeschränkt oder ausgehöhlt werden dürfen.

4.2.2 Schengener Informationssystem

Mängel im Programm des sog. Schengener Informationssystems (vgl. 10. Tätigkeitsbericht, S. 33) haben das Inkrafttreten des Schengener Durchführungsübereinkommens (SDÜ) weiter hinausgezögert. Dies hat dem Bund und den Ländern im Zusammenwirken mit dem Bundesbeauftragten und den Landesbeauftragten für den Datenschutz Gelegenheit gegeben, sich mit der Frage der datenschutzrechtlichen Kontrollinstanz dieses Informationssystems nach Artikel 115 Abs. 1 SDÜ weiter zu beschäftigen. Die Kontrollinstanz soll sich aus je zwei Vertretern der jeweiligen nationalen Kontrollinstanz zusammensetzen. Auf Grund des föderalen Aufbaus der Bundesrepublik Deutschland kommt allerdings mit dem Bundesbeauftragten und den 16 Lan-

desbeauftragten für den Datenschutz mehr als nur eine nationale Kontrollinstanz in Frage, die Vertreter in die Kontrollinstanz des Schengener Informationssystems entsenden könnte. Da es sich bei den im Schengener Informationssystem zu verarbeitenden Daten im wesentlichen auch um Länder-(polizei-)daten handelt, wäre zur Bestimmung der nationalen Kontrollinstanz im Sinne des Artikels 115 Abs. 1 SDÜ eine Bund-Länder-Vereinbarung, etwa in Form eines Staatsvertrages, notwendig, um die Länderinteressen ausreichend zu wahren. Inzwischen hat sich der Hessische Datenschutzbeauftragte bereit erklärt, bis auf weiteres als Vertreter der Landesbeauftragten an der gemeinsamen Kontrollinstanz teilzunehmen.

Das Dokument über das Inkraftsetzen des Schengener Durchführungsübereinkommens vom 19.6.1990 wurde vom Exekutivausschuß auf seiner Sitzung am 22.12.1994 unverändert beschlossen. Als Termin für das Inkrafttreten ist der 26. März 1995 festgelegt worden.

4.2.3 EG-Führerscheinrichtlinie

Auf überwiegende Kritik der Datenschutzbeauftragten stieß die Absicht des Bundesverkehrsministeriums, ein ca. fünfzig Millionen Datensätze umfassendes zentrales Fahrerlaubnisregister beim Kraftfahrt-Bundesamt zu errichten. Das Ministerium begründete die Notwendigkeit hierfür vornehmlich mit dem in der 2. EG-Führerscheinrichtlinie vom 29. Juli 1991 vorgesehenen Informationsaustausch zwischen den EG-Staaten, mit der Verbesserung des Verwaltungsverfahrens bei der Erteilung und dem Umtausch von Fahrerlaubnissen und der Ausstellung von Ersatzführerscheinen sowie schließlich mit der schnelleren Prüfung, ob und in welchem Umfang eine Fahrerlaubnis erteilt worden ist.

Diese Gründe überzeugen nicht. Vielmehr kann mit den vorhandenen Kontrollmöglichkeiten, insbesondere wegen der Pflicht zur Mitführung des Führerscheins festgestellt werden, ob dem Führerscheininhaber die Fahrerlaubnis erteilt wurde. Außerdem ist ein gegenseitiger Informationsaustausch entsprechend der EG-Richtlinie auch ohne ein zentrales Register möglich. Schließlich rechtfertigt die Verbesserung eines Verwaltungsverfahrens allein noch nicht die mit der Einrichtung eines bundesweiten Fahrerlaubnisregisters verbundenen Eingriffe in das Grundrecht der Betroffenen auf Datenschutz.

4.2.4 Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik

Die Europäische Union strebt im Zuge der Harmonisierung von Statistiken der EG-Mitgliedstaaten gemeinschaftsrechtliche Regelungen an, die tiefgreifende Auswirkungen auf die nationalen statistikrechtlichen Vorschriften, insbesondere das Statistikgeheimnis haben werden (vgl. meinen 11. Tätigkeitsbericht, S. 17). In diesem Zusammenhang liegt ein Vorschlag der Kommission der Europäischen Union für eine Verordnung (EG) des Rates über die

Tätigkeit der Gemeinschaft im Bereich der Statistik - EG-Statistikverordnung - vor. Dessen allgemeine Regelungen für die Gemeinschaftsstatistik sind zwar zu begrüßen, im einzelnen bestehen gegen den Vorschlag allerdings zum Teil erhebliche datenschutzrechtliche Bedenken, die die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrem Beschluß vom 25. August 1994 (s. Anlage 6, S.176 bis 178) präzisiert haben. Es bleibt abzuwarten, ob diese kurzfristig der Bundesregierung übermittelten Bedenken im Zuge der weiteren Verhandlungen mit der Europäischen Union und den Mitgliedstaaten Berücksichtigung finden werden.

5. Datenschutz in einzelnen Bereichen

5.1 Einwohnerwesen

5.1.1 Weitergabe von Daten des Anzeigeerstatters

In einer Reihe von Fällen bin ich auf die Problematik eines ausreichenden Datenschutzes bei **Beschwerden** an die Gemeindeverwaltung angesprochen worden. So sind die Sachverhalte zusammen mit den personenbezogenen Daten der Petenten aus den Beschwerdeschreiben an andere Verwaltungsstellen oder an private Dritte weitergegeben worden. Als Rechtsgrundlage für eine derartige Weitergabe kann allgemein § 14 Abs. 5 i.V.m. Abs. 1 DSG NW in Betracht kommen, wonach eine Übermittlung personenbezogener Daten zulässig ist, wenn sie zur rechtmäßigen Erfüllung der Aufgaben des Empfängers erforderlich ist und die Voraussetzungen für eine Zweckänderung nach § 13 DSG NW vorliegen. Dabei ist der Begriff der Erforderlichkeit eng auszulegen. Die Daten müssen zur Aufgabenerfüllung des Empfängers unbedingt notwendig und nicht nur dienlich oder nützlich sein. Dies gilt bereichspezifisch auch für die Ordnungsämter (§ 24 Nr. 11 OBG NW i.V.m. § 29 Abs. 1 Nr. 1 PolG NW).

Das Beschwerdeschreiben mit allen, auch personenbezogenen Daten des Beschwerdeführers kann ansonsten nur mit Einwilligung des Betroffenen weitergegeben werden. Zur Vermeidung von Verstößen gegen Vorschriften über den Datenschutz habe ich in diesen Fällen empfohlen, vor der Weitergabe an andere städtische Stellen oder auch private Dritte derartige Schreiben zu anonymisieren oder die Einwilligung der Betroffenen zu einer Datenweitergabe einzuholen. Die betroffenen Gemeinden sind meiner Empfehlung durchweg gefolgt.

5.1.2 Daten Verstorbener

Eine Gemeinde hat die Frage an mich herangetragen, inwieweit eine Auskunft an private Dritte aus dem **Friedhofsregister** über einen Verstorbenen zulässig sei. Dabei handelte es sich nicht um eine Person der Zeitgeschichte, jedoch um einen Verstorbenen, der in seinem Leben eine hervorgehobene Stellung innehatte.

Rechtsgrundlage für das Friedhofsregister war eine Satzung der Gemeinde über die Benutzung der Friedhöfe. In dieser Satzung war eine Auskunfterteilung nicht geregelt. Für eine Datenübermittlung an private Dritte kommt im vorliegenden Fall § 16 DSG NW in Betracht. Die Übermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs ist nur unter den dort genannten Voraussetzungen zulässig.

Welches Interesse (rechtliches, berechtigtes) der Anfragende an dieser Auskunft hatte, war seinem Schreiben nicht zu entnehmen. Für die Prüfung der schutzwürdigen Belange ist sowohl auf die Belange des Verstorbenen, als

auch seiner Angehörigen abzustellen. Soweit lediglich von einem berechtigten Interesse auszugehen wäre, müßten die Angehörigen (als Betroffene) wegen der Ausübung des Widerspruchs unterrichtet werden (§ 16 Abs. 1 Satz 1 Buchstabe d i.V.m. Satz 2 DSG NW). Soweit auch ein berechtigtes Interesse nicht gegeben sein sollte, wäre die gewünschte Datenübermittlung nur mit ausdrücklicher schriftlicher Einwilligung der betroffenen Angehörigen zulässig (§ 4 Satz 2 DSG NW).

5.1.3 Forschung

Bei einem Forschungsvorhaben „Fall-Kontrollstudie über akute Leukämien", das sich mit den in jüngster Zeit aufgetretenen **Leukämie-Clustern** beschäftigt, sollten im Rahmen der Untersuchung neben den Eltern krebskranker Kinder Eltern gesunder Kinder als Kontrollgruppe befragt werden. Die Kontrollgruppe sollte über die Einwohnermeldeämter rekrutiert werden. Dabei sollte eine Kontrollgruppe aus den Gemeinden gewählt werden, in denen Patienten wohnen. Für eine zweite Kontrollgruppe sollten Gemeinden zufällig ausgewählt werden.

Als Rechtsgrundlage für eine derartige Auskunft kommt § 31 Abs. 1 Satz 1 i.V.m. Satz 3 MG NW in Betracht. Allerdings dürfen die dort genannten Daten nur an andere öffentliche Stellen übermittelt werden, wenn dies zur rechtmäßigen Erfüllung der Aufgaben des Empfängers erforderlich ist. Werden diese Daten für eine Personengruppe listenmäßig oder in sonst zusammengefaßter Form übermittelt, so dürfen für die Zusammensetzung der Personengruppe nur die in Satz 1 genannten Daten zugrunde gelegt werden (Satz 3). Aus den mir übersandten Unterlagen ging hervor, daß die Datenübermittlung vom Einwohnermeldeamt an die Forschungseinrichtung zu deren Aufgabenerfüllung nicht erforderlich war. Wie den Erläuterungen zur Befragung zu entnehmen war, diente die Adresse außer zur Übersendung des Erstschreibens nur dazu, die betroffenen Eltern später bei evtl. Rückfragen noch einmal ansprechen zu können. Die Adressen von Personen, die nicht an der Studie teilnehmen wollten, wurden sofort gelöscht. Folglich mußte auch bei Nichtrücksendung des Fragebogens die Adresse sofort gelöscht werden.

Die jeweilige Adresse wurde somit nur für ein einmaliges Anschreiben genutzt. Ohne Datenübermittlung an die Forschungseinrichtung konnte die Versendung des Schreibens somit auch durch die jeweilige Gemeinde erfolgen. Mit diesem Versendungsweg würde auch den schutzwürdigen Belangen der Betroffenen (§ 7 MG NW) Rechnung getragen.

Als Ergebnis bleibt festzustellen, daß, soweit nicht der Weg der Adressierung durch die Einwohnermeldeämter gewählt wird, eine Datenübermittlung an die Forschungseinrichtung nur mit Einwilligung der betroffenen Eltern (§ 4 Satz 1 Buchstabe b DSG NW) erfolgen kann. Diese Einwilligung müßte ggf. von den Einwohnermeldeämtern eingeholt werden.

In einem weiteren Forschungsprojekt bin ich auf die Problematik einer datenschutzrechtlichen **„Unbedenklichkeitsbescheinigung"** angesprochen

worden. Dazu habe ich darauf verwiesen, daß von mir eine derartige Bescheinigung zur Datenverarbeitung im Zusammenhang mit einem Forschungsvorhaben nicht erteilt wird. Die Frage der Übermittlung von Meldedaten zu Forschungszwecken fällt in die ausschließliche Zuständigkeit der Meldebehörden des Landes Nordrhein-Westfalen. Wenn sich Gemeinden an mich wenden und datenschutzrechtliche Bedenken vortragen, werden diese von mir überprüft und die Gemeinden entsprechend beraten.

Es bestand wiederholt Anlaß, Forscher darauf hinzuweisen, daß bei Forschungsvorhaben, in denen personenbezogenen Daten verarbeitet werden, der Gewährleistung des Rechts auf informationelle Selbstbestimmung eine besondere Bedeutung zukommt. In die Planung und Durchführung eines Forschungsprojekts sollte daher nach meiner Auffassung von vornherein auch der Zeit- und Verwaltungsaufwand mit einbezogen werden, der zur Gewährleistung des Rechts auf informationelle Selbstbestimmung notwendig ist.

5.2 Wahlen

5.2.1 Unterstützungsunterschriften

Eine Gemeinde hat mir mitgeteilt, daß nach einer Überprüfung bei den Kommunalwahlen 1989 in mehreren Fällen Unterstützungsunterschriften gefälscht worden sind. Auf Grund dieser Tatsache sind für die Kommunalwahlen im Jahre 1994 stichprobenartige Überprüfungen der Unterstützungsunterschriften durchgeführt worden. Dabei sind zunächst die betroffenen Personen von Mitarbeitern des Wahlamtes telefonisch befragt worden, ob sie eine Unterstützungsunterschrift für eine bestimmte Partei abgegeben hätten. Gegen eine fernmündliche Abklärung bestehen datenschutzrechtliche Bedenken, da u. a. die Identität des Gesprächspartners nicht zuverlässig festgestellt werden kann.

Da aus der Sicht des Datenschutzes auch ein persönliches Aufsuchen der betroffenen Personen als kritisch anzusehen ist, eine schriftliche Befragung der Personen (per Einschreiben) bedingt durch die in den Kommunalwahlgesetzen und Kommunalwahlordnungen vorgegebenen Fristen faktisch nicht möglich war, wurde die Stichprobenüberprüfung an Hand der Daten aus dem Personalausweisregister vorgenommen.

Nach § 2 b Abs. 2 Ziffer 3 des Gesetzes über Personalausweise (PAG) dürfen die Personalausweisbehörden anderen Behörden auf deren Ersuchen Daten aus dem Personalausweisregister übermitteln. Voraussetzung ist, daß die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden könnten oder nach der Art der Aufgabe, zu deren Erfüllung die Daten erforderlich sind, von einer solchen Datenerhebung abgesehen werden muß. Gegen die dargestellte Verfahrensweise bestehen keine datenschutzrechtlichen Bedenken. Sollte nach Ausschöpfen der Möglichkeiten nach § 2 Abs. 2 Ziffer 3 PAG gleichwohl eine persönliche Rück-

frage erforderlich sein, so bestehen dagegen im Ergebnis ebenfalls keine datenschutzrechtlichen Bedenken.

5.2.2 Wählerverzeichnis

Zur öffentlichen Auslegung des Wählerverzeichnisses bei melderechtlicher **Auskunftssperre** habe ich schon mehrfach Stellung genommen und als datenschutzrechtlich besonders bedenklich herausgestellt, daß bei der Auslegung des Wählerverzeichnisses die Auskunftssperre nach § 34 Abs. 5 bis 7 MG NW nicht berücksichtigt werde. Im Ergebnis führt dies dazu, daß Personen, denen eine Gemeinde wegen einer Gefahr für das Leben, die Gesundheit, die persönliche Freiheit oder für ähnliche schutzwürdige Belange dieser Personen eine Auskunftssperre eingeräumt hat, über die im Wählerverzeichnis enthaltenen Informationen schutzlos ihren Verfolgern preisgegeben werden.

Diese Problematik habe ich auch in meinem 11. Tätigkeitsbericht (S. 23/24) dargelegt. Die Landesregierung hat in ihrer Stellungnahme dazu u. a. geäußert, daß der Transparenz des Wählerverzeichnisses Vorrang vor den Interessen Einzelner auf Geheimhaltung einzuräumen sei.

Nachdem mir bekanntgeworden ist, daß sich der sächsische Verordnungsgeber in der Landeswahlordnung um einen Ausgleich bemüht hat, habe ich das Innenministerium erneut gebeten, auch in Nordrhein-Westfalen entsprechende Regelungen zu treffen.

Weiter ist bei der Beratung meines 11. Tätigkeitsberichts im Ausschuß für Innere Verwaltung des Landtags der Innenminister gebeten worden, darüber nachzudenken, ob es notwendig sei, anläßlich von Wahlen das Wählerverzeichnis und dessen Eintragungen uneingeschränkt für jedermann öffentlich auszulegen. Die Beschlußempfehlung des Ausschusses ist vom Landtag in der Sitzung vom 7.9.1994 (Plenarprotokoll 11/138, S. 17425) so angenommen worden.

Nach einer mir nunmehr zugegangenen Äußerung will das Innenministerium den Schutz der so gefährdeten Bürgerinnen und Bürger des Landes Nordrhein-Westfalen erst dann verbessern, wenn der Bund für seinen Zuständigkeitsbereich eine Verbesserung vornimmt. Im Hinblick auf die im Jahre 1995 stattfindende Landtagswahl ist dieser Standpunkt aus datenschutzrechtlicher Sicht nicht tragbar.

5.2.3 Wahlhelfer

Zur Gewinnung von Wahlhelfern sind wiederholt Anfragen an mich gerichtet worden, da Gemeindedirektoren zu diesem Zweck um Übersendung von **Personallisten** von verschiedenen öffentlichen Stellen auch außerhalb des Gemeindegebietes gebeten haben.

Die bisherige Fassung des Kommunalwahlgesetzes sah eine Datenübermittlung der gewünschten Art nicht vor. Nach § 2 Abs. 5 des Kommunalwahl-

gesetzes vom 15. August 1993 ist nunmehr eine gesetzliche Grundlage geschaffen worden (für Landtagswahlen: vgl. entsprechend § 11 Abs. 2 Landeswahlgesetz). Danach sind die Körperschaften und sonstigen juristischen Personen des öffentlichen Rechts verpflichtet, auf Anforderung des Gemeindedirektors bei ihnen Beschäftigte aus der Gemeinde zum Zwecke der Berufung als Mitglieder des Wahlvorstandes zu benennen.

Der Umfang der zu übermittelnden Daten ist in dieser Vorschrift nicht genannt. Insoweit ist der verfassungsrechtliche Erforderlichkeitsgrundsatz zu beachten. Im übrigen bestehen aber gegen eine Übersendung der von den Gemeinden gewünschten Auflistung nach dem gegenwärtigen Erkenntnisstand keine durchgreifenden datenschutzrechtlichen Bedenken.

Es blieb darauf hinzuweisen, daß eine entsprechende gesetzliche Grundlage für die Europawahl und die Bundestagswahl fehlte. Für die Europawahl konnten Mitglieder für die Wahlvorstände nur gewonnen werden, wenn die Mitarbeiter mit der Aufnahme in die Listen einverstanden waren. Für die Bundestagswahl trat das Problem deshalb nicht auf, da sie zugleich mit den Kommunalwahlen durchgeführt wurde.

5.2.4 Landwirtschaftskammerwahlen

Zur Durchführung der Landwirtschaftskammerwahlen wurden 1993 erstmalig die Gemeindedirektoren nach den §§ 4 bis 8 der Verordnung zur Durchführung des Gesetzes über die Errichtung von Landwirtschaftskammern im Lande Nordrhein-Westfalen (Lk-Wahlordnung) vom 28. Dezember 1989 (GV. NW. 1990 S. 6) für die Aufstellung, Auslegung und Schließung der **Wählerlisten** für die Wahlen der Mitglieder der Landwirtschaftskammer zuständig. Dazu sollten die Gemeinden gebeten werden, im Rahmen eines Abgleiches mit der Einwohnermeldedatei ein Wählerverzeichnis aufzustellen. Vor Auslegung sollte dieses Wählerverzeichnis einer Prüfung der Wahlberechtigten durch zuständige Mitarbeiter der Landwirtschaftskammer sowie des Kreislandwirtes unterzogen werden.

In diesem Zusammenhang habe ich darauf hingewiesen, daß ein Rückgriff auf die Daten des Einwohnermelderegisters zur Erstellung der Wählerliste ausscheidet, zumal da die Daten, von denen die Wahlberechtigung abhängt, nicht im Melderegister enthalten sind. Die Wählerliste kann dagegen im wesentlichen mit Daten erstellt werden, die von der Landwirtschaftskammer übermittelt werden. Soweit die auf der Grundlage dieser Daten gefertigte Wählerliste Lücken aufweist und deshalb unrichtig ist, können diese Unrichtigkeiten durch das ohnehin vorgesehene Verfahren der öffentlichen Auslegung beseitigt werden. In dieser Zeit könnte auch der Kreislandwirt Einblick nehmen und auf bestehende Unrichtigkeiten hinweisen. Zuvor würde eine Datenübermittlung an den Kreislandwirt wegen Fehlens einer entsprechenden Rechtsgrundlage ausscheiden.

Im übrigen bestanden gegen einzelne Spalten des Wählerverzeichnisses datenschutzrechtliche Bedenken, die ich mit dem Ministerium für Umwelt,

Raumordnung und Landwirtschaft des Landes Nordrhein-Westfalen dahingehend geklärt habe, daß die von ihm überarbeitete Anlage 1 der Landwirtschaftskammerwahlordnung in der geänderten Fassung Anwendung fand, auch wenn dazu eine Änderung der Wahlordnung noch nicht erfolgt war.

5.3 Liegenschafts- und Vermessungswesen

5.3.1 Kontrolle der Katasterverwaltung

Im Berichtszeitraum habe ich einen ersten **Kontrollbesuch** in einem Vermessungs- und Katasteramt durchgeführt. Auf Grund erheblicher Mängel in der Vorbereitung durch die kontrollierte Stelle war eine Kontrolle in der zur Verfügung stehenden Zeit nur eingeschränkt möglich.

Der Kontrollbesuch hat gleichwohl ergeben, daß eine verbindliche, auf die spezifischen Belange bei der Datenverarbeitung eines Vermessungs- und Katasteramtes abgestellte Dienstanweisung fehlt. Die vorliegenden Dateianmeldungen waren fehlerhaft. Alle eingeräumten On-line-Zugriffe auf das Liegenschaftskataster waren auf ihre rechtliche Zulässigkeit hin zu überprüfen. Die vorgesehene Protokollierung ließ eine nachträgliche Kontrolle der Zulässigkeit der einzelnen On-line-Abrufe nicht zu. Der bestehende On-line-Zugriff auf das Einwohnermelderegister verstieß gegen den verfassungsrechtlichen Erforderlichkeitsgrundsatz. Demgegenüber war die festgestellte Praxis der Erteilung von Auskünften aus dem Liegenschaftskataster gegenüber privaten Dritten ausdrücklich zu begrüßen.

Durch weitere Kontrollbesuche wird festzustellen sein, ob und inwieweit die vorgefundenen Mängel, aber auch die positiven Ergebnisse, als repräsentativ für die Vermessungs- und Katasterverwaltung des Landes Nordrhein-Westfalen angesehen werden können.

5.3.2 Öffentlich bestellte Vermessungsingenieure

Eine Bürgerin hatte einen öffentlich bestellten Vermessungsingenieur beauftragt, einen Lageplan eines in ihrem Eigentum befindlichen Grundstücks zu fertigen. In diesem Zusammenhang ist sie mit ihrem Namen, Adresse, Rufnummer usw. in die **Kundenkartei** des Vermessungsingenieurs aufgenommen worden. Diese Daten sind ohne Einholung des Einverständnisses der Betroffenen auf Nachfrage an Dritte herausgegeben worden. Mangels Rechtsgrundlage war die Speicherung dieser Daten über den Zweck eines internen Arbeitshilfsmittels hinaus unzulässig. Ebenso fehlte es an einer Rechtsgrundlage für die Datenübermittlung aus einer solchen Datei, so daß auch diese unzulässig war. Auf das Vorliegen eines rechtlichen oder berechtigten Interesses kam es in diesem Zusammenhang nicht an.

Ebenso bestehen Zweifel an der Aufgabenstellung und Befugnis des öffentlich bestellten Vermessungsingenieurs, außerhalb bestimmter Verfahren, wie beispielsweise Abmarkung von Grundstücksgrenzen (§§ 18, 19 des Vermessungs- und Katastergesetzes - VermKatG NW), Auskünfte über personen-

bezogene Daten zu erteilen. Insoweit fehlt es an einer Aufgabenzuweisungs- und Befugnisnorm. Eine dem § 12 VermKatG NW entsprechende Vorschrift für öffentlich bestellte Vermessungsingenieure ist nicht erkennbar. Der Vorgang konnte bisher wegen einer noch ausstehenden Stellungnahme nicht zum Abschluß gebracht werden.

5.3.3 Katasterauszüge an die Pächter

Im Rahmen des **Flächenstillegungsprogramms** der EG-Agrarreform wurden von Landwirten Anträge auf Beihilfen für die Landwirtschaft gestellt, für die Buch- und Katasterauszüge aus dem Liegenschaftskataster als Nachweis verlangt wurden. Die benötigten Auskünfte bezogen sich sowohl auf Eigentums- als auch auf Pachtflächen. Soweit in diesem Zusammenhang Auszüge an Pächter ohne Vollmacht der jeweiligen Eigentümer erteilt wurden, begegnet das Verfahren insgesamt datenschutzrechtlichen Bedenken, da die Datenschutzrechte der betroffenen Eigentümer nicht hinreichend berücksichtigt worden sind.

Dem berechtigten Interesse des Pächters stehen die schutzwürdigen Belange des Eigentümers entgegen. Besonders wurden schutzwürdige Belange der betroffenen Grundeigentümer verletzt, weil unzulässigerweise auch Katasterauszüge und Flurkarten über den gesamten Grundbesitz der Verpächter, d. h. auch den nichtverpachteten Flächen, an die Pächter erteilt wurden.

Zur Vermeidung von Verstößen gegen Vorschriften über den Datenschutz hatte ich empfohlen, in Zukunft eine derartige Datenübermittlung an die Pächter von der Vorlage einer schriftlichen Einwilligung des Verpächters abhängig zu machen. Das Ministerium für Umwelt, Raumordnung und Landwirtschaft des Landes Nordrhein-Westfalen hat mitgeteilt, daß künftig den Datenschutzrechten der Grundeigentümer in ausreichendem Umfang Rechnung getragen werde. Eine Wiederholung der Vorfälle aus der Vergangenheit dürfte damit ausgeschlossen sein.

5.3.4 Kartenauszüge an den Rat

In öffentlicher Sitzung wurde ein Kartenauszug über eine Straßenausbaumaßnahme mit den Namen der betroffenen und auch der nicht-betroffenen Grundeigentümer verteilt. Bei der Beratung im Zusammenhang mit Ausbauplänen ist die Bekanntgabe personenbezogener Daten an den Rat und seine Ausschüsse nicht grundsätzlich erforderlich, so daß eine Weitergabe des Kartenauszuges an die Ausschußmitglieder nur nach Schwärzung der Namen hätte erfolgen dürfen. Soweit der Ausschuß auf der Bekanntgabe einzelner Grundstückseigentümer aus plausiblen Gründen bestanden hätte, hätte die Angelegenheit zu diesem Grundeigentümer in nicht-öffentlicher Sitzung beraten und entschieden werden müssen. Eine Weitergabe derartiger Unterlagen mit personenbezogenen Daten der Grundeigentümer an die Presse ist in jedem Fall unzulässig. Ergänzend verweise ich auf die Ausführungen zur Bekanntgabe personenbezogener Daten an Rats- und Ausschußmitglieder,

Zuhörer öffentlicher Sitzungen und die Presse in meinem 10. Tätigkeitsbericht (S. 50/51).

5.3.5 Liegenschaftskataster und Auskunft an die Presse

Zur Beurteilung der Frage, inwieweit aus dem Liegenschaftskataster Auskünfte an die Presse erteilt werden können, ist zunächst auf die generelle Darstellung der rechtlichen Probleme in meinem 9. Tätigkeitsbericht (S. 42/43) zu verweisen. Zu dieser Problematik haben mich neue Anfragen erreicht.

Nach § 4 Abs. 1 des Pressegesetzes für das Land Nordrhein-Westfalen (Landespressegesetz NW - LPG -) sind zwar Behörden verpflichtet, den Vertretern der Presse die der Erfüllung ihrer öffentlichen Aufgabe dienenden Auskünfte zu erteilen. Ein Anspruch auf Auskunft besteht aber u. a. nicht, wenn Vorschriften über die Geheimhaltung entgegenstehen oder ein überwiegendes öffentliches oder ein schutzwürdiges privates Interesse verletzt wird (§ 4 Abs. 2 Nr. 2 und 3 LPG).

Das bedeutet im Ergebnis, daß im Rahmen der Einschränkung nach § 4 Abs. 2 Nr. 2 LPG Geheimhaltungsvorschriften zu prüfen sind. Hierzu gehören bereichspezifische Vorschriften, wie etwa § 12 Abs. 2 Satz 3 des Gesetzes über die Landesvermessung und das Liegenschaftskataster (Vermessungs- und Katastergesetz - VermKatG NW), § 12 Grundbuchordnung (GBO), § 10 der Verordnung über die Gutachterausschüsse für Grundstückswerte (Gutachterausschußverordnung NW - GAVO NW) oder auch die allgemeine Regelung in § 16 Abs. 1 Satz 1 Buchstabe d DSG NW.

Auf jeden Fall darf aber, auch wenn keine Geheimhaltungsvorschriften entgegenstehen, durch die Bekanntgabe personenbezogener Daten kein schutzwürdiges privates Interesse verletzt werden (§ 4 Abs. 2 Nr. 3 LPG). Ein privates Interesse der Betroffenen an der Geheimhaltung der Daten wird im Zweifelsfall unterstellt werden müssen. Ob dieses gegenüber dem Informationsinteresse der Öffentlichkeit schutzwürdig ist, kann nur in jedem Einzelfall im Wege der Abwägung der Interessen entschieden werden.

Die in diesem Zusammenhang bei Auskünften aus dem Liegenschaftskataster vorzunehmende Prüfung kann im Einzelfall dazu führen, daß der Betroffene im Hinblick auf seine schutzwürdigen Belange anzuhören ist. Als Beispiel, welche Erwägungen u. U. anzustellen sind, können die Ausführungen in meinem 6. Tätigkeitsbericht (S. 151/152) dienen.

5.4 Bau- und Wohnungswesen

5.4.1 Gutachterausschuß

Im Berichtszeitraum habe ich mehrere **Kontrollbesuche** bei verschiedenen Gutachterausschüssen durchgeführt. Dabei konnte festgestellt werden, daß die Gutachterausschüsse im Gegensatz zu ihrer unabhängigen Stellung nach § 192 Abs. 1 BauGB überwiegend weisungsabhängig im Verwaltungsaufbau

der Städte und Kreise eingegliedert waren. Weiter bestand die Gefahr von Interessenkollisionen; so etwa dann, wenn dem Gutachterausschuß auch die Aufgabe der kommunalen Bewertungsstelle zur Erledigung übertragen wurde. Eine solche Organisationsentscheidung verstößt auch gegen die Geheimhaltungsverpflichtung nach § 9 der Verordnung über die Gutachterausschüsse für Grundstückswerte (Gutachterausschußverordnung NW - GAVO NW -).

Als besonders bedenklich war zu bewerten, daß die Einzelheiten der Führung der Kaufpreissammlung für die Gutachterausschüsse immer noch verbindlich in der Technischen Anleitung für die Sammlung von Grundstückskaufpreisen aus dem Jahre 1963 geregelt sind. Eine Überarbeitung dieses Erlasses unter Beachtung der neueren Gesetzgebung (Baugesetzbuch, Gutachterausschußverordnung) hat bisher nicht stattgefunden. Der Erlaß ist in vielen Punkten überholt oder steht im Gegensatz zu den neueren gesetzlichen Bestimmungen. So empfiehlt der Erlaß für die Führung der Kaufpreissammlung generell die Karteikarte und für größere Kaufpreissammlungen die Randlochkarte; tatsächlich kommt bei den kontrollierten Gutachterausschüssen durchweg die automatisierte Datenverarbeitung zum Einsatz.

Neben einer Reihe anderer Mängel ist weiter hervorzuheben, daß die Gutachterausschüsse zur Auswertung von Kaufverträgen zusätzliche Daten von den Käufern erheben, ohne die Betroffenen auf die Freiwilligkeit der Preisgabe der Daten hinzuweisen. Ebenfalls ohne Einwilligung der Betroffenen werden Fotos von Grundstücken und Gebäuden gefertigt und in Akten oder Karteien übernommen.

So bleibt zu hoffen, daß durch entsprechende Vorgabe des Innenministeriums des Landes Nordrhein-Westfalen als oberste Aufsichtsbehörde eine datenschutzkonforme Datenverarbeitung der Gutachterausschüsse erreicht werden kann. Die kontrollierten Gutachterausschüsse haben das Innenministerium um eine zeitnahe Erledigung gebeten.

5.4.2 Auskunft aus und Einsicht in Bauakten

Ein Petent hat sich an mich gewandt, da ihm die Erstellung von Fotokopien eines internen Schriftverkehrs aus seit mehr als 20 Jahren **abgeschlossenen Bauakten** verweigert wurde. In diesem Zusammenhang habe ich darauf verwiesen, daß während eines Verfahrens die Vorschriften des § 29 Verwaltungsverfahrensgesetz, die die Akteneinsicht durch Verfahrensbeteiligte regeln, Anwendung finden. Nach Abschluß des Verfahrens steht einem Beteiligten als datenschutzrechtlich Betroffenem das Akteneinsichtsrecht nach § 18 DSG NW zu.

§ 18 Abs. 3 DSG NW dürfte hierbei im Ergebnis eine Auskunftsverweigerung bzw. Verweigerung der Akteneinsicht nicht rechtfertigen. Bei einem seit 20 Jahren abgeschlossenen Vorgang dürfte das Vorliegen der Voraussetzungen von § 18 Abs. 3 Buchstaben a und b ausgeschlossen sein. Die Verpflichtung zur Auskunftserteilung oder zur Gewährung der Akteneinsicht

entfällt, soweit dies die ordnungsgemäße Erfüllung der Aufgaben der speichernden Stelle gefährden würde (Buchstabe a), dies die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde (Buchstabe b). Zu den Voraussetzungen des Buchstaben c, wonach die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen der berechtigten Interessen einer dritten Person, geheimgehalten werden müssen, ist anzumerken, daß, je länger ein Vorgang zeitlich zurückliegt, es hinsichtlich der Interessen Dritter zunehmend schwieriger sein dürfte, solche Interessen noch als „berechtigt" anzuerkennen. In der Regel dürfte deshalb der Anspruch auf Auskunft überwiegen.

Die betroffene Gemeinde hatte mir mitgeteilt, daß sie meine Rechtsauffassung teile, und daß die Akteneinsicht tatsächlich nicht verweigert wurde. Das pflichtgemäße Ermessen im Sinne von § 18 Abs. 2 DSG NW werde auch ausgeübt, wenn dem Betroffenen aus abgeschlossenen Bauakten nur diejenigen Vorgänge schriftlich in Form von Fotokopien überlassen würden, von denen Rechtswirkungen nach außen ausgingen (Baugenehmigung und genehmigte Bauvorlagen). Die Vorschrift verpflichte in diesem Fall jedoch nicht, auf Antrag einem Betroffenen Fotokopien von dem behördeninternen Schriftverkehr abgeschlossener Bauakten zur Verfügung zu stellen.

In einem weiteren Fall bin ich auf das Problem der Aktenführung und Akteneinsicht im Zusammenhang mit sog. **„Hausakten"** im Bauaufsichtsamt aufmerksam gemacht worden. Bei diesen Hausakten wird zu jedem Gebäude unter einer bestimmten Hausnummer ein Verwaltungsvorgang geführt, zu dem alle das Gebäude betreffenden Verwaltungsvorgänge und der mit Dritten geführte Schriftverkehr genommen wird.

Dabei hat mir die betroffene Kommune mitgeteilt, daß die in meinem 11. Tätigkeitsbericht (S. 27/28) gemachten Empfehlungen berücksichtigt werden. So wird etwa Akteneinsicht in abgeschlossene Verfahrensakten, die sich bei den zum jeweiligen Grundstück gehörenden Hausakten befinden, nur dem jeweiligen Grundstückseigentümer oder seinem schriftlich Bevollmächtigten in den Räumen der Registratur gestattet. Hierbei dürfen grundsätzlich nur Bauzeichnungen eingesehen werden; evtl. in der Akte befindlicher Schriftverkehr unterliegt nicht der Einsichtnahme. Die Einhaltung dieser Regelung, auf die durch Aushang mehrfach hingewiesen werde, werde kontrolliert. Diese Handhabung ist datenschutzgerecht.

5.4.3 Baugenehmigungen an den Rat

Eine Gemeinde hat mir einen Auszug einer **Sitzungsvorlage** für eine nichtöffentliche Sitzung des Bau- und Grundstücksausschusses über Bauanträge und deren Genehmigung durch das Bauordnungsamt mit der Bitte um Überprüfung zugesandt. Aus dieser Liste waren u. a. folgende Daten zu entnehmen: Baunummer, Name, Bauadresse, Wohneinheiten, Baugenehmigung mit Datum, Bauvorhaben. Bereits in meinem 8. Tätigkeitsbericht (S. 23 bis 25)

und 10. Tätigkeitsbericht (S. 50/51) habe ich zu Datenübermittlungen bei Bekanntgabe von Bauanträgen im Bauausschuß Stellung genommen.

Nach § 41 Abs. 1 und § 42 Abs. 1 Satz 1 der Gemeindeordnung für das Land Nordrhein-Westfalen - GO NW - a. F. kann der Rat mit der Vorbereitung seiner Entscheidung einen Ausschuß beauftragen. Soweit dies für eine sachgerechte Entscheidung des Rates und für eine sachgerechte Vorbereitung dieser Entscheidung durch den Ausschuß erforderlich ist, dürfen deren Mitgliedern auch personenbezogene Daten Betroffener bekanntgegeben werden. An die Erforderlichkeit ist ein strenger Maßstab anzulegen. Es genügt nicht, wenn die Bekanntgabe der personenbezogenen Daten zur Aufgabenerfüllung nur dienlich ist; sie muß vielmehr hierfür unbedingt notwendig sein. Dies macht eine Entscheidung in jedem einzelnen Fall erforderlich. Ich habe für die Zukunft angeregt, eine entsprechende Einwilligungserklärung, die die Voraussetzungen des § 4 Satz 2 bis 4 DSG NW berücksichtigt, in die Antragsformulare für die Erteilung von Baugenehmigungen aufzunehmen.

Ansonsten bliebe nur die Möglichkeit, die Datensätze in der Auflistung zuverlässig zu anonymisieren. In der überwiegenden Zahl der Fälle könnte hierzu bereits die Schwärzung des Namens des Bauherrn und der Hausnummer in der Bauadresse ausreichen. Gegen die Weitergabe einer derart anonymisierten Auflistung bestehen nach dem derzeitigen Erkenntnisstand keine durchgreifenden datenschutzrechtlichen Bedenken. Derartige Baulisten könnten in öffentlicher Sitzung beraten werden.

In einem weiteren Fall hatte ich darauf hinzuweisen, daß, soweit zusätzlich Daten „zur besseren Orientierung" gewünscht werden, sie zur Aufgabenerfüllung des Ausschusses nicht erforderlich, d. h. unbedingt notwendig, sondern lediglich dienlich oder nützlich sind. Derartige Daten können nur mit Einwilligung der Betroffenen von der Verwaltung an den Ausschuß weitergegeben werden.

Soweit im konkreten Einzelfall die Nennung des Namens der Bauherrin und des Bauherrn für erforderlich angesehen wird, würde eine Beratung in nichtöffentlicher Sitzung den schutzwürdigen Belangen in besonderer Weise Rechnung tragen.

Nach meiner Auffassung sind die Grundsätze, die es bei öffentlichen Ratssitzungen verbieten, Daten an die Zuhörer zu übermitteln, entsprechend auf die Zuhörer nach § 33 Abs. 3 GO NW a. F. anzuwenden. Das bedeutet im Ergebnis, daß die Sitzungsvorlagen nicht an diese Zuhörer verteilt werden dürfen. Auch die neue Gemeindeordnung hat hier keine Rechtsänderung gebracht (vgl. oben S. 23).

5.4.4 Umwandlung von Miet- in Eigentumswohnungen

Ein Bürger hatte beim Bauordnungsamt einer Gemeinde die Ausstellung einer Abgeschlossenheitsbescheinigung nach dem Wohnungseigentumsgesetz (WEG) beantragt. Dabei handelte es sich um die Umwandlung von

Mietwohnungen in Eigentumswohnungen. Die betroffene Gemeinde plante daraufhin, alle Mieter des Hauses, die von der Umwandlung betroffen waren, mittels eines Informationsschreibens über den gesetzlichen Mieterschutz zu informieren.

Für den **öffentlich-geförderten Wohnungsbau** sind bereichspezifische Regelungen in §§ 2 a, 3 des Gesetzes zur Sicherung der Zweckbestimmung von Sozialwohnungen (Wohnungsbindungsgesetz - WoBindG) vorhanden, die eine derartige Unterrichtung zulassen. Als Aufgabenzuweisungsnorm ist insoweit § 3 WoBindG in Verbindung mit den landesrechtlichen Regelungen anzusehen. Die Befugnis zur Datenverarbeitung durch das Amt für Wohnungswesen der Gemeinde ist ihrem Inhalt und Umfang nach in § 2 a Abs. 2 WoBindG geregelt. Als Verpflichtungsnorm für den Bürger, entsprechende Angaben für die Datenverarbeitung der zuständigen Stelle zu machen, ist § 2 a Abs. 1 WoBindG zu qualifizieren.

Entsprechende bereichspezifische Regelungen einer solchen Datenverarbeitung für den **freifinanzierten Wohnungsbau** fehlen. Nach meiner Auffassung kann daraus geschlossen werden, daß der Bundesgesetzgeber die Mieter des freifinanzierten Wohnungsbaus im Gegensatz zu den Mietern des öffentlich-geförderten Wohnungsbaus nicht in dieser Weise schützen wollte. Andererseits macht die bereichspezifische Regelung in § 2 a WoBindG deutlich, daß die Verarbeitung von personenbezogenen Daten in diesem Zusammenhang einer bereichspezifischen Regelung bedarf. Ein Rückgriff auf die Rechtsgrundlagen der allgemeinen Datenschutzgesetze ist ausgeschlossen. Das Datenschutzgesetz Nordrhein-Westfalen findet auf eine derartige Datenverarbeitung nach meiner Auffassung keine Anwendung.

Selbst wenn für eine derartige Datenübermittlung vom Amt für Wohnungswesen an die Mieter eines freifinanzierten Mietshauses auf § 16 DSG NW zurückgegriffen werden sollte, lägen im Ergebnis die Voraussetzungen für eine zulässige Datenverarbeitung auch dann nicht vor.

Die Verwendung der gespeicherten Daten der betroffenen Eigentümer für eine Unterrichtung der Mieter stellt eine Zweckänderung der Daten dar. Eine Übermittlung solcher Daten nach § 16 Abs. 1 Buchstabe a DSG NW kommt danach nicht in Betracht.

Eine Datenübermittlung nach § 16 Abs. 1 Buchstabe b i.V.m. § 13 Abs. 2 Satz 1 Buchstabe a DSG NW scheidet aus, da eine Rechtsvorschrift diese Datenverarbeitung nicht ausdrücklich erlaubt oder die Wahrnehmung dieser Aufgabe nicht durch Gesetz oder Rechtsverordnung der Gemeinde (Amt für Wohnungswesen) ausdrücklich zugewiesen worden ist. Ebenso fehlt die Einwilligung des betroffenen Eigentümers (§ 13 Abs. 1 Satz 1 Buchstabe b DSG NW). Von einer schwerwiegenden Beeinträchtigung der Rechte der Mieter kann im Hinblick auf das Fehlen von einer dem § 2 a WoBindG entsprechenden Regelung für den freifinanzierten Wohnungsbau und der darin erkennbaren Wertentscheidung des Gesetzgebers nicht ausgegangen werden (§ 13 Abs. 2 Satz 1 Buchstabe d DSG NW). Die Voraussetzungen von § 13

Abs. 2 Satz 1 Buchstabe f DSG NW liegen erkennbar ebenfalls nicht vor. Somit wäre auch nach den allgemeinen Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen eine Übermittlung personenbezogener Daten der Eigentümer an die Mieter in diesem Zusammenhang nicht zulässig.

Nach § 4 Satz 1 Buchstabe b DSG NW kommt bei einer solchen Sachlage eine Datenverarbeitung jeweils nur mit Einwilligung der betroffenen Grundeigentümer in Betracht. Bei der Einholung der Einwilligung ist § 4 Satz 2 bis 4 DSG NW zu beachten. Fehlt eine solche Einwilligung, so ist von der beabsichtigten Datenübermittlung abzusehen. Sie wäre dann unzulässig.

Zur Vermeidung von Verstößen gegen Vorschriften über den Datenschutz habe ich daher empfohlen, in einem solchen Fall auf die beabsichtigte Unterrichtung der Mieter zu verzichten. Die Angelegenheit konnte bisher auf Grund der ausstehenden Stellungnahme der Gemeinde noch nicht zum Abschluß gebracht werden.

5.4.5 Fehlbelegungsabgabe

Ein Bürger hat mir in Kopie das von einer Gemeinde verwandte Formular eines Antrags auf Beschränkung der Ausgleichszahlung gemäß § 6 des Gesetzes über den Abbau der Fehlsubventionierung im Wohnungswesen für das Land Nordrhein-Westfalen (AFWoG NW) zugesandt. Der Fragebogen, der vom Vermieter unterschrieben werden sollte, enthielt eine Reihe von Informationen über den Mieter, die nicht notwendig waren. So waren auf dem Bogen einmal die Bescheinigungen des Vermieters über Miethöhe sowie der Antrag des Mieters an das Amt für Wohnungswesen miteinander verknüpft, wobei die Notwendigkeit dieser Verknüpfung nicht zu erkennen war.

Die Gemeinde, die ich um Stellungnahme gebeten hatte, hat darauf verwiesen, daß das Weiterleiten des Vordrucks an den Vermieter freiwillig sei und auch die darin abgefragten Daten anderweitig nachgewiesen werden könnten. Ich habe daher empfohlen, das Formblatt um den Hinweis zu ergänzen, welche Angaben auch durch andere Nachweise ersetzt werden können und diese Nachweismöglichkeiten beispielhaft aufzuzählen. Die Gemeinde hat mir mitgeteilt, daß der Vordruck „Antrag auf Beschränkung der Fehlbelegungsabgabe" überarbeitet und um die von mir angeregten Zusätze erweitert würde.

5.4.6 Architektenliste

Im Berichtszeitraum ist die Frage an mich herangetragen worden, ob und inwieweit die Erteilung einer Auskunft aus der für alle Architekten bei der Baukammer geführten Architektenliste, wie etwa Zeitpunkt der Eintragung, datenschutzrechtlichen Grundsätzen vereinbar sei.

In § 17 Abs. 2 des Baukammerngesetzes (BauKaG NW) ist bereichspezifisch geregelt, wer ein Recht auf Auskunft aus den Listen nach § 3 Abs. 1 sowie den nach § 6 Abs. 2 Satz 3 geführten Verzeichnissen hat. Diese Vorschrift

stellt keine abschließende bereichspezifische Regelung dar. Vielmehr ist darüber hinaus das DSG NW auch ohne einen ausdrücklichen Hinweis im Baukammerngesetz anwendbar, da § 17 Abs. 2 Satz 1 BauKaG NW die Möglichkeiten der Auskunfterteilung („jeder") gegenüber der entsprechenden Vorschrift des DSG NW erweitert und nicht einschränkt.

Eine Auskunft nach § 17 Abs. 2 Satz 1 BauKaG NW über die dort genannten Daten ist danach gleichsam voraussetzungslos und ohne Abwägung mit den schutzwürdigen Belangen der Betroffenen zulässig. Demgegenüber ist eine weitergehende Auskunft wie etwa Zeitpunkt der Eintragung in die Architektenliste nach den Vorschriften des DSG NW nur unter den dort genannten Voraussetzungen zulässig.

Je nach Empfänger der Übermittlung ist daher im jeweiligen Einzelfall zu prüfen, welche der Übermittlungsvorschriften der §§ 14 und 16 DSG NW einschlägig ist. Soweit etwa im Rahmen eines Rechtsstreits von einer Privatperson Auskünfte benötigt werden, kommt als Rechtsgrundlage § 16 Abs. 1 Buchstabe c DSG NW in Betracht. Danach wäre die Übermittlung personenbezogener Daten zulässig, wenn der Auskunftbegehrende ein rechtliches Interesse an der Kenntnis der Daten glaubhaft macht und kein Grund zu der Annahme besteht, daß das Geheimhaltungsinteresse der Betroffenen überwiegt. Die Entscheidung hierüber trifft im Einzelfall nach pflichtgemäßem Ermessen die Architektenkammer.

5.5 Rechtswesen

5.5.1 Datenschutz bei den Gerichtsvollziehern

Die Zwangsvollstreckung in EDV-Anlagen - Hard- und Software - nimmt offenbar in jüngster Zeit zu. Zu den damit verbundenen datenschutzrechtlichen Problemen habe ich in meinem 11. Tätigkeitsbericht (S. 32/33) insbesondere unter dem Aspekt Stellung genommen, ob den Gerichtsvollziehern nicht Hilfen für die **Zwangsvollstreckung in EDV-Anlagen** vom Justizministerium des Landes Nordrhein-Westfalen zur Verfügung gestellt werden müssen. Ohne bereits abschließend Stellung nehmen zu können, ist das Justizministerium der Auffassung, daß zunächst weitere Erfahrungen in der Praxis mit diesen Problemen abzuwarten seien. Der vom Justizministerium zu dieser Problematik eingeleitete Meinungsaustausch unter den Landesjustizverwaltungen ist noch nicht abgeschlossen.

Im Berichtszeitraum wurde weiter ein Fall bekannt, in dem Unterlagen eines Gerichtsvollziehers in Kartons gestapelt am Straßenrand von einem Bürger gefunden wurden. In diesem Zusammenhang habe ich gegenüber dem Präsidenten des Amtsgerichts darauf hingewiesen, daß auch hier die Vorschriften des § 10 DSG NW zu beachten sind. Der Präsident des Amtsgerichts hat darauf hingewiesen, daß sich die von dem Gerichtsvollzieher eigenverantwortlich durchzuführende Aufbewahrung und **Vernichtung von Akten** nach § 61 der Gerichtsvollzieherordnung (GVO) richtet. Danach hat der Gerichtsvollzieher die Akten nach Jahrgängen geordnet und so aufzubewahren, daß

jeder Mißbrauch, insbesondere eine Einsichtnahme durch Unberechtigte, ausgeschlossen ist.

Sonder- und Sammelakten sind von dem Gerichtsvollzieher fünf Jahre nach Erledigung des letzten in ihnen enthaltenen Vorgangs zu vernichten oder zur Vernichtung zu verkaufen. Die Vorschriften über die Vernichtung oder den Verkauf des ausgesonderten Schriftgutes bei den Justizbehörden gelten entsprechend. In der Regel soll der Gerichtsvollzieher seine vernichtungsreifen Sonder- und Sammelakten der Dienstbehörde zur gleichzeitigen Vernichtung mit gerichtlichen Akten überlassen. Ergänzend dazu hat der Präsident des Amtsgerichts eine Anordnung erlassen, wonach die ausgesonderten Schriftgute ausschließlich bei Gericht in der dafür vorgesehenen Aktenvernichtungsanlage zu vernichten sind. Die von mir entwickelte „Organisationshilfe zur Datensicherung beim Vernichten von Unterlagen (Organisationshilfe - Unterlagenvernichtung)" sei dabei berücksichtigt worden.

5.5.2 Aussonderung von Karteikarten der Zentralnamenkartei

Zur Frage der **Aufbewahrung von Schriftgut** der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden fehlt immer noch die erforderliche bereichspezifische Regelung in der Strafprozeßordnung. Die Dauer richtet sich bis heute nach den Aufbewahrungsbestimmungen, die durch Beschluß der Konferenz der Justizverwaltungen des Bundes und der Länder vom 23. und 24.11.1971 festgelegt und in der Folgezeit mehrfach überarbeitet wurden. Bei diesen Aufbewahrungsbestimmungen handelt es sich um Verwaltungsvorschriften, nicht um Rechtsnormen.

Auch die Aufbewahrung von Schriftgut greift in das informationelle Selbstbestimmungsrecht der in den Vorgängen erfaßten Personen ein. Nach den Ausführungen des Bundesverfassungsgerichts im Volkszählungsurteil sind Einschränkungen des Rechts auf informationelle Selbstbestimmung nur im überwiegenden Allgemeininteresse und auf Grund einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit und dem Grundsatz der Verhältnismäßigkeit entsprechen muß, möglich. Die bisherigen Entwürfe eines Strafverfahrensänderungsgesetzes sahen Regelungen über die Verarbeitung personenbezogener Daten in Dateien, nicht jedoch über die Dauer der Aufbewahrung von Schriftgut vor. Eine derartige Regelung ist jedoch ebenfalls erforderlich.

Gleichwohl wird die Anwendung der Aufbewahrungsbestimmungen im Hinblick auf die Grundsätze der Rechtsprechung des Bundesverfassungsgerichts zum sog. Übergangsbonus nicht generell für unzulässig erklärt werden können.

In einem Fall war trotzdem zu beanstanden, daß Daten im Zusammenhang mit einem abgeschlossenen Ermittlungsverfahren nicht gelöscht und die hiermit im Zusammenhang stehenden Unterlagen nicht vernichtet wurden.

Die Speicherung personenbezogener Daten in der Zentralnamenkartei der Staatsanwaltschaft und in der jeweiligen Ermittlungsakte ist stets als ein besonders schwerwiegender Eingriff zu qualifizieren. Hinsichtlich der Dauer der Speicherung wird nicht unterschieden zwischen überführten Tätern, Tatverdächtigen und Personen, deren Unschuld sich erwiesen hat. Die weitere Aufbewahrung der Ermittlungsakten über unschuldige Personen und die Speicherung ihrer Daten in Dateien der Staatsanwaltschaft über den gleichen Zeitraum wie die Daten der anderen Personengruppen ist somit nach der Rechtsprechung des Bundesverfassungsgerichts zum sog. Übergangsbonus unzulässig.

Zwar ist nicht zu verkennen, daß es, auch wenn sich als Ergebnis des Ermittlungsverfahrens die Unschuld eines zunächst Tatverdächtigen herausgestellt hat, der Staatsanwaltschaft möglich sein muß, über einen gewissen Zeitraum hin, eine ordnungsgemäße Sachbearbeitung dokumentieren zu können. Dies setzt allerdings eine Zweckbindung der Unterlagen als Dokumentation und eine Sperrung solcher Unterlagen und Daten für alle übrigen Aufgaben der Staatsanwaltschaft voraus. Nach einem Zeitraum von längstens zwei Jahren bei Erwachsenen und einem Jahr bei Minderjährigen dürfte auch diese Zweckbestimmung der gespeicherten Daten entfallen, und somit dürften die Unterlagen zu vernichten sowie die sonst gespeicherten Daten zu löschen sein (vgl. hierzu auch die Regelungen der Aktenordnung der Polizei).

5.5.3 Unbefugte Offenbarung durch Familiengerichte in Scheidungssachen

Aus der Sicht des Datenschutzes ist es als bedenklich einzustufen, wenn bei der Übersendung einer auszugsweisen Ausfertigung eines Urteils durch Amtsgerichte - Familiengericht - in einer Familiensache an die versorgungsausgleichspflichtige Beschäftigungsbehörde die Briefumschläge nicht besonders gekennzeichnet werden, so daß die sensiblen Daten jedermann zugänglich gemacht werden. Bei der Bearbeitung einer Eingabe ist mir die Praxis eines Amtsgerichts - Familiengericht - bekanntgeworden, wonach zur Wahrung des Datenschutzes die Briefumschläge, mit denen derartige Urteile übersandt werden, besonders gekennzeichnet werden. So wird durch einen Stempel „Vertraulich z. H. des Personalsachbearbeiters oder seines Vertreters" den Datenschutzbelangen Rechnung getragen.

Eine stichprobenartige Umfrage zu der Praxis anderer Amtsgerichte - Familiengericht - hat ergeben, daß zum Teil auch dort die Briefumschläge besonders gekennzeichnet werden, um den Datenschutzbelangen Rechnung zu tragen. Einige Amtsgerichte haben mein Anschreiben zum Anlaß genommen, künftig eine entsprechende Kennzeichnung vorzunehmen, bei weiteren Amtsgerichten erfolgte keine besondere Kennzeichnung und war auch für die Zukunft nicht vorgesehen. Die Problematik habe ich daraufhin an das Justizministerium des Landes Nordrhein-Westfalen herangetragen, damit bei

den einzelnen Amtsgerichten ein einheitliches Verfahren sichergestellt wird. Das Justizministerium hat mir auf meine Anfrage hin zunächst mitgeteilt, es werde um Stellungnahmen aus der gerichtlichen Praxis bitten.

Nach § 8 Ziffer 3 Abs. 4 der Geschäftsordnung für die Gerichte und Staatsanwaltschaften des Landes Nordrhein-Westfalen ist bei Schreiben an Arbeitgeber von Verfahrensbeteiligten, die personenbezogene Daten enthalten, auf dem Briefumschlag zu vermerken: „Vertrauliche Personalsache".

Zwischenzeitlich hat das Justizministerium durch Erlaß die Präsidenten der Oberlandesgerichte gebeten, das Erforderliche zu veranlassen, damit künftig einheitlich im Sinne des Datenschutzes verfahren wird.

5.5.4 Wertanfrage in Testaments- und Nachlaßsachen

Im Bereich der Justiz ist als datenschutzrechtlicher Fortschritt festzustellen, daß in einem Vordruck der Nachlaßgerichte, den Erben zur Ermittlung des Nachlaßwertes in Testaments- und Nachlaßsachen gegenüber dem Nachlaßgericht abgeben, ein Hinweis auf die Freiwilligkeit der Angaben aufgenommen wurde. Auf meine Empfehlung hin wurde der entsprechende Vordruck unter Hinweis auf § 4 DSG NW ergänzt.

5.5.5 Weitergabe von Fotos ohne Anonymisierung an die Presse

Einer Berichterstattung in der Presse war zu entnehmen, daß durch eine Staatsanwaltschaft Bilder von Drogenopfern aus staatsanwaltschaftlichen Unterlagen an eine Zeitung weitergeleitet worden waren. Die Datenübermittlung war im Hinblick auf die schutzwürdigen Belange des Betroffenen und seiner Angehörigen gemäß § 4 Abs. 2 Nr. 3 des Pressegesetzes für das Land Nordrhein-Westfalen (Landespressegesetz NW) unzulässig.

Es hat sich an diesem Fall gezeigt, daß es zur Wahrung der schutzwürdigen Belange der Betroffenen nicht ausreicht, dem Anliegen des die Fotos anfordernden Journalisten mit der Maßgabe zu entsprechen, die Zeitung werde (wohl) durch eigene Maßnahmen vor einer Veröffentlichung sicherstellen, daß die auf den Fotos abgebildeten Personen nicht zu erkennen sind. Die Opfer waren deutlich auf den Fotos in der Zeitung zu erkennen, sehr zum Leidwesen ihrer Angehörigen. Ich habe daher empfohlen, in derartigen Fällen künftig Fotos nur nach Anonymisierung durch die Justiz an die Presseorgane herauszugeben. Die Staatsanwaltschaft hat mitgeteilt, daß sie meiner Empfehlung folgt.

Nach meiner Auffassung wäre dieser Eingriff in die Datenschutzrechte der Angehörigen von Drogenopfern unterblieben, wenn entsprechend meiner Empfehlung (vgl. 11. Tätigkeitsbericht, S. 31/32) das Justizministerium des Landes Nordrhein-Westfalen die Richtlinien für die Zusammenarbeit mit der Presse überarbeitet hätte. Eine entsprechende Überarbeitung wurde seinerzeit als nicht erforderlich abgelehnt. Es bleibt abzuwarten, wieviele Fälle dieser Art notwendig sind, um die Haltung des Justizministeriums in dieser Frage zu ändern.

5.5.6 Ratenzahlungsantrag

Durch eine Eingabe bin ich auf den bei einer Staatsanwaltschaft verwandten Vordruck für die Beantragung von Ratenzahlung bei Geldstrafen aufmerksam gemacht worden, mit dem eine sehr umfangreiche Datenerhebung erfolgt. Obwohl die Betroffenen an Hand von Belegen oder Ablichtungen sämtliche Angaben nachzuweisen haben, haben sie sich von vornherein zusätzlich mit der Einholung von Auskünften beim zuständigen Arbeitsamt und ihrer Bank einverstanden zu erklären, obwohl fast nie die Notwendigkeit der Einholung solcher Auskünfte entsteht.

Die Staatsanwaltschaft hat in diesem Zusammenhang zu Recht darauf verwiesen, daß ein gestellter Ratenzahlungsantrag der sorgfältigen Prüfung bedarf, um die Geldstrafe in ihrem Wesen nicht zu verändern. Aber auch bei dieser Prüfung dürfen wesentliche Verfassungsgrundsätze wie der Grundsatz der Verhältnismäßigkeit, der Erforderlichkeit und der Wahl des mildesten Mittels nicht unberücksichtigt bleiben. Ich habe daher zur Vermeidung von Verstößen gegen Grundsätze des Datenschutzes empfohlen, von einer vorsorglichen Einholung des Einverständnisses abzusehen. Die Staatsanwaltschaft ist meiner Empfehlung gefolgt.

5.5.7 Geldwäsche

Datenschutzfragen haben sich bei der Anwendung des neuen Gesetzes über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz - GWG) vom 25. Oktober 1993 (BGBl. I S. 1770) ergeben. Mit diesem Gesetz besteht für Kredit- und Finanzinstitute sowie Spielbanken die Verpflichtung, unter bestimmten Voraussetzungen Finanztransaktionen den zuständigen Strafverfolgungsbehörden anzuzeigen (§ 11 GWG). Wie eine Erörterung unter den Datenschutzbeauftragten gezeigt hat, erfolgt die weitere Verarbeitung der mit den „Anzeigen" an die Strafverfolgungsbehörden übermittelten personenbezogenen Daten in den einzelnen Bundesländern unterschiedlich.

Datenschutzrechtlich bedenklich wäre es, wenn die „Anzeigen" nach § 11 GWG wie (normale) Anzeigen nach der Strafprozeßordnung behandelt und mit einem Js-Aktenzeichen versehen würden. Dies hätte zum Ergebnis, daß auch die Daten unbescholtener Bürger auf längere Zeit bei der Staatsanwaltschaft gespeichert werden und in den verschiedenen Informationssystemen der Justiz auf örtlicher, Landes- und Bundesebene auf Jahre dem Zugriff anderer Stellen ausgesetzt sind. Besonders bedenklich ist eine derartige Datenspeicherung, da diese Datensätze immer im Zusammenhang mit dem schwerwiegenden Vorwurf der Teilhabe an der Organisierten Kriminalität stehen.

Die datenschutzrechtliche Problematik würde nur unwesentlich entschärft, wenn statt des Js-Aktenzeichens ein AR-Aktenzeichen für derartige „Anzeigen" vergeben würde. Entsprechend dem Charakter dieser „Anzeigen" als Kontrollmitteilungen sollten eigene Aktenzeichen vergeben und ein eigenes Register angelegt werden. Erst wenn die Überprüfungen der Strafverfol-

gungsbehörden den Schluß der Institute und Spielbanken zu einem konkreten Verdacht verdichtet haben, könnten diese Daten in ein (normales) Js-Verfahren überführt werden. Dies hätte den entscheidenden Vorteil, daß die Daten unbescholtener Betroffener nach Überprüfung unverzüglich vollständig im Bereich der Strafverfolgungsbehörden gelöscht werden könnten.

Besondere datenschutzrechtliche Probleme ergeben sich auch im Polizeibereich, wenn jede „Anzeige" zum Anlaß genommen würde, die Daten in die Arbeitsdatei PIOS - Organisierte Kriminalität (APOK) einzuspeichern, auf die bundesweit zugegriffen werden kann.

Es bleibt abzuwarten, wie die Strafverfolgungsbehörden die Datenschutzrechte der zu Unrecht von derartigen „Anzeigen" betroffenen Bürger in Zukunft gewährleisten werden.

5.6 Polizei

5.6.1 Außen- und Medienkontakte

Aus Anlaß eines Einzelfalles habe ich bereits in meinem 10. Tätigkeitsbericht (S. 73/74) auf die Bedeutung des Persönlichkeitsschutzes bei der Weitergabe von personenbezogenen Daten durch die Polizei an die Medien hingewiesen.

Zu begrüßen ist, daß das Innenministerium des Landes Nordrhein-Westfalen inzwischen durch Runderlaß vom 10.3.1994 (MBl. NW. S. 437) die Zusammenarbeit der Polizei mit den Medien auch unter Berücksichtigung des Rechts auf informationelle Selbstbestimmung Betroffener neu geregelt und den sog. Presseerlaß vom 3.12.1963 aufgehoben hat. Meine Anregungen, in dem Erlaß auch Regelungen zur Wahrung des informationellen Selbstbestimmungsrechts Verstorbener, seien es Verkehrsopfer oder Opfer von Straftaten, aufzunehmen, wurden ebenso aufgegriffen, wie der Hinweis auf die Rechtslage nach § 29 DSG NW für den Fall, daß Personaldaten Gegenstand der Medienauskünfte werden.

5.6.2 KpS-Richtlinien

Auf die dringende Notwendigkeit der Überarbeitung der Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien) vom 10.2.1981 (MBl. NW. S. 192) habe ich bereits in meinem 11. Tätigkeitsbericht (S. 39 bis 41) hingewiesen. Leider ist es der Polizei auf der Bund-Länderebene nicht gelungen, einen bundesweit einheitlichen Entwurf zur Neufassung dieser Richtlinien vorzulegen.

In verschiedenen Bundesländern sind bereits unterschiedliche Richtlinien in Kraft getreten. Unter dem Gesichtspunkt der Wahrung des Rechts auf informationelle Selbstbestimmung kann dies nur als Rückschritt für die betroffenen Bürgerinnen und Bürger gewertet werden. Auch Nordrhein-Westfalen hat einen ersten Entwurf neuer KpS-Richtlinien vorgelegt. Von einer Stel-

lungnahme habe ich zunächst abgesehen, da mir eine Überarbeitung dieses Entwurfs zuvor angekündigt worden war.

Es bleibt zu hoffen, daß dieser neue Entwurf meine datenschutzrechtlichen Hinweise berücksichtigt, die ich als Ergebnis einer Reihe von Kontrollbesuchen bei Kreispolizeibehörden dem Innenministerium des Landes Nordrhein-Westfalen übermittelt habe. Der neue Entwurf wurde für Anfang 1995 angekündigt.

5.6.3 Praxis der Auskunftsverweigerung

Hinsichtlich der Rechtsansprüche Betroffener auf Auskunft über ihre bei der Polizei gespeicherten Daten haben die Ausführungen in meinem 11. Tätigkeitsbericht (S. 51/52) zwar zur Klarheit bei den Polizeibehörden beigetragen, daß die Auskunftserteilung die Regel, die Auskunftsverweigerung hingegen die Ausnahme sein muß. Vereinzelt wurde allerdings sodann der Ausnahmefall des § 18 Abs. 3 Buchstabe a DSG NW zur Begründung einer Auskunftsverweigerung durch die Polizei herangezogen, weil die Auskunftserteilung angeblich die polizeiliche Aufgabenerfüllung gefährde. Hinsichtlich der Auskunftserteilung aus Kriminalakten habe ich jedoch bisher bei meinen Überprüfungen in keinem Fall das Vorliegen der Voraussetzungen des § 18 Abs. 3 Buchstabe a DSG NW feststellen können, worüber mit den jeweiligen Polizeibehörden letztlich auch Einvernehmen erzielt wurde.

Im Zusammenhang mit der Verarbeitung personenbezogener Daten eines Betroffenen auf Grund bestimmter Präventionsmaßnahmen zur Verhinderung terroristischer Aktivitäten war demgegenüber die Begründung einer Polizeibehörde für die Auskunftsverweigerung nach § 18 Abs. 3 Buchstabe a DSG NW schlüssig und nach dem bei meinen Überprüfungen gewonnenen Erkenntnisstand nicht zu beanstanden.

In einem weiteren Fall hatte sich die auskunftsverweigernde Polizeidienststelle auf § 18 Abs. 5 DSG NW gestützt und sich auf die fehlende Zustimmung einer weiteren Polizeibehörde zur Auskunftserteilung berufen. Diese weitere, die Zustimmung verweigernde Polizeibehörde wollte in dem Verfahren nicht einmal als an der Datenverarbeitung beteiligte Stelle genannt werden. Sie unterlag jedoch nicht meiner Kontrollzuständigkeit, weshalb ich den Betroffenen zur weiteren Überprüfung seines Auskunftsanspruchs an die dafür zuständige Datenschutzkontrollinstanz habe verweisen müssen.

5.6.4 WE-Meldungen

Das Beratungsersuchen eines Polizeipräsidenten gab mir Anlaß, zu der schon im 10. Tätigkeitsbericht (S. 66) und 11. Tätigkeitsbericht (S. 49) aufgezeigten Praxis der Polizei, bei wichtigen Ereignissen eine Vielzahl von öffentlichen Stellen durch Meldungen zu informieren (sog. WE-Meldung), unter dem Gesichtspunkt der Verwertbarkeit für dienstrechtliche Maßnahmen Stellung zu nehmen. Sind nach dem Runderlaß des Innenministeriums des Landes Nordrhein-Westfalen über Meldungen wichtiger Ereignisse

- WE-Erlaß - vom 6.12.1991 (MBl. NW. 1992 S. 66) Straftaten von Polizeibeamten Gegenstand einer WE-Meldung, so ist der Regelungsbereich der Anordnung über Mitteilungen in Strafsachen (MiStra) bzw. des Justizmitteilungsgesetzes betroffen.

Die Verwertung nach dem WE-Erlaß übermittelter personenbezogener Daten zu dienstrechtlichen Zwecken hat sich, sofern die Voraussetzungen des § 29 DSG NW vorliegen, auf die Fälle zu beschränken, in denen ein Sachverhalt, der nicht in den Regelungsbereich der MiStra/des Justizmitteilungsgesetzes fällt, hierzu Anlaß gibt. Darüber hinaus wird für diese Datenverarbeitung eine (landes-)gesetzliche Regelung zu fordern sein.

Die bereits jetzt zu berücksichtigenden Zuständigkeiten und Befugnisse zu Mitteilungen in Strafsachen nach der MiStra, die eindeutig zu Gunsten des Gerichts oder der Staatsanwaltschaft geregelt sind, führen im Ergebnis dazu, daß selbst ein Oberkreisdirektor als Dienstvorgesetzter der Beschäftigten einer Selbstverwaltungskörperschaft Daten, die ihm in seiner Funktion als Leiter der Kreispolizeibehörde im Rahmen eines Strafverfahrens übermittelt worden sind, nicht ohne weiteres zum Zwecke der Durchführung eines Disziplinarverfahrens nutzen darf. Praktische Bedeutung erlangen diese Überlegungen, wenn ein Oberkreisdirektor als Leiter der Kreispolizeibehörde eine Strafanzeige vorgelegt bekommt, die gegen eine bei der Selbstverwaltungskörperschaft beschäftigte Person gerichtet ist.

Das Innenministerium des Landes Nordrhein-Westfalen teilt im Ergebnis meine Auffassung, daß für Auskünfte zu personenbezogenen Daten im Rahmen eines strafrechtlichen Ermittlungsverfahrens nicht die Polizei, sondern allein die Staatsanwaltschaft kraft ihrer Leitungsfunktion im Ermittlungsverfahren (vgl. § 152 Gerichtsverfassungsgesetz, §§ 161, 163 Strafprozeßordnung) zuständig ist. Demgemäß sehen auch die Nrn. 182 Abs. 2, 183, 185 Abs. 2 der Richtlinien für das Straf- und Bußgeldverfahren (RiStBV) vor, daß die Staatsanwaltschaft und nicht die Polizei zu entscheiden hat, ob anderen Behörden bei Vorliegen eines berechtigten Interesses Auskünfte aus dem Strafverfahren gegeben werden. Auch § 478 Abs. 1 Strafverfahrensänderungsgesetz 1994 (Stand: 14.10.1994) sieht die alleinige Zuständigkeit der Staatsanwaltschaft für die Auskunftserteilung aus Ermittlungsverfahren vor. Entsprechende Übermittlungsbefugnisse, allerdings auch nur für Gerichte und Staatsanwaltschaften, enthielt darüber hinaus § 13 des Entwurfs eines Justizmitteilungsgesetzes vom 31.8.1992 (Bundestagsdrucksache 12/3199). Daher ist auch ein Rückgriff auf die allgemeinen Übermittlungsvorschriften des Datenschutzgesetzes Nordrhein-Westfalen für eine Übermittlung durch Polizeibehörden im strafrechtlichen Ermittlungsverfahren nicht zulässig. Er würde zu einer Umgehung der staatsanwaltschaftlichen Zuständigkeit im Strafprozeß führen.

Daß in Eilfällen gleichwohl eine unmittelbare Information des Dienstvorgesetzten möglich ist, gewährleistet derzeit Nr. 29 MiStra. Sie sieht ebenso wie § 14 Abs. 4 des Entwurfs eines Justizmitteilungsgesetzes vor, daß

Dienstvorgesetzte zu informieren sind, wenn aus Sicht der Staatsanwaltschaft z. B. unverzüglich disziplinarrechtliche Entscheidungen oder andere Maßnahmen der Dienstvorgesetzten geboten sind. Es bleibt der Polizeibehörde daneben unbenommen, ihrerseits auf eine unverzügliche Entscheidung der Staatsanwaltschaft hinzuwirken, wenn aus Sicht der Polizei eine Datenübermittlung von der Staatsanwaltschaft an Dienstvorgesetzte zur Abwehr erheblicher Nachteile für das Allgemeinwohl für erforderlich erachtet wird. Liegen diese Voraussetzungen nicht vor, kommt die Erteilung von Auskünften erst nach Abschluß des Ermittlungsverfahrens in Betracht.

5.6.5 Erfolgskontrolle der polizeilichen Maßnahmen zur Verbrechensbekämpfung

In den vergangenen Jahren sind die Befugnisse der Polizei mehrfach nicht unerheblich erweitert worden. Verschiedene der gesetzlich geregelten und weitere geplante Maßnahmen sind mit Eingriffen in Grundrechte verbunden. Zu berücksichtigen ist in diesem Zusammenhang, daß der Einsatz immer neuer technischer Mittel den Kreis der Personen, die bei einer Störung oder Straftat nicht beteiligt sind, erheblich erweitert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf ihrer Sitzung am 26./27. September 1994 einen Beschluß über „Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen" gefaßt (vgl. Anlage 5, S. 175/176). Es bleibt zu hoffen, daß die geforderte rechtzeitige Beteiligung der Datenschutzbeauftragten in der Praxis auch tatsächlich realisiert wird.

5.7 Verfassungsschutz

5.7.1 Mitwirkung der Verfassungsschutzbehörden im Einbürgerungsverfahren

Das Verfassungsschutzgesetz Nordrhein-Westfalen enthält für die Einbürgerung durch Landesbehörden keine Regelung über die Mitwirkungsbefugnis des Innenministeriums als Verfassungsschutzbehörde. Eine geplante Bund-Länder-Abstimmung über eine einheitliche Verfahrensweise hinsichtlich der Beteiligung der Verfassungsschutzbehörden in Einbürgerungsangelegenheiten ist nach Mitteilung des Innenministeriums bislang nicht zustandegekommen. Ein vom Bayerischen Staatsministerium des Innern im Arbeitskreis IV der Innenministerkonferenz unternommener Vorstoß mit dem Ziel einer bundesweiten Wiedereinführung der sog. Regelanfrage (Beteiligung der Verfassungsschutzbehörden bei allen Einbürgerungsverfahren) sei bislang gescheitert.

In Nordrhein-Westfalen wird in den Fällen der Ermessenseinbürgerung regelmäßig eine Anfrage an die Verfassungsschutzabteilung des Innenministeriums gerichtet. In den Fällen der sog. Anspruchseinbürgerung hat dagegen eine Anfrage nur im Einzelfall zu erfolgen, wenn der Einbürgerungsbehörde selbst bereits konkrete Anhaltspunkte für eine mögliche Sicherheitsgefähr-

dung vorliegen. Die Beteiligung der Verfassungsschutzabteilung in den genannten Fällen ist nach Meinung des Innenministeriums des Landes Nordrhein-Westfalen nach dem derzeitigen Beurteilungsstand zur rechtmäßigen Aufgabenerfüllung der Einbürgerungsbehörden erforderlich. Hiergegen bestehen nach dem gegenwärtigen Erkenntnisstand im Ergebnis keine durchgreifenden datenschutzrechtlichen Bedenken.

5.7.2 Auskunfts- und Versendungspraxis

Aus gegebenem Anlaß habe ich mich mit der Frage der Versendungsart bei Positivauskünften im Bereich der Sicherheitsbehörden des Landes befaßt. So ist es bei mir in diesen und vergleichbaren Fällen gängige Praxis, derartige Mitteilungen zum Schutz vor unbefugtem Empfang als „Einschreiben-Eigenhändig" zu versenden, wenn ich das Auskunftsersuchen eines Betroffenen beantworte.

Im Gegensatz zu Verfassungsschutzbehörden einiger anderer Bundesländer hat sich das Innenministerium des Landes Nordrhein-Westfalen auf meine Anregung hin bereit erklärt, in Einzelfällen auf Wunsch der Auskunftsbegehrenden eine Versendung von Positivauskünften per „Einschreiben-Eigenhändig" zu veranlassen.

5.8 Sozialwesen

5.8.1 Automatisierter Datenabgleich zwischen Sozialamt und Straßenverkehrsamt

Großes Aufsehen in der Öffentlichkeit erregte der Oberstadtdirektor der Stadt Aachen dadurch, daß sein Sozialamt zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe die Identifikationsdaten sämtlicher Hilfeempfänger aus der Sozialhilfeempfänger-Datei an das Straßenverkehrsamt zwecks Abgleichs mit der dortigen Datei und Rückmeldung der Eigenschaft als Kraftfahrzeughalter sowie des amtlichen Kennzeichens und des Fahrzeugstatus übermittelt hatte.

Der Oberkreisdirektor des Kreises Neuss hatte seine kommunale Datenverarbeitungszentrale beauftragt, im Wege des automatisierten Datenabgleichs der Sozialhilfeempfänger-Dateien der kreisangehörigen Kommunen mit der Kraftfahrzeughalter-Datei des Kreises Listen mit Familiennamen, Geburtsdatum sowie der Eintragung als Kraftfahrzeughalter, amtlichem Kennzeichen und ggf. Stillegungsdatum zu erstellen und an die jeweils zuständige Kommune zwecks Auswertung zu übermitteln.

In beiden Fällen mußte ich die Durchführung des automatisierten Datenabgleichs förmlich beanstanden.

Die Träger der Sozialhilfe sind befugt, zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe Daten von Personen, die Leistungen nach diesem Gesetz beziehen, bei anderen Stellen ihrer Verwaltung, bei ihren wirtschaftlichen Unternehmen und bei den Kreisen, Kreisverwaltungsbehörden

und Gemeinden zu überprüfen, soweit diese für die Erfüllung ihrer Aufgaben erforderlich sind. Sie dürfen für die Überprüfung Name, Vorname, Geburtsdatum, Geburtsort, Nationalität, Geschlecht, Anschrift und Sozialversicherungsnummer übermitteln, um folgende Daten zu überprüfen:

a) Geburtsdatum und -ort;

b) Personen- und Familienstand;

c) Wohnsitz;

d) Dauer und Kosten von Miet- oder Überlassungsverhältnissen von Wohnraum;

e) Dauer und Kosten von bezogenen Leistungen über Elektrizität, Gas, Wasser, Fernwärme oder Abfallentsorgung;

f) Eigenschaft als Kraftfahrzeughalter.

Die ersuchten Stellen sind verpflichtet, diese Daten zu übermitteln (§ 117 Abs. 3 Satz 1 bis 4 BSHG).

Mit dieser Regelung war die Vorgehensweise der beiden Sozialhilfeträger nicht vereinbar. Eine Überprüfung von Personen, die Leistungen nach dem Bundessozialhilfegesetz beziehen, im Wege des - auch regelmäßigen - automatisierten Datenabgleichs ist den Trägern der Sozialhilfe ausdrücklich untereinander sowie bei der Bundesanstalt für Arbeit und bei den Trägern der gesetzlichen Renten- oder Unfallversicherung gestattet (§ 117 Abs. 1 und 2 BSHG). Diese Regelung ermöglicht den Trägern der Sozialhilfe, die in Betracht kommenden Daten aller Sozialhilfeempfänger pauschal und ohne Anhaltspunkte für eine rechtswidrige Inanspruchnahme von Sozialhilfe an die genannten Stellen zu übermitteln, damit diese den automatisierten Datenabgleich durchführen und die Daten über den festgestellten Leistungsbezug an die Träger der Sozialhilfe übermitteln.

Demgegenüber ist eine Überprüfung zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe durch die Träger der Sozialhilfe bei anderen Stellen ihrer Verwaltung erlaubt, soweit die zu überprüfenden Daten für die Erfüllung ihrer Aufgaben erforderlich sind. Der Erforderlichkeit begriffsimmanent ist die Einzelfallbezogenheit. Wenn also der Gesetzgeber die Überprüfung der Eigenschaft als Kraftfahrzeughalter an die Erforderlichkeit bindet, so hat er damit eine **Überprüfung nur im Einzelfall** (oder in einer Mehrzahl von Einzelfällen) zulassen wollen. Insoweit hat er den Regelungsgehalt des § 117 Abs. 3 BSHG signifikant gegenüber dem Regelungsgehalt der Absätze 1 und 2 dieser Vorschrift abgegrenzt. Denn eine wahllose Überprüfung sämtlicher Sozialhilfeempfänger im Wege des automatisierten Datenabgleichs, wie sie in den Absätzen 1 und 2 zugelassen ist, und eine **Erforderlichkeitsprüfung**, wie sie Absatz 3 verlangt, schließen einander aus. Dementsprechend hat der Gesetzgeber den automatisierten Datenabgleich in den Absätzen 1 und 2 - folgerichtig - nicht an eine Erforderlichkeitsprü-

fung gebunden und - wiederum folgerichtig - in Absatz 3 den automatisierten Datenabgleich nicht vorgesehen.

Soweit aus der Kraftfahrzeughalter-Datei dem Sozialamt auch das amtliche Kennzeichen, der Fahrzeugstatus und ggf. das Stillegungsdatum übermittelt worden sind, geht dies über das allein zu prüfende Datum „Eigenschaft als Kraftfahrzeughalter" hinaus.

Das Bundesministerium für Familie und Senioren hat in einer vom Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen erbetenen Stellungnahme den automatisierten Datenabgleich der Sozialhilfeträger mit den Stellen ihrer eigenen Verwaltung für zulässig befunden und stellte dabei allein auf den „ausdrücklichen Zweck der möglichsten Verhinderung von Mißbrauch" ab. Die gesetzliche Regelung enthalte keine Einschränkung, daß ein Datenabgleich nur im Einzelfall zulässig sei. Aus gutem Grunde sei auch offengelassen, ob ein Datenabgleich bei einem einzelnen Sozialhilfeempfänger oder bei einer Gruppe von Sozialhilfeempfängern erfolge. Beides müsse möglich sein. Auch die Größe und Zusammensetzung einer solchen Gruppe bis hin zu der Frage, ob die Gesamtheit aller Sozialhilfeempfänger überprüft werden kann, hänge von einer Prüfung der Voraussetzungen vor Ort ab. Überdies wäre es nicht verständlich, die auf Grund der prekären öffentlichen Haushaltslage erforderlichen Einsparungen auch in der Sozialhilfe zu Lasten aller Sozialhilfeempfänger vorzunehmen und gleichzeitig unredliche Sozialhilfeempfänger durch Untätigkeit zu belohnen.

Das Bundesministerium für Familie und Senioren hat den Grundrechtscharakter des Datenschutzes sowie die daraus folgende Eingriffsqualität der Datenverarbeitung verkannt und ist infolgedessen von einem falschen Ansatz ausgegangen: Nicht das Verbot des Eingriffs in das informationelle Selbstbestimmungsrecht bedarf der gesetzlichen Legitimation, sondern umgekehrt der Eingriff selbst. Daraus folgt, daß der Gesetzgeber, wenn er eine Überprüfung nach § 117 Abs. 3 BSHG im Wege des automatisierten Datenabgleichs hätte zulassen wollen, dies - ebenso wie in den Absätzen 1 und 2 dieser Vorschrift geschehen - ausdrücklich hätte regeln müssen.

Im Gegensatz zur Auffassung des Bundesministeriums für Familie und Senioren kann eine generelle, nicht am Einzelfall orientierte Bejahung der Erforderlichkeit nicht dem Rechtsanwender vor Ort überlassen bleiben; diese Entscheidung muß vielmehr der Gesetzgeber selbst treffen. Die Verwaltung ist gehalten, das Gesetz so anzuwenden, wie es ist, und nicht so, wie es ihr wünschenswert erscheint, um die „auf Grund der prekären öffentlichen Haushaltslage erforderlichen Einsparungen" zu erzielen.

Das Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen, das in der Stellungnahme des Bundesministeriums für Familie und Senioren keinen Beitrag zur Klärung der Rechtslage sah, hat mit Erlaß vom 21. März 1994 in Übereinstimmung mit meiner Rechtsauffassung die nachgeordneten Behörden darauf hingewiesen, daß es eine Datenüberprüfung im Rahmen des § 117 Abs. 3 BSHG nur dann für zulässig hält, wenn

im Einzelfall der Verdacht einer rechtswidrigen Inanspruchnahme von Sozialhilfeleistungen besteht.

Der Oberstadtdirektor der Stadt Aachen hat inzwischen mitgeteilt, daß er sich entsprechend der vom Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen für maßgeblich erklärten Rechtsauffassung verhalten werde. Damit ist er letztlich meiner Empfehlung gefolgt.

Den Oberkreisdirektor des Kreises Neuss, der mir auf die Beanstandung hin mitgeteilt hatte, er beabsichtige, künftig einen quantitativ reduzierten Datenabgleich durchzuführen, bei dem von vornherein gewisse Personengruppen auf Grund bestimmter Merkmale außer acht bleiben sollen, habe ich darauf hingewiesen, daß die Durchführung eines automatisierten Datenabgleichs schlechthin der Gesetzeslage widerspricht. Inzwischen hat mir der Oberkreisdirektor mitgeteilt, daß beabsichtigt sei, über seinen kommunalen Spitzenverband das zuständige Bundesministerium zu bitten, sich für eine Änderung des § 117 Abs. 3 BSHG einzusetzen. Daraus schließe ich, daß der Oberkreisdirektor meiner Empfehlung, den vorgesehenen reduzierten Datenabgleich nicht durchzuführen, folgen wird. Andere Träger der Sozialhilfe, die ebenfalls einen reduzierten Datenabgleich erwogen oder schon durchgeführt hatten, sind meiner Empfehlung, davon abzusehen bzw. einen solchen Abgleich nicht zu wiederholen, ausdrücklich gefolgt.

5.8.2 Auszahlung von Sozialleistungen an Empfänger ohne Bankverbindung

Ein Bürger beschwerte sich darüber, daß er gezwungen war, gegenüber dem Geldinstitut die Tatsache des Bezuges von Sozialhilfe sowie Art und Zeitraum der Leistung zu offenbaren. Der Betroffene hatte keine Bankverbindung und konnte die Auszahlung der ihm gewährten Hilfe nur „unter Vorlage des Bescheides" erlangen, aus dem die o. g. Daten ersichtlich waren.

Zwar findet eine Offenbarung durch den Leistungsträger hier nicht statt, weil der Bescheid nicht vom Leistungsträger, sondern von dem Betroffenen selbst dem Geldinstitut vorgelegt wird. Aus der Verpflichtung des Leistungsträgers zur Wahrung des Sozialgeheimnisses kann jedoch ein Anspruch des Betroffenen hergeleitet werden, bei der Auszahlung von Sozialleistungen an Empfänger ohne Bankverbindung ein Verfahren zu wählen, das den Betroffenen nicht zwingt, sich **selbst** als Sozialhilfeempfänger **zu offenbaren**. Nach meiner Auffassung würde es für die Auszahlung des Leistungsbetrages ausreichen, wenn dem Geldinstitut nur die Stadt (nicht das Sozialamt) als anweisende Stelle, der Auszahlungsbetrag, der Berechtigte und allenfalls noch ein anonymisiertes Aktenzeichen bekannt wird. Meiner entsprechenden Empfehlung wurde gefolgt.

5.8.3 Vereinfachte Zustellung durch Leistungsträger

Ein Oberstadtdirektor machte bei der vereinfachten Zustellung auf dem Postzustellungsauftrag neben der Anschrift des Betroffenen sowie der absen-

denden Behörde und deren Geschäftsnummer auch Angaben zum Inhalt des Schriftstücks wie z. B. „Mitt. § 91 III BSHG" und führte den Namen des Hilfeempfängers auf.

Da eine gesetzliche Befugnis zur Offenbarung gegenüber Dritten, wie z. B. den Postbediensteten, nicht ersichtlich war, hatte ich empfohlen sicherzustellen, daß künftig Postzustellungsaufträge (ggf. auch Postzustellungsurkunden) keine Angaben zum Inhalt des zuzustellenden Schriftstücks und nicht den Namen des Hilfeempfängers enthalten. Der Oberstadtdirektor hielt die Angaben zur eindeutigen Identifizierung des Schriftstücks zunächst für erforderlich, ließ sich aber dann doch davon überzeugen, daß dies auch auf andere Weise, jedenfalls **ohne Offenbarung von Sozialdaten** geschehen kann.

5.8.4 Pflicht zur Unterrichtung des Datenempfängers über die Unrichtigkeit offenbarter Daten

Ein Bürger beschwerte sich darüber, daß ein Stadtdirektor Angaben zum Bezug/Nichtbezug von Sozialhilfeleistungen sowie den melde- und ausländerrechtlichen Status des Betroffenen, die zudem nicht zutreffend seien, an das Arbeitsamt offenbart hatte. Der Stadtdirektor wandte ein, die Daten seien erst nach Übermittlung durch ihn von den zuständigen Dienststellen ihm gegenüber korrigiert worden, so daß er keine unzutreffenden Daten übermittelt habe.

Sowohl das Sozialamt als auch das Arbeitsamt sind Leistungsträger, die, wenn es zur Aufgabenerfüllung des jeweils anderen erforderlich ist, personenbezogene Daten austauschen dürfen. So ist es für die Aufgabenerfüllung des Arbeitsamtes nach dem Arbeitsförderungsgesetz erforderlich, darüber unterrichtet zu sein, ob der Betroffene Leistungen nach dem Bundessozialhilfegesetz erhält, ob er gemeldet ist oder ob er eine Aufenthaltserlaubnis hat. Allerdings hätte das Sozialamt, nachdem es von der Unrichtigkeit der in seinen Akten vorhandenen Daten über den melde- und ausländerrechtlichen Status des Betroffenen erfahren hatte, im Wege der gebotenen **Folgenbeseitigung** nicht nur die eigenen Akten korrigieren, sondern im Hinblick auf die gegenüber dem Arbeitsamt bereits erfolgte Offenbarung dieses über die Unrichtigkeit der Daten informieren müssen, damit das Arbeitsamt auch die eigenen Akten berichtigen konnte. Meiner Empfehlung, entsprechend zu verfahren, wird gefolgt.

5.8.5 „Antrag auf Sozialhilfe"

Im Zusammenhang mit Fragen zur Durchführung der Sozialhilfestatistik (vgl. unten 5.11.2) wies mich ein Sozialhilfeträger darauf hin, daß der vom Landkreistag überarbeitete Vordruck „Antrag auf Sozialhilfe" neuerdings die Frage nach dem **Schulabschluß** und dem **Berufsabschluß** vorsieht.

Nach Auskunft des Landkreistages ist die Frage nach dem Schulabschluß und dem Berufsabschluß deshalb in den Vordruck aufgenommen worden, weil

diese Angabe für die Hilfe zur Wiedereingliederung in das Berufsleben (§ 19 BSHG) erforderlich sei.

Hierzu ist festzustellen, daß eine solche Datenerhebung nicht **generell** erfolgen darf, sondern nur soweit die Angabe für die Aufgabenerfüllung nach § 19 BSHG **im Einzelfall** erforderlich ist. Immerhin birgt die Verwendung des Antragsvordrucks, der keinen Hinweis auf die Rechtsgrundlage für die Erhebung dieser Angaben enthält, die Gefahr in sich, daß nach Schulabschluß und Berufsabschluß schematisch, d. h. ohne konkrete Prüfung der Erforderlichkeit auch in allen übrigen Fällen gefragt wird und die Betroffenen, die die Rechtslage nicht überblicken, nicht zuletzt wegen des ausdrücklichen Hinweises auf ihre Mitwirkungspflicht schematisch antworten.

Hieraus folgt, daß die Fragen zum Schulabschluß und Berufsabschluß, weil sie nicht in allen Fällen erforderlich sind, mit einem Hinweis versehen werden müssen, unter welchen Voraussetzungen diese Fragen zu beantworten sind, damit es nicht zu einer Datenerhebung im Übermaß kommt. **Keinesfalls** wäre es zulässig, diese Angaben - sozusagen im Wege der Datenerhebung auf Vorrat - in allen Fällen zu verlangen, um der Auskunftspflicht des Sozialhilfeträgers im Rahmen der **Sozialhilfestatistik** zu genügen.

Ich habe daher empfohlen, entweder - wie bisher - davon abzusehen, die Angaben zum Schulabschluß und Berufsabschluß mittels Vordrucks zu erheben, oder den Vordruck mit einem Hinweis zu versehen, unter welchen Voraussetzungen diese Fragen zu beantworten sind.

5.8.6 Anforderung von Fremdberichten durch das Versorgungsamt

Ein niedergelassener Arzt fragte bei mir an, ob er verpflichtet sei, dem Versorgungsamt im Rahmen eines Verfahrens der Kriegsopferversorgung auf Anforderung nicht nur die von ihm selbst erstellten Patientenunterlagen, sondern auch Berichte anderer Ärzte, von Krankenhäusern, Sanatorien und Kureinrichtungen aus jüngerer Zeit (nicht älter als fünf Jahre) zu übersenden. Das Versorgungsamt stützte sein Begehren auf den Umstand, daß der Antragsteller alle beteiligten Ärzte von der Schweigepflicht entbunden hatte.

Nach dem Gesetz über das Verwaltungsverfahren der Kriegsopferversorgung (KOV-VfG) kann die Verwaltungsbehörde von privaten Ärzten, die den Antragsteller oder Versorgungsberechtigten behandeln oder behandelt haben, Auskünfte einholen und Untersuchungsunterlagen zur Einsicht beiziehen. Indem diese Vorschrift ausdrücklich auf **behandelnde** Ärzte abhebt, kann ihr bei verständiger Würdigung nur die Befugnis entnommen werden, Unterlagen mit Angaben über den Betroffenen auf dessen Wunsch oder mit seinem Einverständnis von **dem** Arzt beizuziehen, der sie auf Grund eigener Behandlung selbst erstellt hat. Aus der genannten Vorschrift ergibt sich auch nicht andeutungsweise, daß die behandelnden Ärzte berechtigt oder gar verpflichtet sind, Unterlagen, die ihnen von anderen Ärzten, Krankenhäusern usw. für einen bestimmten Zweck (etwa Weiterbehandlung) zur Verfügung gestellt wurden, an das Versorgungsamt für dessen Aufgabenerfüllung zu

übermitteln, zumal der ersuchte Arzt verantwortlich nur über die Herausgabe seiner eigenen Unterlagen entscheiden kann, weil nur insoweit ein Behandlungsverhältnis zwischen ihm und dem Betroffenen besteht.

Hinzu kommt, daß das **pauschale Ersuchen** des Versorgungsamts gegenüber dem behandelnden Arzt um Beifügung der Berichte anderer Ärzte usw. von der dem Antragsteller abverlangten Einverständniserklärung, die auf die **erforderlichen** Auskünfte und Unterlagen abstellt, insofern nicht gedeckt ist, als dem Versorgungsamt nicht bekannt ist, über welche Unterlagen der ersuchte Arzt verfügt, es also nicht weiß, ob die verlangten Unterlagen (Fremdberichte) für die konkrete Aufgabenerfüllung erforderlich sind. Damit ist das Gebot der vorgehenden Erforderlichkeitsprüfung verletzt.

Ich habe dem Versorgungsamt empfohlen, davon abzusehen, von behandelnden Ärzten Unterlagen, die diese nicht selbst erstellt haben, anzufordern.

5.8.7 Interessenkonflikt bei Sozialarbeitern

Ein Sozialarbeiter hat meinen Rat erbeten, weil er der Ansicht war, daß die ihm zugewiesenen Aufgaben miteinander nicht vereinbar seien. So sah er sich z. B. in dem Konflikt, für Stellungnahmen, die er gegenüber dem Sozialamt abzugeben hatte, auf Daten zurückgreifen zu müssen, die ihm im Rahmen seiner Aufgabenerfüllung nach dem Kinder- und Jugendhilfegesetz **persönlich anvertraut** worden waren und die deshalb dem in diesem Gesetz ausdrücklich normierten besonderen Vertrauensschutz unterlagen.

Der hier aufgezeigte Konflikt erscheint mit datenschutzrechtlichen Mitteln nur schwer lösbar. Dabei ist zu bedenken, daß nach Artikel 28 Abs. 2 des Grundgesetzes den Gemeinden das Recht gewährleistet sein muß, alle Angelegenheiten der örtlichen Gemeinschaft im Rahmen der Gesetze in eigener Verantwortung zu regeln. Dies bedeutet, daß die Gemeinden die Organisationshoheit innehaben und damit auch das Recht, die Erfüllung der von ihnen wahrzunehmenden Aufgaben ihren Bediensteten selbst zuzuweisen.

Allerdings dürfen die Gemeinden dabei den aus dem informationellen Selbstbestimmungsrecht folgenden, ebenfalls im Grundgesetz verankerten Persönlichkeitsschutz nicht außer acht lassen. Daraus folgt nach meiner Auffassung die Verpflichtung der Gemeinden, die einzelnen Sachgebiete ihren Mitarbeitern so zuzuordnen, daß es nicht durch Aufgabenkumulierung zu Inkompatibilitäten und Interessenkonflikten kommt, die die Gefahr einer unzulässigen Datennutzung auf Grund der bestehenden Personalunion in sich bergen. Auf den vorliegenden Fall bezogen würde dies bedeuten, daß der Sozialarbeiter wegen der ihm auferlegten Verpflichtung zur Wahrung des besonderen Vertrauensschutzes Stellungnahmen für das Sozialamt zu Sachverhalten, die ihm auf Grund seiner Zuständigkeit im Rahmen des Kinder- und Jugendhilfegesetzes persönlich anvertraut sind, nicht abgeben

könnte. Hieraus ergibt sich die Unvereinbarkeit der Erledigung beider Aufgaben durch eine und dieselbe Person.

5.8.8 Blindenbefragung

Durch eine Betroffene erfuhr ich davon, daß ein Landschaftsverband eine Blindenbefragung mit der Zielsetzung durchführte, herauszufinden, durch welche Maßnahmen die berufliche Integration von Blinden verbessert werden kann. Mit dieser Untersuchung hatte der Landschaftsverband das Institut für angewandte Sozialwissenschaft - INFAS - beauftragt.

Durch die Hauptfürsorgestelle wurde allen 3 300 Blindengeldempfängern im erwerbsfähigen Alter eine Tonkassette zugeschickt, auf der die vorgesehene Blindenbefragung und deren Zweck vorgestellt, auf die Freiwilligkeit hingewiesen und um Teilnahme gebeten wurde. Für den Fall, daß die Betroffenen nicht bereit waren, an der Befragung teilzunehmen, wurden sie aufgefordert, den Landschaftsverband unter einer bestimmten Telefonnummer anzurufen und dabei auf einem Anrufbeantworter ihren Widerspruch kundzutun. Bevor sie die Möglichkeit wahrnehmen konnten, den Widerspruch zu erklären, hörten die Betroffenen folgenden Text:

> „Hier ist der Anrufbeantworter der Blindenbefragung. Wenn Sie wirklich nicht mitmachen wollen, ich wiederhole, wenn Sie nicht mitmachen wollen, nennen Sie langsam und deutlich Ihren Namen und Ihre Adresse und den Grund, weshalb Sie nicht mitmachen wollen."

Die Namen und Adressen aller Betroffenen, die telefonisch nicht widersprochen hatten, wurden an INFAS übermittelt, das seinerseits nach dem Zufallsprinzip eine Auswahl von Personen traf, die dann kontaktiert wurden. Vor Durchführung des Interviews sei ihnen, wie der Landschaftsverband vorträgt, eine Einverständniserklärung vorgelesen worden, aus der die Alternative hervorgehe, an der Befragung teilzunehmen oder sie abzulehnen.

Diesen Vorgang habe ich förmlich beanstandet.

Zwar können, soweit erforderlich, personenbezogene Daten für die Planung im Sozialleistungsbereich durch eine öffentliche Stelle im Rahmen ihrer Aufgaben offenbart werden. Die Offenbarung ist jedoch nicht zulässig, soweit es zumutbar ist, die Einwilligung des Betroffenen einzuholen (§ 75 Abs. 1 SGB X a. F.).

Hier war es schon deshalb zumutbar, vor der Datenoffenbarung gegenüber INFAS die **Einwilligung** der Betroffenen einzuholen, weil die Mitwirkung der Betroffenen Voraussetzung für die Durchführung des Projekts ist. In allen Fällen, in denen die Betroffenen an der Untersuchung mitwirken sollen, ist es auch zumutbar, sie um ihr Einverständnis in die Datenoffenbarung zu bitten (so ausdrücklich Walz in Borchert/Hase/Walz, Rdnr. 65 zu § 75 SGB X; Hauck/Haines, Rdnr. 28 zu § 75 SGB X). Dies muß insbesondere dann gelten, wenn der Leistungsträger - wie hier - lediglich über die dem Sozial-

geheimnis unterliegenden Identifikationsdaten (Namen und Anschrift) der potentiellen Interviewpartner verfügt, aber die für das Planungsprojekt substantiellen Informationen, die erst durch Interview bei den Betroffenen mit Teilnahmebereitschaft erhoben werden sollen, nicht kennt und deshalb auch nicht offenbaren könnte. Aus diesem Grunde ist auch die Fortführung der Kommentierung bei Hauck/Haines (a.a.O.), wonach etwas anderes gilt, wenn der Rückgriff auf die Einwilligung dazu führen kann, daß das Forschungsvorhaben nicht mehr repräsentativ ist, für den hier vorliegenden Fall nicht einschlägig. Der Landschaftsverband kann mit der Offenbarung von Namen und Anschriften der Blindengeldempfänger zur Repräsentativität des Planungsvorhabens nichts beitragen; allein entscheidend ist letztlich die Teilnahmebereitschaft der Betroffenen. Es steht ihnen jederzeit frei, sich einem Interview zu stellen oder dies abzulehnen, was auch der Landschaftsverband nicht in Zweifel zieht.

Soweit der Landschaftsverband das informationelle Selbstbestimmungsrecht der Betroffenen durch die Möglichkeit, der Datenoffenbarung gegenüber INFAS zu widersprechen, als gewahrt ansah, weil ein Widerspruch angesichts des betroffenen Personenkreises das am ehesten geeignete Mittel zur Wahrnehmung des Persönlichkeitsrechts sei, ist ihm entgegenzuhalten, daß das Gesetz eine solche Möglichkeit nicht vorsieht, sondern ausdrücklich die Einwilligung verlangt, soweit deren Einholung zumutbar ist. Diese gesetzlichen Vorgaben stehen nicht zur Disposition des Rechtsanwenders, dem es folglich verwehrt ist, nach eigenem Gutdünken das ihm „am ehesten geeignete Mittel" (hier: Widerspruchslösung) für die Wahrnehmung des informationellen Selbstbestimmungsrechts durch die Betroffenen zu bestimmen; er hat das Gesetz so anzuwenden, wie es ist. Im übrigen wird die Unzulässigkeit der Datenoffenbarung gegenüber INFAS nicht etwa dadurch „geheilt", daß INFAS selbst vor Durchführung des Interviews die Einwilligung der Betroffenen eingeholt hat.

Hinzu kommt, daß gegen den Text auf dem Band des Anrufbeantworters der Blindenbefragung erhebliche Bedenken bestehen. Hier wird durch die gewählte Formulierung in ihrer durch Wiederholung verstärkten Eindringlichkeit auf die Entscheidung der an sich zur Nichtteilnahme entschlossenen Betroffenen Einfluß zu nehmen versucht. Dies kann sich für die Betroffenen durchaus als Hemmschwelle auswirken, die noch erhöht wird durch die - überdies unzulässige - Frage nach dem Grund des „Nichtmitmachenwollens", so daß sich die Betroffenen **unter Druck gesetzt** fühlen könnten, ihren Namen nicht preiszugeben mit der Folge, daß der Landschaftsverband von der Teilnahmebereitschaft ausgeht. Ein derart tendenziöses, nicht neutrales Vorgehen begründet erhebliche Zweifel an der Freiwilligkeit der - bereits mangels rechtswirksamer Einwilligung - unzulässigen Befragung.

Das Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen hat inzwischen den Landschaftsverband darauf hingewiesen, daß es meine Rechtsauffassung bei zukünftigen Entscheidungen über eine Genehmigung im Rahmen des § 75 SGB X berücksichtigen werde, und ihn

gebeten, bei zukünftigen Untersuchungsvorhaben, die der Forschung und Planung in Durchführung des Schwerbehindertengesetzes dienen sollen, meine Rechtsauffassung ebenfalls zu beachten.

5.8.9 Offenbarung des zweiten Arbeitgebers bei Mehrfachbeschäftigung

Eine Innungskrankenkasse (IKK) fragte bei mir an, ob es zulässig sei, in dem Bescheid bzw. Widerspruchsbescheid zur Feststellung der Versicherungspflicht im Falle einer Zweitbeschäftigung eines geringfügig Beschäftigten dem Arbeitgeber Name und Anschrift **des jeweils anderen Arbeitgebers** zu offenbaren.

Zu den durch das Sozialgeheimnis geschützten Angaben gehören auch Name und Anschrift des Arbeitgebers, der der Einzugsstelle geringfügig Beschäftigte zu melden hat. Eine Offenbarung ist daher nur zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe der IKK nach dem Sozialgesetzbuch erforderlich ist.

Mehrere geringfügige Beschäftigungen sind zusammenzurechnen, d. h. daß sich die Versicherungspflicht bzw. -freiheit auf Grund der Zusammenrechnung der wöchentlichen Arbeitszeiten und der Arbeitsentgelte aus mehreren geringfügig entlohnten Beschäftigungen beurteilt (§ 8 Abs. 2 SGB IV). Die Einzugsstelle entscheidet über die Versicherungspflicht und die Beitragshöhe in der Kranken- und Rentenversicherung sowie über die Beitragspflicht und Beitragshöhe nach dem Arbeitsförderungsgesetz; sie erläßt auch den Widerspruchsbescheid (§ 28 h Abs. 2 Satz 1 SGB IV).

Erstbescheid und Widerspruchsbescheid stellen jeweils einen Verwaltungsakt dar, der schriftlich zu begründen ist. In der Begründung sind die wesentlichen tatsächlichen und rechtlichen Gründe mitzuteilen, die die Behörde zu ihrer Entscheidung bewogen haben (§ 35 Abs. 1 Satz 2 SGB X). Die Verwaltungsakte sind hier ausreichend begründet, wenn dem Arbeitgeber die Tatsache des Bestehens einer Zweitbeschäftigung sowie der Umfang (Zeit, Stundenzahl und/oder Entgelt) der jeweils anderen Beschäftigung mitgeteilt wird. Die Angabe des Namens und der Anschrift des anderen Arbeitgebers ist zur Aufgabenerfüllung der Einzugsstelle nach dem Sozialgesetzbuch, wenn überhaupt, so keinesfalls im Widerspruchsverfahren erforderlich und deshalb unzulässig.

Allerdings hat das Sozialgericht Münster in einer Entscheidung von 3.3.1993 - S 9 Kr 46/91 - einen entsprechenden Bescheid einer Krankenkasse wegen Fehlens der Angabe über den zweiten Arbeitgeber, also wegen unzureichender Begründung, aufgehoben. Diese Entscheidung kann schon deshalb nicht überzeugen, weil das Gericht ohne Begründung als „selbstverständlich" davon ausgegangen ist, daß es zur Nachvollziehbarkeit durch den von dem Verwaltungsakt betroffenen Arbeitgeber gehöre, diesem den anderen Arbeitgeber genau zu benennen. Im übrigen befindet sich die von mir

vertretene Rechtsauffassung in Übereinstimmung mit einem Urteil des Sozialgerichts Gießen vom 1.7.1992 - S 9 Kr 429/91 -.

5.8.10 Verwendung von Versichertenanschriften durch die AOK bei Ausdehnung einer BKK

Eine BKK beabsichtigte, ihre Zuständigkeit auf ein Zweigwerk ihres Trägerunternehmens auszudehnen. Die bis dahin zuständige AOK versuchte, ihre Versicherten in der Belegschaft vor der Entscheidung über den Beitritt zur BKK zu beeinflussen, indem sie ihnen Postkarten, Briefe und Werbegeschenke übersandte und sie durch ihre Außendienstmitarbeiter in ihrer Wohnung aufsuchen ließ.

Wenn die AOK gezielt diejenigen Versicherten anschreibt oder aufsucht, die von der Ausdehnung der BKK betroffen sind, so verwendet sie dafür aus ihren Datenbeständen Adresse und Arbeitgeber ihrer Mitglieder für **Werbezwecke**. Krankenkassen dürfen ihre Versichertendaten nur für die im Gesundheitsstrukturgesetz enumerativ aufgeführten Zwecke der Krankenversicherung verwenden; eine Verwendung für andere Zwecke muß durch Rechtsvorschriften des Sozialgesetzbuchs ausdrücklich angeordnet oder erlaubt sein (§ 284 Abs. 1 und 3 SGB V).

Zu den im Gesetz genannten Zwecken der Krankenversicherung gehört die Mitgliederwerbung im Hinblick auf die beabsichtigte Ausdehnung der BKK nicht. Eine Verwendung von Versichertendaten zu einem derartigen Zweck ist auch nicht durch Rechtsvorschriften des Sozialgesetzbuchs angeordnet oder erlaubt. Insbesondere kann eine solche Verwendung weder auf die dem Leistungsträger obliegende Aufklärungspflicht (§ 13 SGB I) noch auf den Beratungsanspruch der Versicherten (§ 14 SGB I) gestützt werden.

Die Leistungsträger haben die Bevölkerung über die Rechte und Pflichten nach dem Sozialgesetzbuch aufzuklären. Adressat der Aufklärung ist „die Bevölkerung", also die Allgemeinheit. Damit handelt es sich insoweit zwangsläufig um eine generelle, nicht um eine auf den einzelnen Versicherten abgestellte individuelle Information.

Eine Verpflichtung zur gezielten individuellen Beratung ergibt sich allerdings aus dem Beratungsanspruch des Versicherten. Dabei muß jedoch die Initiative von dem Versicherten ausgehen, indem er seinen Anspruch auf Beratung gegenüber seiner Krankenkasse geltend macht und diese um Beratung ersucht. Die Krankenkasse darf dem Versicherten keine Beratung aufdrängen, indem sie ihn gezielt anschreibt oder aufsucht, um ihm einen Überblick über das breitgefächerte Leistungsangebot der AOK, das ihm im übrigen bekannt sein dürfte, zu vermitteln und den Versicherten über die Vorgänge im Zusammenhang mit der beabsichtigten Ausdehnung der BKK zu unterrichten. Aus den gleichen Gründen kann die AOK ihr Vorgehen auch nicht auf den Auskunftsanspruch des Versicherten über alle sozialen Angelegenheiten nach dem Sozialgesetzbuch (§ 15 SGB I) stützen.

Meiner Empfehlung, künftig von der Verwendung der Versichertendaten für Mitgliederwerbung abzusehen, ist die AOK nicht gefolgt. Sie widerspricht meiner Auffassung, daß die Initiative zur Beratung vom Versicherten ausgehen muß. § 14 SGB I enthalte keine Aussage, wie die Beratung einzuleiten sei.

Diesem Einwand ist entgegenzuhalten, daß § 14 SGB I einen **Anspruch** des Versicherten auf Beratung normiert. Daraus folgt, daß die Beratung - abgesehen von den Fällen einer Beratungspflicht aus Anlaß eines (Leistungs-)Antrages nach dem Grundsatz von Treu und Glauben - nicht von Amts wegen erfolgt, sondern einen Antrag des Ratsuchenden voraussetzt (so ausdrücklich Schnapp in Bochumer Kommentar zum SGB, Allg. Teil, § 14 Rdnr. 8 unter Hinweis auf die Rechtsprechung des Bundessozialgerichts). Zudem steht nach meiner Auffassung ein Beratungsbedarf der Versicherten hier nicht im Vordergrund; vielmehr verfolgt die AOK ersichtlich ihr eigenes Interesse an der Erhaltung ihres Mitgliederbestandes. Die Verfolgung derartiger **kassenpolitischer Ziele** ist aber durch den Normzweck des § 14 SGB I nicht gedeckt.

5.8.11 Verletzung des Sozialgeheimnisses durch eine unzuständig gewordene Krankenkasse

Nach Gründung einer Betriebskrankenkasse hat die vorher zuständige AOK ihr irrtümlich zugegangene Arbeitsunfähigkeitsbescheinigungen und andere Unterlagen mit Diagnosen trotz eines Hinweises durch die Betriebskrankenkasse wiederholt **unmittelbar** an deren **Trägerunternehmen** übersandt.

Auf diese Weise wurden sensible, dem Sozialgeheimnis unterliegende Versichertendaten dem Arbeitgeber unbefugt offenbart. Erst nachdem ich die AOK auf den fortgesetzten Verstoß gegen das Sozialgeheimnis hingewiesen und für den Wiederholungsfall die sofortige förmliche Beanstandung angekündigt hatte, wurde der Mißstand abgestellt.

5.8.12 Erfassung von Versichertendaten eigens für Forschungszwecke

Durch ein Beratungsersuchen des Landesversicherungsamtes ist mir bekanntgeworden, daß eine AOK für ein externes Forschungsvorhaben die bei ihr vorhandenen Rezepte und Krankenscheine versichertenbezogen auswertete und dabei Daten erfaßte, die dann anonymisiert an die Forschergruppe weitergegeben wurden. Das Landesversicherungsamt hatte hiergegen Bedenken, weil auch Daten erfaßt wurden, die für die Erfüllung **kasseneigener Aufgaben nicht erforderlich** waren. Hierbei handelte es sich um das Produkt auf den Rezepten sowie um die Diagnose auf den Krankenscheinen ausgewählter Versicherter.

Die AOK darf Versichertendaten nur erheben und erfassen, soweit dies für die im Gesetz enumerativ genannten Zwecke erforderlich ist (§ 284 Abs. 1 SGB V a. F.). Da die Erfassung des Produkts und der Diagnose durch die

AOK keinem dieser Zwecke zuzuordnen und eine Erfassung von Versichertendaten eigens für Forschungszwecke in der genannten Vorschrift nicht vorgesehen ist, ist die Datenerfassung unzulässig.

Zwar darf die AOK mit Erlaubnis der Aufsichtsbehörde die Datenbestände leistungserbringer- und fallbeziehbar für zeitlich befristete und im Umfang begrenzte Forschungsvorhaben, insbesondere zur Gewinnung epidemiologischer Erkenntnisse, von Erkenntnissen über Zusammenhänge zwischen Erkrankungen und Arbeitsbedingungen oder von Erkenntnissen über örtliche Krankheitsschwerpunkte, selbst auswerten (§ 287 SGB V a. F.). Diese Voraussetzungen liegen hier aber nicht vor. Zum einen wertet hier die AOK nicht selbst Datenbestände aus, dies besorgt vielmehr die Forschergruppe, so daß es sich nicht um Eigenforschung der AOK, sondern um Fremdforschung handelt, wobei unbeachtlich ist, daß die AOK aus dieser Forschung womöglich auch selbst (z. B. für die ihr obliegende Qualitätssicherung) Nutzen zieht. Zum anderen wäre die AOK gehalten, im Rahmen ihrer Eigenforschung nur solche Datenbestände auszuwerten, die sie für ihre Aufgabenerfüllung nach § 284 Abs. 1 SGB V a. F. zulässigerweise erfaßt hat. Die Aufgabe der Eigenforschung gestattet der AOK nicht, allein hierfür Datenbestände zu schaffen, die sie für ihre Aufgabenerfüllung nach § 284 Abs. 1 SGB V nicht benötigt. Wenngleich § 287 Abs. 1 SGB V nur „die Datenbestände" nennt, so können hierunter bei verständiger und gesetzessystematischer Auslegung nur solche Datenbestände verstanden werden, die die AOK für ihre Aufgabenerfüllung **rechtmäßig** erfaßt hat. Somit ist § 287 Abs. 1 SGB V in Anknüpfung an § 284 Abs. 1 SGB V a. F. mit den ungeschriebenen, weil als selbstverständlich vorausgesetzten Tatbestandsmerkmalen „die **rechtmäßig erfaßten** Datenbestände" zu lesen. An ebendiese Voraussetzungen ist, und zwar ausdrücklich, eine Zweckänderung gebunden (§ 284 Abs. 3 SGB V a. F.). Auch nach dieser Vorschrift dürfen nur die „rechtmäßig erfaßten" Daten für andere Zwecke nach Maßgabe des Sozialgesetzbuchs verwendet werden.

Nichts anderes gilt nach dem am 1. Juli 1994 in Kraft getretenen Zweiten Gesetz zur Änderung des Sozialgesetzbuchs, wobei ich erhebliche Zweifel habe, ob hier für eine Beurteilung der Nutzung des fraglichen Datenbestandes nach neuem Recht überhaupt Raum sein kann, da doch dieser Datenbestand unzulässigerweise erfaßt worden ist. Die Anwendbarkeit der hier allenfalls in Betracht kommenden Vorschrift des § 67 c Abs. 2 Nr. 3 SGB X scheitert schon daran, daß die durch diese Vorschrift legitimierte Datenverarbeitung unter der ausdrücklichen - im übrigen selbstverständlichen - Prämisse steht, daß die zu verarbeitenden Daten zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden gesetzlichen Aufgaben erforderlich sind. Ebendies ist, wie oben dargelegt, hier nicht der Fall, denn sowohl das Produkt auf dem Rezept als auch die Diagnose auf dem Krankenschein ist für die gesetzliche Aufgabenerfüllung der AOK nicht erforderlich.

Meiner Empfehlung, den fraglichen Datenbestand unverzüglich zu löschen, ist die AOK entsprechend einer Bitte des Ministeriums für Arbeit, Gesund-

heit und Soziales des Landes Nordrhein-Westfalen bislang nicht gefolgt. Sie hat mir jedoch versichert, daß die Daten unter Verschluß gehalten werden, so daß jegliche Nutzung ausgeschlossen sei. Die AOK werde nur dann bereit sein, die Daten für eine Auswertung freizugeben, wenn alle datenschutzrechtlichen Bedenken hiergegen ausgeräumt sind.

Im Hinblick auf diese Erklärung sehe ich derzeit von einer förmlichen Beanstandung ab.

5.8.13 Überprüfung des Kindergeldanspruchs

Auf Grund der Bestimmungen des Artikels 5 des 1. Gesetzes zur Umsetzung des Spar-, Konsolidierungs- und Wachstumsprogramms hatten die für die Zahlung von Kindergeld an Angehörige des öffentlichen Dienstes zuständigen Stellen in einer Sonderaktion bei allen Beziehern von Kindergeld die Voraussetzungen für das Weiterbestehen eines Kindergeldanspruchs ab 1. Januar 1994 zu überprüfen. Hierfür verwandte das Landesamt für Besoldung und Versorgung (LBV) auf Weisung des Finanzministeriums des Landes Nordrhein-Westfalen einen Vordruck, der vom Bundesministerium für Familie und Senioren zusammen mit dem Bundesministerium des Innern den Ländern im Rahmen der Bundesauftragsverwaltung vorgegeben worden war. In dem Vordruck wurde u. a. zur Abfrage des Kindschaftsverhältnisses die Unterscheidung „leibliches Kind, **Adoptivkind**, Pflegekind" vorgenommen.

Eine derartige differenzierte Angabe ist im Hinblick auf die rechtliche Gleichstellung von leiblichen und Adoptivkindern nach § 1754 BGB für die Erfüllung der gesetzlichen Aufgabe der Kindergeldstelle nicht erforderlich. Zudem ist der Betroffene nicht verpflichtet und kann deswegen auch nicht dazu angehalten werden, das **Adoptionsgeheimnis** preiszugeben. Die zahlungsbegründenden Voraussetzungen können durch eine nach § 62 Abs. 2 des Personenstandsgesetzes auszustellende Geburtsurkunde nachgewiesen werden, in der als Eltern nur die Annehmenden angegeben werden.

Da der Versand der Vordrucke und zum großen Teil auch deren Rücklauf bereits erfolgt war, kam weder eine Korrektur noch eine nachträgliche Information der Befragten in Betracht. Das Finanzministerium hat jedoch im Hinblick auf meine Bedenken mit Runderlaß vom 9. Juni 1994 das LBV angewiesen, in den Fällen, in denen Kindergeldberechtigte ihr Adoptivkind als leibliches Kind bezeichnet haben, auf weitere Nachfragen zu verzichten und, soweit ein Adoptivkindschaftsverhältnis erstmalig offengelegt wurde, diese Information nicht aktenkundig zu machen bzw. - soweit bereits erfolgt - wieder zu löschen. Anfragen betroffener Bediensteter zur Notwendigkeit der Angabe eines Adoptivkindschaftsverhältnisses seien in diesem Sinne zu beantworten.

5.9 Gesundheitswesen

5.9.1 Fragen zum Gesundheitsdatenschutzgesetz

Im Zusammenhang mit der Anwendung des neuen Gesundheitsdatenschutzgesetzes (GDSG NW) sind eine Reihe von Auslegungsfragen an mich herangetragen worden.

- So sah ein im Sozialpsychiatrischen Dienst tätiger Arzt bei der Anwendung der **Akteneinsichtsvorschrift** (§ 9 GDSG NW) Schwierigkeiten für seine praktische Arbeit. Insbesondere wollte er wissen, wie der Begriff „subjektive Daten und Aufzeichnungen im Rahmen der Behandlung" (§ 9 Abs. 3 GDSG NW) zu verstehen sei und ob die Akteneinsichtsvorschrift überhaupt den Sozialpsychiatrischen Dienst des Gesundheitsamtes erfasse, da im Gesundheitsamt üblicherweise keine Behandlungen, sondern Untersuchungen, Befunderhebungen und gutachterliche Stellungnahmen erfolgen. Außerdem war dem Arzt unklar, ob er einem Patienten trotz unverhältnismäßiger Beeinträchtigung der Gesundheit Akteneinsicht über die objektiven physischen Befunde und Berichte über Behandlungsmaßnahmen zu erteilen habe und ob mit dem Begriff „Maßnahmen" nur solche im Sinne von § 9 PsychKG gemeint seien.

  Indem § 2 Abs. 1 Nr. 2 GDSG NW allgemein und undifferenziert von „Maßnahmen auf Grund des Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (PsychKG)" spricht, ist der Begriff „Maßnahmen" im umfassenden Sinne zu verstehen, also nicht auf Maßnahmen des Gesundheitsamtes nach § 9 PsychKG beschränkt, sondern umfaßt die gesamte Tätigkeit des Gesundheitsamtes auf der Grundlage des PsychKG.

  Nach § 9 Abs. 3 GDSG NW können subjektive Daten und Aufzeichnungen im Rahmen der Behandlung nach ärztlichem Ermessen zurückgehalten werden. Dieser Vorschrift liegt ersichtlich die Rechtsprechung des BGH (NJW 1983, 328 bis 330) zur Einsicht des Patienten in die von seinem behandelnden Arzt im Rahmen des Vertragsverhältnisses gefertigten Krankenunterlagen zugrunde. Danach braucht der behandelnde Arzt, der seine Tätigkeit auf privatrechtlich-vertraglicher Grundlage ausübt, in den Krankenunterlagen dokumentierte persönliche Eindrücke und Motive, die emotional gefärbt sein mögen und subjektive Wertungen (z. B. Verdachtsdiagnosen) enthalten, dem Patienten nicht zu offenbaren.

  Diese Rechtsprechung läßt sich jedoch auf die Situation im Gesundheitsamt nicht übertragen. Hier tritt der Arzt dem Patienten (Klienten) nicht als Partner eines privatrechtlichen Behandlungsvertrages, sondern als Verwaltungsbeamter im Rahmen eines außervertraglichen, öffentlich-rechtlichen Rechtsverhältnisses gegenüber, indem er eben nicht behandelt, sondern Aufgaben der Eingriffsverwaltung (z. B. Gefahrenabwehr) oder Leistungsverwaltung (z. B. Gesundheitsberatung) wahrnimmt oder amtliche Bescheinigungen, Zeugnisse und Gutachten erstellt.

In diesem Bereich bleibt es daher bei dem grundsätzlich uneingeschränkten Einsichtsrecht des Patienten (Klienten) in die beim Gesundheitsamt über ihn geführten Akten (§ 9 Abs. 1 GDSG NW). Beim Gesundheitsamt ist es lediglich gerechtfertigt, das Akteneinsichtsrecht zum Schutz höherwertiger Interessen Dritter einzuschränken, wie dies in § 9 Abs. 4 GDSG NW geregelt ist. Allerdings enthält § 9 Abs. 2 letzter Halbsatz GDSG NW eine Beschränkung des Akteneinsichtsrechts der Personen im Sinne von § 2 Abs. 1 Nr. 2. Diese Beschränkung, wenngleich als Entscheidung des Gesetzgebers gegen das informationelle Selbstbestimmungsrecht für die gesetzanwendende Verwaltung bindend, widerspricht indes der Rechtsprechung des Bundesverwaltungsgerichts: „Besteht bei dem Patienten keine akute Selbstmordgefahr und ist seine freie Willensentschließung nicht beeinträchtigt, so gibt es keine verfassungsrechtliche Legitimation dafür, die Handlungsfreiheit des Betroffenen in dessen eigenem Interesse einzuschränken" (Urteil vom 27.4.1989; NJW 1989, 2960).

Nach der dieser Rechtsprechung zuwiderlaufenden Regelung in § 9 Abs. 2 letzter Halbsatz GDSG NW hat der Patient zwar **kein Recht** auf Akteneinsicht und dementsprechend der Arzt keine Verpflichtung zur Gewährung von Akteneinsicht. Dessenungeachtet kann allerdings der Arzt **nach eigenem Ermessen**, das nur durch die vom Bundesverwaltungsgericht (a.a.O.) markierten Ausnahmefälle eingeschränkt ist, auch einer Person im Sinne von § 2 Abs. 1 Nr. 1 GDSG NW Einsicht in die **von ihm selbst erstellten** (vgl. § 23 Abs. 3 GDSG NW) Aufzeichnungen gewähren.

Von der Ausnahme des § 9 Abs. 2 letzter Halbsatz GDSG NW abgesehen, ist dem Patienten - allerdings unter Beachtung des § 23 Abs. 3 GDSG NW- „auf Verlangen uneingeschränkt Auskunft zu erteilen und Akteneinsicht zu gewähren", d. h. der Patient braucht sich nicht mit einer Vermittlung des Akteninhalts durch einen Arzt (§ 9 Abs. 2 Satz 2 GDSG NW) zu begnügen und kann sogar das Zurückbehaltungsrecht des Arztes (§ 9 Abs. 2 Satz 3 GDSG NW) mit seinem Recht auf **uneingeschränkte** Akteneinsicht überspielen.

- Amtsärzte baten um Beratung, inwieweit das Gesundheitsdatenschutzgesetz es zuläßt, bei Erstellung eines Gutachtens auf Daten zurückzugreifen, die bei **früheren Untersuchungen** des Patienten erhoben worden sind.

Sind begutachtende und voruntersuchende Stelle **identisch**, so handelt es sich nicht um einen Übermittlungsvorgang, sondern um **Nutzung** früherer Untersuchungsergebnisse. Hierfür existiert eine bereichspezifische Befugnisnorm im Gesundheitsdatenschutzgesetz nicht. Deshalb gelten nach der Subsidiaritätsklausel des § 3 GDSG NW in diesen Fällen die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen.

Gesetzliche Grundlage für die Nutzung von Daten aus früheren Untersuchungen ist § 13 DSG NW. Danach ist ein Rückgriff des Gutachters auf derartige Daten bei Zweckidentität ohne weiteres zulässig. Dies gilt insbesondere dann, wenn beide Untersuchungen in einem sachlichen Zusammenhang stehen. Dienen die Untersuchungen jedoch unterschiedlichen Zwecken, so verbietet sich grundsätzlich ein Rückgriff auf im Gesundheitsamt bereits vorhandene Daten, es sei denn, es liegt eine der im Gesetz ausdrücklich geregelten Voraussetzungen für die Durchbrechung des Zweckbindungsgebots vor (§ 13 Abs. 2 DSG NW).

Sind begutachtende und voruntersuchende Stelle **unterschiedliche** Abteilungen des Gesundheitsamtes, so gilt die Weitergabe von Patientendaten aus der früheren Untersuchung an den Gutachter als Übermittlung, die sich nach §§ 5 Abs. 1, 23 Abs. 2 GDSG NW richtet, also, soweit der Betroffene nicht eingewilligt hat, nur zulässig ist, wenn sie zur Erfüllung einer gesetzlichen Pflicht erforderlich ist, eine Rechtsvorschrift sie erlaubt oder die Übermittlung zur Abwehr einer gegenwärtigen Gefahr für Leben, körperliche Unversehrtheit oder persönliche Freiheit des Betroffenen oder eines Dritten erforderlich ist. Diese Voraussetzungen dürften bei einem Rückgriff auf Daten aus früheren Untersuchungen in der Regel nicht vorliegen.

Somit bleibt festzuhalten, daß - von seltenen Ausnahmefällen abgesehen - eine Verwendung von Daten aus früheren Untersuchungen nur bei **Zweckidentität** zulässig ist. Insofern bleibt es also bei dem Gebot der informationellen Gewaltenteilung mit der Folge, daß die Führung von **Gesamtakten unzulässig** ist. Die Aktenführung hat je nach Aufgabe und Untersuchungszweck getrennt zu erfolgen. Eine „Gedächtnisauffrischung" durch Beiziehung alter Vorgänge ist nicht gestattet.

- Ein Krankenhausarzt fragte an, ob es nach dem Gesundheitsdatenschutzgesetz zulässig sei, Krankenakten für eine **Qualitätskontrolle** der pneumologischen Patientenversorgung an externe Gutachter zu übersenden.

  Die Übermittlung von Patientendaten durch ein Krankenhaus richtet sich nach § 5 Abs. 1 Satz 1 i.V.m. § 11 GDSG NW. Danach ist die Übermittlung nur zulässig, soweit sie zur Erfüllung einer gesetzlichen Pflicht erforderlich ist, eine Rechtsvorschrift sie erlaubt oder der Betroffene im Einzelfall eingewilligt hat (§ 5 Abs. 1 Satz 1 GDSG NW). Diese Voraussetzungen waren hier nicht erfüllt. Auch die Spezialvorschrift des § 11 GDSG NW deckt die Versendung von Patientenakten an die Gutachter nicht. § 11 Abs. 2 GDSG NW gestattet für die Qualitätssicherung lediglich den **krankenhausinternen Zugriff** auf Patientendaten, wobei zusätzlich die Anonymisierung vorgeschrieben ist, soweit dadurch der Verwendungszweck nicht gefährdet wird.

  Somit konnte die Versendung von Patientenakten an die externen Gutachter im Rahmen der geplanten Qualitätskontrolle nur mit Einwilligung der betroffenen Patienten im Einzelfall erfolgen. Die Einwilligung be-

durfte der Schriftform (§ 4 Abs. 1 Satz 1 GDSG NW). Dabei waren die Betroffenen in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten sowie über die Empfänger der Daten aufzuklären (§ 3 GDSG NW i.V.m. § 4 Satz 4 DSG NW) und auf die Freiwilligkeit - am besten durch drucktechnische Hervorhebung - deutlich hinzuweisen.

5.9.2 Berichtigung von Daten in ärztlichen Unterlagen

In mehreren Eingaben wandten sich Betroffene gegen die in ärztlichen Unterlagen über sie festgehaltenen Daten.

So war ein Patient der Ansicht, daß ein anläßlich seiner Behandlung über ihn gefertigter Vermerk die von ihm im Zusammenhang mit seiner Erkrankung gemachten Mitteilungen in beleidigender Form entstellt wiedergab.

Da es sich bei dem Vermerk um die handschriftliche Wiedergabe eines **ersten Eindrucks** von dem Patienten bei der Aufnahme handelte und letztlich im **Arztbericht** die endgültige diagnostische Zuordnung erfolgt, sich aber dort die entsprechenden Passagen nicht wiederfanden, war die Klinik bereit, den Vermerk aus der Akte zu entfernen und dem Patienten auszuhändigen. Damit waren die Daten in der Krankenakte gelöscht und eine Berichtigung gegenstandslos.

Daß in der Krankenakte eine Empfangsbestätigung über die Aushändigung des Vermerks verbleibt, ist datenschutzrechtlich unbedenklich, da die Empfangsbestätigung weder unrichtige Angaben enthält noch Rückschlüsse auf den Inhalt des Vermerks zuläßt.

Hingegen konnte dem Begehren eines anderen Patienten, die in der Krankenakte von Internisten festgehaltene psychiatrische Verdachtsdiagnose sowie andere gegenüber den Ärzten gemachte Äußerungen nicht medizinischer Art zu berichtigen bzw. zu löschen, nicht entsprochen werden.

Die Aufzeichnung der (Verdachts-)Diagnose war nach Auffassung der Klinik zur Dokumentation des Krankheitsverlaufs aus medizinisch-internistischer Sicht unumgänglich und somit im Rahmen der **ärztlichen Dokumentationspflicht** geboten. Aber auch die Aufzeichnung der nicht medizinischen Äußerungen des Patienten sei notwendig, weil hierdurch offenkundig geworden sei, daß das **Vertrauensverhältnis** zwischen dem Betroffenen und seinen behandelnden Ärzten zerstört sei. Die ärztliche Dokumentationspflicht gebiete es, diese Tatsache und die hierfür ausschlaggebenden Gründe in den klinischen Unterlagen festzuhalten.

Anhaltspunkte dafür, daß hier die Grenzen einer angemessenen ärztlichen Dokumentation überschritten sind und damit der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz verletzt ist, ergeben sich danach nicht. Jeder approbierte Arzt gilt - auch über sein Fachgebiet hinaus - als fachlich qualifiziert und befugt, eine Diagnose zu stellen. Deshalb kann einem Internisten, der gelegentlich der fachärztlichen Untersuchung eine psychiatrische Dia-

gnose stellt, nicht entgegengehalten werden, ihm fehle von vornherein die Kompetenz für einen Verdacht auf eine solche Erkrankung. Daraus folgt, daß ein Löschungsanspruch insoweit nicht besteht. Etwas anderes könnte allenfalls dann gelten, wenn nachgewiesen würde, daß die Diagnose ohne den geringsten tatsächlichen Anhaltspunkt allein als verärgerte Reaktion auf Unzuträglichkeiten und Auseinandersetzungen geäußert wurde.

Im übrigen ist jeder Arzt auf Grund der Approbation zur Ausübung der Heilkunde ohne Einschränkung berechtigt. Zwar darf, wer eine Gebietsbezeichnung (z. B. Internist) führt, grundsätzlich nur in diesem Gebiet tätig werden. Dies bedeutet aber nicht, daß der Arzt Feststellungen, die über sein Gebiet hinausgehen, unterdrücken, also den Patienten in seinem Fachgebiet gleichsam „einsperren" muß. Vielmehr ist dem behandelnden Arzt die Äußerung einer Verdachtsdiagnose auch über sein Fachgebiet hinaus nicht verwehrt. Ein solcher Arzt handelt sogar pflichtgemäß im Interesse des Patienten.

5.9.3 Heilpraktikerüberprüfung

Durch Eingaben wurde mir bekannt, daß Gesundheitsämter in einem Vordruck für die Zulassung zur Heilpraktikerüberprüfung von dem Antragsteller mit dem Hinweis, daß für die Bearbeitung des Zulassungsantrages die vollständige Beantwortung aller Fragen erforderlich sei, u. a. folgende Angaben verlangen:

- Es handelt sich bei dieser Bewerbung um einen Erstantrag.
- Ich habe bereits an einer Heilpraktikerüberprüfung im Bundesgebiet ohne Erfolg teilgenommen, ja/nein; wenn ja, Zeitpunkt und Ort der Überprüfung.

Eine gesetzliche Grundlage für die Erhebung dieser Angaben ist nicht vorhanden. Insbesondere können hier die Vorschriften des Gesundheitsdatenschutzgesetzes keine Anwendung finden, weil es dem Gesundheitsamt schon an einer Aufgabe fehlt, zu deren Erfüllung die Erhebung dieser Daten erforderlich ist.

Nach dem Heilpraktikergesetz in Verbindung mit der Ersten Durchführungsverordnung zu diesem Gesetz bedarf der Heilpraktiker zur Ausübung der Heilkunde der Erlaubnis, die dann nicht erteilt wird, wenn sich aus einer Überprüfung der Kenntnisse und Fähigkeiten des Antragstellers durch das Gesundheitsamt ergibt, daß die Ausübung der Heilkunde durch den Betreffenden eine Gefahr für die Volksgesundheit bedeuten würde. Dieser Regelung ist auch nicht andeutungsweise zu entnehmen, daß das Gesundheitsamt die Aufgabe hat, sich darüber zu informieren, wie oft und wo ein Heilpraktiker an einer Heilpraktikerüberprüfung im Bundesgebiet teilgenommen hat.

Diese Information ist für die Erfüllung der Aufgabe, wie sie im Heilpraktikergesetz und in der dazu ergangenen Ersten Durchführungsverordnung normiert ist, irrelevant, weil sie keine Erkenntnisse über die **gegenwärtigen**

„Kenntnisse und Fähigkeiten des Antragstellers" vermittelt. Relevant könnte diese Information insofern sein, als sie geeignet wäre, psychologische Hemmschwellen aufzubauen, die den Heilpraktiker abschrecken, sich mehrmals einer Überprüfung zu unterziehen. Die mehrmalige Teilnahme an einer Heilpraktikerüberprüfung zu verhindern - und sei es durch psychologische Einflußnahme auf die Bewerber -, sprengt jedoch den gesetzlich gesteckten Rahmen und bedeutet eine Aufgabenerweiterung, die einer gesetzlichen Regelung, etwa in einer **Prüfungsordnung**, die die Häufigkeit der Teilnahme an einer Heilpraktikerüberprüfung bestimmt, vorbehalten bleiben muß.

Die öffentliche Verwaltung - insonderheit als Eingriffsverwaltung - kann nicht, und zwar auch nicht im Wege einer sog. „Übergangsregelung" ihre Aufgaben selbst, etwa durch Erlaß beliebig festlegen; sie sind ihr vielmehr im Hinblick auf das Verfassungsgebot der Gesetzmäßigkeit der Verwaltung (Artikel 20 Abs. 3 GG) durch Gesetz zuzuweisen. Fehlt es hieran, ist kein Raum für eine Datenverarbeitung - und sei es mit Einwilligung des Betroffenen; einer Einwilligung zumal, die hier der Beschaffung von Daten dient, deren Verwendung dem Betroffenen nicht etwa zum Vorteil, sondern zum Nachteil (Stigmatisierungseffekt) gereicht, weil bei deren Kenntnis die Gefahr eines Objektivitätsverlustes besteht. Dies könnte dazu führen, daß dem Bewerber nicht unvoreingenommen begegnet wird, er also in seinen Chancen von vornherein beeinträchtigt ist. Hinzu kommt die Gefahr, daß sich der Bewerber bei Verweigerung der Information dem Verdacht aussetzt, bereits einmal an einer Heilpraktikerüberprüfung teilgenommen zu haben. Hier die Einwilligung einzuholen, liefe selbst bei Aufklärung über alle diese Umstände auf eine **Pervertierung** des Rechtsinstituts **der Einwilligung** hinaus. Ich habe daher empfohlen, von der Erhebung abzusehen.

Im Hinblick darauf, daß sich die Gesundheitsämter auf einen Erlaß des Ministeriums für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen beriefen, habe ich das Ministerium, dessen Erlaß die fehlende Rechtsgrundlage nicht ersetzen kann, über meine Rechtsauffassung unterrichtet. Daraufhin hat das Ministerium den entsprechenden Erlaß aufgehoben. Die von mir angesprochenen Gesundheitsämter haben mir inzwischen mitgeteilt, daß sie meiner Empfehlung folgen werden.

5.9.4 Unterrichtung vorbehandelnder Ärzte

Mit Befremden mußte ich feststellen, wie wenig problembewußt Ärzte mitunter ihrer Schweigepflicht gegenüberstehen. So mußte ich förmlich beanstanden, daß eine Universitäts-Zahnklinik den von ihr über einen Patienten gefertigten **Arztbrief**, der u. a. eine psychiatrische Schlußdiagnose enthielt, mit OP-Berichten nicht nur seiner einweisenden Hausärztin, sondern **sämtlichen Ärzten übersandt** hat, die den Patienten früher behandelt hatten. Die Einwilligung des Betroffenen war nicht eingeholt worden.

Für die Übersendung des Arztberichtes mit den OP-Berichten ohne Einwilligung des Betroffenen ist eine gesetzliche Grundlage weder in bereichspezifischen Vorschriften noch in den Vorschriften des DSG NW ersichtlich.

Daneben verbot das Arztgeheimnis die Weitergabe des Arztberichtes mit den OP-Berichten. Der Arzt ist zur Offenbarung befugt, soweit er von der Schweigepflicht entbunden worden ist oder soweit die Offenbarung zum Schutze eines höheren Rechtsgutes erforderlich ist (§ 2 Abs. 4 der ärztlichen Berufsordnung - BO -). Beide Voraussetzungen lagen hier nicht vor. Dies gilt auch, soweit der Arztbericht an gleichzeitig oder nacheinander behandelnde Ärzte weitergegeben wurde.

Nach § 2 Abs. 6 der Berufsordnung sind Ärzte, wenn sie denselben Patienten gleichzeitig oder nacheinander behandeln, untereinander von der Schweigepflicht insoweit befreit, als das Einverständnis des Patienten vorliegt oder anzunehmen ist. Hiervon konnte schon im Hinblick auf den häufigen Wechsel der von dem Betroffenen in Anspruch genommenen Ärzte nicht ausgegangen werden. Allenfalls wäre es vertretbar gewesen, im Rahmen des Üblichen Unterlagen an den nachbehandelnden Hausarzt auf Grund einer mutmaßlichen Einwilligung zu übersenden. Eine auf die hypothetische Einwilligung gestützte Offenbarung kommt aber umso weniger in Betracht, je heikler der Inhalt der Unterlagen ist, insbesondere, wenn wie hier aus einer Zahnklinik immerhin eine psychiatrische Schlußdiagnose herausgeht.

In den Fällen, in denen keine Einverständniserklärung des Patienten vorliegt, ist dessen Wille sorgfältig zu erforschen. Dabei ist zu beachten, daß die ärztliche Schweigepflicht **um des Patienten willen** besteht, der Arzt also grundsätzlich zur Offenbarung nur befugt ist, soweit ihn der Patient von der Schweigepflicht entbindet. Daraus folgt, daß an eine Offenbarung auf Grund mutmaßlicher Einwilligung ein strenger Maßstab anzulegen ist. Somit dürfte als Empfänger von Patientendaten auf Grund einer mutmaßlichen Einwilligung (2. Alternative § 2 Abs. 6 BO) in der Regel nur der gleichzeitig oder zuletzt behandelnde Arzt in Betracht kommen. Keinesfalls dürfen schematisch sämtliche den Patienten vorbehandelnden Ärzte, sei es, daß sie von ihm genannt oder aus den Unterlagen ersichtlich sind, informiert werden. Aber auch bei dem geringsten Zweifel, ob der Patient mit einer Unterrichtung des gleichzeitig oder zuletzt behandelnden Arztes einverstanden ist, sollte er ausdrücklich gefragt werden. Der Patient ist keinesfalls gehalten, eine „Negativerklärung" dergestalt abzugeben, daß bestimmte Ärzte nicht unterrichtet werden dürfen. Das Fehlen einer solchen Erklärung kann daher die Offenbarung von Patientendaten nicht legitimieren.

5.9.5 Vergabe von Schreibarbeiten für das Gesundheitsamt

Ein Oberkreisdirektor fragte bei mir an, ob es zulässig sei, Schreibarbeiten für das Gesundheitsamt an private Schreibbüros oder an den Zentralen Schreibdienst der Kreisverwaltung zu vergeben.

In meinem 11. Tätigkeitsbericht (S. 73) habe ich ausgeführt, daß die Vergabe von Schreibarbeiten durch Krankenhausärzte an ein privates Schreibbüro nur mit Einwilligung des Patienten zulässig ist, die aus Beweissicherungsgründen schriftlich erfolgen sollte. Für die Ärzte des Gesundheitsamtes kann nichts anderes gelten. Sowohl das Gebot der informationellen Gewaltenteilung als auch die ärztliche Schweigepflicht verbieten grundsätzlich die Erledigung von Schreibarbeiten für den ärztlichen Bereich des Gesundheitsamtes durch nicht im Gesundheitsamt beschäftigte Schreibkräfte. Soweit im Zentralen Schreibdienst „freie Kapazitäten" vorhanden sind, müßten diese dem Gesundheitsamt zugeordnet werden.

Sofern diese datenschutzrechtlich einwandfreie Lösung - etwa aus Gründen des Stellenplans oder sonstigen personalplanerischen Erwägungen - nicht durchsetzbar erscheint, könnte ein Verbleiben von Schreibkräften, die für die Ärzte des Gesundheitsamtes Schreibarbeiten verrichten, im Zentralen Schreibdienst nur hingenommen werden, wenn diese Schreibkräfte **als berufsmäßig tätige Gehilfen** der Ärzte (§ 203 Abs. 3 Satz 1 StGB) angesehen werden könnten. Dies wäre dann der Fall, wenn sie allein nach Weisung der Ärzte tätig werden und sichergestellt ist, daß niemand außer der jeweiligen Schreibkraft selbst Kenntnis von den dem Arztgeheimnis unterliegenden Daten erhält. Daneben sollten für Ärzte des Gesundheitsamtes tätige Schreibkräfte zum Schutz der ihnen anvertrauten sensiblen Daten auf ihre Geheimhaltungsverpflichtung besonders hingewiesen werden.

5.9.6 Gesundheitskarte

Nachdem in Nordrhein-Westfalen am 1. Juli 1994 die gesetzliche Krankenversichertenkarte eingeführt worden ist, die nur die im Gesetz abschließend aufgeführten Angaben enthalten darf, mehren sich Bestrebungen von Krankenkassen und privaten Anbietern, zusätzlich Gesundheitskarten (z. B. „Sana-Card", „Service-Karten" von Krankenversicherungen, „Notfall-Karten", „APO(-theken)-Cards", „Röntgen-Karten") als **freiwillige Patienten-Chipkarten** anzubieten und zu empfehlen. Damit kann über viele medizinische Daten schnell und umfassend verfügt werden.

Diese Entwicklung ist aus datenschutzrechtlicher Sicht nicht unbedenklich. Deshalb hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder der Problematik angenommen und am 9./10. März 1994 den Beschluß zu Chipkarten im Gesundheitswesen gefaßt (vgl. Anlage 7, S. 179 bis 181).

Auf der Grundlage dieses Beschlusses habe ich zu der geplanten Einführung einer „BKK-Gesundheitscard" gegenüber dem zuständigen Krankenkassenverband auf die vordringlichen datenschutzrechtlichen Anforderungen hingewiesen.

Eine Gesundheitskarte kann nur auf freiwilliger Grundlage, also mit (schriftlicher) Einwilligung des Versicherten eingeführt werden. Das Freiwilligkeitspostulat gewährleistet nur dann den notwendigen Versichertenschutz, wenn

sich die Betroffenen wirklich **frei von faktischem Zwang**, insbesondere von sozialem Anpassungsdruck in Richtung auf eine elektronische Selbstauskunft (Offenbarungszwang) entscheiden können. Dies bedeutet insbesondere:

- Jeder Versicherte muß selbst entscheiden können, ob er seine Gesundheitsdaten einem IT-System anvertraut oder nicht. Dies umschließt das Recht, aus dem System jederzeit auch wieder „auszusteigen" (Möglichkeit des Widerrufs der Einwilligung).
- Dem Versicherten dürfen keine Nachteile durch die Nichtteilnahme entstehen.
- Der Versicherte darf keinem institutionellen Druck, etwa in Form eines Bonus-Malus-Mechanismus ausgesetzt sein.
- Der Versicherte darf nicht gezwungen sein, seine medizinischen Daten pauschal zu offenbaren. Er muß selbst selektiv eine Auswahl treffen können, welche der verfügbaren Daten er im Einzelfall seinem Partner (z. B. dem Röntgenarzt) präsentiert.

Im Hinblick auf diese Anforderungen an die Freiwilligkeit ist eine umfassende Aufklärung des Versicherten, insbesondere über die Tragweite seiner Einverständniserklärung für deren Rechtswirksamkeit von erheblicher Bedeutung.

5.10 Personalwesen

5.10.1 Speicherung von Bewerberdaten

Einer Beamtin des höheren vermessungstechnischen Verwaltungsdienstes, die in einem anderen Bundesland bereits Berufserfahrungen gesammelt hatte und um Übernahme in den nordrhein-westfälischen Landesdienst nachsuchte, wurde von der Einstellungsbehörde entgegengehalten, daß es nicht möglich sei, ihre **erneute Bewerbung** anzunehmen, da sie bereits zwei Jahre zuvor an einem Vorstellungstermin teilgenommen habe und seinerzeit von der Auswahlkommission für eine Einstellung nicht empfohlen worden sei. Hierbei stützte sich die Einstellungsbehörde auf die anläßlich der Erstbewerbung mit einem Personalbogen abgefragten und in einem Tagebuch registrierten Daten, wie z. B.

- Name der Bewerberin/des Bewerbers,
- Anschrift,
- Bewerbungsdatum,
- Geburtsjahr,
  Note der Diplom-Hauptprüfung und des großen Staatsexamens,
  Datum des Vorstellungstermins,
- Absage der Einstellung,
- Datum der Rücksendung der Bewerbungsunterlagen sowie ein Vermerk über Schwerbehinderung, Promovierung und zusätzliche Qualifikationen,

deren Speicherung nach Abschluß des Vorstellungstermins sie für die Erfüllung ihrer Aufgabe, eine **mehrmalige Teilnahme an Auswahlverfahren** zu vermeiden, für erforderlich hielt, weil nach den Voraussetzungen für die Einstellung bzw. Übernahme in den höheren vermessungstechnischen Verwaltungsdienst des Landes Nordrhein-Westfalen lediglich die einmalige Teilnahme am Vorstellungstermin vorgesehen sei.

Der Auffassung, daß die bei der Einstellungsbehörde verbleibenden Bewerberdaten sowie eine Niederschrift über den Vorstellungstermin erforderlich und deshalb nicht zu löschen seien (§ 19 Abs. 3 DSG NW), kann nicht gefolgt werden. Die allgemeine Löschungsvorschrift kann hier deshalb keine Anwendung finden, weil sie durch die Spezialvorschrift für die Löschung von Bewerberdaten (§ 29 Abs. 3 Satz 1 DSG NW) verdrängt wird. Hiernach ist die Einstellungsbehörde verpflichtet, personenbezogene Daten eines Bewerbers unverzüglich zu löschen, sobald feststeht, daß ein Beschäftigungsverhältnis nicht zustande kommt. Dadurch wird das allgemeine **Löschungsgebot** konkretisiert, ein Hinausschieben der Löschung oder ein Absehen von ihr und die Übernahme durch ein Archiv ausgeschlossen.

Meiner Empfehlung, sämtliche über die Betroffene noch vorhandenen Daten sofort zu löschen, ist die Einstellungsbehörde in diesem Einzelfall gefolgt. Sie vertritt aber unter Hinweis auf Stähler, Datenschutzgesetz Nordrhein-Westfalen, Kommentar, 2. Aufl., § 29 Anm. 8, die Auffassung, die bei ihr gespeicherten Daten seien weiterhin zu ihrer Aufgabenerfüllung erforderlich. Hieraus war zu schließen, daß die Einstellungsbehörde generell derartige Bewerberdaten speichert, um eine mehrmalige Teilnahme an Auswahlverfahren zu verhindern.

Selbst wenn man der Auffassung von Stähler (a.a.O.) folgen wollte, wonach die Spezialvorschrift über die Löschung von Bewerberdaten (§ 29 Abs. 3 Satz 1 DSG NW) den personenbezogenen Tatbestand, daß sich ein Bewerber überhaupt beworben hat, nicht erfaßt, so ist dieses Datum nach der dann zur Anwendung kommenden allgemeinen Löschungsvorschrift (§ 19 Abs. 3 DSG NW) zu löschen. Deren Voraussetzungen liegen hier schon deshalb vor, weil es an einer Aufgabe fehlt, zu deren Erfüllung die weitere Speicherung erforderlich sein könnte.

Eine Aufgabe der öffentlichen Verwaltung, deren Erfüllung mit einem Eingriff in das informationelle Selbstbestimmungsrecht verbunden ist, bedarf im Hinblick auf das Verfassungsgebot der Gesetzmäßigkeit der Verwaltung (Artikel 20 Abs. 3 GG) der Zuweisung durch eine Rechtsvorschrift. Eine solche Regelung, wonach für die Einstellung von Bewerbern lediglich die einmalige Teilnahme am Vorstellungstermin vorgesehen ist, existiert nicht. Eine im Erlaßwege geregelte Verwaltungsübung reicht für einen derartigen Eingriff nicht aus.

Fehlt es somit an der durch Rechtsnorm zugewiesenen Aufgabe, die mehrmalige Teilnahme von Bewerbern am Vorstellungstermin zu verhindern, so kann die weitere Speicherung der Tatsache, daß sich eine bestimmte Person

beworben hat, nicht erforderlich sein. Auch dieses Datum ist daher zu löschen.

Ich habe der Einstellungsbehörde empfohlen, nach Maßgabe des § 29 Abs. 3 Satz 1 bzw. § 19 Abs. 3 DSG NW sämtliche Bewerberdaten einschließlich der Tatsache, daß sich ein Bewerber überhaupt beworben hat, zu löschen.

5.10.2 Personalaktenführung im Justizdienst

Anläßlich eines Informations- und Kontrollbesuchs bei einer Justizvollzugsanstalt habe ich eine in datenschutzrechtlicher Hinsicht bedenkliche Führung der Personalakten der Beschäftigten festgestellt und diese Problematik gegenüber dem Justizministerium des Landes Nordrhein-Westfalen aufgegriffen.

- Nach der Allgemeinen Verfügung „Führung der Personalakten" des Justizministers vom 9. April 1979 - AV - (zuletzt geändert durch AV vom 22. Juni 1990) sind in der JVA sog. „unterbehördliche Personalakten" der Beamten, Angestellten und Arbeiter der Behörde (mit Ausnahme der Personalakte des Behördenleiters) und bei dem für die Dienst- und Fachaufsicht zuständigen Justizvollzugsamt sog. „oberbehördliche Personalakten" angelegt.

  Datenschutzrechtliche Bedenken bestehen hier insofern, als nicht klar geregelt ist, bei welcher Behörde die Personalakte als Grundakte zu führen ist (§ 102 Abs. 2 LBG). Mangels abschließender Regelungen in den beamten- und tarifrechtlichen Vorschriften, welche Stelle die personalaktenführende ist, läßt sich dies allein aus der Festlegung der Aufgaben des Dienstvorgesetzten herleiten. Dieser trifft nach § 3 Abs. 4 LBG die beamtenrechtlichen Entscheidungen über die persönlichen Angelegenheiten der ihm nachgeordneten Beamten, soweit nicht nach Gesetz oder Verordnung eine andere Stelle zuständig ist. Aus der Verordnung über richter- und beamtenrechtliche Zuständigkeiten im Geschäftsbereich des Justizministers vom 19. Dezember 1982 läßt sich im Hinblick auf die darin jeweils dem Leiter der dienst- und fachaufsichtführenden Stelle und dem Leiter der Beschäftigungsstelle zugewiesenen Entscheidungszuständigkeiten nicht herleiten, welcher Stelle die Führung der Personalakten (als Grundakten) obliegt. Im übrigen bestimmt zwar die AV, bei welchen (Beschäftigungs-)Stellen Personalakten zu führen sind; gleichzeitig sind Personalakten mit inhaltsgleichem Personalbogen nach Nr. I. B. 4. AV aber auch bei den übergeordneten Gerichten bzw. Justizbehörden zu führen. Infolge der insoweit angeordneten Mitteilungs- und Berichtspflicht entstehen zwangsläufig spiegelbildliche Personalakten bei der übergeordneten Stelle, wenn davon ausgegangen wird, daß die Grundakten bei der Beschäftigungsstelle angelegt sind. Diese bei den übergeordneten Gerichten bzw. Justizbehörden zu umfangreichen Sammlungen von Beschäftigtendaten führende Praxis begegnet erheblichen datenschutzrechtlichen Bedenken. Ein Vorgesetzter darf nur die zu seiner Auf-

gabenerfüllung erforderlichen personenbezogenen Daten verarbeiten, mithin auch nur in dementsprechendem Umfang Personalnebenakten führen (vgl. 10. Tätigkeitsbericht, S. 98/99). Dies stellt die gesetzliche Neuregelung des § 102 Abs. 2 LBG nunmehr eindeutig klar, weshalb ich beim Justizministerium auf eine Anpassung der AV an die gesetzlichen Vorschriften hingewirkt habe.

Das Justizministerium hat sich zunächst der Auffassung des Justizvollzugsamtes angeschlossen, nach der die **Doppelaktenführung** bei der übergeordneten Stelle im Bereich der beamtenrechtlich relevanten Fragestellungen erfolge. Insofern sei es richtig, daß der Präsident des Justizvollzugsamtes in gewisser Weise Dienstvorgesetzter der Beamten der Justizvollzugsanstalten seines Bezirks sei. Diese doppelte Dienstvorgesetzteneigenschaft sei in mehrstufig gegliederten Verwaltungen nicht unüblich, im Interesse eines ordnungsgemäßen Geschäftsablaufs in den Justizvollzugsanstalten sinnvoll und datenschutzrechtlich zu respektieren. Sowohl in den Justizvollzugsanstalten als auch im Justizvollzugsamt müsse im Interesse der betroffenen Bediensteten zwar Vertraulichkeit hinsichtlich aller den Beamten in seinen rechtlich geschützten Interessen betreffenden Informationen gewährleistet sein. Damit sei jedoch den schutzwürdigen Interessen der Bediensteten auf Datenschutz Rechnung getragen.

Dieser Auffassung kann nicht gefolgt werden. Die Dienstvorgesetzteneigenschaft ist nicht duplizierbar. Je nach festgelegter Entscheidungszuständigkeit ist vielmehr der Leiter der Beschäftigungsstelle oder der Leiter einer übergeordneten Stelle Dienstvorgesetzter. Im übrigen hat sich das Justizministerium nicht konkret zu den von mir aufgezeigten Bedenken geäußert, sondern auf die Vorrangigkeit der vom Innenministerium vorzunehmenden Überarbeitung der Verwaltungsverordnung zur Ausführung des Landesbeamtengesetzes verwiesen. Sobald ein entsprechender Entwurf vorliege, werde die Neufassung der AV vom Justizministerium in Angriff genommen.

Nach einer Stellungnahme des Innenministeriums kann u. a. wegen einer abermaligen Novellierung des Landesbeamtengesetzes mit einer kurzfristigen Neufassung der entsprechenden VV zum LBG nicht gerechnet werden. Im Hinblick hierauf habe ich gegenüber dem Justizministerium angeregt, mit der Neufassung der AV über die Führung von Personalakten im Justizbereich nicht bis zu einem ungewissen zukünftigen Zeitpunkt zuzuwarten, sondern diese partiell den neuen personalaktenrechtlichen Gesetzesvorschriften anzupassen. Für besonders dringlich halte ich insoweit die Umsetzung der Gesetzesvorschriften über die Führung von Personalakten und Nebenakten (§ 102 Abs. 2 Satz 3 LBG).

- Festgestellt habe ich ferner, daß alle **Erkrankungszeiträume und Abwesenheitstage** der Beschäftigten der JVA auf einem Ergänzungsblatt zum Personalbogen in den Personalakten der Betroffenen gespeichert und so listenmäßig von Beginn des Dienstverhältnisses an fortgeschrieben

werden. In einer Personalakte war z. B. die **lückenlose Übersicht** über Krankheits- und Abwesenheitszeiten eines Beschäftigten seit 1977 enthalten.

Diese (weitere) Speicherung der Abwesenheitszeiten der Beschäftigten in deren Personalakten ist datenschutzrechtlich unzulässig, weil sie sich nicht auf die hier maßgebliche bereichspezifische Vorschrift des § 29 Abs. 1 Satz 1 DSG NW stützen läßt. Es ist bereits nicht ersichtlich, daß diese separate Speicherung von Beschäftigtendaten einem der in dieser Vorschrift enumerativ genannten Zwecke zuzuordnen, geschweige denn dafür erforderlich ist. Diese Daten sind aus den Arbeitsunfähigkeitsbescheinigungen selbst ersichtlich und bedürfen erkennbar keiner weiteren Speicherung, weshalb ich dem Justizministerium empfohlen habe, in seinem Geschäftsbereich eine Regelung zu treffen, die unzulässigerweise gespeicherten Daten zu löschen, künftig derartige Daten nicht mehr auf dem Vordruck speichern zu lassen und diesen entsprechend zu ändern.

Das Justizministerium hat demgegenüber unter Bezugnahme auf einen Bericht des Justizvollzugsamtes zunächst die Auffassung vertreten, die gesonderte Zusammenstellung der Krankheitszeiträume eines Beschäftigten diene dem Leiter der JVA als notwendige Unterstützung für die Wahrnehmung seiner Aufgaben als Dienstvorgesetzter, zu denen gehöre, Personal sachgerecht einzusetzen und evtl. notwendige Maßnahmen hinsichtlich der vollen Dienstfähigkeit zu treffen. Dem Leiter der JVA seien die Erkrankungszeiträume der Beschäftigten ohnehin dienstlich bekannt geworden. Gerade bei den Beschäftigten des allgemeinen Vollzugsdienstes sei es wegen der dienstlichen Erschwernisse oft im Interesse einer die Persönlichkeit des Beschäftigten berücksichtigenden Diensteinteilung unbedingt erforderlich, sich einen schnellen Überblick über die Ausfallzeiten von Beschäftigten zu verschaffen, die Rückschlüsse auf die dienstliche Belastbarkeit zulassen. Für die Wahrnehmung von Aufgaben der Personalsteuerung, die wegen der zunehmenden Fälle von Dienstunfähigkeit im Bereich des Schichtdienstes immer wichtiger werden, bedürfe der Leiter der JVA eines Überblicks über die krankheitsbedingten dienstlichen Abwesenheitszeiten.

Dieser Auffassung vermag ich ebenfalls nicht zu folgen. Aus der Kenntnis des Leiters der JVA von den Erkrankungszeiträumen der Beschäftigten folgt keineswegs bereits die Befugnis zur Auflistung dieser Zeiträume auf einem Ergänzungsblatt zum Personalbogen. Im Einzelfall mag es durchaus den Zwecken des § 29 Abs. 1 Satz 1 DSG NW zuzuordnen und geboten sein, solche Daten in dem nach § 102 g Abs. 2 Satz 1 LBG zulässigen zeitlichen Rahmen aufzulisten, um etwa einen amtsärztlichen Untersuchungsauftrag vorzubereiten oder an Hand der Aufstellung die an den Amtsarzt zu stellenden Fragen zu präzisieren. Keineswegs kann ein entsprechendes Verfahren jedoch für alle Beschäftigten des Geschäftsbereichs des Justizministeriums vorgegeben werden. Abgesehen hiervon erfordert die gesetzliche Einführung der fünfjährigen Aufbewahrungs-

dauer von Unterlagen über Erkrankungen ohnehin eine gemäß dem Sicherstellungsauftrag des Justizministeriums (§ 7 DSG NW) gebotene Aufhebung der ausnahmslosen Praxis der separaten Speicherung aller Erkrankungszeiträume in dem Ergänzungsblatt zum Personalbogen.

Im Hinblick darauf, daß das Justizministerium nunmehr die nachgeordneten Stellen seines Geschäftsbereichs um Stellungnahme zu Überlegungen über eine Neufassung der AV und des Personalbogens gebeten hat, habe ich zunächst von einer Beanstandung abgesehen.

5.10.3 Automatisierte Personalsachbearbeitung

Das Innenministerium des Landes Nordrhein-Westfalen hat mich über ein projektiertes ADV - unterstütztes Personalsachbearbeitungsverfahren (ADV-System) unterrichtet und um Stellungnahme gebeten. Das ADV-System soll für die Personalsachbearbeitung innerhalb des Ministeriums Informationen für unterschiedliche Personalmaßnahmen bereitstellen. Auswertungen aus dem Datenbestand können nach verschiedenen Auswahl- und Ordnungskriterien sowohl am Bildschirm angezeigt als auch dezentral ausgedruckt werden. Die Personalsachbearbeitung soll unterstützt und entlastet werden durch u. a. Bereitstellung von aktuellen Arbeitspapieren und -unterlagen, Vereinfachung der Routinetätigkeiten, Verbesserung der Arbeitsqualität durch Bereitstellung relevanter Informationen und Beschleunigung der einzelnen Verfahrensabläufe.

Mit automatisierter Personaldatenverarbeitung und Stelleninformationssystemen habe ich mich zuletzt in meinem 11. Tätigkeitsbericht (S. 80/81) befaßt und auf das von diesen ausgehende Gefahrenpotential hingewiesen. Nach Inkrafttreten der durch das Sechste Gesetz zur Änderung dienstrechtlicher Vorschriften geschaffenen Regelung des § 102 f LBG dürfen Personalaktendaten von Beamten in Dateien nur für Zwecke der Personalverwaltung oder der Personalwirtschaft verarbeitet werden, wobei hinsichtlich des Umfangs der in einer automatisierten Datei verarbeiteten Daten der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz zu beachten ist [s. a. Gesetzesbegründung zu § 56 f BRRG - Bundestagsdrucksache 12/544 S. 13 -: Die automatisierte Verarbeitung beschränkt sich auf Hilfs- und Unterstützungsfunktionen. In der Regel handele es sich um die „Erstellung von Arbeitsunterlagen zur Unterstützung administrativer Planungs- und Führungsaufgaben (Personalwirtschaft) sowie die Vorbereitung von Personalentscheidungen (einzelfallbezogene Personalverwaltungsaufgaben)".]

Die Personalsachbearbeitung soll künftig in einem zunächst auf Beamte bezogenen Teilprojekt zum einen für die im Innenministerium selbst sowie in meiner Dienststelle tätigen Beamtinnen und Beamten aller Laufbahngruppen und des weiteren für die im nachgeordneten Bereich tätigen Beamtinnen und Beamten des höheren Dienstes, deren Dienstvorgesetzter der Innenminister ist, erfolgen. Insoweit bestehen keine grundsätzlichen Bedenken gegen die Erfassung der jeweils erforderlichen Personalaktendaten der

betroffenen Beamtinnen und Beamten aus deren Personalakten und die Speicherung dieser Daten in dem ADV-System. Soweit die Personalakten der Betroffenen bei dem Innenministerium geführt werden, ist Rechtsgrundlage für diese Datenverarbeitung § 102 f Abs. 1 Satz 1 LBG; hinsichtlich der bei den nachgeordneten Behörden geführten Personalakten der dort tätigen Beamtinnen und Beamten des höheren Dienstes läßt sich die Datenübermittlung auf § 102 f Abs. 1 Satz 1 und 2 i.V.m. § 102 d Abs. 1 Satz 1, Abs. 3 LBG stützen.

Nach der Konzeptdarstellung soll das ADV-System zwar nicht mit Datenverarbeitungssystemen anderer Organisationseinheiten vernetzt werden. Dennoch bedarf es der Klärung, ob und in welchem Umfang dieses System aus technischer Sicht in ein Netz automatisierter Datenverarbeitung innerhalb des Innenministeriums oder darüber hinaus eingebunden ist, was mit dem Grundsatz der Abschottung eines Personalverwaltungssystems unvereinbar wäre (vgl. Bundestagsdrucksache 12/544 S. 14).

Zu dem ADV-System habe ich spezielle Hinweise zu organisatorischen und technischen Maßnahmen des Datenschutzes und der Datensicherheit gegeben und zu einzelnen Fragen der Datenverarbeitung u. a. folgendes bemerkt:

- Datenschutzrechtliche Bedenken habe ich gegen den Umfang der **Speicherung von Beurteilungsdaten** der Betroffenen wegen der hiermit verbundenen Nutzungsrisiken und der Gefahr erhoben, daß diese Datenverarbeitung über bloße Hilfs- und Unterstützungsfunktionen im Rahmen der Personalwirtschaft und -planung hinausgeht. Insoweit besteht die Besorgnis, daß die Verknüpfung der Beurteilungsdaten mit anderen, für eine Beförderung erheblichen personenbezogenen Daten zu einer maschinellen Reihung führt, die eine Beförderungsentscheidung in aller Regel maßgeblich beeinflussen wird. Es ist nicht ersichtlich, zu welchen konkreten Zwecken die separate Speicherung langjährig zurückliegender Beurteilungsdaten (hier: Ergebnisse und Erstellungsdaten der letzten drei Beurteilungen) in dem ADV-System erforderlich sein soll. Zur Vorbereitung von Personal(auswahl)entscheidungen reicht nach meiner Auffassung die Aufnahme des Ergebnisses und des Datums der letzten und allenfalls der vorletzten Beurteilung aus, um den durch Kontextverlust entstehenden Verzerrungen und den damit einhergehenden Beeinträchtigungen des Rechts auf informationelle Selbstbestimmung zu begegnen, die nach § 102 f Abs. 4 LBG wie auch bisher schon nach § 29 Abs. 6 DSG NW strikt auszuschließen sind.

- Weiter halte ich es für erforderlich, daß bereits für die Grundstufe des ADV-Systems eine **arbeitsplatzbezogene Zuordnung** der Zugriffsbefugnisse vorgesehen wird. Eine konkrete Zuordnung solcher Befugnisse zu den einzelnen, mit der Personalsachbearbeitung befaßten Bediensteten und deren Vorgesetzten ist unerläßlich, was auch aus dem Grundsatz folgt, daß der Kreis der sowohl mit Personalakten als auch mit Personal-

aktendaten befaßten Beschäftigten zur Wahrung des Personalaktengeheimnisses möglichst eng zu halten ist.

- Es ist nicht ersichtlich, welche zwingenden und unabweisbaren Gründe die Speicherung der **LBV-Personalnummer** innerhalb der Personalstammdaten als Zuordnungsmerkmal für das ADV-System erfordern. Die LBV-Personalnummer ist nur für Zwecke der Besoldung und Vergütung vorgesehen und bestimmt. Sie kann bereits deshalb keine gleichzeitige Verwendung in dem ADV-System finden, zumal dies wegen der Gefahr, daß mit ihrer Hilfe ohne weiteres Datensätze zu derselben Person aus anderen Dateien verknüpft werden können, mit erheblichen Risiken für die Persönlichkeitsrechte der Betroffenen verbunden wäre. Im übrigen lassen die Hinweise in dem Konzept des ADV-Systems selbst den Schluß zu, daß die LBV-Personalnummer als Identifikationsmerkmal nicht erforderlich ist.
- Nicht ersichtlich ist des weiteren, welchen Zwecken der Personalverwaltung und der Personalwirtschaft Datenbank-Tabellen zur Aufnahme der Personaldaten der „Ehemaligen" zuzuordnen sind. Eine weitere Datenspeicherung aus dem Dienst ausgeschiedener oder in einen anderen Geschäftsbereich versetzter Beamter wäre mangels Rechtsgrundlage unzulässig.

Im übrigen habe ich das Innenministerium darauf aufmerksam gemacht, daß die Mitteilungs-, Dokumentations- und Bekanntmachungspflichten nach § 102 f Abs. 5 LBG zu beachten sein werden.

5.10.4 Automatisierte Führung einer Personaldatei

Im Rahmen eines Informations- und Kontrollbesuchs habe ich bei einer obersten Landesbehörde eine zur automationsunterstützten Personalplanung eingerichtete Personaldatei überprüft. Die darin gespeicherten Daten von Beschäftigten des höheren Dienstes und vergleichbaren Angestellten des nachgeordneten Bereichs wurden hauptsächlich zur Vorbereitung von Beförderungen und zur Überwachung des Stellenplans verwendet, wohingegen die in der Datei ebenfalls gespeicherten Daten der behördeneigenen Beschäftigten aus dienstinternen Gründen nicht mehr genutzt und daher auch nicht mehr aktualisiert wurden.

Personalaktendaten dürfen in Dateien nur für Zwecke der Personalverwaltung oder Personalwirtschaft verarbeitet und genutzt werden (§ 102 f Abs. 1 Satz 1 LBG). Da die in der Datei gespeicherten Personalaktendaten der behördeneigenen Beschäftigten weder für Zwecke der Personalverwaltung noch für solche der Personalwirtschaft verarbeitet und genutzt, sondern nur noch ohne konkrete Zweckbestimmung vorgehalten wurden, war ihre Speicherung zur Aufgabenerfüllung nicht mehr erforderlich. Eine **Datenspeicherung auf Vorrat** für den Fall, daß die Daten später einmal zur Erfüllung einer Aufgabe gebraucht werden könnten, verstößt gegen den Erforderlichkeits-

grundsatz. Daten, deren Kenntnis für die speichernde Stelle nicht mehr erforderlich ist, sind zu löschen (§ 19 Abs. 3 Satz 1 Buchstabe b DSG NW).

Hinsichtlich der für die Beschäftigten des nachgeordneten Bereichs eingerichteten Personaldateien habe ich festgestellt, daß die Verarbeitungs- und Nutzungsformen des automatisierten Personalverwaltungsverfahrens im einzelnen nicht dokumentiert waren und es an der Unterrichtung der Betroffenen mangelte (§ 102 f Abs. 5 LBG). In diesen Personaldateien waren langjährig zurückliegende Beurteilungsdaten gespeichert, was erheblichen datenschutzrechtlichen Bedenken begegnet (s. oben 5.10.3, S. 85). Im übrigen habe ich darauf hingewiesen, daß die zu speichernden Merkmale konkret formuliert und der jeweiligen Rechtsgrundlage der Datenverarbeitung zuzuordnen sein müssen. Ein Datenfeld für (frei zu definierende) „Bemerkungen" ist in datenschutzrechtlicher Hinsicht unzulässig, weil es die Gefahr der Speicherung personenbezogener Daten im Übermaß in sich birgt. Der Stellungnahme der obersten Landesbehörde zufolge werden die datenschutzrechtlichen Bestimmungen künftig beachtet.

5.10.5 Abschottung der Beihilfestelle im kommunalen Bereich

Informations- und Kontrollbesuche bei verschiedenen Stadtverwaltungen haben mir die Erkenntnis vermittelt, daß die zur Abschottung der Beihilfestelle von der Personalverwaltung gebotenen Maßnahmen nicht oder nicht in vollem Umfang getroffen sind. Zwar werden in den von mir überprüften Fällen die Unterlagen über Beihilfen von den Personalakten getrennt als Teilakten geführt und auch räumlich gesondert aufbewahrt. Die Beihilfestellen selbst sind jedoch in die für Personalangelegenheiten zuständigen Ämter eingegliedert. Unter Hinweis auf die nunmehr gesetzlich verankerte Verpflichtung zur Bearbeitung der Beihilfeakte in einer von der übrigen Personalverwaltung getrennten Organisationseinheit (§ 102 a Satz 3 LBG) habe ich empfohlen, die hierfür erforderlichen Maßnahmen zu treffen. Die gesetzliche Regelung verlangt - jedenfalls bei größeren Verwaltungen, denen eine entsprechende Umorganisation ohne weiteres möglich ist - die **Realisierung** der Abschottung durch eine vollständige Trennung der Beihilfestelle von der Personalverwaltung. Allenfalls bei kleineren Verwaltungen, in denen die organisatorische Trennung nicht in vollem Umfang durchgeführt werden kann, werden anderweitige Maßnahmen zu treffen sein, die einen Einblick in Beihilfevorgänge durch einen für Personalangelegenheiten zuständigen Vorgesetzten aber dennoch ausschließen müssen.

Keinesfalls hinnehmbar ist es, wenn eine Stadtverwaltung mit ca. 1 400 Beschäftigten nicht einmal Maßnahmen trifft, die eine Kenntnisnahme von Beihilfedaten durch den Leiter des Personalamtes ausschließen. Muß die Beihilfestelle etwa aus besonderen (z. B. personalwirtschaftlichen) Gründen dem Personalamt angegliedert bleiben, so verlangt das Abschottungsgebot mindestens eine anderweitige fachliche Unterstellung der mit der Beihilfebearbeitung betrauten Beschäftigten. Der Einwand des Stadtdirektors, die Beihilfestelle sei seit Jahren personell und räumlich abgeschottet, so daß

sich das datenschutzrechtliche Problem auf die theoretische Möglichkeit der Kenntnisnahme von Beihilfevorgängen durch die Amtsleitung reduziere, ist im Hinblick auf die gesetzlich gebotene Abschottung unbeachtlich.

5.10.6 Weiterleitung von Amtsarztgutachten innerhalb einer Bezirksregierung an den Medizinaldezernenten

Förmlich beanstanden mußte ich, daß der Personaldezernent einer Bezirksregierung die zur Abklärung von Dienstunfallfolgen eingeholte gutachtliche Stellungnahme eines Amtsarztes über den Gesundheitszustand eines Beamten dieser Behörde an deren Medizinaldezernenten weitergeleitet hatte, ohne daß hierfür eine gesetzliche Grundlage bestand oder der Betroffene eingewilligt hatte.

Nach § 3 Abs. 1 Nr. III des Gesetzes über die Vereinheitlichung des Gesundheitswesens (GesVG) obliegt dem Gesundheitsamt die amts- und vertrauensärztliche Tätigkeit, soweit sie, wie dies in Nordrhein-Westfalen der Fall ist, durch Landesrecht den Amtsärzten übertragen ist. Die Bezirksregierung hat als Aufsichtsbehörde gesetzlich näher beschriebene und begrenzte Weisungsrechte gegenüber den Gesundheitsämtern (§ 4 Abs. 2 GesVG). Außerdem hat die Aufsichtsbehörde die Geschäftsführung des Gesundheitsamtes in regelmäßiger Wiederkehr an Ort und Stelle nachzuprüfen sowie nach Bedarf außerörtliche Geschäftsprüfungen vorzunehmen. Diesen Vorschriften ist nicht zu entnehmen, daß ein im konkreten Einzelfall erstelltes amtsärztliches Gutachten vom Medizinaldezernenten überprüft werden darf. Zwar sieht Nr. 6 des Runderlasses des Innenministers vom 11. Juli 1966 vor, daß der Medizinaldezernent des für die Fachaufsicht über das Gesundheitsamt zuständigen Regierungspräsidenten mit einer Überprüfung des amtsärztlichen Gutachtens zu beauftragen ist, falls im Einzelfalle gegen das Gutachten des Gesundheitsamtes Einwendungen erhoben werden. Es kann dahinstehen, ob dies im Fall der amtsärztlichen Untersuchung des Beamten zutraf. Jedenfalls handelt es sich bei dieser Erlaßregelung nicht um eine gesetzliche, sondern um eine Verwaltungsvorschrift, die die Verarbeitung personenbezogener Daten nicht legitimieren kann.

Meiner Empfehlung, in vergleichbaren Fällen von einer Übersendung des Amtsarztgutachtens an den Medizinaldezernenten abzusehen, ist die Bezirksregierung nicht gefolgt. Sie hält daran fest, in Fällen unklarer Begutachtung das Medizinaldezernat zu beteiligen und beruft sich dabei auf die Verarbeitung von Beschäftigtendaten regelnde Vorschrift des § 29 Abs. 1 DSG NW. Aus dieser Vorschrift ergibt sich indessen nicht, daß der Medizinaldezernent dazu berufen ist, in Personalangelegenheiten der Bezirksregierung die Tätigkeit des Amtsarztes im Einzelfall gleichsam wie ein **Obergutachter** zu überprüfen. Inzwischen hat das Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen die Bezirksregierungen darauf hingewiesen, daß der Runderlaß vom 11. Juli 1966 als Verwaltungsvorschrift die Verarbeitung personenbezogener Daten - auch innerhalb der Bezirksregierung - nicht legitimieren kann.

5.10.7 Teilnehmerkreis der Beurteilerbesprechung

- Ein bei einer kleinen Gemeinde beschäftigter Beamter hat zu dem dortigen Beurteilungsverfahren meine Stellungnahme erbeten. Um die Vergleichbarkeit der Beurteilungen zu erreichen, werden die Entwürfe dienstlicher Beurteilungen der Beamtinnen und Beamten von einer aus dem Gemeindedirektor und sämtlichen Amtsleitern bestehenden Kommission beraten.

  Die Beratung der Beurteilungsentwürfe innerhalb der Kommission und die hiermit verbundene Bekanntgabe personenbezogener (Beurteilungs-) Daten an deren Mitglieder bedarf als Eingriff in das Recht der zu beurteilenden Betroffenen auf informationelle Selbstbestimmung einer gesetzlichen Grundlage. Da die beamtenrechtlichen Vorschriften keine normenklaren gesetzlichen Regelungen darüber enthalten, wer an der Erstellung einer dienstlichen Beurteilung zu beteiligen ist und Kenntnis von beurteilungsrelevanten Beschäftigtendaten erhalten darf, beurteilt sich die Datenverarbeitung nach der bereichspezifischen Vorschrift des § 29 Abs. 1 Satz 1 DSG NW. Hiernach dürfen Beschäftigtendaten - auch innerhalb einer öffentlichen Stelle - nur verarbeitet werden, wenn die Kenntnis der Daten zur Durchführung des Dienstverhältnisses (hier: Erstellung einer Beurteilung) erforderlich ist.

  Die Beratung von Beurteilungsentwürfen in einer Kommission ist zur Erstellung von Beurteilungen dann erforderlich, wenn die Vergleichbarkeit der Beurteilungen untereinander als Beurteilungselement notwendig und nur durch die **Beteiligung aller Amtsleiter** in den Beratungen der Kommission zu gewährleisten ist. Zweck und Wert dienstlicher Beurteilungen bestehen in der Objektivierung der Personalauslese und des Personaleinsatzes. Diese Zweckbestimmung erfordert, daß die fachlichen Leistungen des Beamten in Bezug auf sein Amt und im Vergleich zu den anderen Beamten seiner Besoldungsgruppe und Laufbahn darzustellen sind. Insoweit ist die Beurteilung auch als Grundlage für am Leistungsgrundsatz orientierte Entscheidungen über die Verwendung der Beamten zu verstehen; sie dient also der Auswahl des jeweils bestgeeigneten Beamten (BVerwGE 21, 127/129). Insofern bestehen keine grundsätzlichen Bedenken, die fachliche Leistung des zu beurteilenden Beamten auch im Vergleich zu anderen Beamten derselben Besoldungsgruppe und Laufbahn darzustellen.

  Damit ist aber noch nicht geklärt, ob die Vergleichbarkeit der Beurteilungen nur durch eine Beteiligung der Amtsleiter (einer kleineren Gemeinde) in einer Kommission mit entsprechenden Beratungsaufgaben zu gewährleisten ist. Das Bundesverwaltungsgericht hat es allgemein für zulässig erachtet, daß der Dienstherr im Rahmen seiner organisatorischen Gestaltungsfreiheit bestimmt, durch wen er die Aufgabe der dienstlichen Beurteilung tatsächlich wahrnimmt. Allerdings dürfe er den sachlichen Zusammenhang dieser Aufgabe mit der Wahrnehmung der Dienst- und

Fachaufsicht nicht außer acht lassen (Urteil vom 17. April 1986 - 2 C 28.83 -, in: Schütz, Beamtenrecht, ES/D I 2 Nr. 25).

Entsprechend diesen beurteilungsrechtlichen Maßstäben begegnet auch die Beratung von Beurteilungsentwürfen in einer kleineren Gemeinde durch eine aus dem Gemeindedirektor und allen Amtsleitern gebildeten Kommission keinen datenschutzrechtlichen Bedenken. Eine derartige Beratung dürfte nicht nur einer möglichst gerechten Auslese qualifizierter Bewerber dienen, sondern auch zu Zwecken der Personalplanung und des Personaleinsatzes erforderlich sein. Die Amtsleiter müssen insoweit auch Kenntnis über besonders leistungsfähige Beamte aus anderen Ämtern der Gemeinde erhalten, die für einen späteren Einsatz in ihrem Amt in Frage kommen. Hat der Dienstherr bei der Beratung von Beurteilungsentwürfen in einer zu diesem Zweck eingerichteten Kommission einen gewissen, nur eingeschränkt nachprüfbaren Ermessens- und Beurteilungsspielraum, muß er allerdings dafür Sorge tragen, daß derartige Besprechungen und Beratungen auf die Leitungsebene der Verwaltung beschränkt bleiben. Nur dies bietet die Gewähr, daß die Beurteilungsentwürfe mit dem Ziel beraten werden, leistungsgerecht abgestufte, untereinander vergleichbare Beurteilungen zu erstellen und Beurteilungsdaten nicht unbeteiligten Dritten offenbart werden.

- Der Personalrat einer Bezirksregierung hat mir eine andere, in datenschutzrechtlicher Hinsicht allerdings problematische Verfahrensweise bei der Durchführung des (mehrstufigen) Beurteilungsverfahrens nach Maßgabe der Beurteilungsrichtlinien des Innenministeriums (BRL) vom 25. Mai 1991 geschildert. Die Behördenleitung hatte die vor der Schlußzeichnung der Beurteilungen von Beamtinnen und Beamten vorgesehene Beurteilerbesprechung zusammen mit Erstbeurteilern durchgeführt. Unter Hinweis auf den Wortlaut der Beurteilungsrichtlinien hat sie dies mit der Schwierigkeit des für die Anwendung gleicher Beurteilungsmaßstäbe verantwortlichen Schlußzeichners der Beurteilung begründet, eine präzise und verläßliche Leistungseinschätzung vorzunehmen.

  Hierzu habe ich festgestellt, daß die das Beurteilungsverfahren regelnden Vorschriften der Nrn. 10.2.1 und 10.2.2 BRL die beiden Phasen der Erstellung des (ausdrücklich als Erstbeurteilung definierten) Beurteilungsvorschlags sowie der Schlußzeichnung als zwei eigenständige, getrennt voneinander ablaufende Beurteilungsabschnitte betreffen. Die aus dieser **Zweistufigkeit** folgende Selbständigkeit des Beurteilungsvorschlags schließt es nach meiner Auffassung aus, daß der Erstbeurteiler nach Abgabe seines Beurteilungsvorschlags mit diesem nochmals befaßt wird, um sich auch mit den Maßstäben anderer Erstbeurteiler auseinanderzusetzen, und damit in die von dem Schlußzeichnenden zu erfüllende Aufgabe einbezogen wird.

  Die Teilnahme der Erstbeurteiler an der Beurteilerbesprechung halte ich darüber hinaus für unvereinbar mit dem von der Rechtsprechung auf-

gestellten Grundsatz, nach dem der Kreis der mit Personalakten und Personalaktendaten befaßten Bediensteten möglichst klein zu halten ist. Im übrigen ist der Stellungnahme der Landesregierung zu meinem 11. Tätigkeitsbericht (Drucksache 11/6876, S. 62 oben) zu entnehmen, daß als Teilnehmer der Beurteilerbesprechung nicht die Erstbeurteiler in Betracht gezogen werden. Meine Auffassung wird im Ergebnis vom Innenministerium des Landes Nordrhein-Westfalen geteilt, das mir u. a. mitgeteilt hat, es müsse erwartet werden, daß die Angehörigen der Leitungsebene in der Lage sind oder sich in die Lage versetzt haben, dem Schlußzeichner der Beurteilung ein abgestuftes und differenziertes Bild von Eignung, Leistung und Befähigung der zu beurteilenden Mitarbeiterinnen und Mitarbeiter zu vermitteln, so daß dieser die Schlußzeichnung verantwortlich übernehmen könne.

5.10.8 Gleitzeitdaten

Bei Informations- und Kontrollbesuchen erhielt ich Kenntnis von der Praxis verschiedener Stadtverwaltungen, Amtsleitern monatlich die Arbeitszeitguthaben und -defizite ihrer nachgeordneten Beschäftigten listenmäßig mitzuteilen.

Diese behördeninterne Weitergabe personenbezogener Daten zur Information von Fachvorgesetzten über Arbeitszeitkontingente der Beschäftigten mag zwar allgemeinen Zwecken der Personalplanung und des Personaleinsatzes zuzuordnen sein; die Weitergabe dieser Beschäftigtendaten an die **Amtsleiter** ist aber nur dann zulässig, wenn sie für diese Zwecke auch erforderlich ist (§ 29 Abs. 1 Satz 1 DSG NW). Das Erforderlichkeitsprinzip zwingt die öffentliche Verwaltung, sich auf das zur rechtmäßigen Erfüllung ihrer Aufgaben unerläßliche Minimum zu beschränken (BVerfGE 65, 1, 46). Es reicht nicht aus, wenn die Kenntnis personenbezogener Daten lediglich dienlich oder, etwa zur Abrundung des Bildes oder als Hintergrundinformation, nützlich ist. Sie muß vielmehr zur Aufgabenerfüllung des einzelnen Amtsleiters unbedingt notwendig sein mit der Konsequenz, daß er ohne Kenntnis dieser Daten eine konkrete Aufgabe nicht oder nicht sachgerecht erfüllen kann.

Gemessen hieran ist die **laufende Unterrichtung** der Amtsleiter über Zeitguthaben und -defizite der ihnen nachgeordneten Beschäftigten allenfalls in Ausnahmefällen dienstlich notwendig und damit auch in datenschutzrechtlicher Hinsicht unbedenklich, in denen die Gleitzeitregelung bei einzelnen Mitarbeitern zu den Dienstablauf beeinträchtigenden Zeitguthaben oder -defiziten führt. Die in den von mir aufgesuchten Stadtverwaltungen bestehenden Regelungen, die das „Gleitzeitverhalten" von Beschäftigten widerspiegeln, stellen eine dem Verhältnismäßigkeitsgebot zuwiderlaufende Datenverarbeitung im Übermaß dar, weil den Amtsleitern mehr Daten weitergegeben werden, als diese zur Erfüllung ihrer Aufgaben brauchen. Solche Datenweitergaben können demnach auch nicht in einer Dienstvereinbarung geregelt werden (§ 70 Abs. 1 Satz 1 LPVG).

Ich habe den Stadtdirektoren empfohlen, die Weitergabe derartiger personenbezogener Daten auf Ausnahmefälle zu beschränken. Ein Stadtdirektor hat mir inzwischen mitgeteilt, daß er den Amtsleitern die gespeicherten Arbeitszeitdaten nicht mehr generell zur Verfügung stellen wird.

5.10.9 Verarbeitung personenbezogener Daten durch Schwerbehindertenvertretungen

- Gegenüber einer **Hauptschwerbehindertenvertretung** habe ich zu der Frage Stellung genommen, ob diese zur Speicherung personenbezogener Daten aller schwerbehinderter Beschäftigter des Geschäftsbereichs, dem sie zugeordnet ist, befugt ist.

  Eine bereichspezifische gesetzliche Grundlage zur Speicherung personenbezogener Daten dieser Beschäftigtengruppe durch die Hauptschwerbehindertenvertretung ist nicht ersichtlich. Insbesondere begründet § 13 des Schwerbehindertengesetzes (SchwbG) keine dementsprechende Befugnis. Als Empfänger des nach § 13 Abs. 2 Satz 4 SchwbG von den Arbeitgebern auszuhändigenden Verzeichnisses der bei ihnen beschäftigten Schwerbehinderten (§ 13 Abs. 1 SchwbG) kommt nur die für die in einem Betrieb oder einer Dienststelle beschäftigten Schwerbehinderten zuständige Schwerbehindertenvertretung in Betracht. Dies ist in der Regel der unter den Voraussetzungen des § 24 SchwbG gewählte Vertrauensmann (Vertrauensfrau).

  Die Hauptschwerbehindertenvertretung wird für die Wahrnehmung der Belange der schwerbehinderten Beschäftigten nach § 27 Abs. 5 SchwbG erst dann zuständig, wenn diese in einem Betrieb oder einer Dienststelle tätig sind, für die eine Schwerbehindertenvertretung nicht gewählt werden kann oder worden ist. Nur in diesem Fall hätte die nächsthöhere Schwerbehindertenvertretung (Bezirks- bzw. Hauptschwerbehindertenvertretung) die Rechtsstellung und Funktion der örtlichen Schwerbehindertenvertretung.

  Damit die Hauptschwerbehindertenvertretung vom Vorliegen der zuständigkeitsbegründenden Voraussetzungen Kenntnis erlangt, bedarf es ebenfalls keiner Liste mit personenbezogenen Daten der schwerbehinderten Beschäftigten des Geschäftsbereichs, die im übrigen zur Erfüllung dieses Zwecks gar nicht geeignet wäre. Sollte in einem Betrieb oder einer Dienststelle eine Schwerbehindertenvertretung nicht gewählt werden können oder gewählt worden sein, ist diese Tatsache vielmehr eine die dort tätigen schwerbehinderten Beschäftigten als Gruppe berührende Angelegenheit, über die die nächsthöhere Schwerbehindertenvertretung vom Arbeitgeber rechtzeitig und umfassend zu unterrichten ist (§ 25 Abs. 2 Satz 1 i.V.m. § 27 Abs. 6 SchwbG).

  Eine Befugnis zur Speicherung personenbezogener Daten aller schwerbehinderten Beschäftigten des Geschäftsbereichs durch die Hauptschwerbehindertenvertretung läßt sich auch nicht daraus herleiten, daß sie die

Interessen der schwerbehinderten Beschäftigten in Angelegenheiten vertritt, die mehrere Dienststellen des Arbeitgebers betreffen und von den Schwerbehindertenvertretungen der einzelnen Dienststellen nicht geregelt werden können (§ 27 Abs. 5 SchwbG). Die Zuständigkeit der Hauptschwerbehindertenvertretung für die Wahrnehmung der Interessen der betroffenen schwerbehinderten Beschäftigten ist hiernach nur dann begründet, wenn die gesetzlichen Voraussetzungen kumulativ vorliegen. Zwar ist im Gesetzgebungsverfahren erwogen worden, den Aufgabenbereich der nächsthöheren Schwerbehindertenvertretung in diesem Zusammenhang auszuweiten. Diese Bestrebungen haben jedoch keinen Niederschlag im Gesetz gefunden, weshalb die Hauptschwerbehindertenvertretung insoweit nur subsidiär zuständig bleibt, mithin auch in dienststellenübergreifenden Angelegenheiten nur tätig werden kann, wenn diese von den örtlichen Schwerbehindertenvertretungen nicht geregelt werden können. Speicherte die Hauptschwerbehindertenvertretung insoweit dennoch die personenbezogenen Daten aller schwerbehinderten Beschäftigten, stellte dies eine datenschutzrechtlich unzulässige Datenaufbewahrung auf Vorrat dar, weil zum Zeitpunkt der Aufnahme der personenbezogenen Daten in die Datei noch gar nicht absehbar ist, ob die Daten zur Interessenwahrnehmung aus diesem Anlaß je benötigt werden.

Schließlich ergibt sich eine Befugnis zur Speicherung personenbezogener Daten dieser Beschäftigtengruppe auch nicht daraus, daß die Hauptschwerbehindertenvertretung in persönlichen Angelegenheiten, über die eine übergeordnete Stelle entscheidet, zuständig ist (§ 27 Abs. 5 Satz 3 SchwbG). Abgesehen davon, daß aus dieser Aufgabenzuweisungsvorschrift noch keine Befugnis folgt, zur gesetzlichen Aufgabenerfüllung personenbezogene Daten betroffener schwerbehinderter Beschäftigter zu speichern, ist hierbei die Zuständigkeit der Hauptschwerbehindertenvertretung nur von Fall zu Fall begründet. Die insoweit erforderlichen personenbezogenen Daten des/der betroffenen schwerbehinderten Beschäftigten gibt der Arbeitgeber der nächsthöheren (zuständigen) Schwerbehindertenvertretung aus Anlaß der vorgeschriebenen Beteiligung bekannt (§ 25 Abs. 2 i.V.m. § 27 Abs. 6 SchwbG). In diesem Zusammenhang wäre die Speicherung der personenbezogenen Daten aller schwerbehinderten Beschäftigten folglich ebenso eine unzulässige Datenaufbewahrung auf Vorrat.

Im übrigen kann eine Befugnis zur Speicherung der personenbezogenen Daten der genannten Beschäftigtengruppe auch nicht auf die Bestimmung der Nr. 2.4.2 des Runderlasses des Innenministers vom 10. Juni 1987 zur Durchführung der §§ 11 und 13 des Schwerbehindertengesetzes in der Landesverwaltung (MBl. NW. S. 762) gestützt werden. Die hiermit verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht der Betroffenen lassen sich nicht auf Verwaltungsvorschriften, sondern nur auf eine gesetzliche Grundlage stützen. Ich habe

mich insoweit an das Innenministerium des Landes Nordrhein-Westfalen gewandt und eine Klarstellung dieser Erlaßregelung angeregt.

- Schwerbehindertenvertretungen verschiedener öffentlicher Stellen habe ich ferner darüber unterrichtet, unter welchen Voraussetzungen die Verarbeitung personenbezogener Daten von bestimmten Maßnahmen betroffener schwerbehinderter Beschäftigter durch den **örtlichen Vertrauensmann (Vertrauensfrau)** zulässig ist.

  Soweit das Schwerbehindertengesetz keine normenklaren bereichspezifischen Vorschriften über die Verarbeitung personenbezogener Daten der schwerbehinderten Beschäftigten der Dienststelle durch die Schwerbehindertenvertretung enthält, ist die Datenverarbeitung nur auf Grund einer (z. B. anläßlich eines Beratungsgesprächs mit der Schwerbehindertenvertretung erteilbaren) Einwilligung des/der Betroffenen zulässig (§ 4 DSG NW). Hierbei muß der/die Betroffene in Schriftform über die jeweilige Maßnahme (z. B. Einrichtung/Verbesserung eines bestimmten Arbeitsplatzes) und die Erhebung und Speicherung der insoweit erforderlichen personenbezogenen Daten unterrichtet werden. Der/die Betroffene muß hierbei insbesondere auch über die Dauer der Speicherung der personenbezogenen Daten und deren Verbleib informiert werden.

  Ebenfalls nur mit Einwilligung des/der schwerbehinderten Beschäftigten kann das bei bevorstehenden Beurteilungen zu führende Gespräch der Schwerbehindertenvertretung mit dem Erstbeurteiler in Betracht kommen (vgl. 11. Tätigkeitsbericht, S. 80). Hierbei können die Betroffenen dem Vertrauensmann/der Vertrauensfrau im einzelnen vorgeben, welche Gesichtspunkte dem Erstbeurteiler von der Schwerbehindertenvertretung mitgeteilt und von dieser auch in einer schriftlichen Stellungnahme zur Beurteilung genutzt werden dürfen.

5.11 Statistik

5.11.1 Abschottung der Statistikstelle vom Verwaltungsvollzug

Einer Anfrage habe ich entnommen, daß im Statistischen Amt und Wahlamt einer Stadtverwaltung die zur Abschottung der dort eingerichteten Statistikstelle vom Verwaltungsvollzug erforderlichen Maßnahmen nicht in vollem Umfang getroffen worden sind (vgl. 9. Tätigkeitsbericht, S. 86/87, 10. Tätigkeitsbericht, S. 108). Nach der Dienstanweisung für die Kommunalstatistik und für die Statistikstelle sowie dem Dienstverteilungsplan des Oberstadtdirektors war nicht sichergestellt, daß alle Aufgaben, bei deren Erledigung dem Statistikgeheimnis unterliegende Einzelangaben anfallen, ausschließlich der Statistikstelle zugewiesen sind. Derartige **Regelungsdefizite** ermöglichen, daß statistische Aufgaben, z. B. die Anforderung und Auswertung von Einzelangaben, unter Verletzung des Statistikgeheimnisses (§ 16 BStatG) auch außerhalb der Statistikstelle erledigt werden können. Darüber hinaus waren dem Leiter des Statistischen Amtes und Wahlamtes fachaufsichtliche Befugnisse über die Statistikstelle übertragen. Auch eine

solche Regelung trägt dem Gebot einer organisatorischen und personellen Trennung der Statistik vom allgemeinen Verwaltungsvollzug nicht Rechnung (§ 32 Abs. 2 DSG NW), weil der Amtsleiter in Ausübung der Fachaufsicht mit dem Statistikgeheimnis unterliegenden Vorgängen nicht befaßt werden darf.

Die zur Abschottung erforderlichen Maßnahmen habe ich mit dem Oberstadtdirektor erörtert. Hiernach hat dieser meinen Bedenken Rechnung tragende Regelungen in der Dienstanweisung sowie dem Dienstverteilungsplan getroffen und die Fachaufsicht über die Statistikstelle dem Leiter des Rechnungsprüfungsamtes übertragen.

5.11.2 Sozialhilfestatistik

Mehrere Eingaben richteten sich gegen den von Sozialämtern als Anlage zum Sozialhilfebescheid versandten Fragebogen über ergänzende Angaben zur Sozialhilfestatistik. Teilweise wurden die Empfänger aufgefordert, unter Hinweis auf ihre „Auskunftspflicht" nach dem Bundessozialhilfegesetz sowie ihre Mitwirkungspflicht nach dem Sozialgesetzbuch eigene und Daten von anderen Haushaltsmitgliedern, die Sozialhilfe erhalten, anzugeben.

Bei der Sozialhilfestatistik handelt es sich um eine Sekundärstatistik, für die nur solche Daten genutzt werden dürfen, die im Rahmen des Verwaltungsvollzugs, d. h. für die Gewährung von Sozialhilfe als im jeweiligen Einzelfall erforderlich erhoben worden sind. Dementsprechend ist nach § 131 Abs. 2 BSHG auskunftspflichtig allein der Sozialhilfeträger.

Eine **Datennacherhebung** (etwa mittels Fragebogen) beim Betroffenen eigens für die Sozialhilfestatistik ist - auch auf freiwilliger Basis - unzulässig. Für eine derartige primärstatistische Erhebung innerhalb der Sekundärstatistik fehlt eine gesetzliche Grundlage. Somit widerspricht der Hinweis auf die Auskunftspflicht des Hilfeempfängers bei gleichzeitiger Androhung der Leistungsverweigerung evident der Gesetzeslage.

Meiner Empfehlung, davon abzusehen, Daten eigens für die Sozialhilfestatistik beim Betroffenen nachzuerheben sowie bereits (unzulässigerweise) nacherhobene Daten im Wege der Folgenbeseitigung unausgewertet zu löschen, sind die Träger der Sozialhilfe gefolgt.

Da davon auszugehen war, daß auch andere Sozialhilfeträger zur Erfüllung ihrer Auskunftspflicht Daten, die ihnen im Rahmen ihrer Aufgabenerfüllung nicht bekanntgeworden sind, allein für die Sozialhilfestatistik bei den Hilfeempfängern nacherheben, habe ich das Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen gebeten, alle Sozialhilfeträger über meine Rechtsauffassung zu unterrichten. Das Ministerium hat daraufhin mit Erlaß vom November 1994 die Bezirksregierungen und die örtlichen Träger der Sozialhilfe darauf hingewiesen, daß „eine Datenerhebung nur zum Zwecke der Sozialhilfestatistik durch die Vorschriften des Bundessozialhilfegesetzes nicht gedeckt ist".

5.12 Wissenschaft und Forschung

5.12.1 Einschreibungsordnungen

In den Einschreibungsordnungen nach § 64 Abs. 1 des Universitätsgesetzes (UG) sollen die Hochschulen Regelungen darüber treffen, welche Daten von den Studierenden im Rahmen der Einschreibung erhoben werden dürfen. Außerdem können weitere Datenverarbeitungen wie etwa die Speicherung dieser Daten, die Weitergabe innerhalb der Hochschulverwaltung und innerhalb der Hochschule, aber auch die technischen Verfahren der Datenverarbeitung geregelt werden.

Eine Universität hatte mich zu dem Entwurf ihrer Einschreibungsordnung um Stellungnahme gebeten. Dabei stellte ich fest, daß anders als bei den bisherigen Einschreibungsordnungen - jedenfalls soweit mir bekannt - neben der Feststellung, welche Daten der Studierenden im einzelnen von der Hochschulverwaltung zur Einschreibung erhoben werden dürfen, auch Regelungen zur Weitergabe von Daten der Studierenden innerhalb der Hochschule vorgesehen waren. Grundsätzlich begrüße ich es, wenn entsprechend den Anforderungen des Datenschutzes die Studierenden durch die Einschreibungsordnung erfahren können, welche Einrichtung der Hochschule - insbesondere außerhalb der Hochschulverwaltung bzw. des Studentensekretariats - welche Daten erhält.

Allerdings reicht die **Regelungsbefugnis** der Hochschule in der Einschreibungsordnung nur soweit, wie die Ermächtigungsgrundlage des § 64 UG den Rahmen zulässiger Datenverarbeitung vorgibt. Sie gilt für jede mit der Einschreibung in unmittelbarem Zusammenhang stehende Datenverarbeitung. Deshalb halte ich beispielsweise eine Regelung über die Weitergabe von Daten der Studierenden, die ihre Regelstudiendauer überschritten haben, zur Überprüfung des ordnungsgemäßen Studienverlaufs durch die Dekanate mit dem in § 64 UG festgelegten Verwendungszweck nicht mehr für vereinbar. Ebensowenig trifft dies auf die Übermittlung von Daten aller eingeschriebenen Studierenden an die Prüfungsämter zu, weil nicht erkennbar ist, aus welchen Gründen die Prüfungsämter bereits zu diesem Zeitpunkt die Daten der eingeschriebenen Studierenden benötigen. Im Hinblick darauf, daß in vielen Fällen noch nicht feststeht, ob der Studierende seine Prüfungen bei diesem Prüfungsamt absolvieren wird, würde durch eine solche Übermittlung beim Prüfungsamt eine unzulässige Datenspeicherung auf Vorrat entstehen. Dagegen dürften die Daten nur derjenigen eingeschriebenen Studierenden erforderlich sein, die vor einer Prüfung stehen.

Mit der Einschreibung hängen weiterhin unmittelbar zusammen das Erstellen von Wählerverzeichnissen, die Weitergabe der Daten der eingeschriebenen Studierenden an die Dekanate, Institute und die Universitätsbibliothek im erforderlichen Umfang sowie die Weitergabe von Daten ausländischer Studierender an das Akademische Auslandsamt. Voraussetzung für eine zulässige Weitergabe an andere Einrichtungen der Hochschule muß sein, daß die Daten der Studierenden zur rechtmäßigen Aufgabenerfüllung benötigt

werden. Vor Weitergabe von personenbezogenen Daten an die Dekanate ist deshalb zu prüfen, ob die Kenntnis der Daten für die Erfüllung der in §§ 25 und 27 UG festgelegten Aufgaben des Dekanates notwendig ist. Wenn etwa bedarfsgerecht die Daten derjenigen Studierenden, die im 6. klinischen Semester stehen, an das Dekanat der medizinischen Fakultät weitergegeben werden sollen, damit von dort die Anmeldung für das praktische Jahr erfolgen kann, ist die Weitergabe unzulässig, weil es nicht gesetzliche Aufgabe des Dekanates der medizinischen Fakultät ist, alle im 6. klinischen Semester stehenden Studierenden zum praktischen Jahr anzumelden.

5.12.2 Überwachung der Studiendauer

Um sog. „Langzeitstudierenden" ein individuelles Beratungsangebot zu unterbreiten und sie beim erfolgreichen Abschluß des Studiums zu unterstützen, ließ der Kanzler einer Universität eine Liste mit allen Studierenden erstellen, die die **Regelstudienzeit** im jeweiligen Studiengang um mehr als drei Semester überschritten hatten. Studiengangsbezogene Auszüge dieser Liste wurden den Dekaninnen und Dekanen der jeweiligen Fachbereiche übersandt. In dem Begleitschreiben bat der Kanzler darum, die betroffenen Studierenden anzusprechen und die Hochschulverwaltung über weitere Aktivitäten zu informieren. Nach Auffassung des Kanzlers bestanden keine rechtlichen Hindernisse, den Dekaninnen und Dekanen Namenslisten der Studierenden zur Verfügung zu stellen. Als Rechtsgrundlage verwies der Kanzler auf § 6 Abs. 1 Nr. 5 i.V.m. Abs. 2 Satz 1 des Universitätsgesetzes (UG) und § 1 Abs. 6 der Einschreibungsordnung der Universität. Nach kritischen Berichten in der Tagespresse stoppte das Rektorat jedoch die Aktion und ließ alle Listen sofort einziehen.

Auf die vom Kanzler herangezogenen Vorschriften konnte eine derartige Datennutzung nicht gestützt werden, da sie nicht normenklar sind. Nach dem Universitätsgesetz soll die Studienreform gewährleisten, daß das Studium innerhalb der Regelstudienzeit abgeschlossen werden kann. An die in § 84 UG festgelegte Regelstudiendauer ist aber eine für die Studierenden verbindliche Rechtsfolge nicht geknüpft, so daß eine Sanktionsmöglichkeit für die Hochschule gegenüber den die Regelstudiendauer überschreitenden Studierenden selbst ausscheidet. Die von den Hochschulen zu treffenden Maßnahmen (§ 6 Abs. 2 Satz 1 UG) können sich daher nur auf Maßnahmen wie etwa die Gestaltung der Studienordnung, Sicherstellung des Lehrangebots und die Gestaltung des Prüfungsverfahrens beziehen (§ 84 Abs. 1 Satz 2 UG). Außerdem enthält die Einschreibungsordnung keine Übermittlungsregelung, die Rechtsgrundlage für eine Datenweitergabe dieser Art an die Dekaninnen und Dekane der Fachbereiche sein könnte.

Nach Darstellung des Kanzlers der Universität war die Aktion auch nur als individuelles Beratungsangebot und nicht als Zwangsberatung gedacht. Für ein derartiges Angebot war eine personenbezogene Datenverarbeitung - insbesondere die Weitergabe von Daten einer bestimmten Gruppe an die Dekaninnen und Dekane - somit nicht erforderlich.

5.12.3 Presseauskünfte

Im Hochschulbereich hat die datenschutzrechtlich nicht unproblematische Frage der Erteilung von Presseauskünften über das Hochschulpersonal unter zwei besonderen Aspekten eine Rolle gespielt. Zum einen war festzustellen, daß im Zusammenhang mit Auskünften über zwei Professoren die neue, einschlägige Vorschrift zum Personalaktenrecht keine Beachtung gefunden hat. Zum anderen wurde die Bestätigung der Einleitung eines Disziplinarverfahrens gegenüber einer Journalistin als datenschutzrechtlich unbedeutend angesehen.

Zunächst sind bei jeder Auskunft gegenüber der Presse über Angelegenheiten des Hochschulpersonals die Regelungen des § 4 Abs. 1 und Abs. 2 Nr. 2 des Landespressegesetzes zu beachten. Danach ist die grundsätzlich bestehende Verpflichtung einer Behörde, den Vertretern der Presse die der Erfüllung ihrer öffentlichen Aufgabe dienenden Auskünfte zu erteilen, ausgeschlossen, wenn der Auskunftserteilung Vorschriften über die Geheimhaltung entgegenstehen.

Nach dem Inkrafttreten des durch Gesetz vom 6. Juli 1993 (GV. NW. S. 468) neugefaßten § 102 Abs. 1 Satz 1 des Landesbeamtengesetzes (LBG), der eine zur Verarbeitung von Personalaktendaten speziellere Vorschrift enthält und gegenüber § 29 DSG NW vorrangig anzuwenden ist, wird die Geheimhaltung aller Personalaktendaten ausdrücklich vorgeschrieben. Zu den Personalaktendaten gehören auch Daten aus oder über Disziplinarverfahren. Eine Bekanntgabe von Personalaktendaten an die Presse ist daher grundsätzlich verboten. Nur im Ausnahmefall des § 102 d Abs. 2 Satz 1 LBG wird der grundsätzliche Ausschluß von Auskünften an die Presse durchbrochen, wenn der Schutz berechtigter, höherrangiger Interessen eines Dritten die Auskunftserteilung zwingend erfordert. Dritter ist jede Person oder Stelle außerhalb der Personalaktendaten verarbeitenden Stelle, also auch jeder anfragende Journalist. An eine ausnahmsweise Bekanntgabe von Daten des Hochschulpersonals an die Presse sind daher strenge Anforderungen zu stellen.

In dem einen von mir zu beurteilenden Fall war von einem Presseorgan Auskunft über den universitären und klinischen **Werdegang** und über die Prüfungsbewertung der erworbenen beruflichen Studien- und Ausbildungsabschlüsse eines Professors erbeten worden, dessen fachliche Eignung als Sachverständiger in einem Strafprozeß in Zweifel gezogen wurde. Weder war zum damaligen Zeitpunkt ein gegenüber dem Geheimhaltungsinteresse des Betroffenen höherrangiges Informationsinteresse erkennbar. Noch war es zum Zeitpunkt der Berichterstattung zwingend notwendig, daß das Ministerium Auskunft über den beruflichen Werdegang des Professors erteilte, um dem Bedürfnis nach Informationen gerecht zu werden. Es war vielmehr davon auszugehen, daß die Einvernahme des Sachverständigen im Strafprozeß die für die Berichterstattung erforderlichen Informationen über den Prozeß erbringen würde.

In einem anderen Fall handelte es sich um das Verhalten eines Professors, das zu einer großen Unruhe unter den Studierenden in seinem Fachbereich und einer kritischen Berichterstattung in der Presse geführt hatte. Zur Klärung der Richtigkeit seines Verhaltens hatte der Professor ein **Disziplinarverfahren** gegen sich selbst beantragt. Auch hier war nicht ersichtlich, aus welchen Gründen das Informationsbedürfnis der Presse gegenüber dem Geheimhaltungsanspruch des Betroffenen höherrangig und eine Auskunftserteilung darüber, daß der Professor ein Disziplinarverfahren gegen sich selbst beantragt hat, zwingend erforderlich war.

Darüber hinaus stellte sich die Frage, ob dann, wenn das Ministerium der Presse gegenüber lediglich bestätigt, daß der in der Anfrage vorgetragene Sachverhalt zutrifft, eine Datenschutzverletzung nicht eintreten könnte. Zunächst gilt hier grundsätzlich, daß auch die Bestätigung eines Sachverhaltes die Aussage enthält, daß gegen den Betroffenen ein Disziplinarverfahren eingeleitet ist. Unabhängig davon, daß diese Aussage eine andere Qualität erhält, weil sie vom Dienstvorgesetzten unmittelbar kommt und nicht nur auf eigenen Recherchen beruht, stellt sie inhaltlich die Bekanntgabe eines personenbezogenen Datums dar. Für die Feststellung, ob eine Übermittlung stattgefunden hat, kommt es nicht darauf an, daß die übermittelte Angabe bereits bekannt war. Daher sind aus datenschutzrechtlicher Sicht an die Bestätigung personenbezogener Angaben über Hochschulpersonal gegenüber der Presse die gleichen Anforderungen zu stellen wie an die Erteilung von Presseauskünften.

5.12.4 Personalbogen der Hochschulen

Bereits in meinem 10. Tätigkeitsbericht (S. 96 bis 98) hatte ich die Datenerhebung zur Anlegung von Personalbogen bei Eingehung eines Dienst- oder Arbeitsverhältnisses behandelt.

Nunmehr habe ich den Personalbogen einer Universität - diesmal der Medizinischen Einrichtungen - datenschutzrechtlich geprüft, der von den Betroffenen nach der Entscheidung über die Einstellung auszufüllen war. Dabei mußte ich feststellen, daß unzulässigerweise Fragen nach Geburtsdatum und -ort des Ehegatten sowie dessen Staatsangehörigkeit, Fragen zur Versorgung und zum Versicherungsverhältnis sowie zum Beihilfeanspruch des Antragstellers und nach Schulden und Vorstrafen enthalten waren. Nachdem ich die Universität um Stellungnahme zur Erforderlichkeit dieser Angaben gebeten hatte, überarbeitete sie den Personalbogen; die entsprechenden Fragen sind entfallen.

Im neuen Personalbogen wurde aber weiterhin nach Angaben zu den Kindern des Antragstellers (Geburtsdaten, Kindschaftsverhältnis, Kindergeld) gefragt, die nicht für die Universität, sondern für die Zahlbarmachung der Bezüge durch das Landesamt für Besoldung und Versorgung (LBV) bestimmt sind. Solche Angaben sind nach dem Runderlaß des Finanzministeriums vom 6.5.1993 (MBl. NW. S. 898) auf vorgegebenen separaten Fragebogen

für das LBV zu erheben. Eine parallele Erhebung dieser Daten ist nicht erforderlich und daher datenschutzrechtlich unzulässig.

Auch der überarbeitete Personalbogen enthielt noch die Frage nach der Art der Behinderung. Diese Erhebung personenbezogener Daten geht über die - allgemein als zulässig erachtete - Frage nach der Schwerbehinderteneigenschaft hinaus. Die Frage nach der Art der Behinderung kann in datenschutzrechtlicher Hinsicht nur dann als unbedenklich erachtet werden, wenn dem Dienstherrn insoweit ein Fragerecht zusteht, er also ein berechtigtes und schutzwürdiges Interesse an der Beantwortung speziell dieser Frage für das Dienstverhältnis hat. Soweit daher die Fragestellung nicht darauf abzielt, Informationen zu einer gerade durch die Körperbehinderung möglichen Beeinträchtigung seiner Tätigkeit oder zur behindertengerechten Ausgestaltung des Arbeitsplatzes zu erlangen, ist sie vom Fragerecht des Dienstherrn nicht gedeckt und damit auch in datenschutzrechtlicher Hinsicht unzulässig. Die Universität wird meinen Empfehlungen zum Datenschutz folgen und den Personalbogen nochmals überarbeiten.

Zur Verwendung der gleichen Personalbogen auch bei Einstellungen von Kurzzeitbeschäftigten an einer anderen Universität habe ich festgestellt, daß der Umfang der erfragten Daten zu groß ist. Fragen nach Geburtsort, Staatsangehörigkeit, Familienstand und den Kindern sind im Hinblick auf eine Pauschalvergütung für Hilfskräfte nicht erforderlich. Ebenso gehen Fragen nach einer evtl. Lebensversicherung oder sonstigem Einkommen bei diesem Personenkreis zu weit.

5.12.5 Qualifikationsüberprüfung

Der geschäftsführende Direktor des Instituts einer westfälischen Universität hat über einen wissenschaftlichen Mitarbeiter **Eignungsgutachten** von zwei Professoren des Fachbereichs anläßlich einer anstehenden Vertragsverlängerung eingeholt. Auch nach umfangreichem Schriftwechsel konnte die Universität nicht klären, ob das Rektorat als für die Entscheidung zuständige Stelle die Gutachten über den Direktor angefordert hatte oder ob sie ohne Veranlassung durch den geschäftsführenden Direktor vorgelegt worden waren. In einem Schreiben an den Betroffenen legte der Institutsleiter aber selbst dar, daß das Direktorium des Instituts über den Verlängerungsantrag beraten und zwei sachverständige Kollegen des Fachbereichs um fachliche Stellungnahme gebeten hätte; er selbst und ein weiteres Mitglied des Direktoriums hätten ebenfalls eine schriftliche Stellungnahme angefertigt; die ablehnenden Stellungnahmen hätte er dem Kanzler der Universität mitgeteilt. Nach der Entscheidungsfindung wurden die Gutachten nicht etwa zur Personalakte des Betroffenen genommen, sondern den Gutachtern unmittelbar wieder zugeleitet. Wie sich aus dem arbeitsgerichtlichen Verfahren zur Frage der Vertragsverlängerung ergab, waren die Gutachten zur Entscheidungsfindung nicht erforderlich gewesen.

Dieser Sachverhalt ist datenschutzrechtlich wie folgt zu bewerten:

Die Einholung von Eignungsgutachten oder entsprechenden Stellungnahmen ist als Datenerhebung über den wissenschaftlichen Mitarbeiter nach § 29 Abs. 1 Satz 1 DSG NW nur zulässig, wenn sie zur Entscheidung über die Weiterführung des Arbeitsverhältnisses erforderlich war. Eine solche Mitarbeiterbewertung konnte zunächst einmal nur von der zuständigen Stelle, also dem Rektorat, veranlaßt werden. Das Rektorat hatte außerdem selbst zu prüfen, ob Stellungnahmen und mit welcher Fragestellung eingeholt werden mußten. Diese Entscheidung durfte es nicht dem Institutsdirektor überlassen. Auch im Hochschulbereich kann nicht jeder Vorgesetzte nach Gutdünken Gutachten oder Stellungnahmen über Mitarbeiter einholen. Nach der Feststellung im arbeitsgerichtlichen Urteil waren die Gutachten bzw. Stellungnahmen überdies nicht erforderlich. Dafür spricht auch, daß letztlich die Gutachten bzw. schriftlichen Stellungnahmen nicht zur Personalakte genommen wurden. Eine Aufbewahrung der Gutachten in der Personalakte wäre aber dann geboten gewesen, wenn sich die Entscheidung über die Personalmaßnahme auf die Gutachten gestützt hätte.

Nach dem Vortrag der Universität mußte ich davon ausgehen, daß die Gutachten noch im Fachbereich gespeichert sind. Eine Speicherung liegt datenschutzrechtlich auch dann vor, wenn sie bei den Gutachtern erfolgt. Unzulässig gespeicherte Daten sind zu vernichten. Ich habe daher der Universität empfohlen, die Gutachter anzuweisen, die Unterlagen zu vernichten und dem Betroffenen in diesem Zusammenhang vorher Gelegenheit zu geben, zu entscheiden, ob er nach § 19 Abs. 2 b DSG NW die Sperrung der Daten verlangen will.

Die Universität will dieser Empfehlung nicht folgen, weil sie nach ihrer Auffassung mit der Rückgabe der Stellungnahmen und der Gutachten an die Wissenschaftler für die Zulässigkeit einer weiteren Speicherung der Daten über den Betroffenen nicht mehr verantwortlich sei. Außerdem hält sie die Einholung der Stellungnahmen und Gutachten nunmehr aus einem anderen Grund für erforderlich; sie habe darüber entscheiden müssen, ob von der Hochschule eine weitere Förderung des von dem Betroffenen durchgeführten Forschungsprojekts befürwortet und ein entsprechender Förderungsantrag gestellt werden konnte. Unabhängig davon, daß datenschutzrechtliche Bedenken gegen die Art der weiteren Speicherung der Stellungnahmen und Gutachten bestehen bleiben, habe ich erhebliche Zweifel an der Zulässigkeit der Einholung von vier Stellungnahmen und zwei Gutachten für eine Entscheidung über die Förderung eines Forschungsvorhabens.

5.12.6 Forschungsvorhaben „Gefühle Jugendlicher in Ost und West"

Eine nordrhein-westfälische Hochschule wollte bundesweit eine Befragung an Schulen durchführen, die von einigen Kultusministerien u. a. auch aus Datenschutzgründen nicht genehmigt worden ist. Die Befragung, von der ich nicht unterrichtet wurde, sollte mit Schülerinnen und Schülern der Klas-

sen 5 bis 10 - also mit Kindern im Alter von 11/12 Jahren an aufwärts - durchgeführt werden. Die in der Klasse ausgeteilten Fragebogen sollten unter Aufsicht der Lehrer ausgefüllt und an diese zurückgegeben werden.

Bei der datenschutzrechtlichen Prüfung war besonders zu berücksichtigen, daß mit nahezu 90 Fragen aus den Bereichen Familie, Freizeit, Schule und Politik auch sensible Angaben über das Verhältnis zu den Eltern, über das Verhalten der Eltern untereinander, über Alkohol- und Drogenkonsum und Straffälligkeit der Befragten erhoben werden sollten. Die Art der Befragung sowie die zugesagte Anonymität stießen deshalb auf datenschutzrechtliche Bedenken. Einmal war fraglich, ob von einer für die Erteilung einer wirksamen Einwilligung notwendigen Einsichtsfähigkeit zumindest der Schülerinnen und Schüler in den Klassen 5 und 6 ausgegangen werden konnte, oder ob nicht für einen Teil der Kinder die Einwilligung der Erziehungsberechtigten eingeholt werden mußte. Weiterhin schien mir die Freiwilligkeit der Teilnahme dann zweifelhaft zu sein, wenn sich die Schülerinnen und Schüler dem Ausfüllen der Fragebogen im Klassenverband unter Aufsicht der Lehrkräfte wohl eher einem gewissen Gruppenzwang hätten entziehen müssen. Schließlich war auch bei der Art der Durchführung die Anonymität der Befragten nicht gewährleistet. Weder war ausgeschlossen, daß die Schülerinnen und Schüler Kenntnis von den Antworten der Mitschüler hätten erlangen können. Noch war bei der Rückgabe der ausgefüllten Fragebogen über die Lehrkraft auszuschließen, daß Lehrer Kenntnis von den Angaben einzelner Schülerinnen und Schüler erlangen und die Angaben - etwa durch die Handschrift - auf konkrete Personen beziehen konnten.

Meine dementsprechenden Fragen an die Hochschule zogen nicht eine datenschutzgerechte Änderung der Verfahrensweise sondern die Einstellung des Forschungsvorhabens in Nordrhein-Westfalen nach sich.

5.13 Schule

5.13.1 Datenflüsse im Schulamt

Bereits in meinem 11. Tätigkeitsbericht (S. 99) hatte ich darauf hingewiesen, daß vermutlich eine klare Trennung zwischen Schulamt als unterer Schulaufsichtsbehörde und dem Schulverwaltungsamt als Verwaltungsbehörde des Schulträgers fehlt. Diese Annahme hat sich bei meinen Informations- und Kontrollbesuchen in mehreren Schulämtern bestätigt.

In allen besuchten Schulämtern mußte ich feststellen, daß durch die hierarchische Unterordnung des verwaltungsfachlichen Personals des Schulamtes unter die Dienst- und Fachaufsicht des für das Schulverwaltungsamt verantwortlichen Amtsleiters bzw. Dezernenten besonders in kreisfreien Städten Kollisionen in datenschutzrechtlicher Hinsicht nicht ausgeschlossen waren. Soweit nämlich der Leiter des Schulverwaltungsamtes gegenüber dem verwaltungsfachlichen Leiter des Schulamtes - meist seinem Vertreter - Weisungsbefugnis besitzt, können sich Interessenkonflikte dadurch ergeben, daß er Zugang zu den im Schulamt gespeicherten Personaldaten der Lehrer hat.

Beispielsweise kann sich der Amtsleiter bzw. Dezernent auf Grund seines Weisungsrechts ohne weiteres die Personalakte eines bestimmten Lehrers vorlegen lassen. Dies ist in kreisfreien Städten, also bei Schulträgern für eine große Anzahl von Schulen, im Hinblick auf das Vorschlagsrecht zur Besetzung von Schulleiterstellen nach § 21 a des Schulverwaltungsgesetzes nicht unvorstellbar.

Um solche unzulässigen Datenflüsse zwischen Schulamt und Schulverwaltungsamt zu verhindern, darf nach meiner Auffassung die Fachaufsicht über das Schulamt nicht vom Amtsleiter des Schulverwaltungsamtes wahrgenommen werden. Entsprechende organisatorische Maßnahmen sollten schriftlich in einer **Dienstanweisung** angeordnet werden, damit sich der etwa angewiesene verwaltungsfachliche Leiter des Schulamtes im Konfliktfall darauf berufen kann. Außerdem könnte die Geschäftsordnung für das Schulamt (BASS 10-32 Nr. 2) entsprechend ergänzt werden.

Zum anderen stieß ich im Rahmen meiner Besuche in den Schulverwaltungsämtern zweier kreisfreier Städte auf eine Datei mit personenbezogenen Daten **aller Schüler** dieser Stadt. Diese Datei wird unter Auswertung des Melderegisters und der Rückmeldungen der Schulen über Schulbesuch und Schulwechsel ständig fortgeschrieben. Die Rechtsgrundlage für eine derartige Datei mit über 20 000 Schülerdaten ist ebensowenig ersichtlich, wie die Frage beantwortet werden konnte, zu welcher Aufgabenerfüllung die Speicherung einer derartigen Datenfülle durch den Schulträger erforderlich ist; für planerische Zwecke ist ein Personenbezug jedenfalls nicht notwendig. Es handelt sich hierbei offensichtlich um datenschutzrechtlich bedenkliche Datenfriedhöfe.

Als problematisch habe ich schließlich noch die „automatische" Übermittlung von Durchschriften an andere Stellen wie z. B. im Falle der Verhängung eines Bußgeldes wegen fortgesetzter Schulversäumnisse u. a. an das Jugendamt der Stadt angesehen. Eine Rechtsgrundlage für derartige Übermittlungen - ohne Prüfung des Einzelfalles - gibt es nicht. Nach § 19 Abs. 5 des Schulverwaltungsgesetzes ist eine Übermittlung nur zulässig, soweit der Empfänger die Daten für seine gesetzliche Aufgabenerfüllung benötigt. Dies bedeutet, daß vor Übermittlung der Durchschrift eine **Einzelfallprüfung** erforderlich ist. Ebenso ist eine Übermittlung der kompletten Durchschrift des Bußgeldbescheides an den Schulleiter unzulässig, da die Kenntnis des Bußgeldbescheides für die Aufgabenerfüllung des Schulleiters nicht erforderlich ist. Es reicht aus, wenn er erfährt, daß ein Bußgeld verhängt wurde.

Gleichfalls halte ich die Praxis für unzulässig, dem örtlichen Personalrat informationshalber Durchschriften von Berichten an die obere Schulaufsichtsbehörde in Personalangelegenheiten zukommen zu lassen, über die allein die obere Schulaufsichtsbehörde zu entscheiden hat, wie z. B. die amtsärztliche Untersuchung zur Entscheidung über eine vorzeitige Zurruhesetzung oder aber die Verlängerung der Probezeit. Personalvertretungsrechtlich ist nicht der örtliche Personalrat, sondern der Bezirkspersonalrat zu

beteiligen. Die nach § 65 LPVG notwendigen Informationen werden dem Bezirkspersonalrat von der Bezirksregierung gegeben. Die unzulässige Datenweitergabe wird auch nicht dadurch gerechtfertigt, daß sie auf Wunsch der Bezirksregierung einerseits und mit der Begründung andererseits erfolgt, der örtliche Personalrat würde vom Bezirkspersonalrat sowieso informiert und um Stellungnahme gebeten. Letztere Verfahrensweise ist im Landespersonalvertretungsgesetz nicht vorgesehen und daher ebenfalls datenschutzrechtlich bedenklich.

5.13.2 Gesteuerter Schulwechsel

Datenschutzrechtlichen Bedenken begegnete das Verfahren eines Schulträgers zur Anmeldung von Schülerinnen und Schülern an weiterführende Schulen. Die Erziehungsberechtigten der Kinder, die die Klasse 4 der Grundschulen besuchten, erhielten einen vom Schulträger erstellten Anmeldevordruck, der ausgefüllt von den Grundschulen an den Schulträger zurückgereicht wurde. In einem sog. Abstimmungsgespräch mit den Schulleiterinnen und Schulleitern der weiterführenden Schulen wurden diesen die Anmeldebogen übergeben. In dem Fall, der meiner Überprüfung zugrunde lag, wurde die Anmeldung eines Schülers für ein bestimmtes Gymnasium jedoch an den Leiter einer Gesamtschule weitergegeben, die noch über eine entsprechende Aufnahmekapazität verfügte.

Die Zuleitung der Anmeldebogen von der Grundschule an den Schulträger und die Steuerung der Verteilung der einzelnen Anmeldungen durch den Schulträger erfolgten ohne jede Rechtsgrundlage. § 3 Abs. 6 Satz 2 und 3 der Verordnung zu § 5 des Schulfinanzgesetzes (BASS 11-11 Nr. 1) bestimmt, daß die Schulaufsichtsbehörde die Entscheidungen der Schulleitungen über die Aufnahme von Schülern unter Beteiligung des Schulträgers koordiniert. Der Schulträger entscheidet lediglich darüber, an welchen Schulen die erforderlichen Eingangsklassen gebildet werden. Entscheidungen über die Aufnahme einzelner Schülerinnen und Schüler an weiterführenden Schulen müssen vom Schulträger nicht getroffen werden, sie sind vielmehr als Eingriffe in das Erziehungsrecht der Eltern verfassungsrechtlich bedenklich.

So hat auch der Verfassungsgerichtshof des Landes Nordrhein-Westfalen in seinem Urteil vom 24. August 1993 (VerfGH 13/92; DVBl. 1993, 1209) festgestellt, daß § 5 des Schulfinanzgesetzes keine Ermächtigung zum Eingriff in Grundrechte der Eltern enthält. Die letztendliche Entscheidung über die Aufnahme eines Schülers an eine Schule trifft nach § 26 Abs. 3 Nr. 1 des Schulverwaltungsgesetzes i.V.m. § 5 Abs. 2 Satz 1 der Allgemeinen Schulordnung allein der Schulleiter.

Deshalb ist für eine Übermittlung von Schülerdaten an den Schulträger im Zusammenhang mit dem Verteilungsverfahren kein Raum. Voraussetzung für die Zulässigkeit einer derartigen Datenverarbeitung wäre, daß die Kenntnis der Schülerdaten für die rechtmäßige Erfüllung seiner Aufgaben

erforderlich ist. Selbst in den Fällen, in denen die Aufnahme an eine gewünschte Schule aus Kapazitätsgründen nicht möglich ist, braucht der Schulträger keine Schüler- und Elterndaten. Es dürfte ausreichen, wenn der Schulträger anonymisierte (aggregierte) Daten von der Schule erhält, in die der Schüler aufgenommen werden will, damit der Schulträger in der Konferenz mit den Schulleitern entsprechende notwendige Verteilungsvorgaben erarbeitet. Der Schulleiter kann dann den Erziehungsberechtigten entsprechende Hinweise auf weiterführende Schulen mit freien Plätzen geben.

Ich habe daher dem Schulträger empfohlen, das Verfahren so zu gestalten, daß keine personenbezogenen Daten der Schüler und Eltern von den abgebenden Schulen wie auch von den in der Anmeldung gewünschten Schulen an den Schulträger übermittelt werden. Der Schulträger ist meiner Empfehlung gefolgt.

5.13.3 Gestörte Vertrauensverhältnisse

Welche tiefgreifenden Auswirkungen die Mißachtung des Datenschutzes auf das Vertrauensverhältnis zwischen Lehrkraft und Erziehungsberechtigten haben kann, stellte sich in einem Fall heraus, in dem die Mutter eines Schülers anläßlich einer bevorstehenden Klassenfahrt, an der sie wie schon vorher als Begleitperson teilnehmen wollte, der Klassenlehrerin in einem vertraulichen Brief sehr offen über sich und ihr Kind geschrieben hatte. Ihrer Bitte um ein Gespräch mit der Klassenlehrerin wurde in der Weise entsprochen, daß zum vereinbarten Gesprächstermin außer der Klassenlehrerin noch der Schulleiter und eine andere Mutter, die an ihrer Stelle als Begleitperson für die Klassenfahrt vorgesehen war, erschienen. Die Betroffene mußte dann erleben, daß die Klassenlehrerin den vertraulichen Inhalt ihres Schreibens diesen beiden Personen zur Kenntnis gegeben hatte.

In der darauffolgenden Klassenpflegschaftssitzung, die der Vorbereitung der Klassenfahrt diente, berichtete die Klassenlehrerin über den Brief der Betroffenen und informierte damit auch alle weiteren Eltern über die private Situation der Mutter, die selbst als Klassenpflegschaftsvorsitzende anwesend war. Weiter wurde der inzwischen zu einem gespannten Verhältnis angewachsene Konflikt zwischen der Klassenlehrerin und der Mutter sowohl in der Schulkonferenz als auch in der Schulpflegschaft beraten. Mittlerweile ging es um die Versetzung des Kindes in eine andere Klasse zu einer anderen Klassenlehrerin, dann sogar um den Antrag einiger Eltern, das Kind von der Schule zu verweisen.

Das Schulamt bzw. der zuständige Schulrat war - obwohl vom Schulleiter informiert - nicht in der Lage, der schließlich mit gegenseitigen Strafanzeigen ausartenden Entwicklung Einhalt zu gebieten. Dabei wäre es entscheidend darauf angekommen, rechtzeitig den Beteiligten klarzumachen, daß die Auseinandersetzung ursächlich durch den Vertrauensbruch ausgelöst war, durch den sich die Mutter, wie sie mir wiederholt mitteilte, besonders in ihrem Persönlichkeitsrecht verletzt fühlte.

Dieser Fall - mit der grundsätzlichen Problematik übrigens nicht der einzige im Berichtszeitraum - zeigt, wie sorgfältig Vertrauensverhältnisse zwischen Erziehungsberechtigten und Lehrkräften respektiert und geschützt werden müssen. Daten, zu deren Angabe die Erziehungsberechtigten nach § 19 Abs. 2 Satz 1 des Schulverwaltungsgesetzes nicht verpflichtet sind, die also freiwillig offenbart werden, sind mit besonderer Vorsicht zu behandeln. Sie dürfen nur mit Einwilligung der betroffenen Erziehungsberechtigten Dritten zugänglich gemacht werden. Das gilt auch für eine Weitergabe innerhalb der Schule, also auch gegenüber dem Schulleiter. Nur im Ausnahmefall, d. h. unter Abwägung höherrangiger Rechtsgüter - etwa bei einer Gefahr für Leib oder Leben einer Schülerin oder eines Schülers - darf das Vertrauensverhältnis auch gegen den Willen des Betroffenen durchbrochen werden.

Ein weiteres datenschutzrechtliches Problem stellte sich in diesem Fall heraus. Der Schulleiter hatte nämlich in den gerichtlichen Verfahren den Schulpflegschaftsvorsitzenden - der, in der Schulpraxis keineswegs selten, Rechtsanwalt war - zu seinem Rechtsvertreter bestellt. Da er diesem aber die zu seiner Rechtsverteidigung erforderlichen Angaben machen mußte, offenbarte er ihm zwangsläufig Daten der Mutter, die der Rechtsanwalt in seiner Funktion als Schulpflegschaftsvorsitzender auch nutzte und an die Teilnehmer der Schulpflegschaftssitzung unzulässigerweise weitergab. Bei einer derartigen Interessenkollision hätte der Schulleiter besser das Rechtsamt des Schulträgers oder einen anderen Rechtsanwalt eingeschaltet.

5.13.4 Ermittlungen durch den Schulleiter

In mehreren Eingaben habe ich mich mit den Befugnissen von Schulleitern im Rahmen der **Schulpflichtüberwachung** beschäftigt. Dabei habe ich festgestellt, daß die Zuständigkeiten und Befugnisse der beteiligten Stellen im Rahmen der Schulpflichtüberwachung nicht klar geregelt sind.

In einem m. E. die Persönlichkeitsrechte der Betroffenen erheblich beeinträchtigenden Fall ging es um die erstmalige **Einschulung** in eine Grundschule. Nachdem die Erziehungsberechtigten ein schulpflichtig gewordenes Kind nicht angemeldet und auch auf ein entsprechendes Schreiben des Schulleiters nicht reagiert hatten, forschte der Schulleiter gleich bei mehreren Stellen nach dem Verbleib des Kindes: bei den benachbarten Grundschulen, einer Konfessionsschule, dem städtischen Kindergarten, dem Einwohnermeldeamt sowie dem Gesundheitsamt. Außerdem versuchte der Schulleiter wiederholt und vergeblich, Kontakt mit der Familie aufzunehmen. Schließlich befragte er sogar die an seiner Schule unterrichteten Geschwister dieses Kindes und eine Nachbarin der Familie. Das von ihm gesuchte Kind war schwerstbehindert und seit seiner Geburt in einer Pflegeeinrichtung untergebracht. Durch die Aktivitäten des Schulleiters erfuhren die Geschwister und die angesprochene Nachbarin erstmals von der Existenz dieses Kindes.

Das zum Vorgehen des Schulleiters um Stellungnahme gebetene Schulamt vertrat die Auffassung, daß die Überwachung der Schulpflicht nach §§ 18 und 19 des Schulpflichtgesetzes grundsätzlich dem Schulleiter obliegt. Dies gelte nicht nur für die gesamte Dauer des Schulbesuchs, sondern bereits zum Zeitpunkt des Anmeldeverfahrens. Den genannten Vorschriften vermag ich nur zu entnehmen, daß Lehrer und Schulleiter in gewissem Umfang auf einen ordnungsgemäßen Schulbesuch hinwirken sollen. Ich habe aber erhebliche Zweifel, ob die Vorschriften des Schulpflichtgesetzes den Schulleiter grundsätzlich berechtigen, Datenerhebungen über schulpflichtige Schüler, die an seiner Schule noch nicht angemeldet sind, auch außerhalb der Schule vorzunehmen. Dies ergibt sich nach meiner Auffassung weder aus dem Schulpflichtgesetz noch aus dem Runderlaß des Kultusministeriums vom 27.11.1979 zur Überwachung der Schulpflicht (BASS 12-51 Nr. 5). Nach meiner Auffassung hätten weitere Schritte zur Nachforschung allein vom zuständigen Schulamt unternommen werden dürfen.

In einem etwas anders gelagerten Fall hatte sich ein volljähriger, **nicht mehr schulpflichtiger Schüler** von einem Gymnasium abgemeldet, ohne dem Schulleiter mitzuteilen, welche Schule er künftig besuchen werde. Nachdem der Betroffene nicht bereit war, die neue Schule zu benennen, schaltete der Schulleiter das Rechtsamt der Stadt ein. Dabei wurde dem Rechtsamt neben Namen und Geburtsdatum des Betroffenen auch mitgeteilt, daß dieser die Klassen 5 und 12 wiederholen mußte. Die Forderung nach Angabe der neuen Schule stützte der Schulleiter darauf, daß es seine Pflicht sei, sich zu vergewissern, daß der Betroffene seiner Schulpflicht genüge.

Der um Stellungnahme gebetene Stadtdirektor hat bestätigt, daß der Betroffene nicht mehr der allgemeinen Schulpflicht unterlag. Die Vollzeitschulpflicht war mit Ablauf des zehnten Schuljahres erfüllt. Auch die grundsätzlich an die zehnjährige Vollzeitschulpflicht anschließende Berufsschulpflicht bestand für den Betroffenen nicht mehr. Die Nachforschung des Schulleiters wie auch die Übermittlung der Schülerdaten an das Rechtsamt des Schulträgers waren also unzulässig.

Die zuständige obere Schulaufsichtsbehörde begründete allerdings die Zulässigkeit der Frage nach der aufnehmenden Schule damit, daß ein Abgangs- oder Überweisungszeugnis ausgestellt und ggf. eine Kopie des Schülerstammblattes auf dem Dienstweg an die aufnehmende Schule übermittelt werden müsse. Nach § 19 Abs. 1 Satz 1 des Schulverwaltungsgesetzes dürfen die Daten eines Schülers nur übermittelt werden, soweit sie zur Erfüllung der durch Rechtsvorschrift übertragenen Aufgabe benötigt werden. Eine Übermittlung ist daher nur zulässig, wenn es zur Aufgabenerfüllung des Schulleiters der abgebenden Schule gehört, die Schulpflicht des Schülers zu überwachen, denn nur dann stünde ihm das Recht zu, selbst - allerdings auch nur beim Schüler bzw. den Erziehungsberechtigten unmittelbar - zu recherchieren, welche neue Schule der Schüler besuchen wird. Nur in diesem Fall wären auch der Schüler bzw. die Erziehungsberechtigten ver-

pflichtet, dem Leiter der abgebenden Schule eine entsprechende Auskunft zu erteilen.

5.13.5 Kollegiumsliste

Beanstanden mußte ich die Erstellung einer Kollegiumsliste und deren Verteilung an alle Mitglieder des Lehrerkollegiums an einer Hauptschule. Ein Lehrer des Kollegiums hatte mir vorgetragen, es werde jährlich eine sog. Kollegiumsliste mit Namen, Vornamen, privaten Telefonnummern und Adressen aller Lehrkräfte erstellt und in Kopie an alle Mitglieder des Kollegiums (32 Lehrerinnen und Lehrer) verteilt.

Da die zuständige Bezirksregierung meiner Empfehlung, den Leiter der betreffenden Hauptschule anzuweisen, solche Listen künftig nicht mehr zu erstellen und die bereits erstellten Listen von den Lehrkräften zurückzufordern und zu vernichten, nicht folgen wollte, mußte ich diesen Vorgang gegenüber dem Kultusministerium des Landes Nordrhein-Westfalen beanstanden. Der Beanstandung liegen folgende Überlegungen zugrunde:

Nach § 29 Abs. 1 Satz 1 DSG NW dürfen Daten von Beschäftigten nur verarbeitet werden, wenn dies zur Durchführung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere zu Zwecken des Personaleinsatzes erforderlich ist. Ich kann nicht erkennen, für welche gesetzliche Aufgabenerfüllung der Schulleitung es erforderlich sein soll, daß jede Lehrkraft die private Telefonnummer und Anschrift aller Kolleginnen und Kollegen kennt. Keiner der in § 29 Abs. 1 Satz 1 DSG NW genannten Zwecke - auch nicht der des Personaleinsatzes - verlangt eine solche Bekanntgabe. Selbst die Bezirksregierung hat ihre Auffassung lediglich damit begründet, daß die Aushändigung der Kollegiumsliste an die Mitglieder des Kollegiums „zweckmäßig" sei. Dies reicht jedoch nicht aus. An die Erforderlichkeit ist ein strenger Maßstab anzulegen. Die Datenverarbeitung ist nur zulässig, wenn sie für die Aufgabenerfüllung unbedingt notwendig ist, so daß ohne sie die Aufgaben nicht oder nur mangelhaft erfüllt werden können. Ich habe daher festgestellt, daß die Speicherung der genannten Daten aller Lehrkräfte der Schule in einer sog. Kollegiumsliste und ihre Weitergabe an alle Kolleginnen und Kollegen der Schule unzulässig war.

In seiner Stellungnahme hat das Kultusministerium ausgeführt, Rechtsgrundlage für das Erstellen und Verteilen der Liste sei der inzwischen in Kraft getretene § 19 a des Schulverwaltungsgesetzes. Diese Vorschrift erlaube den Schulen die Verarbeitung von Lehrerdaten, soweit dies u. a. zur Aufgabenerfüllung bei der **Unterrichtsorganisation** erforderlich sei. Die zunehmende Teilzeitbeschäftigung von Lehrerinnen und Lehrern, der zeitlich unterschiedliche Unterrichtseinsatz als Folge der Fünf-Tage-Woche an Schulen und die zunehmende Unterbringung von Schulen an getrennten Standorten mit getrennten Lehrerzimmern, Teilsekretariaten etc. verhinderten zunehmend, daß Lehrerinnen und Lehrer die für die Organisation des Unterrichts erfor-

derlichen Dienstgespräche in der Schule führen könnten. Gleichzeitig ergäbe sich durch die in den neuen Richtlinien und Lehrplänen vorgesehene Ausweitung des fächerübergreifenden und projektorientierten Unterrichts in allen Schulformen ein erhöhter - häufig nicht vorhersehbarer - Abstimmungsbedarf zwischen den an der Durchführung des Unterrichts beteiligten Lehrkräften. In der Praxis sei an vielen Schulen nicht mehr sichergestellt, daß die für die Organisation des Unterrichts erforderlichen Abstimmungen und Gespräche allesamt innerhalb der Präsenzzeiten der Lehrkräfte an der Schule erfolgen könnten. Von daher müßten Lehrerinnen und Lehrer auch außerhalb der Schule für die Kolleginnen und Kollegen erreichbar sein. Dazu bedürfe es der Kenntnis der privaten Telefonnummer und der Privatanschrift.

Für die Organisation und Durchführung des Vertretungsunterrichts hätten die zu Vertretenden außerdem sicherzustellen, daß die für einen ordnungsgemäßen Vertretungsunterricht erforderlichen Unterlagen und Informationen zur Verfügung stünden. Der Informationsfluß könne sinnvollerweise nicht ausschließlich über die Schulleitung oder die für die Organisation des Vertretungsunterrichts allgemein zuständige Lehrkraft erfolgen. Insbesondere die fachliche Abstimmung könne letztlich nur unmittelbar zwischen dem Vertretenen und dem Vertreter geleistet werden. Das Kultusministerium bejaht daher grundsätzlich die Frage der Erforderlichkeit des Erstellens und Verteilens einer kompletten Kollegiumsliste. Nach Auffassung des Kultusministeriums könne den datenschutzrechtlichen Belangen der Lehrkräfte dadurch Rechnung getragen werden, daß die Schulleitung bei Vorliegen triftiger Gründe im Einzelfall auf eine Eintragung verzichte.

Die Ausführungen des Kultusministeriums vermögen mich nicht zu überzeugen. Bei allen genannten Gründen, die an vielen Schulen des Landes zutreffen mögen, wird verkannt, daß die Erforderlichkeit nicht generell und abstrakt, sondern in jedem **Einzelfall** begründet sein muß.

Die Argumentation des Kultusministeriums trifft jedenfalls in dem von mir geprüften Fall nicht zu, da es sich um eine Hauptschule mit 32 Lehrkräften in einem Schulgebäude handelt, bei der sich das Problem mangelnder Kommunikation nicht im geschilderten Umfang stellen kann. Dieser Fall wird von mir deshalb dargestellt, weil hier deutlich wird, daß der vom Gesetzgeber angelegte Maßstab der Erforderlichkeit immer eine Einzelfallprüfung verlangt. Es muß der Eingriff in die Rechte der Betroffenen auf Datenschutz von demjenigen, der eingreift, gerechtfertigt sein und nicht - wie vom Kultusministerium vorgeschlagen - den Betroffenen abverlangt werden, daß sie der Schulleitung „triftige Gründe" nennen müssen, um eine Beeinträchtigung abzuwenden.

5.14 Finanzwesen

5.14.1 Automatisierte Besteuerungsverfahren

Von den obersten Finanzbehörden des Bundes und der Länder ist ein gemeinsames, bundesweites Automationsprojekt mit der Bezeichnung **FISCUS** (Föderales Integriertes Standardisiertes Computerunterstütztes Steuersystem) erarbeitet und durch Beschluß der Finanzministerkonferenz in einem Verwaltungsabkommen zur Zusammenarbeit des Bundes und der Länder auf dem Gebiet der Automationsunterstützung im Besteuerungsverfahren ausgestaltet worden, dem sich Nordrhein-Westfalen bisher noch nicht angeschlossen hat. Für die Entwicklung des FISCUS sind mehrere Arbeitsgruppen mit detaillierter Aufgabenstellung vorgesehen. Die Programme sollen arbeitsteilig von den Ländern entwickelt werden, und die Länder sollen verpflichtet werden, die im Rahmen dieser Zusammenarbeit entwickelten Programme unverändert einzusetzen.

Das Verwaltungsabkommen umfaßt die Automationsunterstützung bei allen Vorgängen des Besteuerungsverfahrens, einschließlich der steuerlichen Nebenleistungen und der Steuerstraf- und Bußgeldverfahren in Finanzämtern, Oberfinanzdirektionen und obersten Finanzbehörden. FISCUS wird deshalb eines der größten und anspruchsvollsten Automationsvorhaben sein, das in den letzten Jahren in der bundesdeutschen Verwaltung initiiert wurde. Deshalb muß besonders sorgfältig geprüft werden, ob das Automationsverfahren so gestaltet ist, daß es den datenschutzrechtlichen Anforderungen insbesondere im Hinblick auf den technisch möglichen, schnellen Datenaustausch unter den Finanzbehörden entsprechen wird. Nur so kann ein solches Automationsverfahren neben den aus der steuerlichen Sicht anzustrebenden Zielen auch eine demokratieverträgliche Gestaltung erfahren. Das bedeutet, daß die Steuerpflichtigen durch FISCUS nicht neue Gefahren im automatisierten Umgang mit ihren Steuerdaten befürchten müssen, vielmehr sicher sein können, daß auch in einem umfassenden und weitreichenden Automationsverfahren ihr Grundrecht auf Datenschutz gewahrt bleibt. Deshalb ist es bedauerlich, daß in dem Verwaltungsabkommen der Datenschutz unerwähnt bleibt. Im Vergleich hierzu wird beispielsweise in dem Projekt zur Einrichtung eines Automatisierten Gebührenerfassungssystems auf Autobahnen dem Datenschutz hohe Priorität beigemessen (vgl. unten 5.16.1).

Nach der Stellungnahme des Finanzministeriums des Landes Nordrhein-Westfalen beziehen sich die bisherigen Arbeiten am Projekt im wesentlichen auf die Festlegung der Projektorganisation und auf systemtechnische Grundlagen. Entscheidungen zu systemtechnischen und anwendungsbezogenen Fragen seien noch nicht oder nur auf hohem Abstraktionsniveau getroffen worden. Die Zuordnung von Analyse- und Programmieraufgaben zu den „Ausführenden Gremien" habe begonnen. Abgestimmte Arbeitsergebnisse seien erst im Jahre 1995 zu erwarten. Die rechtliche Rahmenregelung für das Automationsprojekt wird die in

Vorbereitung befindliche **Steuerdaten-Abrufverordnung** gemäß § 30 Abs. 6 der Abgabenordnung sein.

Der von den Datenschutzbeauftragten des Bundes und der Länder gebildete Arbeitskreis Steuerverwaltung wird sich unter meinem Vorsitz mit den durch das Automationsprojekt eröffneten technischen Möglichkeiten der Datenverarbeitung kritisch auseinandersetzen.

Neben diesem bundesweiten flächendeckenden Automationssystem ist in Nordrhein-Westfalen für die Finanzverwaltung das Automationssystem GFD Gesamtfestsetzung - Dezentral entwickelt und etwa zur Hälfte in den Finanzämtern umgesetzt worden. Dieses Automationsvorhaben bezweckt, die bisher zentral im Rechenzentrum der Finanzverwaltung erfaßten und ausgewerteten Daten aus den Steuererklärungen künftig dezentral, d. h. bei den Finanzämtern durch die Steuersachbearbeiter selbst, automatisiert zu verarbeiten. Die dann **digitalisierte „Steuerakte"** wird das alte datenschutzrechtliche Problem der sicheren Aufbewahrung von Steuerakten in den Arbeitsräumen der Sachbearbeiter von selbst lösen. Mit neuen datenschutzrechtlichen Problemen dieses Automationssystems habe ich mich bisher noch nicht beschäftigen müssen.

5.14.2 Lohnsteuerkarten von Schwerbehinderten

Eine Schwerbehindertenvertretung hat mich auf die datenschutzrechtliche Problematik eines von den Gemeinden automatisch eingetragenen Freibetrages auf der Lohnsteuerkarte aufmerksam gemacht.

Nach Beantragung eines **Steuerfreibetrages** für Schwerbehinderung gemäß § 39 a des Einkommensteuergesetzes beim Finanzamt wird durch die Mitteilung des gewährten Freibetrages an die Gemeinden bewirkt, daß bei Ausstellung der Lohnsteuerkarte in den Folgejahren der Freibetrag mit aufgeführt wird. Da aber die Steuerfreibeträge für die einzelnen Abstufungen des Grades der Behinderung allgemein bekannt sind, kann der Arbeitgeber ohne weiteres erkennen, daß und mit welchem Grad der Behinderung sein Arbeitnehmer eingestuft ist. Dies kann sich für den Arbeitnehmer, insbesondere solange er noch nicht den verstärkten Kündigungsschutz nach dem Schwerbehindertengesetz genießt, nachteilig auswirken.

Das Finanzministerium des Landes Nordrhein-Westfalen hat zum Verfahren ausgeführt, nach § 39 a Abs. 2 des Einkommensteuergesetzes hätten die Gemeinden bei der Ausstellung der Lohnsteuerkarten die Pauschbeträge für Behinderte - im Innenverhältnis nach Anweisung des Finanzamtes - in eigener Zuständigkeit als Freibetrag auf der Lohnsteuerkarte einzutragen. Hierzu teilten die Finanzämter den Gemeinden die notwendigen Angaben in der Regel durch Übersendung von Listen oder Eingabebögen mit. Das Verfahren zur Eintragung von Freibeträgen auf der Lohnsteuerkarte sei grundsätzlich antragsabhängig. Bei Behinderten werde - der allgemeinen Interessenlage folgend - der Antrag unterstellt. Dem behinderten Arbeitnehmer bleibe es aber unbenommen, die für die Ausstellung seiner Lohnsteuerkarte zu-

ständige Gemeinde davon zu unterrichten, daß er auf die Eintragung eines Behindertenpauschbetrages auf der Lohnsteuerkarte zukünftig verzichte. In diesem Falle werde der Freibetrag erst im Rahmen der Einkommensteuerveranlagung berücksichtigt.

Aus datenschutzrechtlicher Sicht muß dem Steuerpflichtigen grundsätzlich die Möglichkeit erhalten bleiben, zwischen einer Eintragung des Freibetrages auf der Lohnsteuerkarte oder der Geltendmachung in der Einkommensteuererklärung bzw. im Jahresausgleich zu wählen. Außerdem war aus dem Formular „Antrag auf Lohnsteuerermäßigung" für den Betroffenen nicht ersichtlich, daß zukünftige Datenübermittlungen vom Finanzamt an die Gemeinde vorgenommen werden sollen.

Auf meine Empfehlung, in den Vordruck den Hinweis auf die künftigen Datenübermittlungen an die Gemeinde aufzunehmen und den Steuerpflichtigen bei der erstmaligen Antragstellung angeben zu lassen, ob er auch künftig eine Übermittlung der Daten an die Gemeinde wünscht, hat das Finanzministerium des Landes Nordrhein-Westfalen mitgeteilt, der Vordruck sei für das Jahr 1995 wie folgt ergänzt worden:

> „Mir ist bekannt, daß erforderlichenfalls Angaben über Kindschaftsverhältnisse und Pauschbeträge für Behinderte der für die Ausstellung der Lohnsteuerkarten zuständigen Gemeinde mitgeteilt werden."

Mit diesem Hinweis allein dürfte dem Steuerpflichtigen nicht geholfen sein, da ihm damit die genannte Wahlmöglichkeit für die folgenden Jahre nicht deutlich wird. Ich habe deshalb vorgeschlagen, den Steuerpflichtigen in dem Vordruck angeben zu lassen, ob er eine Eintragung des Freibetrages auf der Lohnsteuerkarte wünscht.

Das vom Bundesbeauftragten für den Datenschutz um Stellungnahme gebetene Bundesministerium der Finanzen hat erklärt, die für lohnsteuerrechtliche Fragen zuständigen Referatsleiter der obersten Finanzbehörden des Bundes und der Länder hätten sich gegen ein Auswahlfeld im Antrag auf Lohnsteuerermäßigung ausgesprochen. Sie hielten es für ausreichend, einen Hinweis auf die mögliche Weitergabe von Daten an die Gemeinden einzufügen. Diese Ansicht teile ich nicht, sie ist nach meinen Erfahrungen lebensfremd.

5.14.3 Übermittlung an die Gewerbeüberwachung

In mehreren Eingaben bin ich auf die Problematik der Übermittlung von Steuerdaten durch Finanzämter an Gewerbebehörden hingewiesen worden. Die Zulässigkeit derartiger Übermittlungen wird von der Finanzverwaltung auf § 30 Abs. 4 Nr. 5 der Abgabenordnung (AO) gestützt. Danach ist eine Offenbarung von Steuerdaten zulässig, wenn hierfür ein **zwingendes öffentliches Interesse** besteht. Für die Auslegung dieses Begriffs ist den beispielhaft unter Nr. 5 Buchstaben a bis c aufgezählten Fällen zu entnehmen, in

welcher Höhe die Schwelle anzusetzen ist, die aus Gründen eines zwingenden öffentlichen Interesses bei der Abwägung mit dem Steuergeheimnis eine Offenbarung zu rechtfertigen vermag. Danach muß die Bedeutung des Sachverhalts im Einzelfall einem der aufgeführten Fälle vergleichbar sein. Eine solche Vergleichbarkeit kann nicht allgemein für jedes Gewerbeuntersagungsverfahren angenommen werden. Vielmehr müssen im Einzelfall besondere Umstände (Handlungsweise des Gewerbetreibenden oder Umfang des durch ihn verursachten Schadens) vorliegen, die die Gefahr einer erheblichen Störung der wirtschaftlichen Ordnung oder die Gefahr einer Erschütterung des Vertrauens der Allgemeinheit auf die Redlichkeit des Geschäftsverkehrs oder auf die ordnungsgemäße Arbeit der Behörden besorgen lassen (vgl. § 30 Abs. 4 Nr. 5 Buchstabe b AO).

Ein formelles Antragsrecht zur Einleitung eines Gewerbeuntersagungsverfahrens steht dem Finanzamt nicht zu; es kann ein derartiges Verfahren bei der Gewerbebehörde lediglich anregen. Von dieser Befugnis und der damit verbundenen Offenbarung der steuerlichen Verhältnisse des Betroffenen gegenüber der zuständigen Gewerbebehörde soll das Finanzamt nach der Vollstreckungskartei NRW wegen des Gebotes der Verhältnismäßigkeit der Mittel nur dann Gebrauch machen, wenn die steuerliche Unzuverlässigkeit derart schwerwiegt, daß sich aus ihr allein die gewerberechtliche Unzuverlässigkeit ergibt.

Dem wird aber die weitere Festlegung in der Vollstreckungskartei NRW (Karte 5 Nr. 1.2) nicht gerecht, weil sich die Praxis häufig an solchen Rahmenbeträgen orientiert. Ich habe Zweifel, ob bereits ab einer Steuerschuld von 5 000,-- DM, selbst wenn weitere Umstände wie ständig schleppender Zahlungseingang und die Entwicklung der Steuerrückstände hinzutreten, von einem zwingenden öffentlichen Interesse an jedweder Gewerbeuntersagung gesprochen werden kann. Im Vergleich zu den enumerativ aufgezählten Fallgruppen in § 30 Abs. 4 Nr. 5 AO erscheint ein derartiger Beurteilungsmaßstab als unverhältnismäßig. Meines Erachtens muß die Vollstreckungskartei NRW insoweit korrigiert werden.

5.14.4 Kommunale On-line-Zugriffe auf Grundsteuerdaten

Auf Grund eines Beratungsersuchens habe ich mich mit der Zulässigkeit von On-line-Verfahren zum Abruf von Grundsteuerdaten kreisangehöriger Gemeinden durch den Kreis befaßt.

Das Umweltamt eines Kreises hatte die kreisangehörige Gemeinde gebeten, den On-line-Zugriff auf die in der **Grundbesitzabgabendatei** der Gemeinde gespeicherten Namen und Anschriften von Grundstückseigentümern zu ermöglichen, um die Daten in ordnungsbehördlichen Verfahren nach dem Abfall-, Landschafts- und Wassergesetz verwenden zu können. Zur Zulässigkeit des Abrufs hatte das Umweltamt auf den geänderten § 31 Abs. 3 AO hingewiesen. Die Gemeinde bat mich um Überprüfung.

Meine datenschutzrechtlichen Bedenken gegen einen On-line-Abruf durch den Kreis ergeben sich aus folgenden Überlegungen:

Name und Anschriften, die in der Grundbesitzabgabendatei gespeichert sind, unterliegen dem Steuergeheimnis nach § 30 AO. Eine Offenbarungsbefugnis nach § 30 Abs. 4 AO für einen Zugriff auf diese Daten durch das Umweltamt des Kreises besteht nicht. Allerdings bestimmt § 31 Abs. 3 AO neuerdings, daß die für die Verwaltung der Grundsteuer zuständigen Behörden berechtigt sind, die nach § 30 AO geschützten Namen und Anschriften von Grundstückseigentümern zur Erfüllung sonstiger öffentlicher Aufgaben zu verwenden bzw. anderen Behörden mitzuteilen, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen. Diese Regelung allein eröffnet in Nordrhein-Westfalen aber noch nicht den automatisierten Datenabruf durch andere Behörden.

Neben der Prüfung nach § 31 Abs. 3 AO, ob nicht überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen, müssen zusätzlich die Voraussetzungen des § 9 Abs. 2 DSG NW erfüllt sein. Nach § 9 Abs. 2 Satz 1 DSG NW ist zur Einrichtung automatisierter Abrufverfahren eine Rechtsverordnung zu erlassen, da das Abrufverfahren nicht nur innerhalb der Kreisverwaltung (vgl. § 9 Abs. 4 DSG NW), sondern unter verschiedenen Behörden eingerichtet werden soll. Vor Erlaß einer Rechtsverordnung ist zu prüfen, ob die Einrichtung eines automatisierten Datenabrufverfahrens mit direktem Zugriff auf die Grundsteuerdaten der kreisangehörigen Gemeinden unter Berücksichtigung des informationellen Selbstbestimmungsrechts des betroffenen Personenkreises und der Aufgaben der beteiligten Stellen angemessen ist.

Im vorliegenden Fall ergaben sich Zweifel an der Angemessenheit bereits daraus, daß nach dem Vortrag der kreisangehörigen Gemeinde die Daten auch auf andere Weise beschafft werden konnten. Bei einem Zugriff auf die Grundbesitzabgabendatei wären mehr Daten abrufbar gewesen, als für den Kreis zur Aufgabenerfüllung erforderlich waren, denn die Datei enthielt nicht nur Daten von Grundeigentümern sondern auch von Mietern, Pächtern und anderen Nutzungsberechtigten; außerdem wäre jederzeit ein Zugriff auf die Daten aller Gespeicherten möglich, obwohl nur Daten bestimmter Personen in umweltrelevanten Fällen benötigt werden. Fraglich war also auch die Geeignetheit des Zugriffs auf die Grundbesitzabgabendatei, da diese nicht nur Grundstückseigentümer enthielt.

Da aus einem Schreiben des Oberkreisdirektors an die Gemeinde hervorging, daß bereits 13 kreisangehörige Städte und Gemeinden ihr Einverständnis zum gewünschten Zugriff auf die Grundsteuerdaten erklärt hatten, habe ich die Angelegenheit gegenüber dem Oberkreisdirektor aufgegriffen. Eine Stellungnahme liegt mir noch nicht vor.

5.15 Landwirtschaft

5.15.1 Integriertes Verwaltungs- und Kontrollsystem

Besorgnis über eine weiter zunehmende Kontrolldichte verursachte das europäische Integrierte Verwaltungs- und Kontrollsystem (InVeKoS), das die Mitgliedstaaten verpflichtet, zur Verhinderung einer mißbräuchlichen Verwendung von Fördermitteln eine Datenbank nach einheitlichen Kriterien zu errichten. In ihr werden die Daten aller Landwirte gespeichert, die an den Förderungsmaßnahmen der Europäischen Union teilnehmen. Neben einer lückenlosen Erfassung der geförderten landwirtschaftlichen Flächen und der Flächennutzungsart werden Daten zur wirtschaftlichen Situation der Betriebe erfaßt und automatisiert verarbeitet. Die wirtschaftlichen Flächen sollen nach einheitlichen Kriterien so bezeichnet werden, daß eine Kontrolle der einzelnen Förderungsmaßnahmen bereits durch einen Vergleich mit Satellitenaufnahmen möglich wird. In Nordrhein-Westfalen findet allerdings eine Flächenkontrolle durch Satellitenaufnahmen nicht statt, vielmehr bleibt die Überprüfung auf eine Kontrolle vor Ort beschränkt.

In der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 (vgl. Anlage 8, S. 181) wird festgestellt, daß die EU mit InVeKoS ein Überwachungssystem verordnet hat, das dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot, widersprechen kann. Zur Vermeidung unverhältnismäßiger Einschränkungen des informationellen Selbstbestimmungsrechts der betroffenen Landwirte wird daher insbesondere gefordert, ortsunabhängige Überwachungsmöglichkeiten (Fernerkundung mittels Satellit oder Flugzeug) auf Stichproben zu beschränken und an zentrale Datenbanken keine personenbezogenen Daten zu übermitteln.

Nach meinen Feststellungen wird in Nordrhein-Westfalen entsprechend diesen Vorgaben eine **dezentrale Datenbank** bei den Direktoren der Landwirtschaftskammern als Landesbeauftragte zur Antragsbearbeitung geführt. Die gespeicherten Daten bleiben mindestens fünf Jahre für Kontrollzwecke verfügbar. Ein Abgleich der gespeicherten Daten mit Daten aus anderen Förderungsmaßnahmen außerhalb der durch InVeKoS erfaßten Förderungsprogramme erfolgt nur, sofern die entsprechenden Richtlinien dies vorsehen und dies dem Antragsteller bekannt ist.

Im übrigen stellen die landwirtschaftlichen Betriebe ihre Anträge bei den Kreisstellen der Landwirtschaftskammern. Die zur Antragsbearbeitung erforderlichen Nachweise, wie beispielsweise der Einkommensteuerbescheid, werden dort zur Einsichtnahme vorgelegt, wobei es dem Antragsteller unbenommen bleibt, die nicht relevanten Angaben unkenntlich zu machen. Nach einer Überprüfung der Vollständigkeit der Angaben durch die Sachbearbeiter in den Kreisstellen werden diese auf elektronischen Datenträgern erfaßt, an die Landwirtschaftskammern übermittelt und dort in der zentralen Datenbank gespeichert. Die Antragsunterlagen verbleiben bei den Kreisstellen. In den Landwirtschaftskammern werden die Angaben der Landwirte

festgelegten Plausibilitätskontrollen unterworfen, die Förderbeträge berechnet und die Auszahlungsdateien erstellt. Die Daten dürfen nur für Zwecke der Subventionsgewährung verwendet werden, der Zugriff zu diesen Daten ist nur bestimmten hierzu berechtigten Personen möglich. Änderungen in den Datenbeständen werden programmgesteuert protokolliert, so daß sie jederzeit nachvollziehbar sind. Personenbezogene Daten werden nur in Form von Auszahlungslisten und -bändern an die Bundeskasse zur Auszahlung übermittelt. An das Ministerium für Umwelt, Raumordnung und Landwirtschaft des Landes Nordrhein-Westfalen werden Daten zur Erfüllung der vorgeschriebenen Meldepflichten gegenüber dem Bund und der EU ausschließlich in aggregierter Form übermittelt, wie auch nur aggregierte Daten für die vom Landesamt für Datenverarbeitung und Statistik geführte Datei der Landeszuwendungen bestimmt sind.

Die Befürchtung, daß einzelbetriebliche Daten aus InVeKoS über die Europäische Statistik an die Kommission gelangen und dort zu nicht vorgesehenen Kontrollen genutzt werden könnten, hat sich nicht bewahrheitet. Sie könnte auch erst dann Gestalt gewinnen, wenn die Landwirtschaftskammern - anders als bisher - Einzelangaben, die einen Bezug zum einzelnen landwirtschaftlichen Betrieb ermöglichen, übermitteln müßten.

5.15.2 Tierbestandslisten an Privatfirma

Auf Grund einer Eingabe habe ich das Verfahren zur Herstellung von Ohrmarken datenschutzrechtlich geprüft. Nach § 19 b der Viehverkehrsverordnung müssen Schweine in landwirtschaftlichen Betrieben von dem Besitzer mit einer Ohrmarke gekennzeichnet werden. Die Ohrmarken werden dem Kennzeichnungspflichtigen von der zuständigen Behörde oder einer von ihr beauftragten Stelle zugeteilt.

Nach meinen Feststellungen übermittelt hierzu die Tierseuchenkasse beim Landesamt für Ernährung an die jeweils zuständigen Kreisveterinärämter eine Liste aller Tierhalter mit Anschrift, Anzahl der Tiere und der Tierseuchenkassennummer. Der voraussichtliche Bedarf an Ohrmarken wird den Kreisveterinärämtern durch die Betriebe mitgeteilt. Zur Herstellung und zum Versand der Ohrmarken bedienen sich alle Kreisveterinärämter einer Privatfirma.

Es bestehen zwar an sich keine Bedenken dagegen, daß die Kreisveterinärämter die zur Herstellung der Ohrmarken erforderlichen Daten sowie die Anzahl der herzustellenden Marken an eine Privatfirma übermitteln. Bei der Herstellung der Ohrmarken können sie sich nämlich auch einer nicht-öffentlichen Stelle bedienen (§ 19 b Abs. 2 der Viehverkehrsverordnung). Bei der im Sommer 1994 durchgeführten Aktion der Herstellung und Versendung von Ohrmarken war aber m. E. nicht sichergestellt, daß die Privatfirma die ihr zur Verfügung gestellten Daten aller Schweinemastbetriebe in Nordrhein-Westfalen zu keinem anderen Zweck verwenden konnte, obwohl ein erhebliches wirtschaftliches Interesse an der Nutzung der Daten für Marketing-

Zwecke bestand. Die mir hierzu übersandte Verpflichtungserklärung alleine reichte jedenfalls nicht aus. Es fehlten wichtige Regelungen der Datensicherheit wie die Gewährleistung der Auftragskontrolle und konkrete Festlegungen von technischen und organisatorischen Maßnahmen. Im Rahmen der Auftragskontrolle ist es insbesondere erforderlich, daß der Auftraggeber die Datensicherheit der Herstellerfirma im angemessenen Umfang kontrolliert. Der bloße Hinweis, daß sich die Firma verpflichtet, den Weisungen des Auftraggebers Folge zu leisten, reicht nicht aus. Über den Inhalt der Weisungen muß der Auftraggeber in eigener Verantwortung entscheiden, die Weisungen müssen konkret und schriftlich festgelegt sein. Ich habe daher das Ministerium für Umwelt, Raumordnung und Landwirtschaft des Landes Nordrhein-Westfalen gebeten, dafür Sorge zu tragen, daß die technischen und organisatorischen Maßnahmen vor der nächsten Versendungsaktion schriftlich festgelegt werden.

Weil erhebliche wirtschaftliche Interessen und die gegebenen technischen Möglichkeiten bei der beauftragten Firma die Gefahr in sich tragen, daß die zeitweise bei dieser Stelle gespeicherten Daten zu anderen Zwecken genutzt werden können, muß außerdem geprüft werden, ob den Anforderungen des Datenschutzes nicht besser dadurch Rechnung getragen wird, daß die Zusammenstellung der für die einzelnen Betriebe zugeteilten Ohrmarken anonymisiert erfolgt. Dazu dürften die Kreisveterinärämter die benötigten Adreßaufkleber für den Versand der Ohrmarken allerdings nicht durch die Privatfirma herstellen lassen, sondern müßten sie selbst anfertigen bzw. innerhalb der Kreisverwaltung anfertigen lassen.

Schließlich habe ich darauf hingewiesen, daß nach Abschluß jeder Auslieferung die von der beauftragten Firma erstellten Datenträger (Listen oder Disketten) an die Kreisveterinärämter zurückgegeben werden müssen. Sicherungskopien dürfen bei der Firma nicht mehr vorhanden sein.

5.16 Verkehr

5.16.1 Autobahngebühren

Mit großem technischen Aufwand werden auf der A 555 zwischen Wesseling und Bonn ein Jahr lang elektronische Einrichtungen zur automatischen Gebührenerhebung auf Autobahnen erprobt. Im Auftrag des Bundesministeriums für Verkehr testet der TÜV Rheinland verschiedene Systeme, die von mehreren Unternehmen dort installiert sind, auf ihre Brauchbarkeit und Zuverlässigkeit. Darüber hinaus sollen als unverzichtbare Voraussetzung für die Einführung einer Automatischen Gebührenerhebung (AGE) auf Autobahnen sämtliche Fragen des Datenschutzes geklärt sein. Im Herbst 1995 soll das Ergebnis des Feldversuchs vorliegen.

Zusammen mit den anderen Datenschutzbeauftragten werden die zur AGE auftretenden datenschutzrechtlichen Fragen untersucht. Dabei gehe ich von folgenden grundsätzlichen Überlegungen aus.

Vor Einführung einer AGE auf Autobahnen ist zu prüfen, ob und in welchem Umfang mit der Nutzung der AGE Gefahren für die Rechte der betroffenen Autobahnbenutzer verbunden sind. Insbesondere ermöglicht die zentrale Speicherung von personenbezogenen bzw. personenbeziehbaren Verkehrsdaten aller Autobahnbenutzer eine Erstellung von Bewegungsprofilen und die Verknüpfung von Abrechnungsdaten mit Überwachungsdaten sowie deren zweckfremde Verwendungsmöglichkeiten. Außerdem kann der Autobahnbenutzer auch dadurch unverhältnismäßig belastet werden, daß er einen lückenlosen Nachweis über seine reguläre Straßenbenutzung führen muß und damit Gefahr läuft, daß solche Nachweise auch zu anderen Zwekken, wie beispielsweise vom Arbeitgeber zur Kontrolle, verlangt werden. Schließlich können weitere Beeinträchtigungen durch den Ausbau zu einer europäisch integrierten AGE folgen.

Hieraus ergeben sich bereits grundsätzliche datenschutzrechtliche Anforderungen:

- Die AGE muß, jedenfalls soweit es die Abrechnung der regulären Straßenbenutzung betrifft, die **Anonymität** des Autobahnbenutzers gewährleisten. Das bedeutet, daß vom Systembetreiber insoweit keine personenbezogenen Daten der Benutzer erhoben und verarbeitet werden. Zur Gebührenermittlung dürfen also auch keine Angaben verwendet werden, die einen Personenbezug nachträglich ermöglichen. Soweit kein Mißbrauchsverdacht besteht, muß eine reguläre Straßenbenutzung vollständig anonym bleiben.

- Die Überwachung, ob ein Mißbrauch vorliegt, sollte grundsätzlich **stichprobenweise** und nicht vollständig erfolgen. Systeme mit flächendeckender Kontrolle setzen eine Infrastruktur voraus, die sich auch für eine flächendeckende Erfassung der Benutzer bei regulärer Straßenbenutzung eignet und zweckentfremdet werden könnte. Durch die Überwachung darf die Identität des Benutzers nur dann aufgedeckt werden, wenn ein begründeter Mißbrauchsverdacht besteht.

- Sofern im Rahmen der Überwachung personenbezogene Daten erhoben werden, müssen sie **vertraulich** behandelt werden, d. h. eine Kenntnisnahme durch unberechtigte Dritte ist auszuschließen. Die Vertraulichkeit muß auch im Verhältnis Fahrzeughalter und Fahrzeugbenutzer gewahrt bleiben. Dazu kann es notwendig sein, daß die Kontrolle sofort zu erfolgen hat, damit nicht jeder Benutzer gezwungen wird, einen Nachweis über die gefahrenen und bezahlten Strecken zu führen.

- Es ist die **Integrität** zu gewährleisten, d. h. die richtigen Daten müssen jeweils den richtigen Benutzern zugeordnet werden, und es dürfen weder zuviel noch zuwenig Daten erfaßt werden.

- Das gesamte Verfahren muß für die Teilnehmer **transparent** sein, d. h. die Benutzer müssen die realistische Chance haben, sowohl über den

generellen Ablauf als auch über die Datenerhebung und -speicherung im Einzelfall Bescheid zu wissen.

5.16.2 Sünderdatei für Berufskraftfahrer

Von einem Rechtsanwalt bin ich auf eine im Straßenverkehrsamt eines Kreises geführte Datei hingewiesen worden, in der Verstöße gegen das Fahrpersonalgesetz etwa wegen Nichteinhaltung von Lenk- und Ruhezeiten gespeichert werden. Die Speicherung erfolgt, um **wiederholte Verstöße**, die innerhalb der letzten drei Jahre vorgefallen waren, mit einem erhöhten Bußgeld ahnden zu können. Hierzu werden Name, die Anschrift und das Geburtsdatum des Fahrers, das Datum der Rechtskraft des Bußgeldbescheides bzw. des Urteils, die Höhe der festgesetzten Geldbuße und die verletzten Vorschriften festgehalten. Zur Erkennung von Wiederholungsfällen kann auf das Verkehrszentralregister in Flensburg nicht zurückgegriffen werden, da die Verstöße gegen das Fahrpersonalgesetz Zuwiderhandlungen gegen Arbeitsschutzvorschriften sind und nicht in das Verkehrszentralregister eingetragen werden.

Als Grundlage für die Führung der Datei nach dem Fahrpersonalgesetz zieht das Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen die generelle Auffangnorm zur Datenspeicherung (§ 13 Abs. 1 DSG NW) heran. Die Anwendung dieser Vorschrift scheitert bereits daran, daß eine Datenspeicherung nicht in jedem Einzelfall erforderlich ist. Es kann nämlich nicht davon ausgegangen werden, daß jedem Betroffenen, der einmal gegen Vorschriften des Fahrpersonalgesetzes verstoßen hat, eine künftige Wiederholungstat zu unterstellen ist. Deshalb läge eine unzulässige Vorratsspeicherung vor. Vorratsspeicherungen müssen jedoch im überwiegenden Allgemeininteresse erforderlich und die damit einhergehenden Einschränkungen des informationellen Selbstbestimmungsrechts durch eine normenklare gesetzliche Regelung für zulässig erklärt worden sein. Eine derartige Regelung ist nicht vorhanden. Mit dem Entwurf eines Gesetzes zur Änderung des Fahrlehrergesetzes und anderer Gesetze strebte die Bundesregierung zwar eine Verbesserung der Regelungen über die Verfolgung von Ordnungswidrigkeiten nach dem Fahrpersonalgesetz an. Der Gesetzentwurf ist allerdings nicht mehr vor Ablauf der Legislaturperiode verabschiedet worden.

Nach Abwägung der durch die Erfassung von Wiederholungstätern in einer Datei beeinträchtigten Datenschutzrechte der Betroffenen mit den Gefahren für Gesundheit und Leben der Verkehrsteilnehmer, die angesichts der hohen Verkehrsdichte durch wiederholte Zuwiderhandlungen gegen das Fahrpersonalgesetz entstehen können, habe ich nicht die Einstellung und Vernichtung der Datei gefordert, sondern trete vielmehr für die Schaffung einer normenklaren Rechtsgrundlage ein.

5.16.3 Taxilizenz ohne Schufa

Von einer Taxizentrale bin ich darauf aufmerksam gemacht worden, daß verschiedene Straßenverkehrsbehörden zur Verlängerung der Taxi-Konzession die Vorlage einer Schufa-Auskunft verlangen. Eine Behörde begründete diese Vorgehensweise damit, daß verschiedene Antragsteller Angaben über ihre unsolide finanzielle Grundlage verschwiegen. Derartige Umstände wirkten sich nachteilig auf die Leistungsfähigkeit des Taxi-Betriebes aus.

Nach § 13 Abs. 1 Nr. 1 des Personenbeförderungsgesetzes (PBefG) darf eine Taxi-Konzession nur erteilt werden, wenn die Sicherheit und die Leistungsfähigkeit des Betriebs gewährleistet sind. Danach muß der Antragsteller auf Grund seiner Vermögenslage befähigt sein, die aus dem Betrieb erwachsenden Verbindlichkeiten zu erfüllen sowie seine Fahrzeuge und Betriebsanlagen in betriebssicherem Zustand zu halten. Hierzu bestimmt § 2 Abs. 4 der Berufszugangs-Verordnung PBefG, daß der Nachweis der finanziellen Leistungsfähigkeit durch Vorlage eines Prüfungsberichts oder anderer geeigneter Unterlagen einer Bank, einer öffentlichen Sparkasse, eines vereidigten Wirtschaftsprüfers, eines Steuerberaters oder eines vereidigten Buchprüfers geführt werden kann.

Nach dieser Rechtslage ist die regelmäßige Vorlage einer Schufa-Auskunft nicht erforderlich. Lediglich in begründeten Zweifelsfällen kann auf der Grundlage des § 12 Abs. 3 PBefG eine solche Auskunft angebracht sein.

Das Ministerium für Stadtentwicklung und Verkehr des Landes Nordrhein-Westfalen hat im Erlaßwege sichergestellt, daß Straßenverkehrsbehörden künftig nur noch in begründeten Zweifelsfällen Schufa-Auskünfte einholen.

5.16.4 Einwendungen gegen Flugplatzgenehmigung

Zu der datenschutzrechtlichen Problematik der Bekanntgabe personenbezogener Daten von Einwendern im Planfeststellungsbeschluß hatte das Bundesverfassungsgericht in seinem Beschluß vom 24. Juli 1990 (DVBl. 1990, 1041) festgestellt, daß das Recht auf informationelle Selbstbestimmung der betroffenen Einwender gegenüber den Nachteilen, die durch eine Nichtveröffentlichung der Daten entstehen können, abgewogen werden muß. Zu einem ähnlichen Problem hat mich das Ministerium für Stadtentwicklung und Verkehr des Landes Nordrhein-Westfalen um Stellungnahme gebeten. Anders als in dem genannten Beschluß des Bundesverfassungsgerichts war die Frage zu beurteilen, ob die Namen der Einwender in luftverkehrsrechtlichen Genehmigungsverfahren dem Antragsteller (Flugplatzbetreiber) bekanntgegeben werden dürfen.

Im beurteilten Fall lag der Antrag einer Gesellschaft auf die zivile Mitbenutzung eines Militärflughafens vor. Im Zuge des zu diesem Genehmigungsverfahrens durchgeführten **Anhörungsverfahrens** wurde der Großteil der Einwendungen mit dem Zusatz „Der Weitergabe meiner persönlichen Daten

stimme ich nicht zu" versehen, so daß zu prüfen war, ob die Daten der Einwender trotz des Zusatzes zur Gegenäußerung an den Antragsteller weitergegeben werden dürfen.

Für die Gestattung einer zivilen Mitbenutzung von militärischen Flugplätzen ist nach dem Luftverkehrsgesetz lediglich eine Änderungsgenehmigung erforderlich. Eine Planfeststellung oder Plangenehmigung findet nicht statt. Da das Luftverkehrsgesetz zur Durchführung von Genehmigungsverfahren keine speziellen Regelungen enthält, wird ein Anhörungsverfahren nach § 28 Abs. 1 VwVfG NW durchgeführt. In diesem Verfahrensstadium können die Einwender zu den Verfahrensbeteiligten gerechnet werden, dies vor allem im Hinblick auf die öffentliche Auslegung der Antragsunterlagen und die dadurch eröffnete Möglichkeit, Einwendungen gegen das beantragte Vorhaben zu erheben. Deshalb wird zur Beurteilung der Zulässigkeit der Weitergabe von Einwendungen an einen Antragsteller die Vorschrift des § 29 VwVfG NW herangezogen.

Nach § 29 Abs. 1 Satz 1 VwVfG NW hat die Behörde den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Die Akteneinsicht umfaßt auch eine bloße Auskunft über die Namen und Anschriften der Einwender. Nach dieser Regelung muß die Gestattung der Akteneinsicht erforderlich sein. Der Erforderlichkeit begriffsimmanent ist die Einzelfallbezogenheit. In jedem einzelnen Fall muß daher geprüft werden, ob die Kenntnis der personenbezogenen Daten der Einwender zur Gegenäußerung des Antragstellers notwendig ist. Dies kann dann in Betracht kommen, wenn etwa die Lage des Grundstücks zum Flughafen innerhalb des die Zumutbarkeit übersteigenden Lärmbereichs und unterhalb des An- und Abflugsektors festgestellt wird. In einem Anhörungsverfahren dürfte aber auch hier in der Regel eine aggregierte oder sonst anonymisierte Lageangabe ausreichen.

Die Verpflichtung zur Gestattung der Akteneinsicht entfällt, soweit u. a. die Vorgänge wegen berechtigter Interessen der Beteiligten oder dritter Personen geheimgehalten werden müssen (§ 29 Abs. 2 VwVfG NW). Die Behörde hat in diesem Fall nach pflichtgemäßem Ermessen unter Abwägung zwischen den berechtigten Geheimhaltungsinteressen und dem Interesse des Antragstellers auf Einsichtnahme zu entscheiden, ob und ggf. inwieweit sie dem Antrag entspricht. Berechtigte Interessen Beteiligter und Dritter stehen der Akteneinsicht vor allem aus der Verpflichtung der Behörden zur vertraulichen Behandlung von Angaben über den Gesundheitszustand von Personen und Familien sowie deren Einkommensverhältnisse entgegen (vgl. Kopp, Verwaltungsverfahrensgesetz, § 29 Rdnr. 27). Unter Umständen können aber auch erhebliche Nachteile für den Einwender oder Dritten allein durch Bekanntgabe des Namens des Betroffenen eintreten, etwa wenn dieser Mitarbeiter des Antragstellers ist und Belastungen des Arbeitsverhältnisses zu befürchten sind. Soweit aus diesen Gründen bereits die Verpflichtung zur

Gestattung der Akteneinsicht nicht völlig entfällt, ist Einsicht in den insoweit unproblematischen Teil der Akten zu gewähren oder an Stelle der Akteneinsicht nur Auskunft zu erteilen.

In diesem Zusammenhang habe ich die Frage, wie Einwendungen mit dem von Einwendern geschriebenen Zusatz „Der Weitergabe meiner persönlichen Daten stimme ich nicht zu" zu behandeln seien, wie folgt beurteilt: Nach meinen Ausführungen kommt es auf Zustimmung oder **Widerspruch des Betroffenen** nicht an, weil die Anhörungsbehörde nach pflichtgemäßem Ermessen über den Akteneinsichts- bzw. Auskunftsanspruch des Antragstellers selbst zu entscheiden hat. Bei Einwendungen mit dem genannten Zusatz sollte allerdings vor einer beabsichtigten Übermittlung der Einwendung auch mit personenbezogenen Daten dem Betroffenen Gelegenheit gegeben werden, seine Geheimhaltungsinteressen darzulegen, ggf. mit dem Hinweis, daß nach § 29 Abs. 2 VwVfG NW sein Geheimhaltungsinteresse mit dem Interesse des Antragstellers auf Einsichtnahme abzuwägen sei.

5.17 Wirtschaft

5.17.1 Gewerbeüberwachung

Bei mehreren Ordnungsämtern habe ich überprüft, ob die mir in Eingaben vielfach vorgetragenen Beschwerden zutreffen, daß zur Erteilung einer **Gaststättenerlaubnis** zuviele persönliche Daten von den Antragstellern verlangt werden.

Vor Erteilung einer Erlaubnis nach dem Gaststättengesetz hat die Behörde die Zuverlässigkeit des Antragstellers oder der Antragstellerin zu beurteilen. Die hierzu benötigten Daten werden entweder bei dem Betroffenen selbst erfragt oder von anderen Behörden angefordert. Gegen die regelmäßige Vorlage eines polizeilichen Führungszeugnisses, einer Auskunft aus dem Gewerbezentralregister sowie einer Bescheinigung des zuständigen Finanzamtes über etwaige Steuerschulden bestehen keine datenschutzrechtlichen Bedenken. Soweit darüber hinaus regelmäßige Anfragen zur Zuverlässigkeit an die Polizei und die Wohnsitzgemeinde gerichtet werden, habe ich die Ordnungsbehörden davon überzeugt, daß nur in begründeten Einzelfällen derartige Erhebungen vorgenommen werden dürfen. Denn nur dann läßt § 11 Abs. 2 Satz 2 der Gewerbeordnung eine solche Anfrage zu. Die notwendigen Daten dürfen ohne Mitwirkung des Betroffenen nur erhoben werden, wenn die Entscheidung der Behörde eine Erhebung bei anderen Personen oder Stellen erforderlich macht.

Soweit in Antragsvordrucken nach persönlichen Angaben zum **Ehegatten** der Antragstellerin oder des Antragstellers gefragt wird, darf die Erhebung dieser Daten nur in bestimmten Fällen, etwa wenn die Mitarbeit des Ehegatten im Betrieb vorgesehen ist, erfolgen. Einvernehmen bestand auch darüber, daß die Frage nach den Aufenthaltsorten und der beruflichen Betätigung auf ein Jahr vor der Antragstellung beschränkt werden sollte. Soweit

pauschal nach anhängigen Ermittlungsverfahren oder Strafverfahren gefragt wurde, wird diese Fragestellung künftig auf die einschlägigen Verfahren beschränkt.

In einem anderen Konzessionsfall führte die Zuverlässigkeitsprüfung einer Behörde zur Kündigung eines Arbeitsverhältnisses. Der bei einem Buchmacher beschäftigte Betroffene hatte bei der zuständigen Bezirksregierung einen Antrag auf Erteilung einer **Buchmacherkonzession** gestellt. Hierzu wurde neben der Kreispolizeibehörde auch der Deutsche Buchmacherverband angehört. Im Rahmen dieser Anhörungsverfahren sei nach der Darstellung des Betroffenen der Deutsche Buchmacherverband an seinen Arbeitgeber herangetreten und habe ihn über die Tatsache der Antragstellung unterrichtet. Dieser Umstand habe zu der Kündigung seines Arbeitsverhältnisses geführt.

Zur Vorbereitung der Entscheidung über einen Antrag auf Zulassung zum Buchmacher hat die Erlaubnisbehörde eine Stellungnahme des Deutschen Buchmacherverbandes einzuholen, wenn der Antragsteller seine fachliche Eignung nicht durch eine mindestens zweijährige praktische Tätigkeit als Buchmachergehilfe nachweisen kann. Auf die Tatsache der Anhörung des Deutschen Buchmacherverbandes wird zwar vor der Antragstellung hingewiesen. Allerdings wird dem Antragsteller keine Information darüber erteilt, daß der Verband im Rahmen seiner Anhörung eigene Ermittlungen etwa bei dem Arbeitgeber des Antragstellers durchführen und dabei Angaben über die beantragte Erlaubnis bekanntgeben kann. In dieser von der Behörde offen gelassenen Verfahrensweise liegt der datenschutzrechtliche Mangel.

Es kann dem angehörten Verband in einem von der Behörde veranlaßten Verfahren nicht freigestellt sein, ob er eigene Ermittlungen etwa bei dem Arbeitgeber eines Antragstellers durchführen oder weitere Stellen im Rahmen der Überprüfung der fachlichen Eignung des Antragstellers einschalten will. Die Erlaubnisbehörde trägt für die Verfahrensweise die Verantwortung in datenschutzrechtlicher Hinsicht, weil durch die Anhörung des Verbandes in das Grundrecht auf Datenschutz eingegriffen wird. In erster Linie sollte deshalb der Verband angehalten werden, aus eigener Beurteilung heraus festzustellen, ob der Antragsteller über die notwendige fachliche Qualifikation zur Ausübung des Buchmachergewerbes verfügt. Sollte etwa der Verband hierzu ohne Auskunft des Arbeitgebers nicht in der Lage sein, muß die Erlaubnisbehörde vorher den Betroffenen über die Befragung des Arbeitgebers durch den Verband unterrichten (vgl. § 12 Abs. 2 Satz 3 DSG NW). Auf Grund dieser Unterrichtung könnte der Betroffene entscheiden, ob er die Befragung des Arbeitgebers hinnehmen oder seinen Antrag zurückziehen will.

Da sich die Erlaubnisbehörde bei ihrer Vorgehensweise auf einen Runderlaß des Ministeriums für Umwelt, Raumordnung und Landwirtschaft bezieht, habe ich dem Ministerium empfohlen, die Erlaßregelung entsprechend zu überarbeiten.

5.17.2 Kammerleitstelle

Die AKG - Arbeitsgemeinschaft Kammerleitstelle für Gewerbesteuermeßbeträge, ein nicht eingetragener Verein mit Sitz in Dortmund, gehört zu den öffentlichen Stellen des Landes, da sie eine Gemeinschaftseinrichtung der Kammern ist und insoweit Aufgaben der öffentlichen Verwaltung erledigt (vgl. § 9 Abs. 2 IHKG).

Bei einem Informations- und Kontrollbesuch konnte ich mich über die Arbeitsweise der AKG informieren. Ihr gehören alle Industrie- und Handelskammern und Handwerkskammern der Länder Niedersachsen, Nordrhein-Westfalen und Rheinland-Pfalz an. Sie versteht sich als Serviceeinrichtung, die die Kammern mit den notwendigen Daten zur Ermittlung der Beiträge der kammerzugehörigen Firmen versorgt. Die Beiträge zu den Kammern werden als öffentliche Abgaben auf der Grundlage der von den Finanzämtern festgesetzten **Gewerbesteuermeßbeträge** erhoben. Sofern von den Finanzämtern wegen der bei der Gewerbesteuer geltenden Freibeträge keine Gewerbesteuermeßbeträge berechnet werden, wird hilfsweise an den nach dem Einkommen- oder Körperschaftsteuergesetz ermittelten Gewinn aus Gewerbebetrieb angeknüpft.

Die AKG erhält die Steuerdaten von der Finanzverwaltung. Der Austausch der Daten erfolgt in der Weise, daß die AKG von dem Rechenzentrum der Finanzverwaltung Nordrhein-Westfalen viermal im Jahr Magnetbänder mit Daten der Gewerbesteuerpflichtigen sowie Meßbeträgen, Zerlegungsanteilen und Gewinnen aus Gewerbesteuerfestsetzung bzw. Einkommensteuerfestsetzung erhält. Jeder von der Finanzverwaltung übermittelte Datensatz erfaßt zudem die Steuernummer und den amtlichen Gemeindeschlüssel. Mit dem Gemeindeschlüssel wird die örtliche Zuständigkeit der Industrie- und Handelskammer und Handwerkskammer festgestellt, damit der Datensatz an die zuständige Kammer weitergeleitet werden kann.

Zur Frage der Zulässigkeit der Erhebung der Steuerdaten durch die Kammern bei den Finanzbehörden hatte ich in meinem 10. Tätigkeitsbericht (S. 132/133) dargelegt, daß den Kammern die gesetzliche Ermächtigung fehlte, die Steuermeßbeträge unmittelbar bei den Finanzbehörden zu erheben. Mittlerweile ist diese Lücke durch eine Änderung des IHKG für die Industrie- und Handelskammern geschlossen. Für die Handwerkskammern fehlt eine derartige Regelung weiterhin, obwohl auch die Handwerksordnung zwischenzeitlich novelliert worden ist (vgl. oben 3.1.16).

5.18 Öffentliche Unternehmen

5.18.1 Verbund von Sparkasse und Versicherung

Nach dem Vorbild des Allfinanzkonzepts privater Banken streben die Verbundpartner Sparkasse, LBS und Provinzial ebenfalls eine engere Zusammenarbeit an. Die Umsetzung des Konzepts ermöglicht das Gesetz zur Änderung des Sparkassengesetzes vom 8. März 1994, soweit die Sparkassen nunmehr im begrenzten Rahmen alle banküblichen Geschäfte betreiben dürfen.

Der zulässige Austausch von Kundendaten im Verbund kann sich aber nach wie vor nur auf eine wirksame Einwilligung der Kunden stützen. Hierauf habe ich bereits in meinem 11. Tätigkeitsbericht (S. 119/120) hingewiesen. Diese Auffassung wird von den Vertretern der Kredit- und Versicherungswirtschaft geteilt. Es besteht weiter Einigkeit darüber, daß dem Gesichtspunkt der Transparenz und der Freiwilligkeit der Datenverarbeitung eine entscheidende Bedeutung zukommen soll.

Die Überlegungen zur Ausgestaltung der Einwilligungsklausel in der Kreditwirtschaft sind noch nicht abgeschlossen. Es müssen insbesondere die abschließenden Gespräche zwischen dem Zentralen Kreditausschuß, der für die Banken und Sparkassen spricht, und den Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich im „Düsseldorfer Kreis" abgewartet werden. Angestrebt wird hier eine möglichst konkrete Aufzählung der zu übermittelnden Daten und der Datenempfänger.

Demgegenüber haben sich Vertreter der Aufsichtsbehörden und der Datenschutzbeauftragten mit dem Gesamtverband der Deutschen Versicherungswirtschaft auf eine **Verbundklausel** verständigt und ein umfangreiches Merkblatt zur Datenverarbeitung erarbeitet. Die von den Provinzial Versicherungsanstalten verwendete Verbundklausel lautet wie folgt:

> „Ich willige ferner ein, daß die Versicherung der Gruppe der Provinzial-Versicherungen Antrags-, Vertrags- und Leistungsdaten in gemeinsamen Datensammlungen führen und an den/die für mich zuständigen Vermittler weitergeben, soweit dies der ordnungsgemäßen Durchführung meiner Versicherungsangelegenheiten dient.
>
> Ohne Einfluß auf den Vertrag und jederzeit widerrufbar willige ich weiter ein, daß der/die Vermittler meine allgemeinen Antrags-, Vertrags- und Leistungsdaten darüber hinaus für die Beratung und Betreuung auch in sonstigen Finanzdienstleistungen nutzen darf/dürfen.
>
> Diese Einwilligung gilt nur, wenn ich bei Antragstellung vom Inhalt des Merkblatts zur Datenverarbeitung Kenntnis nehmen konnte, das mir vor Vertragsabschluß mit weiteren gesetzlich vorgesehenen Informationen - auf Wunsch auch sofort - überlassen wird."

Mit seiner Unterschrift unter die Verbundklausel erteilt der Kunde seine Einwilligung (§ 4 Abs. 1 BDSG) dazu, daß die Provinzial seine Versicherungsdaten an den Vermittler des Versicherungsvertrages, also an die Sparkasse, die LBS oder an den selbständigen Versicherungsaußendienst, übermittelt, und daß diese die allgemeinen Daten auch für die Beratung und Betreuung in sonstigen Finanzdienstleistungen nutzen dürfen.

Zur Einführung einer Einwilligungsklausel bei den **Altkunden** ist beabsichtigt, diesen Personenkreis in einem gesonderten Schreiben über die Verbundklausel zu unterrichten. In den Fällen, in denen kein Widerspruch gegen den neuen Umfang der Einwilligungserklärung erhoben worden ist, geht die Provinzial von dem Einverständnis der Kunden aus.

Gegen diese Widerspruchslösung können im Hinblick auf die Regelung in § 28 Abs. 3 BDSG keine Einwände erhoben werden. Danach ist eine Nutzung oder Übermittlung für Zwecke der Werbung oder Meinungsforschung zulässig, sofern der Betroffene bei der speichernden Stelle der Nutzung oder Übermittlung seiner Daten für diese Zwecke nicht widerspricht.

5.18.2 Datensammlung bei Kontoeröffnung

Durch die Eingabe eines Kunden bin ich darauf aufmerksam gemacht worden, daß Sparkassen bei der Konto- und Depoteröffnung generell eine Kopie des vorgelegten Ausweises anfertigen. Hierzu hat mir die Sparkasse mitgeteilt, daß sie die Ausweiskopien bei der Konto- und Depoteröffnung zur Durchführung des **Geldwäschegesetzes** erstellt.

Mit diesem Gesetz soll die Organisierte Kriminalität wirksamer bekämpft werden können. Bei konkretem Geldwäscheverdacht sind die Kreditinstitute gehalten, Anzeige zu erstatten. Das Gesetz verpflichtet deshalb neben anderen Wirtschaftsbereichen insbesondere die Kreditinstitute bei einer Reihe von Geschäftsvorgängen ab 20 000 DM, ihre Kunden an Hand des amtlichen Ausweises zu identifizieren und diesen Vorgang durch Kopie der vorgelegten Dokumente festzuhalten. Erleichterungen von der Pflicht zur Identifizierung gelten für früher bereits identifizierte und persönlich bekannte Kunden.

Ausgangspunkt für die Verpflichtung zur Identifikation des Kunden ist die Abgabenordnung (AO). Nach § 154 AO darf niemand auf einen falschen Namen für sich oder einen Dritten ein Konto errichten. Wer ein Konto führt, hat sich zuvor Gewißheit über die Person und Anschrift des Verfügungsberechtigten zu verschaffen und die entsprechenden Angaben in geeigneter Form festzuhalten. Auf diese Regelung kann das Anfertigen einer Ausweiskopie nicht gestützt werden.

Das Bundesaufsichtsamt für das Kreditwesen läßt zwar bei Altkunden die frühere Identifizierung anläßlich der Kontoeröffnung nach § 154 AO genügen, verlangt aber, daß bei allen Neukunden eine Identifizierung im Sinne des Geldwäschegesetzes vorgenommen wird. Daher sehen sich die Sparkassen verpflichtet, Ausweiskopien bei allen Konto-Neueröffnungen zu fertigen, um in späteren Geldwäschefällen die erleichterte Form der Identifizierung bei möglichst vielen Kunden anwenden zu können. In der Regel werde dieses Verfahren von den Kunden nicht beanstandet. Soweit ein Kunde ausnahmsweise der Erstellung von Kopien widerspreche, werde auf das Anfertigen von Kopien verzichtet.

Meines Erachtens bestehen gegen diese Verfahrensweise datenschutzrechtliche Bedenken. Nach dem Geldwäschegesetz greift die Pflicht zur Anfertigung derartiger Dokumente erst bei der Durchführung bestimmter Transaktionen. Sofern diese Voraussetzung bei einer Konto- und Depoteröffnung nicht gegeben ist, kann das Geldwäschegesetz nicht als Rechtfertigung für die Ablichtung eines Ausweisdokuments herangezogen werden. Wegen der bereichspezifischen Regelungen des Geldwäschegesetzes erscheint auch eine Praxis der Sparkassen problematisch, jeweils die Einwilligung des Kunden einzuholen. Die gesetzlich vorgenommene Beschränkung auf die Fallkonstellationen des Geldwäschegesetzes spricht gegen die Speicherung von Ausweiskopien bei jeder Kontoeröffnung auf freiwilliger Basis. Vor allem aber liegt eine unzulässige Vorratsspeicherung vor, weil zu diesem Zeitpunkt nicht feststeht, ob jemals eine dem Geldwäschegesetz unterliegende Transaktion eintreten wird.

In dem konkreten Beschwerdefall habe ich der Sparkasse empfohlen, davon abzusehen, bei einer normalen Kontoeröffnung, ohne daß das Geldwäschegesetz dies verlangt, Kopien der vorgelegten Ausweisdokumente anzufertigen.

5.18.3 Bankinterne Zugriffe auf Kundendaten

Die Frage, ob außerhalb der **kontoführenden Zweigstelle** weitere Sparkassenmitarbeiter auf Kundendaten zugreifen dürfen, wird wiederholt in Eingaben und Beschwerden Betroffener gestellt. Auch der Landesbeauftragte für den Datenschutz Rheinland-Pfalz hat in diesem Zusammenhang ausgeführt, daß sich häufig im ländlichen Bereich Kunden veranlaßt sehen, Mitarbeitern der örtlichen Sparkassenzweigstelle, die ihnen etwa als Nachbarn persönlich näher bekannt sind, nicht unbedingt alle Informationen über ihre finanziellen Verhältnisse zur Verfügung zu stellen. Deshalb würden sie sich lieber von einer anderen Sparkassenzweigstelle betreuen lassen. Konsequenterweise muß dann aber auch gewährleistet sein, daß ein Zugriff auf die Kundendaten nur Mitarbeitern der kontoführenden Zweigstelle möglich ist. Ein gezielter Datenabruf bei der kontoführenden Stelle durch Sparkassenmitarbeiter anderer Zweigstellen - aber auch der Hauptstelle - muß also ausgeschlossen bleiben. Wenngleich die Problematik auf dem Lande eher zu Tage tritt als in Großstädten, besteht oft auch hier der Wunsch von Kunden, nur von einer bestimmten - von ihm gewählten - Zweigstelle betreut zu werden.

Eine große Sparkasse trägt den Kundenwünschen Rechnung, indem sie einvernehmlich mit dem Kunden die betreuende Zweigstelle festlegt. Will der Kunde seine Vertragsbeziehungen von seiner bisherigen Zweigstelle auf eine andere verlagern, wird eine Änderung der Angabe über die kundenbetreuende Stelle im Einvernehmen mit dem Kunden vorgenommen. Allerdings ist mit der Festlegung auf eine bestimmte Zweigstelle für diesen Kunden der Nachteil verbunden, daß die ihm vertraglich zugesicherte Flexibilität bei der Geschäftsabwicklung im gesamten Zweigstellennetz der Sparkasse nicht besteht.

5.18.4 Videoüberwachungssysteme in Geldautomaten

In einem Zeitungsartikel „Ein Foto von jedem Kunden" wurde darüber berichtet, daß auch Sparkassen Geldausgabeautomaten verwendeten, in denen Videokameras mit extremen Weitwinkelobjektiven, nur als harmlose Lampen erkennbar oder hinter Sichtblenden verborgen, zu Überwachungszwecken installiert seien. Die Videokamera halte von jedem Kunden fest, wann wo und wieviel Geld am Automat ausgezahlt werde. Um mir ein eigenes Bild von diesen Überwachungstechniken zu verschaffen, habe ich verschiedene Sparkassen meines Kontrollbereichs besucht. Von Sparkassenmitarbeitern wurden mir in sog. Selbstbedienungs-Servicestellen Geldautomaten gezeigt, die mit Videokameras ausgestattet sind. Bei einer Sparkasse zeichnet eine zweite Kamera auch die Geldentnahme mit einem sog. Nadelöhrobjektiv auf.

Die **Aufzeichnungen** in Videotechnik werden als Serienaufnahmen gefertigt. Zu sehen ist das Porträt des Kunden, der das Gerät bedient. Bei Geldautomaten mit einer zweiten Kamera wird in das Porträtbild ein Kleinbild eingeblendet, das die Entnahme der Geldscheine durch den Kunden festhält. Dabei sind flüchtig die Hände des Kunden zu sehen. Abhängig von der technischen Ausstattung der Videokamera werden zu der Porträtaufnahme Datum, Uhrzeit, Bankleitzahl, Kontonummer, Kartenfolgenummer und Verfalldatum der EC-Karte sowie der abgebuchte Betrag aufgezeichnet. Die Ausstattung der Geldausgabeautomaten mit Videokameras ist bei den einzelnen Sparkassen unterschiedlich. Eine Sparkasse überwacht ca. 20 Prozent ihrer Geldautomaten mit versteckten Videokameras, bei einer anderen Sparkasse sind es bis zu 70 Prozent der Automaten.

Die Videoaufzeichnungen werden aus der Sicht der Sparkassen für die Bearbeitung von Reklamationen, mißbräuchlichen Verfügungen und bei begründetem Verdacht, daß der Kunde solche nur vortäuscht, benötigt. Sie dienen auch der Beweissicherung in Ermittlungsverfahren der Polizei bzw. Staatsanwaltschaft. Darüber hinaus erfolgt die Aufzeichnung zur Aufdeckung und Aufklärung mutwilliger Beschädigungen an Einrichtungen und Geräten. Obwohl ich mich den guten Gründen der Sparkassen nicht verschließen will, habe ich erhebliche datenschutzrechtliche Bedenken, wenn die Videoaufzeichnungen ohne Wissen der Kunden vorgenommen werden.

Im Bereich der Geldautomaten sind folgende Aufkleber angebracht: „Verehrter Kunde, aus Sicherheitsgründen ist unsere SB-Servicestelle ständig kameraüberwacht". Diesem Hinweis kann der Kunde m. E. nicht entnehmen, daß von ihm eine Porträtaufnahme mit seinen Abbuchungsdaten und der Vorgang der Geldentnahme aufgezeichnet wird. Nach Darstellung der Sparkassen würden die Kunden aus grundsätzlichen Erwägungen nur allgemein auf die Überwachung hingewiesen. Auf diese Weise soll dem Diebstahl und der Zerstörung von Videokameras entgegengewirkt werden. Außerdem führten weitergehende Hinweise auf die Videoaufzeichnung nur dazu, daß eine Per-

son, die etwa eine mißbräuchliche Geldautomatenverfügung beabsichtige, dann Geldautomaten ohne Videoüberwachung aufsuchen würde.

Auch wenn diese Argumente nicht von der Hand zu weisen sind, kann eine verdeckte Videoüberwachung in den Geldautomaten nur vorgenommen werden, wenn sie durch Gesetz erlaubt ist. Eine solche gesetzliche Ermächtigung gibt es nicht. Nach der bestehenden Rechtslage müssen die Daten nach Treu und Glauben und auf rechtmäßige Weise erhoben werden (§ 28 Abs. 1 Satz 2 BDSG). Bereits hieraus leitet sich die Verpflichtung ab, daß die Kunden in ausreichendem Umfang auf Videoaufzeichnungen hinzuweisen sind. Denn aus dem Recht auf informationelle Selbstbestimmung folgt der Grundsatz der Transparenz der Datenverarbeitung. Danach muß jeder Betroffene wissen können, wer was wann und bei welcher Gelegenheit über ihn weiß. Transparenz der Datenverarbeitung ist eine notwendige Voraussetzung der Selbstbestimmung. Einschränkungen sind nur im überwiegenden Allgemeininteresse zulässig und bedürfen einer gesetzlichen Grundlage, die dem Gebot der Normenklarheit entspricht und den Verhältnismäßigkeitsgrundsatz beachtet. Daher finden sich in verschiedenen Sicherheitsgesetzen, wie etwa in dem § 17 des Polizeigesetzes des Landes Nordrhein-Westfalen „Datenerhebung durch den verdeckten Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen und Bildaufzeichnungen" besondere Ermächtigungsgrundlagen für die Anfertigung heimlicher Bildaufnahmen und Bildaufzeichnungen.

Eine entsprechende Rechtsgrundlage muß für derart weitgehende Beeinträchtigungen grundsätzlich auch im nicht-öffentlichen Bereich gefordert werden. Da sie fehlt, wäre die Überwachung nur mit Einwilligung der Kunden (§ 4 BDSG) zulässig. Diese Möglichkeit stößt jedoch insbesondere in den Fällen auf praktische Schwierigkeiten, in denen auch Kunden eines fremden Kreditinstituts den Geldausgabeautomaten bedienen. Daher kann von einer Zulässigkeit der Videoaufzeichnungen nur dann ausgegangen werden, wenn die Kunden zumindest unmißverständlich auf die Aufzeichnung hingewiesen und über die Art und den Umfang der Speicherung ihrer Daten unterrichtet werden. Ich werde der Sparkassenorganisation empfehlen, die Kunden in geeigneter Weise aufzuklären.

5.18.5 Rennlisten bei Versicherungen

Als „Anfeuerungspeitsche" bezeichnete ein ehemaliger Geschäftsstellenleiter einer Provinzial Versicherungsanstalt die Herausgabe sog. Rennlisten über den **Versicherungsaußendienst**. In einer weiteren Eingabe teilte mir eine Gruppe von Geschäftsstellenleitern mit, daß die Direktion der Provinzial zu einer generellen Einstellung der Verteilung dieser Listen nicht bewegt werden konnte.

Die Rennlisten enthalten den Namen des Außendienstmitarbeiters und in verschlüsselter Form die von ihm in einem bestimmten Zeitraum in den jeweiligen Versicherungssparten erreichten Bestands-, Umsatz- oder Pro-

visionszahlen. Der umsatzstärkste Vertreter führt die Liste an, sie endet mit dem umsatzschwächsten. Die Rennlisten erfassen alle Außendienstmitarbeiter eines bestimmten Gebiets, beispielsweise einer Bezirksdirektion, und werden monatlich allen in der Liste aufgeführten Mitarbeitern übersandt. Zwar können aus der verschlüsselten Darstellung der Produktionszahlen keine konkreten Nettoverdienste eines Mitarbeiters abgeleitet werden; aber die Mitarbeiter können aus den mitgeteilten Daten grob das Einkommen der anderen für das Neugeschäft erkennen.

Die Verteilung der Rennlisten ist datenschutzrechtlich als Übermittlung personenbezogener Daten an Dritte anzusehen. Die Provinzial stützt die Zulässigkeit der Herausgabe der Rennlisten auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Zu der danach bestehenden Voraussetzung, daß die Übermittlung zur Wahrung berechtigter Interessen der Provinzial erforderlich sein muß, wird vorgetragen, die Rennlisten seien als ein geeignetes Motivations- und Steuerungssystem für den Außendienst in der ganzen Versicherungswirtschaft anerkannt. Mit der Bekanntgabe von Namen und Rangfolge solle dem Geschäftsstellenleiter verdeutlicht werden, wo er innerhalb seiner „Produktionsgemeinschaft Bezirksdirektion" stehe. Diese Tatsache könne für ihn möglicherweise einen Anreiz zur Verbesserung seiner Leistungen darstellen. Diese Anreiz- und Motivationsfunktion entfiele, wenn auf die personenbezogenen Angaben in der Liste verzichtet würde. Gerade der Personenbezug, der einen Vergleich zum Nachbar-Geschäftsstellenleiter möglich mache, sei wesentliches Kriterium für die Bekanntgabe personenbezogener Erfolgslisten.

Ich habe Zweifel, ob der Gesichtspunkt der Motivation bei allen in der Liste genannten Mitarbeitern durchschlägt. Denn nach meiner Auffassung kann nicht davon ausgegangen werden, daß der einzelne Mitarbeiter nur deshalb gute Umsätze anstrebt, weil er dann in die Spitzengruppe der Liste aufrücken würde. Vornehmlich sehe ich den Ansporn zur Erzielung guter Geschäftsergebnisse grundsätzlich in dem jeweiligen finanziellen Erfolg, den der betreffende Mitarbeiter selbst erzielen möchte. Ich vermag daher die Erforderlichkeit solcher Rennlisten, jedenfalls mit personenbezogenen Daten, nicht zu erkennen.

Eine Zulässigkeit der Verteilung solcher Rennlisten scheitert aber auch an der weiteren Voraussetzung des § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Denn die Vorschrift läßt eine Datenübermittlung auch nur dann zu, wenn kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Übermittlung überwiegt. Schlechte Geschäftsverläufe und damit eine etwaige Herabstufung in der Rangfolge der Liste können durch unverschuldete Abwesenheitszeiten, wie Urlaub und Krankheit, begründet sein. Daneben können familiäre Probleme aber auch das Nachlassen der Leistungen aus Altersgründen oder die Verringerung des Leistungsumfanges durch Teilzeitbeschäftigung zu einem Ergebnis führen, das kein objektives Bild des Leistungsstandes widerspiegelt, aber vortäuscht. Deshalb kann durchaus das schutzwürdige Interesse der Betroffenen an der Geheimhal-

tung ihrer Leistungsdaten das Interesse der Versicherung an zusätzlicher Leistungsmotivation durch Rennlisten überwiegen.

Sofern die Provinzial Versicherungsanstalten an der Bekanntgabe der Leistungsdaten ihrer Außendienstmitarbeiter festhalten wollen, muß eine Einwilligung der Betroffenen gemäß § 4 Abs. 1 BDSG eingeholt werden. Nach entsprechender Erörterung hat mir diese Provinzial Versicherungsanstalt mitgeteilt, daß sie den Vertretern künftig nur noch die eigenen Erfolge und ihre Rangfolge beim Vergleich mit den anderen nennen werde. Die Ergebnisse der anderen Vertreter werden nicht mehr bekanntgegeben.

6. Organisatorische und technische Maßnahmen

6.1 Datensicherheit als Führungsziel

Versteht man unter Qualität im Geschäftsleben eine Aussage darüber, in welchem Maße eine Sache oder Dienstleistung den Anforderungen gerecht wird, so ist eine entsprechend definierte Qualität bei der Datenverarbeitung eine Aussage darüber, in welchem Maße sichergestellt ist, daß die Daten entsprechend den bestehenden Vorschriften und Weisungen verarbeitet und Verlust, unzulässige Verarbeitung oder Kenntnisnahme dabei verhindert werden - also eine Aussage darüber, in welchem Maße Datensicherheit gewährleistet ist. Von der Datensicherheit hängt nicht nur die Ordnungsmäßigkeit des Verwaltungshandelns ab; auf der Ansicht über Datensicherheit beruht auch weitgehend die Akzeptanz der Datenverarbeitung.

Datensicherheit entsteht jedoch nicht von selbst. Ob es gelingt, Datensicherheit zu gewährleisten, ist nach meiner Erfahrung vor allem eine Frage der Führung und der gesetzten Prioritäten und damit eine Frage grundsätzlicher Weichenstellungen. Grundsätzliche Weichenstellungen sind Aufgaben der Behördenleitung. Erst hierauf aufbauend kann eine Lösung mittels Organisation und Technik erfolgen.

6.1.1 Dienstanweisung

Eine umfassende Dienstanweisung, die der aktuellen Situation der öffentlichen Stelle gerecht wird, gehört zu den Grundlagen, auf denen die Datensicherheit beruht. Es ist erforderlich, in der Dienstanweisung Regelungen für alle wesentlichen Arbeitsbereiche zu treffen und dabei auf die aktuelle Strukturorganisation Bezug zu nehmen.

Zur Vorbereitung eines Kontrollbesuchs hatte ich darum gebeten, daß mir Kopien der für den Datenschutz bei der automatisierten Datenverarbeitung geltenden Dienstanweisungen und Richtlinien übersandt werden. Neben einigen anderen Unterlagen erhielt ich dazu eine „Geschäftsanweisung für die automatisierte Datenverarbeitung", eine „Geschäftsanweisung für das Kompetenzzentrum" der kontrollierten Stelle und „Interne Regelungen für den Dienstbetrieb im Kompetenzzentrum".

Während des Kontrollbesuchs stellte sich heraus, daß in diesen Unterlagen auf eine Organisationsstruktur Bezug genommen wurde, die nicht mit der aktuellen Aufbauorganisation übereinstimmte. So gab es nicht mehr eine Organisationseinheit mit der Bezeichnung Kompetenzzentrum. Auch lag die Zuständigkeit für die automatisierte Datenverarbeitung bei der Abteilung ADV des Hauptamts, obgleich nach der mir übersandten Geschäftsanweisung für die automatisierte Datenverarbeitung eine „Stabsstelle" u. a. zuständig war für „die Aufgaben der ADV-Organisation im Bereich der herkömmlichen und der individuellen Datenverarbeitung" und „den hard- und softwaretechnischen Datenschutz". Dem mir übersandten Verwaltungsgliederungsplan hatte ich auch entnehmen können, daß es eine Organisations-

einheit mit der Bezeichnung Stabsstelle gab. Während des Kontrollbesuchs wurde allerdings berichtet, die Stabsstelle habe keinerlei Funktion mehr im Zusammenhang mit der automatisierten Datenverarbeitung. Die Ausführungen in der Geschäftsanweisung für die automatisierte Datenverarbeitung seien daher insoweit unzutreffend.

Meinen Mitarbeitern wurde während des Kontrollbesuchs erläuternd berichtet, die Geschäftsanweisung für die automatisierte Datenverarbeitung und die Anweisungen für das Kompetenzzentrum könnten weiterhin als geltende Dienstanweisungen angesehen werden, indem man sowohl an die Stelle der Stabsstelle als auch an die des Kompetenzzentrums in diesen Anweisungen die heutige Abteilung ADV des Hauptamts treten läßt. In diesem Sinne wurden die mir übersandten Unterlagen während des Kontrollbesuchs erörtert. Auch dabei ergaben sich allerdings grundsätzliche Schwierigkeiten, als meinen Mitarbeitern berichtet wurde, daß es die in der Geschäftsanweisung für die automatisierte Datenverarbeitung angeführten „Facharbeitskreise" heute nicht mehr gebe.

Zum Gewährleisten der Datensicherheit ist es erforderlich, daß die einzuhaltenden Regelungen als verbindliche Dienstanweisungen schriftlich formuliert sind. Selbstverständliche Voraussetzung ist, daß sich die Dienstanweisung auf die aktuelle Aufbauorganisation bezieht. Ich habe daher empfohlen, die zum Gewährleisten der Datensicherheit erforderlichen Regelungen durch eine der aktuellen Aufbauorganisation entsprechende Dienstanweisung vorzuschreiben.

Für einen anderen Kontrollbesuch waren mir zur Vorbereitung u. a. das Organisationshandbuch und die Entwürfe einiger Dienstanweisungen übersandt worden. Mit einer Ausnahme waren die übersandten Entwürfe überarbeitete Fassungen von Dienstanweisungen, die sich bereits im Organisationshandbuch befanden. Dem Entwurf der Dienstanweisung für die Pflege von Anwendungen technikunterstützter Informationsverarbeitung entsprach keine gültige Dienstanweisung im Organisationshandbuch.

Auf den Hinweis während des Kontrollbesuchs, es sei doch erforderlich gewesen, auch die Pflege von Anwendungen durch Dienstanweisung zu regeln, wurden meine Mitarbeiter auf eine ältere Dienstanweisung hingewiesen, die noch gelte aber nicht mehr Bestandteil des Organisationshandbuchs sei. Bei der Erörterung dieser älteren Dienstanweisung ergab sich, daß es Überschneidungen zwischen dieser Dienstanweisung und den Dienstanweisungen des Organisationshandbuchs gab. Dagegen wurde das Gebiet der Pflege von Anwendungen durch die ältere Dienstanweisung nicht vollständig abgedeckt.

Eine derartige Regelungslücke und Überschneidungen von Dienstanweisungen bedeuten eine erhebliche Beeinträchtigung der Datensicherheit. Erforderliche Anweisungen sind entweder nicht erteilt, oder es besteht für die Mitarbeiter eine Unsicherheit, welche der erteilten Anweisungen für sie gültig sind.

Es wurde besprochen, daß das Organisationshandbuch überarbeitet wird, damit die mit derartigen Überschneidungen und Regelungslücken verbundenen Unsicherheiten baldmöglichst ausgeräumt werden. Um in der Zukunft jegliche Unsicherheit bezüglich der Gültigkeit von Dienstanweisungen zu beseitigen, könnten die in dem Inhaltsverzeichnis des Organisationshandbuchs angeführten Dienstanweisungen jeweils mit einem Ausgabedatum oder mit einer Versionsnummer versehen werden. Bei Änderung einer einzelnen Dienstanweisung würde dann gleichzeitig die Versionsnummer oder das Datum im Inhaltsverzeichnis geändert. Zweifel über die Gültigkeit von Dienstanweisungen könnten dann nicht mehr entstehen.

Entsprechende Anforderungen an eine Dienstanweisung betraf auch die Anfrage einer Stadt, die wissen wollte, ob sie rechtlich verpflichtet sei, alle Dienstanweisungen zu nur einer Dienstanweisung zusammenzufassen. In meiner Stellungnahme wies ich darauf hin, es sei unter dem Gesichtspunkt der Datensicherheit sinnvoll, alle vorhandenen Dienstanweisungen zur Datensicherung schriftlich zu einer gültigen Dienstanweisung zusammenzufassen. Erfahrungsgemäß wird auf diese Weise sichergestellt, daß jedem Mitarbeiter die ihn betreffenden Anweisungen bekannt sind und daß keine Zweifel über die Verbindlichkeit von Dienstanweisungen entstehen können. Eine rechtliche Verpflichtung, vorhandene Dienstanweisungen zu einer zusammenzufassen, gibt es nicht.

Unvollständig sind Dienstanweisungen häufig bezüglich der Arbeitsgebiete, auf die sich die Regelungen erstrecken. Überraschend war es für mich allerdings, während eines Kontrollbesuchs festzustellen, daß es bei einem großen Rechenzentrum keine Dienstanweisung gab, in der die Arbeiten der Systembetreuung und Maschinenbedienung geregelt waren. Ich habe empfohlen, eine entsprechende Dienstanweisung zu erstellen.

Zu den Arbeitsgebieten, von denen ich bei Kontrollbesuchen feststellte, daß angemessene Regelungen fehlten, gehörte auch die individuelle Datenverarbeitung (IDV). Zur Begriffsbestimmung der IDV verweise ich auf meinen 10. Tätigkeitsbericht (S. 150/151). Gerade bei der IDV ist es besonders bedenklich, wenn diese Arbeitsform zugelassen wird, ohne daß vorab die erforderlichen Regelungen getroffen wurden.

Bei Einsatz von IDV besteht die Gefahr, daß Verantwortlichkeiten verwischt oder ignoriert werden. Diese Gefahr besteht insbesondere dann, wenn die Logik der Verarbeitung der Daten der öffentlichen Stelle verbindlich vorgeschrieben oder von ihr verbindlich zugesagt ist. Den aus einer solchen verbindlichen Verarbeitungslogik resultierenden Anforderungen kann eine öffentliche Stelle bei Einsatz von IDV im allgemeinen nur mit erheblichen Schwierigkeiten entsprechen.

Ein Kontrollbesuch ergab, daß jedenfalls in zwei Fällen automatisierte Datenverarbeitung in dieser Organisationsform durchgeführt wird.

- Durch die Geschäftsstelle des Gutachterausschusses wird ein Geschäftsbuch, das u. a. Kaufpreise enthält, auf einem der Server des Datennetzes geführt. Das Programm, mit dem diese Arbeit durchgeführt wird, hat sich die Geschäftsstelle des Gutachterausschusses selbst von einer Stelle außerhalb der kontrollierten Stelle beschafft. Der Abteilung ADV war weder das Programm noch diese Art der Arbeitsausführung bekannt.

  Eine Erörterung der Art des Einsatzes des Programms ergab, daß sich verschiedene Mitarbeiter der Geschäftsstelle dieses Programms und der mit diesem Programm geführten Datei bedienen. Dabei sind diese Mitarbeiter auf die ordnungsgemäße Funktion des Programms und den ordnungsgemäßen Aufbau der Datei angewiesen. Unter diesen Umständen ist es Aufgabe der Dienststelle zu gewährleisten, daß diesen Anforderungen ständig entsprochen wird, und es bestand Einigkeit darüber, daß hier eine Verarbeitung mit verbindlicher Verarbeitungslogik vorliegt.

- Das Bauordnungsamt verfügt über eine eigene Datenverarbeitungsanlage mit angeschlossenen Datenendgeräten. Auf dieser Datenverarbeitungsanlage werden verschiedene Programme für Aufgaben des Bauordnungsamts eingesetzt. Die Programme wurden im Auftrag des Amtsleiters durch eine Privatfirma entwickelt. Auch in diesem Fall liegt verbindliche Verarbeitungslogik vor.

Besonders bedenklich war die Feststellung, die ich bei diesem und auch bei einem anderen Kontrollbesuch machte, daß weder die Behördenleitung noch der ADV-Bereich, der nach dem Geschäftsverteilungsplan für die ADV insgesamt zuständig war, über diese Art der Arbeitsdurchführung unterrichtet war und daß die im Rahmen der IDV eingesetzten Programme nicht freigegeben worden waren. Ich habe daher jeweils empfohlen vorzuschreiben, daß derartige Programme nur eingesetzt werden dürfen, wenn ihre Quellprogramme in der aktuellen Fassung bei dem ADV-Bereich hinterlegt sind und dieser sich von der Ordnungsmäßigkeit der Programmfreigabe überzeugt hat. Auf verschiedene Hinweise zu dieser Frage in dem von mir herausgegebenen Sammelband Datensicherheit habe ich besonders hingewiesen (Stichwort: „Arbeitsvorbereitung"; Unterstichworte: „Überprüfung des Vorganges der Programmfreigabe" und „Zuständigkeit für freigegebene Programme").

6.1.2 Regelung von Zuständigkeiten

Durch eine unklare oder nicht sachgerechte Regelung von Zuständigkeiten kann die Datensicherheit erheblich beeinträchtigt werden. Daher stehen für mich Fragen der Aufbauorganisation bei Kontrollbesuchen im Zentrum des Interesses.

Während eines Kontrollbesuchs wurde meinen Mitarbeitern ein Vertrag zwischen den Kreisen Borken und Steinfurt zur Kenntnis gebracht. Die Kreise Borken und Steinfurt arbeiten auf dem Gebiet der automatisierten Datenverarbeitung nach Maßgabe der Regelungen dieses Vertrages zusammen. In

dem Vertrag ist u. a. geregelt, daß sich der Kreis Borken verpflichtet, die in einem Aufgaben- und Zeitplan einvernehmlich festgelegten Verfahren vom Kreis Steinfurt bearbeiten zu lassen. Nach Auskunft des Kreises Borken werden im Rahmen dieses Vertrages Programme auf den Gebieten Sozialwesen, Kfz-Zulassung, Ausländerwesen und Vermessungswesen vom Kreis Steinfurt zur Bearbeitung von Daten des Kreises Borken eingesetzt.

Soweit in einem solchen Programm die Bearbeitung von personenbezogenen Daten unter fachlichen Gesichtspunkten durchgeführt wird, liegt in der Anweisung, sich dieses Programms zu bedienen, eine fachliche Weisung an die eigenen Mitarbeiter. Die Logik des Programms ist fachlicher Inhalt der Weisung. Die Verpflichtung des Kreises Borken, die einvernehmlich festgelegten Verfahren vom Kreis Steinfurt bearbeiten zu lassen, sollte daher insoweit eingeschränkt sein, als bei einer Änderung der Logik der Verfahren der Kreis Borken über eine Möglichkeit der Einrede verfügen muß. Ich habe darauf hingewiesen, daß der Vertrag bereits jetzt in diesem Sinne ausgelegt werden und daß bei einer eventuellen Änderung oder Verlängerung des Vertrages eine entsprechende Klarstellung erfolgen solle.

Nach einer mir bei einem Kontrollbesuch vorgelegten Geschäftsanweisung für die automatisierte Datenverarbeitung ist die Abteilung ADV zuständig für

- die Aufgaben der ADV-Organisation im Bereich der herkömmlichen und der individuellen Datenverarbeitung,
- den hard- und softwaretechnischen Datenschutz,
- die Koordination der Zusammenarbeit mit Dritten,
- die Wartung, Pflege und Weiterentwicklung der eingesetzten Verfahren,
- die Beratung, Unterstützung und Schulung der Anwender.

Berichtet wurde mir dagegen, die Abteilung ADV habe nur eine partielle Zuständigkeit. So sei bezüglich des Vermessungs- und Katasteramts und des Bauordnungsamts von einer eingeschränkten Zuständigkeit auszugehen. Für Fragen der Datensicherheit bei bestimmten ADV-Anwendungen in diesen Ämtern werde nicht notwendig die Abteilung ADV eingeschaltet.

Ich habe empfohlen, die Zuständigkeit und die Grenzen der Zuständigkeit der Abteilung ADV unmißverständlich zu regeln. Im allgemeinen ist es vorteilhaft, wenn sich die Zuständigkeit eines ADV-Bereichs für Fragen der Datensicherheit auf alle Organisationseinheiten erstreckt.

Zur Vorbereitung eines Kontrollbesuchs waren mir die alte und die neue Fassung einer Dienstanweisung vorgelegt worden. Nach der alten Fassung lag die Zuständigkeit für das Eingeben von Zugriffsbefugnissen in das ADV-System bei einer Abteilung mit Verwaltungsaufgaben. In der neuen Dienstanweisung war diese Aufgabe der Abteilung zugeordnet worden, die für die Durchführung der automatisierten Datenverarbeitung zuständig ist.

Während des Kontrollbesuchs wurde erörtert, daß die Regelung in der alten Dienstanweisung sachgerechter war als die Regelung in der jetzt gültigen neuen Fassung, da die Zuständigkeit für die Eingabe von Berechtigungen unter dem Gesichtspunkt der Funktionstrennung nicht bei der mit der Durchführung der Datenverarbeitung betrauten Abteilung liegen sollte. Meinen Mitarbeitern wurde daraufhin berichtet, die Änderung der Zuständigkeit sei lediglich aus Gründen der Personalwirtschaft erfolgt. Ich habe empfohlen, die Zuständigkeit für die Eingabe von Berechtigungen wieder der Verwaltung zu übertragen, sobald eine entsprechende Möglichkeit gegeben ist.

6.1.3 Interne Kontrolle

Die institutionalisierte interne Kontrolle der Einhaltung aller Vorschriften ist für die Datensicherheit von besonderer Bedeutung. Gerade im kommunalen Bereich mußte ich in der Vergangenheit mehrfach feststellen, daß es im Hinblick auf die erforderlichen Fachkenntnisse der automatisierten Datenverarbeitung mit erheblichen Schwierigkeiten verbunden war, eine Person oder Stelle zu bestimmen, der die Zuständigkeit für die interne Kontrolle der Einhaltung von Dienstanweisungen zur Datensicherheit hätte übertragen werden können, ohne daß mit dieser Aufgabenübertragung die Gefahr einer Interessenkollision verbunden gewesen wäre. Hinweise auf Lösungsmöglichkeiten können dem von mir herausgegebenen Sammelband Datensicherheit und meinem 11. Tätigkeitsbericht jeweils unter dem Stichwort „Kontrolle" (Unterstichworte: „Institutionalisierung" und „interne") entnommen werden.

Falls der Weg gewählt wird, die interne Kontrolle dem eigenen Rechnungsprüfungsamt zu übertragen, sehe ich darin eine geeignete Lösung. Nach der Geschäftsanweisung einer kontrollierten Kreisverwaltung für die automatisierte Datenverarbeitung wird die Funktion der hausinternen Kontrolle durch den Leiter des Rechnungsprüfungsamtes wahrgenommen. Zu seinen Aufgaben gehören danach insbesondere die regelmäßigen und unvermuteten Kontrollen der Beachtung von Anweisungen für den Datenschutz und die verstärkte Kontrolltätigkeit in besonders sensiblen Bereichen. Die Zuordnung der Aufgabe der internen Kontrolle zum Rechnungsprüfungsamt wurde von mir begrüßt.

Während des Kontrollbesuchs wurde allerdings berichtet, daß Kontrollen im Rahmen dieser Aufgabe bisher nicht durchgeführt wurden. Die geringe Zahl der Mitarbeiter und deren fehlende Vorbildung auf dem Sektor der automatisierten Datenverarbeitung haben es bisher verhindert, diese Aufgabe wahrzunehmen. Berichtet wurde allerdings auch, es sei beabsichtigt, das Rechnungsprüfungsamt im Hinblick auf die Aufgabe der internen Kontrolle zu verstärken.

Ich habe empfohlen, die Voraussetzungen zu schaffen, damit die interne Kontrolle wahrgenommen werden kann und zu gewährleisten, daß die Kontrollen durchgeführt und deren Ergebnisse ausgewertet werden. Der Kreis teilte mir inzwischen mit, zwischenzeitlich sei das Rechnungsprüfungsamt

um einen besonderen ADV-Prüfer personell verstärkt worden. Es werde darüber hinaus festgelegt, daß die Kontrollen durchgeführt und deren Ergebnisse ausgewertet werden.

Falls ein Datenschutzbeauftragter bestellt ist, wird diesem im allgemeinen die Aufgabe der internen Kontrolle übertragen. In der gültigen Fassung der Dienstanweisung einer kommunalen Datenzentrale wird u. a. die Form der Einschaltung des Datenschutzbeauftragten im Rahmen der internen Kontrolle geregelt. In dem mir ebenfalls übersandten Entwurf einer Neufassung der Dienstanweisung wird dann allerdings der Datenschutzbeauftragte nicht mehr erwähnt. Während des Kontrollbesuchs wurde meinen Mitarbeitern berichtet, der Mitarbeiter, dem die Funktion des Datenschutzbeauftragten übertragen worden war, sei ausgeschieden. Ein neuer Datenschutzbeauftragter sei nicht bestellt worden.

Eine eingehende Erörterung ergab, daß auch bei dieser Stelle eine geeignete Möglichkeit, die interne Kontrolle der Einhaltung von Dienstanweisungen zum Datenschutz zu institutionalisieren, darin liegen könnte, diese Aufgabe dem Rechnungsprüfungsamt zuzuordnen. Einige Regelungen der Rechnungsprüfungsordnung konnten bereits als Grundlage dafür angesehen werden.

Die Datenzentrale berichtete allerdings, eine interne Kontrolle in dem hier angesprochenen Sinne werde dort nicht wahrgenommen. Auch das Rechnungsprüfungsamt nehme keine Kontrollen in diesem Sinne wahr. Ich habe empfohlen, eine interne Kontrolle zu Fragen der Datensicherheit zu institutionalisieren.

6.2 Entwicklung und Einsatz von Anwendungsverfahren

6.2.1 Der Fachbereich als Herr der Daten

Der Fachbereich ist verantwortlich für seine Daten und für die Programme, mit denen diese Daten verarbeitet werden. Aufbau- und Ablauforganisation müssen dieser Verantwortung entsprechen. In verschiedenen Kontrollbesuchen hatte ich Veranlassung, zur Abgrenzung der Zuständigkeiten von Fach- und ADV-Bereich und zu entsprechenden Dienstanweisungen Stellung zu nehmen.

- Freigabe von Anwendungsprogrammen

  Die Notwendigkeit der Programmfreigabe besteht bei allen Anwendungsprogrammen, in denen personenbezogene Daten verarbeitet werden, soweit es sich um Programme mit verbindlicher Verarbeitungslogik handelt, weil bei derartigen Programmen die öffentliche Stelle für die Einhaltung dieser Verarbeitungslogik verantwortlich ist. Zuständig für die Programmfreigabe ist jeweils der Fachbereich. Als Voraussetzung muß dieser ein Anwendungsprogramm vor dem ersten Einsatz und nach jeder fachlichen Änderung eingehend testen. Dieser Anwendertest muß unab-

hängig von den vorher durchgeführten Programmierertests erfolgen. Er ist schriftlich zu dokumentieren. Auf der Grundlage des Anwendertests entscheidet der Fachbereich über die Freigabe des Programms und übernimmt damit die Verantwortung für dessen fachlichen Inhalt.

Nach den Unterlagen, die ich zur Vorbereitung eines Kontrollbesuchs erhalten hatte, mußte ich davon ausgehen, daß für die Programmfreigabe einzelne Facharbeitskreise zuständig waren. Während des Kontrollbesuchs wurde meinen Mitarbeitern auf die Frage, welche Facharbeitskreise es gebe und wer die Vorsitzenden seien, allerdings berichtet, es gebe keine Facharbeitskreise mehr. Im weiteren Verlauf des Kontrollbesuchs wurde dann eine Unterlage vorgelegt, in der die Bildung von Facharbeitskreisen vorgesehen war. Eine erneute Rückfrage unter Hinweis auf diese Unterlage führte zu der Auskunft, es handele sich dabei um andere Facharbeitskreise. Facharbeitskreise mit der Aufgabe der Programmfreigabe gebe es heute nicht mehr. Auf weitere Nachfrage wurde erklärt, eine verbindliche Regelung der Programmfreigabe im Sinne des Datenschutzes existiere z. Z. nicht.

Auf meine Empfehlung werden jetzt Erforderlichkeit und Durchführung von Programmtest und Programmfreigabe bei Anwendungsprogrammen umfassend geregelt. Bezüglich des Inhalts angemessener Regelungen habe ich auf den von mir herausgegebenen Sammelband Datensicherheit hingewiesen, dem unter den entsprechenden Stichworten zahlreiche Ausführungen zu diesen Fragen entnommen werden können. Geregelt wird auch, unter welchen Voraussetzungen eine vorläufige Programmfreigabe - etwa durch die Leitung des ADV-Bereichs - zulässig ist.

- Gewährleisten, daß nur freigegebene Programme zum Einsatz kommen

  Während eines Kontrollbesuchs wurde erörtert, daß zur Gewährleistung einer hohen Sicherheit nur freigegebene Programme zum Einsatz kommen dürfen. Zu diesem Zweck soll festgelegt werden, daß eine Programmübergabestelle ein neues Programm oder eine Programmänderung nur dann in die Datei der freigegebenen Programme übernimmt, wenn die Formalien der Freigabe erfüllt sind.

- Parametergesteuerte Auswertungen

  Den Anwendern ist häufig nicht bewußt, daß parametergesteuerte Auswertungen den Charakter von Anwendungsprogrammen besitzen und daß die Parameterliste daher wie ein Anwendungsprogramm des Tests und der Freigabe bedarf. Eine mir vorgelegte Organisationsverfügung enthielt spezielle - sehr eingeschränkte - Regelungen bezüglich des Vorgehens zur Prüfung von DV-Produkten, deren Ergebnis durch die Eingabe von Parametern bestimmt wird. Während des folgenden Kontrollbesuchs wurde besprochen, daß die Datensicherheit verbessert wird, wenn derartige DV-Produkte wie sonstige Programme behandelt werden. Die Organisationsverfügung wird entsprechend geändert.

- Entscheidung über Zugriffsberechtigungen

  In einer mir vorgelegten Dienstanweisung war folgendes geregelt: „Für die Einrichtung von Zugriffsberechtigungen ist der Systemprogrammierer zuständig. Über deren Inhalt entscheidet der Leiter der ADV-Abteilung."

  Ich habe darauf hingewiesen, daß über den Inhalt von Zugriffsberechtigungen zu personenbezogenen Daten nicht durch die Leitung der ADV-Abteilung entschieden werden kann. Zuständig für eine derartige Entscheidung muß vielmehr der Anwenderbereich sein. Die Zuständigkeit könnte etwa dem Leiter des jeweiligen Fachamts übertragen werden.

6.2.2 Quellprogramme

Das Sichern der Quellprogramme ist von erheblicher Bedeutung für die Datensicherheit. Es sollte daher keinesfalls der Entscheidung im Einzelfall überlassen bleiben festzulegen, wie Quellprogramme gesichert werden.

In der Dienstanweisung einer kommunalen Datenzentrale ist folgendes geregelt: „Es ist festzulegen, wie die Quellen der Entwicklung ... regelmäßig gesichert werden." Während des Kontrollbesuchs berichtete die Datenzentrale, bezüglich des Sicherns der Quellprogramme werde wie folgt verfahren: Es gibt eine Datei der jeweils aktuellen Versionen der Quellprogramme. Verantwortlich für diese Datei ist die Arbeitsvorbereitung; nur für die Arbeitsvorbereitung besteht die Möglichkeit des schreibenden Zugriffs zu dieser Datei. Die Programmierer haben lediglich die Möglichkeit des lesenden Zugriffs.

Die Regelung in der Dienstanweisung soll allerdings nicht diese aktuellen Versionen der Quellprogramme, sondern lediglich die nicht mehr aktuellen Versionen betreffen. Für das Sichern der nicht mehr aktuellen Versionen ist bisher der Programmierer zuständig.

Es wurde erörtert, daß auch diese Zuständigkeit auf die Arbeitsvorbereitung übertragen werden sollte. Jede Änderung an einem Quellprogramm, die zu einer Änderung des entsprechenden Programms in der Datei der freigegebenen Programme führt, sollte nach Möglichkeit wenigstens fünf Jahre aufbewahrt werden. Diese Aufbewahrung dient nicht dem Zweck, Programme früherer Versionen zu einem späteren Zeitpunkt erneut zum Ablauf bringen zu können. Die Rekonstruierbarkeit früherer Programmstände soll vielmehr Kontrollmöglichkeiten schaffen, die es erlauben, Programmänderungen nachträglich nachzuweisen.

Mit diesen Anforderungen an die Sicherung der Quellprogramme wäre es aber unvereinbar, wenn Mitarbeiter, deren Aufgabe das Ändern der Programme ist und deren Arbeiten mit Hilfe der oben genannten Maßnahmen überwacht werden sollen, die Möglichkeit zur unbemerkten Änderung von Programmen in einer für ihre Überwachung vorgesehenen Datei haben. Die Datei, die der Rekonstruktion früherer Programmstände dient, darf daher nicht unbemerkt von Programmierern geändert werden können.

In der Geschäftsanweisung einer anderen kontrollierten Stelle ist folgendes geregelt: „Zur Rekonstruierbarkeit früherer Programmstände hat jeder Mitarbeiter die Pflicht, das Blatt 'Nachweis der Programmänderungen' in der Programmakte auszufüllen. Zu löschende Statements sind lediglich auszusternen. Alle veränderten Befehle sind an unschädlicher Stelle innerhalb der Programmliste mit Namenskürzel, Monat und Jahr der Änderung zu versehen." Während des Kontrollbesuchs wurde auch hier besprochen, daß es wünschenswert wäre, ein automatisiertes Verfahren einzusetzen, um das Ziel der Rekonstruierbarkeit früherer Programmstände zu erreichen.

Während des Kontrollbesuchs bei dieser Stelle wurde auch berichtet, daß für einzelne Arbeitsgebiete Fremdprogramme eingesetzt werden.

- Das Ordnungsamt setzt auf einer in diesem Amt stehenden Datenverarbeitungsanlage Programme ein, die im Auftrag des Amtes durch eine Privatfirma entwickelt wurden. Das Amt verfügt nicht über die Quellprogramme, die Eigentum der Privatfirma sind. Quellprogramme und Dokumentation sind nicht bei einer neutralen Stelle hinterlegt. Es gibt auch keine Regelung, daß unter gewissen Umständen Quellprogramme und Dokumentation herauszugeben sind und deren Änderung durch den Kunden zu gestatten ist.
- Auf der zentralen Datenverarbeitungsanlage werden Programme eingesetzt, die über eine Kommunale Anwendergemeinschaft bezogen werden. Auch diese Programme werden von einer Privatfirma entwickelt und gewartet. Die Quellprogramme sind aber bei einem Notar hinterlegt.

Mögliche Gefährdungen der Datensicherheit bei einem Einsatz von Fremdprogrammen und geeignete Maßnahmen, um diesen Gefährdungen zu begegnen, wurden während des Kontrollbesuchs eingehend erörtert. Jedenfalls sollte geregelt sein, daß die Quellprogramme und eine die Wartung ermöglichende Dokumentation von einer evtl. privaten Lieferfirma von Programmen zur Verfügung gestellt werden, wenn diese Lieferfirma ihre Wartungsverpflichtung für diese Programme kündigt oder dieser Verpflichtung aus anderen Gründen nicht nachkommt. Auf die Abhängigkeiten bei Einsatz von Fremdprogrammen, die bereits in meinem 6. Tätigkeitsbericht dargestellt wurden, habe ich ausdrücklich hingewiesen und angeregt, unter Berücksichtigung meiner Hinweise die bestehenden Verträge zu überprüfen.

6.2.3 Programmakten

Eine der Aufgaben von Programmakten ist es, einem sachverständigen Dritten einen zuverlässigen Einblick in Aufbau und Inhalt des Programms zu ermöglichen und die Verantwortlichkeiten bei der Entwicklung des Programms zu dokumentieren. Um dieser Anforderung gerecht zu werden, müssen die Programmakten hinreichend ausführlich sein. Hinweise dazu enthält der von mir herausgegebene Sammelband Datensicherheit unter dem Stichwort „Programmdokumentation".

In einer mir vorgelegten Dienstanweisung ist folgendes geregelt: „Für jedes Programm wird eine Programmakte geführt, die mindestens neben den Programmieraufträgen die letzte gültige Umwandlungsliste und alle Änderungsprotokolle dieses Programms enthält. Bei Programmen der Haushaltswirtschaft müssen die Programmakten darüber hinaus u. a. folgende Informationen enthalten: Datenflußplan, Programmablaufplan, Satzaufbau, Aufbewahrungsfristen, Testbeispiele, vorgesehene Kontrollen."

Soweit die Programmakte ein Programm zur Verarbeitung personenbezogener Daten betrifft, das nicht zum Bereich der Haushaltswirtschaft gehört, sind die hier formulierten Anforderungen an die Programmakte unzureichend. Es sollte vorgeschrieben werden, daß die für den Bereich der Haushaltswirtschaft als erforderlich angesehenen Angaben auch für alle Programme, in denen personenbezogene Daten verarbeitet werden, in die Programmakte aufzunehmen sind. Darüber hinaus ist es erforderlich, auch die Testate über Programmtests und Programmfreigabe (oben S. 138/139) in die Programmakte aufzunehmen. Ich habe empfohlen, entsprechende Regelungen über den Inhalt der Programmakten zu treffen.

Bezüglich der Aufbewahrung der Programmakten war vorgeschrieben: „Die Programmakte ist vom Anwendungsentwickler zu führen." Während des Kontrollbesuchs wurde erörtert, daß es unter Gesichtspunkten der Datensicherheit bedenklich ist, die Programmakten bei den Mitarbeitern und nicht zentral zu führen. Eine Programmakte soll einen unmanipulierbaren Einblick in die Logik des Programms, in seine Entstehungsgeschichte und die dabei getroffenen Entscheidungen geben. Die vollständige, übersichtlich geführte und aussagekräftige Programmakte gehört zu den Grundlagen für die Wartungssicherheit eines Programms.

Erfahrungsgemäß ist es nur sehr schwer möglich, diesen Anforderungen an eine Programmdokumentation zu entsprechen, solange diese dezentral bei den einzelnen Mitarbeitern geführt wird. Bei der Erörterung dieser Frage während des Kontrollbesuchs wurde allerdings von erheblichen räumlichen Schwierigkeiten berichtet, die einer kurzfristigen Zentralisierung der Führung von Programmakten entgegenstehen. Ich habe daher empfohlen, die Führung der Programmakten zu zentralisieren, sobald dazu die räumlichen Möglichkeiten bestehen.

6.2.4 Sichern des Zugriffs auf Schufa-Daten

Ein Bürger hat mir mitgeteilt, Daten, die über ihn bei der Schufa gespeichert waren, habe ein bei einer Sparkasse tätiger Werkstudent unberechtigt abgerufen. In einer von mir erbetenen schriftlichen Stellungnahme stimmte der Vorstand der Sparkasse der Darstellung des Bürgers zum Vorfall der unberechtigten Schufa-Abfrage im wesentlichen zu. Ergänzend berichtete die Sparkasse mündlich, ihr sei nicht bekannt, wie der Abruf durch den Werkstudent möglich gewesen sei. Sie äußerte allerdings die Vermutung, der Werkstudent habe die Möglichkeit des Zugriffs dadurch erhalten, daß er das

Datenendgerät eines Sachbearbeiters benutzen konnte, der den Raum verlassen hatte, ohne sich vorher ordnungsgemäß über sein Datenendgerät abzumelden. Der Sachbearbeiter habe damit gegen die geltende Dienstanweisung verstoßen.

Nach der Anlage zu § 9 Satz 1 BDSG ist die Sparkasse verpflichtet, die unbefugte Kenntnisnahme gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle; Nr. 3 der Anlage), zu verhindern, daß Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle; Nr. 4 der Anlage) sowie die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle; Nr. 10 der Anlage). Um die Wiederholung einer Möglichkeit für die Abfrage von Daten durch einen Mitarbeiter ohne Zugriffsberechtigung zu verhindern, muß die Sparkasse daher gewährleisten, daß sich die Mitarbeiter beim Verlassen ihrer Datenendgeräte ordnungsgemäß abmelden. Dazu habe ich insbesondere folgende Maßnahmen empfohlen:

- Die Mitarbeiter sollten erneut auf die Dienstanweisung und speziell auf die Notwendigkeit hingewiesen werden, sich beim Verlassen eines Datenendgeräts von diesem abzumelden, d. h., das Datenendgerät in einen Zustand zu versetzen, in dem eine eingegebene Berechtigung nicht mehr wirksam ist.

- Die Vorgesetzten sollten angehalten werden, die Einhaltung der Dienstanweisung und insbesondere dieser Regelung zu überwachen.

- Der Datenschutzbeauftragte und die Revision sollten angewiesen werden, entsprechende Kontrollen durchzuführen.

Eine von mir aus Anlaß dieses Vorfalls durchgeführte eingehende Überprüfung der organisatorischen und technischen Maßnahmen bei Schufa-Abfragen der Sparkasse führte zu erheblichen Bedenken bezüglich der Datensicherheit. Daher habe ich eine Reihe weiterer Empfehlungen ausgesprochen, die folgende Sicherungsziele betrafen:

- Es muß durch geeignete technische und organisatorische Maßnahmen gewährleistet werden, daß Schufa-Abfragen im Namen einer Organisationseinheit der Sparkasse nur von Datenendgeräten dieser Organisationseinheit gestellt werden können.

- Es muß gewährleistet werden, daß Zugriffe auf Schufa-Daten nur durch berechtigte Mitarbeiter erfolgen können.

  Es muß gewährleistet werden, daß Schufa-Abfragen nur in zulässigen Fällen erfolgen.

Die Sparkasse ist meinen Empfehlungen inzwischen gefolgt.

6.2.5 Papierlose Bearbeitung von Vorgängen

Eine Stadt bat um Beratung und wies darauf hin, daß der Begriff des papierlosen Büros immer mehr in den Vordergrund rücke. Aus dieser Entwicklung ergäben sich zahlreiche Fragestellungen bezüglich der Schriftform des Verwaltungshandelns. Das Prinzip der papiergebundenen Schriftlichkeit müsse mit dem Einzug der Informations- und Kommunikationstechniken grundsätzlich neu überdacht werden, weil hierbei der Informationsträger Papier vielfach nicht mehr benötigt werde.

Ein privates Unternehmen habe diesen Gedanken aufgegriffen und eine entsprechende Software entwickelt. Es bestehe großes Interesse an diesem Verfahren, da es insbesondere aus organisatorischer und technischer Sicht eine Reihe von Gestaltungsmöglichkeiten für sämtliche Verwaltungsbereiche biete. Einer umfassenden Klärung bedürften allerdings noch die rechtlichen Aspekte einer solchen Umstellung. Konkret wurde u. a. gefragt, wie der Begriff der Akte definiert sei und wie der datenschutzrechtliche Aspekt der Veränderbarkeit von elektronisch gespeicherten Daten zu beurteilen sei.

Zu dieser allgemeinen Anfrage gab ich einige grundsätzliche Hinweise:

- Es gibt sehr unterschiedliche Formen der papierlosen Speicherung von Daten. Als Beispiele kann man etwa das codierte Speichern von Unterlagen, die mit Verfahren der Textverarbeitung erstellt wurden, auf Magnetplatte oder Diskette nennen oder aber das Speichern der optischen Abbildung von Unterlagen auf Mikrofilm oder optischer Speicherplatte. Der Anfrage war nicht zu entnehmen, an welche dieser Techniken gedacht ist.

  Im allgemeinen ist allerdings bei Einsatz jeder dieser Techniken davon auszugehen, daß bei einer solchen Speicherung eine automatisierte Datei (§ 3 Abs. 4 Buchstabe a DSG NW; § 3 Abs. 2 Satz 1 Nr. 1 BDSG) entsteht. Dem Landesbeauftragten für den Datenschutz ist daher eine Beschreibung dieser Datei vorzulegen (§ 23 Abs. 1 Satz 1 DSG NW), und es sind technische und organisatorische Maßnahmen nach § 10 Abs. 1 und 2 DSG NW (bzw. § 9 und Anlage zu § 9 Satz 1 BDSG, soweit das Bundesdatenschutzgesetz anwendbar ist) zu treffen, um eine angemessene Datensicherheit zu gewährleisten. Dabei habe ich die Notwendigkeit einer hinreichenden Dokumentation, um eine Datenschutzkontrolle zu ermöglichen, ausdrücklich betont.

- Ob das Speichern in einer automatisierten Datei zulässig ist, muß für das jeweilige Anwendungsgebiet entschieden werden. Beschränkungen, wie sie etwa in § 102 f Abs. 1 Satz 1 LBG für Personalaktendaten enthalten sind, müssen dabei berücksichtigt werden.

- Bezüglich der Frage nach dem Begriff der Akte wies ich auf mögliche Unterschiede in einzelnen Gesetzen hin. So gehören - abweichend vom Begriff der Akte in § 3 Abs. 5 DSG NW - zur Personalakte (§ 102 Abs. 1 Satz 2 LBG) auch in Dateien gespeicherte Unterlagen.

- Auch bei papierloser Speicherung muß es möglich sein, dem Betroffenen Auskunft gemäß § 18 Abs. 1 Satz 1 DSG NW zu erteilen.
- Vor Einführung eines Verfahrens, das die papierlose Speicherung von Unterlagen vorsieht, sollte geprüft werden, ob das Verfahren auch ein Löschen von Unterlagen möglich macht. Soweit bei Einsatz eines solchen Verfahrens vorhersehbar ist, daß einer gesetzlichen Anforderung zum Löschen nicht entsprochen werden kann, muß eine Umstellung auf dieses Verfahren unterbleiben. Mit Schwierigkeiten beim Löschen kann insbesondere beim Speichern auf optischer Platte oder Mikrofilm gerechnet werden.
- Bei einem Verfahren, das die papierlose Verarbeitung von Vorgängen vorsieht, treten möglicherweise besondere Anforderungen an die Ordnungsmäßigkeit der Verarbeitung auf: Ohne Rückgriff auf die Originalunterlagen muß es möglich sein, die Authentizität von Dokumenten zu gewährleisten und die Verantwortung für deren Form und Inhalt in unmanipulierbarer Weise zuzuordnen.

6.2.6 Unsicherheit bei Selbstbedienungskontoauszugdruckern

Ein Bürger machte mich auf folgenden Fall aufmerksam:

Nach Ausdruck des Kontoauszugs mit Hilfe einer Euroscheckkarte bei einer Sparkasse an einem Samstag gab der Selbstbedienungskontoauszugdrucker die Karte nicht frei. Am darauffolgenden Montag gegen 8.30 Uhr bat der Betroffene einen Mitarbeiter der Sparkasse, die Karte aus dem Drucker zu holen. Es wurde festgestellt, daß die Karte nicht mehr vorhanden war. Nach Auskunft des Mitarbeiters der Sparkasse war es in der Zwischenzeit möglich gewesen, den Drucker durch geeignete Manipulation zu veranlassen, die Karte direkt freizugeben.

In der von mir erbetenen Stellungnahme teilte die Sparkasse mit, in ihrem Hause seien verschiedene Generationen von Selbstbedienungskontoauszugdruckern im Einsatz. Bei einem älteren Gerätetyp könne es zu dem geschilderten Fehler kommen, daß eine steckengebliebene Karte nach geeigneter Manipulation des Geräts wieder ausgegeben werde. Um diesen Fehler abzustellen, sei der Gerätehersteller beauftragt worden, die entsprechenden Geräte umzurüsten. Nach erfolgter Umrüstung könne der geschilderte Fehlerfall nicht mehr eintreten; steckengebliebene Karten würden dann vom Selbstbedienungskontoauszugdrucker sicher einbehalten. Die Umrüstaktion, von der mehrere Geräte betroffen seien, werde in Kürze abgeschlossen sein.

6.3 Telefax

Aus unterschiedlichen Gründen hat das Versenden von Unterlagen als Telefax in den letzten Jahren eine breite Akzeptanz gefunden. Das Telekom-Buch 93/94 nennt für Ende 1993 bereits 1,5 Millionen angeschlossene Geräte und berichtet von einer erwarteten Zunahme von etwa 20 000 Geräten pro

Monat. Sehr bedauerlich ist es daher, wenn nach meinen Feststellungen bei der Benutzung dieses Dienstes den Anforderungen an eine angemessene Datensicherheit allzu oft nicht entsprochen wird.

Zur Datensicherheit bei der Versendung eines Telefax habe ich mich bereits in meinem 10. Tätigkeitsbericht (S. 153 bis 155) und 11. Tätigkeitsbericht (S. 151) geäußert. Zwei Schwachstellen erscheinen mir besonders erwähnenswert:

- Bei Versendung eines Telefax merkt der anwählende Partner nicht von selbst, wenn die Verbindung zu einem anderen als dem gewünschten Telefaxgerät hergestellt wurde. Die Gefahr der Fehlleitung von Unterlagen steigt dadurch erheblich.
- Ein Telefax kann man mit einer offenen Postkarte vergleichen. Dennoch ist es nicht unüblich, selbst Unterlagen mit empfindlichem Inhalt als Telefax zu übertragen. Eine solche Übertragung empfindlicher Daten als Telefax ist aber nur vertretbar, wenn der Absender nicht nur weiß, daß die Verbindung zu dem richtigen Empfänger hergestellt wurde, sondern wenn ihm auch bekannt ist, daß das Telefaxgerät des Empfängers unter räumlichen und organisatorischen Bedingungen aufgestellt ist, die eine angemessene Datensicherheit gewährleisten.

Die mögliche Unsicherheit am Aufstellungsort des Empfängers betraf das Beratungsersuchen einer Stadt. Gefragt wurde ich, ob man immer dann, wenn eine öffentliche Stelle ihre Telefaxnummer offiziell mitteile, eine angemessen sichere Aufstellung des Telefaxgeräts unterstellen dürfe. Ich habe diese Frage verneint.

Obwohl der Telefaxdienst der Deutschen Bundespost TELEKOM in den letzten Jahren bereits eine weite Verbreitung gefunden hat, befindet sich seine Einführung noch in einem Übergangsstadium. In dieser Situation ergeben sich für den Empfänger und den Absender eines Telefax besondere Sorgfaltspflichten. Der Absender kann sich noch nicht darauf verlassen, daß der Empfänger diesen Sorgfaltspflichten bereits genügt.

Eine öffentliche Stelle, die Dritten ihre Telefaxnummer - etwa durch Angabe auf dem Briefbogen - bekannt gibt, hat zwar durch geeignete technische und organisatorische Maßnahmen dafür Sorge zu tragen, daß das entsprechende Telefaxgerät sicher aufgestellt und vor dem Zugriff Unbefugter geschützt ist. Sie hat auch sicherzustellen, daß jedes eingehende Telefax behandelt wird wie sonstige geöffnete Post, die noch nicht ausgezeichnet und zugeleitet wurde.

Dennoch kann - wie die Erfahrung leider zeigt - der Absender eines Telefax wegen des oben erwähnten Übergangsstadiums nicht davon ausgehen, daß der Empfänger tatsächlich für die den Anforderungen des Datenschutzes entsprechenden räumlichen und organisatorischen Gegebenheiten gesorgt hat. Er muß sich daher vor Absendung eines Telefax vergewissern, ob bei dem Empfänger eine angemessene Sicherheit gewährleistet ist.

Ein Bürger sandte mir das Telefax einer Staatsanwaltschaft, das er an seinem Telefaxanschluß empfangen hatte. Dieses Telefax enthielt personenbezogene Daten und war für das Sozialamt einer Stadt als Empfänger bestimmt.

Bei der Aufklärung dieses Vorfalls konnte zwar festgestellt werden, daß eine Ziffer der Telefaxnummer falsch gewählt worden war. Leider gab es aber weder ein Telefax-Vorblatt, auf dem die anzuwählende Nummer vermerkt gewesen wäre, noch stand diese Nummer auf dem Schreiben selbst. Es war davon auszugehen, daß der Fehler durch diesen Mangel in der Organisation des Ablaufs mit verursacht worden war. Um Fehler dieser Art nach Möglichkeit auszuschließen, ist es heute allgemein üblich, bei einer Unterlage die als Telefax versandt wird, die Telefaxnummer auf einem Vorblatt oder auf der Unterlage selbst schriftlich zu vermerken.

Ich habe der Staatsanwaltschaft daher empfohlen, die Anweisung zu erteilen, daß bei der Übertragung einer Unterlage als Telefax die anzuwählende Telefaxnummer auf einem Vorblatt oder auf der Unterlage schriftlich zu vermerken und damit in die Akte zu übernehmen ist und daß nach erfolgter Anwahl ein Vergleich mit der auf dem Telefaxgerät angezeigten Nummer zu erfolgen hat. Durch eine solche Anweisung würde die Datensicherheit erheblich verbessert. Der mit der Einhaltung der Anweisung verbundene Aufwand wäre minimal und steht daher jedenfalls in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck. Die Maßnahme ist damit nach § 10 Abs. 1 Satz 2 DSG NW erforderlich.

Keinesfalls sollte man wegen der Eigenarten des Telefax-Dienstes die damit verbundenen Beeinträchtigungen der Datensicherheit als unabänderlich hinnehmen. Ich gehe vielmehr davon aus, daß es möglich ist, die Datensicherheit des Telefax-Verkehrs durch angemessene Maßnahmen deutlich zu verbessern.

Nicht anschließen möchte ich mich daher der eher resignativen Einstellung, die in der Stellungnahme der Landesregierung zu meinem 11. Tätigkeitsbericht (Drucksache 11/6876, S. 96) zum Ausdruck kommt, wenn zu den Anforderungen beim Absenden eines Telefax bemerkt wird: „So erscheint es z. B. praktisch nicht realisierbar, als Absender immer zu beurteilen, ob beim Empfänger die nötige Datensicherheit gewährleistet ist. Hinzuzufügen ist, daß durch organisatorisch-technische Maßnahmen grundsätzlich weder menschliche Bedienfehler ausgeschlossen noch Schwächen im Telefax-Protokoll behoben werden können."

Sicher ist es niemals möglich, Fehler völlig auszuschließen. Möglich ist es aber durchaus, durch angemessene Maßnahmen die Wahrscheinlichkeit für das Auftreten von Fehlern erheblich zu reduzieren. Einige Maßnahmen, die der Verbesserung der Datensicherheit bei der Übertragung von Unterlagen als Telefax dienen können, sind im folgenden zusammengestellt:

1. Allgemeine Maßnahmen

   a) Die Abwicklung des Telefax-Verkehrs sollte durch Dienstanweisung geregelt werden.

   b) Es muß festgelegt werden, welche Stelle oder welche Person für das Überwachen der Einhaltung der Regelungen im Zusammenhang mit dem Telefax-Verkehr zuständig ist.

   c) Jedes Telefaxgerät muß so aufgestellt sein, daß eine der Empfindlichkeit der zu erwartenden ankommenden und abgehenden Nachrichten angemessene Datensicherheit gewährleistet ist.

   d) Es sollte vorgeschrieben sein, daß jeder Raum, in dem ein Telefaxgerät aufgestellt ist, zu verschließen ist, sobald kein zuständiger Mitarbeiter mehr anwesend ist.

   e) Es sollten nur Telefaxgeräte eingesetzt werden, die bei einem Anruf eine Empfängerkennung abgeben.

   f) Bei einem Telefaxgerät mit Speicherfähigkeit ist zu gewährleisten, daß vor dessen Weitergabe an Dritte (z. B. bei Wartung, Verkauf, Entsorgung) sämtliche in dem Gerät gespeicherten Daten gelöscht werden.

   g) Bei Einsatz von Fax-Servern ist zu gewährleisten, daß kein unbefugter Zugriff aus dem Netz auf die empfangenen oder zu versendenden Nachrichten erfolgen kann.

2. Maßnahmen zum Verbessern der Datensicherheit beim Absenden von Nachrichten

   a) Es sollte festgelegt werden, für Nachrichten welcher Art die Übertragung als Telefax zulässig ist. Für Nachrichten mit empfindlichem Inhalt sollten besondere Sicherheitsmaßnahmen vorgeschrieben werden.

   b) Es sollte die Verwendung eines Vorblatts vorgeschrieben werden, das neben Empfänger und Absender auch die Telefaxnummer des Empfängers enthält.

   c) Es sollte festgelegt werden, daß der/die für die Absendung verantwortliche Mitarbeiter/Mitarbeiterin persönlich dafür verantwortlich ist zu klären, daß

      - die Telefaxnummer auf dem Vorblatt zutreffend ist und

      - beim Empfänger Maßnahmen getroffen sind, die der Empfindlichkeit der zu übertragenden Nachricht angemessen sind.

   d) Für das Versenden eines Telefax mit empfindlichem Inhalt könnten insbesondere die folgenden zusätzlichen Maßnahmen vorgeschrieben werden:

- Der/die für das Absenden verantwortliche Mitarbeiter/Mitarbeiterin nimmt das Absenden persönlich vor.

- Der/die zuständige Mitarbeiter/Mitarbeiterin des Empfängers wird telefonisch veranlaßt, das Telefax an dem dortigen Gerät persönlich in Empfang zu nehmen.

- Die Versendung des Telefax kann im manuellen Betrieb erfolgen. Dabei wird zunächst eine normale Fernsprechverbindung zwischen den Telefax-Anschlüssen aufgebaut, und die Übertragung des Telefax wird erst eingeleitet, wenn der Absender im Gespräch mit seinem Partner an dem angewählten Telefax-Anschluß des Empfängers festgestellt hat, daß er mit der gewünschten Stelle verbunden ist. Damit kann die sonst mögliche Fehlleitung des Telefax vermieden werden.

e) Vor Beginn der Übertragung der Nachricht sollte die von dem angewählten Gerät zurückgesandte Gerätekennung mit der Telefaxnummer auf dem Vorblatt verglichen werden. Bei einer Abweichung ist die Übertragung sofort abzubrechen.

f) Bei automatisiertem Versenden - etwa aus einem Server - hat der Abgleich der zurückgesandten Gerätekennung mit der angewählten Telefaxnummer automatisiert zu erfolgen.

g) Über die Absendung des Telefax ist ein maschinelles Protokoll zu erstellen.

- Die zurückgesandte Gerätekennung auf dem Protokoll ist mit der Telefaxnummer auf dem Vorblatt zu vergleichen. Es kann festgelegt werden, daß für diesen Vergleich der/die für das Absenden verantwortliche Mitarbeiter/Mitarbeiterin zuständig ist.

- Vorblatt und Protokoll sind mit dem Original der übertragenen Nachricht zu den Akten zu nehmen.

h) Falls nach Absendung der Nachricht oder eines Teils der Nachricht eine Fehlleitung festgestellt wird, ist der/die für die Nachricht verantwortliche Mitarbeiter/Mitarbeiterin unverzüglich zu unterrichten, der/die dann angemessene Maßnahmen zur Schadensbegrenzung zu veranlassen hat.

3. Maßnahmen zum Verbessern der Datensicherheit beim Empfang von Nachrichten

a) Es müssen Regelungen getroffen werden, die gewährleisten, daß ein Telefax behandelt wird wie sonstige eingehende Post, die geöffnet aber noch nicht für den Empfänger ausgezeichnet ist. Insbesondere dürfen Unbefugte keine Möglichkeit zur Kenntnisnahme des Inhalts eingehender Telefaxe erhalten. Falls für den Telefax-Anschluß eine Anruf-

umleitung möglich ist, muß gewährleistet sein, daß diesen Anforderungen auch bei der Anrufumleitung entsprochen wird.

b) Spezielle Maßnahmen sind bei Telefaxgeräten erforderlich, die ein Druckverfahren verwenden, bei dem auf einer Trägerfolie ein lesbares Abbild des gedruckten Telefax zurückbleibt. Eine solche Trägerfolie ist zu sichern wie ein permanenter Datenspeicher. Vor der Weitergabe des Telefaxgerätes (z. B. bei Wartung, Verkauf, Entsorgung) ist die Trägerfolie zu entnehmen. Verbrauchte Trägerfolien sind so zu vernichten, daß die darauf gespeicherten Daten als gelöscht gelten können.

c) Bei Änderung der Telefaxnummer sind Maßnahmen zu treffen, um nach Möglichkeit zu verhindern, daß bei einer Neuvergabe der bisherigen Telefaxnummer Telefaxe irrtümlich weiterhin an die bisherige Nummer gelangen und - falls unter der bisherigen Nummer nach der Neuvergabe wieder ein Telefaxgerät angeschlossen wurde - dort angenommen werden. Der Absender würde in einem solchen Fall annehmen, sein Telefax sei ordnungsgemäß bei dem vorgesehenen Empfänger angekommen.

6.4 Einzelfragen der Datensicherheit

6.4.1 Verwendungsbeschränkung von Aufzeichnungen zur Datenschutzkontrolle

Zu den Unterlagen, die im Rahmen von Kontrollbesuchen eingesehen wurden, gehörten auch Dienstvereinbarungen zwischen der öffentlichen Stelle und dem Personalrat. Diese Dienstvereinbarungen enthielten u. a. Regelungen, die das Recht des Personalrats oder der öffentlichen Stelle betrafen, Systemaufzeichnungen anzufertigen und deren Verarbeitungsergebnisse zur Kenntnis zu erhalten.

So enthielt ein Abschnitt über Leistungserfassung und Leistungskontrolle einer mir vorgelegten „Dienstvereinbarung über Arbeitsplatzsicherung und Arbeitsbedingungen bei Anwendung und Ausbau der TUIV" Regelungen, die eine Verwendungsbeschränkung von Daten vorsehen, die mit Hilfe der technikunterstützten Informationsverarbeitung gewonnen wurden. In dieser Dienstvereinbarung wurde aber auch ein Recht der Dienststelle vereinbart, unter gewissen Umständen mit Hilfe der TUIV eine Aufklärung eines Sachverhalts durchzuführen.

In einer anderen „Dienstvereinbarung über den Ausbau und die Anwendung der Informations- und Kommunikationstechnik" wurde geregelt: „Es wird automatisch ein lückenloses Protokoll aller Auswertungsläufe, Datenübermittlungen und Datenzugriffe (einschließlich der Versuche) erstellt. In begründeten Einzelfällen kann der Personalrat das Protokoll einsehen."

Bei derartigen Protokollen handelt es sich um Daten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach

§ 10 Abs. 2 DSG NW gespeichert werden. Das Datenschutzgesetz Nordrhein-Westfalen enthält mehrere Vorschriften, die gewährleisten, daß derartige Daten, 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 Buchstabe d DSG NW vor, daß personenbezogene Daten zu sperren sind, wenn sie nur zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind.

Die Möglichkeit der Verwendung der gespeicherten Protokolle 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.

Auf diese Regelungen des Datenschutzgesetzes Nordrhein-Westfalen und insbesondere darauf, daß die Dienstvereinbarungen nur im Rahmen dieser Regelungen angewandt werden dürfen, habe ich jeweils hingewiesen. Für den Fall einer Überarbeitung der Dienstvereinbarungen regte ich an, einen entsprechenden Hinweis in die Dienstvereinbarungen aufzunehmen.

6.4.2 Zulässigkeit von frei verfügbaren Datenfeldern

Für jede automatisierte Datei ist in einer Dateibeschreibung u. a. die Art der gespeicherten Daten schriftlich festzulegen (§ 8 Abs. 1 Nr. 2 DSG NW). Die Angaben der Dateibeschreibung sind dem Landesbeauftragten für den Datenschutz vorzulegen (§ 23 Abs. 1 Satz 1 DSG NW). Diese Vorschriften sollen gewährleisten, daß ein ständig aktueller Überblick über die Arten der von den öffentlichen Stellen gespeicherten Daten besteht.

Mit diesem Ziel ist es nur schwer verträglich, wenn in Dateien frei verfügbare Datenfelder vorgesehen sind. Eine Anfrage gab mir Veranlassung, zur Zulässigkeit derartiger frei verfügbarer Datenfelder Stellung zu nehmen.

Frei verfügbare Datenfelder können aus unterschiedlichen Gründen in Dateien vorgesehen sein. Soweit sie lediglich aus programmtechnischen Gründen vorgesehen sind und von dem Anwender ohne vorherige Programmänderung nicht genutzt werden können, bestehen unter dem Gesichtspunkt des Datenschutzes keine Bedenken. Frei verfügbar sind derartige Datenfelder nur für den Programmierer. Für den Anwender wären die Datenfelder erst nach einer Programmänderung existent.

Für alle Datenfelder, die der Anwender nutzen kann, ist in der Dateibeschreibung u. a. die Art der gespeicherten Daten anzugeben. Die Angaben in der Dateibeschreibung müssen so konkret sein, daß der Datenschutzbeauftragte

oder der Bürger daraus ein zutreffendes Bild über die Art der gespeicherten Daten gewinnen kann. Die Inhalte aller Datenfelder einer Datei müssen durch die in der Dateibeschreibung genannten Arten der gespeicherten Daten abgedeckt sein.

Bei frei verfügbaren Datenfeldern, die der Anwender nutzen kann, muß daher jedenfalls deren zulässiger Inhalt festgelegt oder deren Nutzung untersagt werden. Falls der festgelegte Inhalt von frei verfügbaren Feldern von den in der Dateibeschreibung genannten Arten der gespeicherten Daten nicht erfaßt wird, ist insoweit eine Ergänzung der Dateibeschreibung erforderlich.

Bei frei verfügbaren Datenfeldern, die nicht vom Anwender genutzt werden dürfen, ist es im allgemeinen angemessen, dem Anwender durch eine Modifikation des Programms die Nutzung dieser Datenfelder unmöglich zu machen.

6.4.3 Verschlüsselung als Sicherheitsmaßnahme

In Nr. 11.2 (Verschlüsselung) der Datenübermittlungsgrundsätze NW (RdErl. des Innenministeriums vom 6.3.1991 - V B 2/51-02.05) wird in Satz 1 ausgeführt, daß Verfahren zur Datenverschlüsselung dem zusätzlichen Schutz der Daten bei der Übermittlung auf Übertragungswegen oder mit Hilfe von Datenträgern sowie bei der Datenspeicherung dienen. In Satz 2 wird dann allerdings vorgeschrieben, daß der im Einzelfall notwendige Einsatz der Verschlüsselung vom Anwender unter Anlegung eines strengen Maßstabs zu begründen ist. Die Datenübermittlungsgrundsätze NW stimmen insoweit mit der KBSt-Empfehlung Nr. 5/90 vom 10. Oktober 1990 des Bundesinnenministeriums überein, der der Kooperationsausschuß ADV Bund/Länder/Kommunaler Bereich zugestimmt hat.

Auf eine Anfrage des Innenministeriums des Landes Nordrhein-Westfalen im Zusammenhang mit der geplanten Überarbeitung der Datenübermittlungsgrundsätze habe ich darauf hingewiesen, daß der Einsatz wirkungsvoller Verschlüsselungsverfahren aus meiner Sicht eine geeignete und zukunftsorientierte Maßnahme ist, um die Datensicherheit zu erhöhen, und daher gefördert und nicht erschwert werden sollte. Ich würde es bedauern, wenn die Einführung derartiger Verfahren unter Bezugnahme auf Satz 2 der Datenübermittlungsgrundsätze verzögert oder wenn aus Satz 2 abgeleitet würde, Verschlüsselungsverfahren sollten möglichst nicht eingesetzt werden. Daher regte ich an, Satz 2 durch eine Formulierung, die diese Einstellung zum Ausdruck bringt, zu ersetzen.

Bei dieser Gelegenheit wies ich auch darauf hin, daß die Datenübermittlungsgrundsätze durch ihren Regelungsgehalt die Weitergabe personenbezogener Daten innerhalb einer öffentlichen Stelle mit einbeziehen. Dies wird wegen der Verwendung des Begriffs „Übermittlung", der nach der Begriffsbestimmung in § 3 Abs. 2 Nr. 4 DSG NW das Bekanntgeben von Daten an einen Dritten bedeutet, nicht hinreichend deutlich.

Ich regte daher an, im Rahmen der Überarbeitung eine begriffliche Klarstellung vorzunehmen. In diesem Zusammenhang wies ich darauf hin, daß in der Regelung zur Transportkontrolle in Nr. 9 der Anlage zu § 6 Abs. 1 Satz 1 DSG NW a. F. auch der Begriff „Übermittlung" verwandt wurde, während in der entsprechenden Regelung in § 10 Abs. 2 Nr. 9 DSG NW n. F. der Begriff „Übertragung" gewählt wird. Naheliegend wäre daher die Bezeichnung „Datenübertragungsgrundsätze"; entsprechende Korrekturen sollten dann auch innerhalb des Textes vorgenommen werden.

6.4.4 Datennetze

Innerhalb der Verwaltung eines kontrollierten Kreises besteht ein lokales Netz (LAN), an das eine größere Zahl von Arbeitsplatzrechnern angeschlossen ist. Auf diesem LAN wird zur Datenübertragung die Technik des Token-Rings eingesetzt. Die angeschlossenen Arbeitsplatzrechner gehören zu unterschiedlichen Ämtern des Kreises. Auf den Arbeitsplatzrechnern und Servern werden auch personenbezogene Daten verarbeitet.

Die Technik des Token-Rings bedingt es, daß eine Nachricht, die eines der angeschlossenen Geräte absendet und die an ein anderes der angeschlossenen Geräte adressiert ist, einer großen Zahl weiterer Geräte angeboten wird. Auf die dadurch bedingte Gefährdung der Datensicherheit habe ich bereits in meinem 10. Tätigkeitsbericht (S. 148 bis 150) und 11. Tätigkeitsbericht (S. 133 bis 135) hingewiesen.

Während des Kontrollbesuchs wurden verschiedene Maßnahmen erörtert, die geeignet sind, dieser Gefährdung der Datensicherheit zu begegnen. Der Kreis berichtete von Überlegungen, das einheitliche LAN in mehrere getrennte LANs aufzuteilen. Diese Aufteilung in getrennte LANs könnte nach Ämtern oder Arbeitsgebieten erfolgen. Bei geeigneter technischer Ausgestaltung wäre es damit möglich zu gewährleisten, daß die Nachrichten bei ihrer Übertragung nur einem erheblich eingeschränkten Kreis von Endgeräten angeboten werden. Günstig wäre es, wenn die Aufteilung so erfolgen könnte, daß jeweils alle Mitarbeiter, die an eines dieser LANs angeschlossen sind, gleiche Zugriffsbefugnisse hätten. In diesem Fall könnte im allgemeinen eine angemessene Datensicherheit gewährleistet werden.

Eine andere Möglichkeit, die Datensicherheit zu gewährleisten, könnte darin bestehen, die Daten vor der Übertragung zu verschlüsseln. Falls hinreichend sichere Verfahren für die Verschlüsselung und den Schlüsselaustausch eingesetzt werden, kann davon ausgegangen werden, daß auch bei der Datenübertragung über den Token-Ring die Datensicherheit gewährleistet ist.

Der Kreis sollte darüber hinaus prüfen, in welchem Umfang die Amtsleiter, in deren Bereich Datenendgeräte an den Token-Ring angeschlossen sind, über die bestehende Gefährdung der Datensicherheit informiert sein müssen.

In der Dienstanweisung einer kommunalen Datenzentrale ist festgelegt, daß diese Dienstanweisung keine Geltung für das Schulungssystem hat. Unter „Schulungssystem" wird hier die Summe der für Schulungszwecke eingesetzten Geräte verstanden. Nach Auskunft der Datenzentrale wurde diese Regelung getroffen, weil für das Schulungssystem keine Dienstanweisung gelten soll. Die Benutzung des Schulungssystems soll keinerlei Beschränkungen unterliegen.

Während des Kontrollbesuchs wurde erörtert, daß eine solche unbeschränkte Freiheit in der Benutzung des Schulungssystems mit den Anforderungen an die Datensicherheit nur vereinbar ist, falls das Schulungssystem physikalisch von der gesamten übrigen Datenverarbeitung getrennt ist. Nach der derzeitigen Konzeption besteht das Schulungssystem aber aus einer Datenverarbeitungsanlage, die an den allgemeinen Token-Ring der Datenzentrale angeschlossen ist, und aus den für die Schulung vorgesehenen Datenendgeräten, die ebenfalls direkt an diesen allgemeinen Token-Ring angeschlossen sind. Bei einem solchen Netzkonzept muß die Datensicherheit als erheblich beeinträchtigt angesehen werden, solange Benutzer, die ein Datenendgerät zur Benutzung des Schulungssystems verwenden, in ihrer Arbeit keinerlei einschränkenden Anweisungen unterliegen.

Da die Datenzentrale Schwierigkeiten sah, die Einhaltung einer Dienstanweisung bei den Benutzern des Schulungssystems durchzusetzen, wurde besprochen, daß es zum Gewährleisten der Datensicherheit erforderlich ist, für das Schulungssystem mit den an dieses angeschlossenen Datenendgeräten einen eigenen Token-Ring vorzusehen, der von dem allgemeinen Token-Ring für die übrigen Arbeiten der Datenzentrale physikalisch getrennt ist. Ein derartiges Konzept würde eine auch für die Datenzentrale praktikable Lösung darstellen. Allerdings wies die Datenzentrale darauf hin, daß es Sonderfälle gebe, die es notwendig machen, den Token-Ring des Schulungssystems mit dem allgemeinen Token-Ring zu verbinden. Die Datenzentrale sagte aber zu, daß in den sehr seltenen Fällen, in denen eine derartige Verbindung hergestellt werden muß, angemessene Sicherheitsmaßnahmen getroffen werden.

Zum Einsparen von Leitungskosten enthält das externe Datennetz dieser Datenzentrale noch eine größere Zahl von Schnittstellenvervielfachern des Typs SK 12 der Deutschen Bundespost TELEKOM. Auf die Gefährdung der Datensicherheit bei Einsatz dieses Schnittstellenvervielfachers habe ich bereits in meinem 7. Tätigkeitsbericht (S. 159 bis 162) hingewiesen.

Eine Darstellung der derzeitigen Möglichkeiten, den Schnittstellenvervielfacher durch Geräte zu ersetzen, die einen sicheren Netzbetrieb ermöglichen, enthält mein 11. Tätigkeitsbericht (S. 132/133). Es ist jetzt ein X.25-Knoten auf dem Markt erhältlich, der es gestattet, ein Netz ohne Verwendung des SK 12 zu konzipieren, bei dem die vom SK 12 bekannten Einschränkungen der Datensicherheit nicht mehr gegeben sind. Einzelheiten zu dieser Frage wurden während des Kontrollbesuchs erörtert.

Die Datenzentrale berichtete, es bestehe mit der TELEKOM ein langfristiger Vertrag. Besprochen wurde während des Kontrollbesuchs, daß die Datenzentrale ihr Netzkonzept überprüfen wird mit dem Ziel, baldmöglichst eine Lösung zu finden und zu realisieren, bei der die Nachteile des SK 12 nicht mehr bestehen.

6.4.5 Sicherheit von Daten auf einem Server

Es entspricht der modernen Verarbeitungstechnik, für zentrale Aufgaben spezielle Geräte, die Server, zur Verfügung zu stellen. An den Token-Ring einer kontrollierten Kreisverwaltung sind mehrere Server angeschlossen. In diesen Servern werden u. a. Daten gespeichert, die in die an das Netz angeschlossenen Arbeitsplatzrechner eingegeben wurden. Gespeichert sind in den Servern z. B. das Geschäftsbuch der Geschäftsstelle des Gutachterausschusses und auch Briefe, die im Personalamt geschrieben wurden.

Zugriff zu den auf einem der Server gespeicherten Daten ist grundsätzlich von jedem Datenendgerät, das an den Token-Ring angeschlossen ist, möglich. Der Benutzer meldet sich mit seiner Benutzerkennung an. An diese Benutzerkennung ist die dem Server bekannte Berechtigung des Benutzers gebunden. Nach der Anmeldung mit der Benutzerkennung authentifiziert sich der Benutzer mit einem Paßwort.

Bei Einsatz eines Paßwortschutzes ist es notwendig, eine Reihe ergänzender Maßnahmen zu treffen, die sicherstellen sollen, daß eine hinreichende Datensicherheit gewährleistet ist. Die Paßworte für den Zugriff auf den Server haben bei der Kreisverwaltung eine Länge von sechs bis acht Stellen, wobei wahlweise Ziffern oder Buchstaben eingesetzt werden können. Die Mitarbeiter vergeben sich die Paßworte selbst. Die Paßworte sind monatlich zu ändern. Ein Abschalten nach mehreren Versuchen der Authentifizierung mit einem falschen Paßwort ist nicht vorgesehen. Es können daher beliebig viele Versuche unternommen werden. Die Fehlversuche werden lediglich registriert.

Bei dem hier eingesetzten Verfahren ist die Zugriffssicherheit erheblich beeinträchtigt. Bedingt durch die Technik des Token-Rings kann die Anfrage an einen Server von jedem der angeschlossenen Arbeitsplatzrechner vorgenommen werden. Es ist daher nicht gewährleistet, daß Zugriffe zu einem Datenbestand nur von einem Arbeitsplatzrechner aus erfolgen können, der bei einer Organisationseinheit aufgestellt ist, deren Angehörige für diesen Datenbestand zugriffsberechtigt sind.

In dieser Situation gewinnt die Sicherheit des Paßwortschutzes eine besondere Bedeutung. Dessen Sicherheit ist aber dadurch erheblich beeinträchtigt, daß beliebig viele Fehlversuche unternommen werden können, ohne daß die betreffende Benutzerkennung abgeschaltet wird. Darüber hinaus sind Zweifel angebracht, ob die Paßworte, die sich die Benutzer selbst vergeben, den an die Datensicherheit zu stellenden Anforderungen gerecht werden. In diesem Zusammenhang habe ich den Kreis auf verschiedene Feststellungen

in dem Sammelband Datensicherheit (Stichwort: „Paßwortschutz"; Unterstichwort: „negative Beispiele") verwiesen. Insbesondere verwies ich auf die Ausführungen in meinem 6. Tätigkeitsbericht (S. 174 bis 177).

Ich habe dem Kreis empfohlen, Maßnahmen zu treffen, um die Zugriffssicherheit bei Zugriff auf den Server zu verbessern. Jedenfalls sollte sichergestellt werden, daß eine Benutzerkennung nach einigen - etwa drei - Fehlversuchen abgeschaltet wird und nur durch Eingreifen einer zentralen Stelle - etwa einer Stelle in der ADV-Abteilung - wieder aktiviert werden kann. Geprüft werden sollte auch der Einsatz von Chipkarten zur Verbesserung der Datensicherheit. Ausführungen dazu enthalten mein 11. Tätigkeitsbericht (S. 146/147) und der Sammelband Datensicherheit (Stichwort: „Chipkarte").

Einer der Server des Kreises wird im Rahmen der Textverarbeitung eingesetzt. Dokumente, die in eines der an den Token-Ring angeschlossenen und für die Textverarbeitung eingesetzten Datenendgeräte eingegeben werden, können auf dem Server gespeichert werden.

Während des Kontrollbesuchs wurde die Frage erörtert, wann und durch welchen Vorgang gespeicherte Dokumente gelöscht werden. Der Kreis berichtete, die Festplatte dieses Servers werde täglich reorganisiert und spätestens bei dieser Reorganisation würden Dokumente gelöscht, soweit sie vorher von den Schreibkräften aufgegeben worden seien. Eingehende Erörterungen und ergänzend eingeholte Auskünfte führten jedoch zu erheblichen Zweifeln an dieser Aussage. Es bestand schließlich Einvernehmen darüber, daß davon auszugehen sei, die Reorganisation bewirke nicht notwendig ein vollständiges Löschen der aufgegebenen Dokumente.

Der Kreis hat daher bereits während des Kontrollbesuchs mit der Prüfung begonnen, auf welche Weise aufgegebene Dokumente auf dem Server gelöscht werden könnten. Er hat inzwischen ein Programm eingesetzt, das ein Löschen ermöglicht. Mit Hilfe dieses Programms wird sichergestellt, daß sensitive Daten auf den Servern physikalisch gelöscht und nicht nur aufgegeben werden.

6.4.6 Arbeitsausführung in privater Umgebung

Zunehmend wird an mich die Frage gerichtet, ob und unter welchen Voraussetzungen es zulässig sei, daß Mitarbeiter öffentlicher Stellen ihre Arbeit nicht in ihrem Büro, sondern in privater Umgebung erledigen. Eine solche Frage habe ich daher zum Anlaß für eine allgemeine Antwort genommen.

Unter Arbeitsausführung in privater Umgebung - mit oder ohne Einsatz von Geräten der Informationstechnik - wird im folgenden die Bearbeitung dienstlicher Vorgänge durch Bedienstete der öffentlichen Stelle in einer privaten Umgebung verstanden.

Soweit bei Arbeitsausführung in privater Umgebung personenbezogene Daten verarbeitet werden, ist es im allgemeinen die öffentliche Stelle und nicht der Mitarbeiter als Privatperson, die - in der privaten Umgebung - die

Arbeit ausführt, da Übermittlung (§ 3 Abs. 2 Nr. 4 DSG NW) an den Mitarbeiter als Privatperson unzulässig sein und Datenverarbeitung im Auftrag (§ 11 DSG NW) praktisch nicht vorkommen wird. Falls die Arbeitsausführung in privater Umgebung durch den in der öffentlichen Stelle organisatorisch zuständigen Mitarbeiter erfolgt, ist daher grundsätzlich davon auszugehen, daß diese Arbeit von der zuständigen Organisationseinheit ausgeführt wird. Wenn z. B. eine innerhalb des ärztlichen Bereichs für eine Schreibarbeit zuständige Mitarbeiterin diese Schreibarbeit in privater Umgebung erledigt, dürfte daher davon auszugehen sein, daß diese Art der Arbeitsausführung nicht bedeutet, daß alleine dadurch personenbezogene Daten den ärztlichen Bereich verlassen.

Die Frage der Zulässigkeit von Arbeitsausführung in privater Umgebung wird damit, soweit dabei personenbezogene Daten verarbeitet werden und falls die Arbeit durch einen in der öffentlichen Stelle zuständigen Mitarbeiter ausgeführt wird, zu einer Frage der Datensicherheit.

Durch Arbeitsausführung in privater Umgebung wird die Datensicherheit grundsätzlich erheblich beeinträchtigt. Diese Beeinträchtigung würde nicht bestehen, falls die Arbeit in Diensträumen ausgeführt würde. Nach § 10 Abs. 1 Satz 2 DSG NW ist, soweit personenbezogene Daten verarbeitet werden, die Arbeitsausführung in Diensträumen daher erforderlich, wenn der damit verbundene Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck - dem Vermeiden einer erheblichen Beeinträchtigung der Datensicherheit - steht. Bei der Verarbeitung personenbezogener Daten ist der Aufwand für die Ausführung dieser Arbeiten in Diensträumen im allgemeinen als angemessen anzusehen, und es ist damit im allgemeinen erforderlich, diese Arbeiten in Diensträumen auszuführen.

Arbeitsausführung in privater Umgebung ist bei Verarbeitung von personenbezogenen Daten daher nur zulässig, wenn diese Art der Arbeitsausführung aus besonderen Gründen, die gegen eine Arbeitsausführung in Diensträumen sprechen, für die öffentliche Stelle notwendig ist. Die Gründe müssen so schwerwiegend sein, daß es im Hinblick auf diese Gründe angemessen ist, die mit der Arbeitsausführung in privater Umgebung verbundene Beeinträchtigung der Datensicherheit in Kauf zu nehmen.

Falls im Einzelfall wegen des Vorliegens entsprechender Gründe die Ausführung einer Arbeit, bei der personenbezogene Daten verarbeitet werden, durch den zuständigen Mitarbeiter in privater Umgebung nicht von vornherein als unzulässig anzusehen ist, hängt die Entscheidung über die Zulässigkeit von einer Bewertung

- der Stärke dieser Gründe,
- der Empfindlichkeit der Daten,
- der Art der Arbeitsausführung und
- der getroffenen oder vorgesehenen Maßnahmen zur Datensicherung

ab.

In einem Beratungsersuchen wurde ich ausdrücklich gefragt, wie die Datensicherheit bei einer Ausführung von Arbeiten im häuslichen Bereich gewährleistet werden könne. In meiner Antwort wies ich auf die spezifischen Schwierigkeiten hin, die bestehen, wenn eine öffentliche Stelle die Datensicherheit bei einer Arbeit zu gewährleisten hat, die im privaten Bereich ausgeführt wird. Auch bei einer Ausführung von Arbeiten in privater Umgebung ist es erforderlich, die Datensicherheit zu gewährleisten. Falls eine öffentliche Stelle nicht in der Lage ist, die Einhaltung einer angemessenen Datensicherheit zu gewährleisten, ist es nicht zulässig, die Arbeiten in privater Umgebung auszuführen.

6.4.7 Löschen von Datenträgern vor dem Beschreiben zur Versendung

In der Dienstanweisung einer kontrollierten Stelle ist folgendes geregelt: „Nach Ablauf der Aufbewahrungsfristen sind die Datenträger zu löschen. Bekommt der ADV-Bereich von anderen Stellen im Wege des Datenträgeraustausches Datenträger zugestellt, sind diese vor ihrer Rücksendung zu löschen, sofern der Absender nichts anderes bestimmt. Versendet der ADV-Bereich seinerseits Datenträger an andere Stellen, sind diese vor ihrer Bespielung mit Daten zu initialisieren."

Je nach Art des Datenträgers, der versandt wird, ist nicht sicher, ob durch dessen Initialisierung alle Daten gelöscht werden, die vorher auf dem Datenträger gespeichert waren. Da auch nicht sicher ist, ob durch das erneute Beschreiben mit Daten alle bisher auf dem Datenträger gespeicherten Daten überschrieben werden, habe ich empfohlen vorzuschreiben, daß Datenträger, die der ADV-Bereich an andere Stellen versendet, vor ihrem Beschreiben mit Daten jedenfalls zu löschen sind.

6.4.8 Sicherheitsbereich

Im Rahmen eines allgemeinen Sicherheitskonzeptes wird bei einem Rechenzentrum das Datenarchiv im allgemeinen als eigener Sicherheitsbereich, dem die höchste Sicherheitsstufe zugeordnet wird, geführt. Die Praxis bei einer kontrollierten Datenzentrale entspricht ungefähr dieser Regelung. Die Datenzentrale verfügt über zwei räumlich getrennte Datenarchive; für die Verwaltung der Bestände der Datenarchive sind Archivverwalter zuständig. Allerdings ist das in die laufende Arbeit einbezogene Datenarchiv vom Maschinenraum insofern nicht abgetrennt, als es keinen Unterschied in der Zugangsbefugnis gibt. Das Zugangskontrollsystem bietet bisher keine Möglichkeit, für den Zugang zu diesem Datenarchiv spezielle Berechtigungen zu vergeben.

Während des Kontrollbesuchs wurde erörtert, daß es wünschenswert wäre, die Datenarchive als getrennten Sicherheitsbereich mit eigener Zugangsbefugnis zu führen. Die Datenzentrale wird prüfen, ob die entsprechenden

Änderungen durchgeführt werden können und damit die Zugangsbefugnis zu den Datenarchiven auf die Archivverwalter beschränkt werden kann.

Bei einer Kreisverwaltung gehören zum Sicherheitsbereich der Maschinenraum mit dem Datenträgerarchiv und das Papierlager, in dem die Maschinen der Arbeitsnachbereitung aufgestellt sind, sowie das Dienstzimmer, in dem die Konsole installiert ist. Um einen Zugang in Notfällen zu ermöglichen, ist folgendes geregelt: „Ein Schlüssel des Sicherheitsbereichs wird auch der Kreisleitstelle zur Verfügung gestellt. Sie gewährt außerhalb der Dienstzeiten in Notfällen Polizei und Feuerwehr den Zutritt."

Ich habe darauf hingewiesen, daß eine derartige Zutrittsmöglichkeit zum Sicherheitsbereich außerhalb der Dienstzeit jedenfalls nur in solcher Weise möglich sein sollte, daß in jedem Einzelfall nachträglich erkennbar wird, daß ein Zutritt erfolgt ist. Dieses Ziel könnte etwa dadurch erreicht werden, daß der Schlüssel in einem versiegelten Umschlag bei der Kreisleitstelle hinterlegt wird. Durch Dienstanweisung sollte dann vorgeschrieben sein, daß jede Benutzung des Schlüssels nachträglich zu melden ist und begründet werden muß.

6.4.9 Auslagerungsarchiv

Innerhalb des Sicherheitsbereichs eines Rechenzentrums ist das Datenarchiv immer diejenige Stelle, an deren Sicherheit die höchsten Anforderungen gestellt werden. Maßnahmen zum Gewährleisten der Sicherheit des Datenarchivs haben daher besonders hohe Priorität. Dennoch ist es erforderlich, auch für den Katastrophenfall Vorsorge zu treffen, damit unter allen Umständen - auch etwa nach einem Brand im Datenarchiv - eine Rekonstruktion der gespeicherten Daten möglich ist.

Zu den selbstverständlichen Vorsorgemaßnahmen gehört es daher, Duplikate aller wesentlichen Datenbestände in möglichst aktueller Fassung in einem vom Rechenzentrum räumlich getrennten Auslagerungsarchiv verfügbar zu halten. Da in dem Auslagerungsarchiv alle wesentlichen Daten des Datenarchivs in duplizierter Form verfügbar sind, bedarf das Auslagerungsarchiv des gleichen Schutzes wie das dem Rechenzentrum räumlich direkt angegliederte Datenarchiv.

Bei einem kontrollierten Kreis wird als Auslagerungsarchiv ein Raum genutzt, der gleichzeitig der Lagerung von Ausstattungsgegenständen für den Katastrophenfall dient. Über einen Schlüssel zu diesem Raum verfügt daher nicht nur der ADV-Bereich. Der Zugang zu diesem Raum muß insoweit als nicht gesichert angesehen werden.

Zur Ablage der ausgelagerten Daten sind in dem Auslagerungsarchiv zwei einfache Stahlschränke aufgestellt. Bei einem dieser Stahlschränke ist die Schlüsselnummer in das Schloß eingeprägt.

Zugang zu dem Auslagerungsarchiv erhält man über eine Tiefgarage. Die Tür des Auslagerungsarchivs führt unmittelbar in diese Tiefgarage. Der Kreis

berichtete, für den Katastrophenfall sei vorgesehen, die Tiefgarage zur Aufnahme Betroffener zu nutzen und im Auslagerungsarchiv Trinkwasserbehälter aufzustellen. Ein entsprechendes Hinweisschild ist bereits an der Tür des Auslagerungsarchivs angebracht.

Im Hinblick darauf, daß bereits heute der Zugang zum Auslagerungsarchiv nicht als gesichert angesehen werden kann und daß gerade in der Zeit nach einem Katastrophenfall das Auslagerungsarchiv voraussichtlich ungesichert sein wird, muß die gewählte Lösung für das Auslagerungsarchiv als unzureichend angesehen werden. Ich habe daher empfohlen, eine andere Lösung zu suchen. Dabei sollten an die Sicherheit der in dem Auslagerungsarchiv liegenden Daten Anforderungen gestellt werden, die den Anforderungen entsprechen, die an ein der laufenden Nutzung dienendes Datenarchiv gestellt werden. Das Auslagerungsarchiv wurde inzwischen entsprechend dieser Empfehlung an einem anderen Ort untergebracht.

6.5 Konventionelle Datenverarbeitung

6.5.1 Sicherheit von Akten

Bei einem Staatlichen Gewerbeaufsichtsamt war anläßlich einer Prüfung des Staatshochbauamtes festgestellt worden, daß die zulässige Deckenbelastung in der Registratur durch die aufgestellten Aktenschränke erheblich überschritten worden war. Um die bestehende Gefahr abzuwenden, waren daraufhin als kurzfristige Lösung zahlreiche Schränke aus der Registratur entfernt und auf einem Flur aufgestellt worden.

Bei einer Ortsbesichtigung stellten meine Mitarbeiter fest, daß die ausgelagerten Aktenschränke nicht verschlossen waren; ein Teil der Schränke war allerdings nicht mit einem Schloß ausgestattet. Die Aktenschränke enthielten überwiegend Akten mit personenbezogenen Daten. Der Flur, auf dem die Schränke standen, war für den Publikumsverkehr frei zugänglich. Es konnte daher nicht ausgeschlossen werden, daß Unbefugte auf personenbezogene Daten zugreifen. Durch die unzureichende Sicherung der auf dem Flur stehenden Aktenschränke war die Datensicherheit erheblich beeinträchtigt.

Nach § 10 Abs. 1 Satz 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. Werden personenbezogene Daten in nicht-automatisierten Dateien oder in Akten verarbeitet, sind Maßnahmen zu treffen, um insbesondere den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern (§ 10 Abs. 3 DSG NW).

Während des Besuchs wurden verschiedene Lösungsmöglichkeiten erörtert, um möglichst bald die Gewährleistung der Datensicherheit zu erreichen:

- Verschließen der Aktenschränke

  Die verschließbaren Aktenschränke auf dem Flur sollten ab sofort ständig verschlossen gehalten werden.

  Da die nicht verschließbaren Aktenschränke auf dem Flur gegen verschließbare aus der Registratur ausgetauscht werden können, ist es möglich, alle auf dem Flur befindlichen Aktenschränke verschlossen zu halten. Das Verschließen der Aktenschränke sollte in einer Dienstanweisung vorgeschrieben und deren Einhaltung angemessen kontrolliert werden.

  Bei dieser Lösungsalternative sollte bedacht werden, daß in die Schlösser der Schränke die Schlüsselnummern ablesbar eingeprägt sind. Dadurch ist die Datensicherheit auch bei verschlossenen Schränken beeinträchtigt.

- Änderungen der Raumzuteilung

  Dem Raumbedarfsplan des Gewerbeaufsichtsamtes war zu entnehmen, daß dem Soll der Geschäftszimmerflächen ein Ist gegenüberstand, nach dem rein rechnerisch ein Raumüberhang von 164 m^2 bestand. Für die Unterbringung der auf dem Flur ausgelagerten Aktenschränke bestand ein theoretischer zusätzlicher Raumbedarf von nur 55 m^2. Daher sollte geprüft werden, ob dieser Raumbedarf durch eine Raumzuteilung aus der rechnerischen Geschäftszimmerflächenreserve gedeckt werden kann.

- Auslagerung der Akten in den Keller

  Eine Auslagerung der Akten in einen abzuschließenden Keller wäre eine mögliche Lösung, da nur sporadische Zugriffe durch die Sachbearbeiter auf die Aktenschränke erforderlich sind.

- Sicherung des Flurs oder Sicherung des Dienstgebäudes

  Die nicht sehr hohe Zahl der täglichen Besucher macht es möglich, alle Besucher durch einen Mitarbeiter des Staatlichen Gewerbeaufsichtsamtes zu begleiten. Als Voraussetzung muß durch Verschließen des Flurs oder des Eingangsbereichs des vom Staatlichen Gewerbeaufsichtsamt belegten Gebäudeteils gewährleistet sein, daß Besucher nicht ohne Begleitung Berechtigter Zugang erlangen können. Das Verschließen des Eingangsbereichs und die Pflicht, Besucher zu begleiten, sollten schriftlich in einer Dienstanweisung festgehalten werden. Die Einhaltung der Dienstanweisung sollte in angemessener Weise kontrolliert werden.

Um die erforderliche Datensicherheit zu gewährleisten, wurde inzwischen eine Lösung gewählt, in der mehrere meiner Vorschläge kombiniert wurden.

In einem Altpapiercontainer waren Patientenunterlagen einer Landesklinik gefunden worden. Ob die Unterlagen in den Container dadurch gelangt waren, daß ein Arzt sie zur Bearbeitung in seine Privatwohnung mitgenommen hatte und die Unterlagen dort irrtümlich zusammen mit Altpapier entsorgt worden waren, konnte nicht abschließend geklärt werden.

Der von mir angeforderten Stellungnahme der Landesklinik entnahm ich allerdings, daß die Aufbewahrung von Patientenunterlagen in verschließbaren Aktenschränken der Stations- bzw. Arztzimmer vorgeschrieben war und daß der Mitführung von Patientenunterlagen aus der Klinik eine Rundverfügung entgegenstand. Diese Anweisungen waren aus den mir vorgelegten Unterlagen aber nicht explizit ersichtlich. Ich empfahl daher, die Aufbewahrung der Patientenunterlagen in verschlossenen Aktenschränken verbindlich vorzuschreiben und festzulegen, daß das Mitführen dieser Unterlagen aus der Klinik nicht erlaubt ist. Darüber hinaus regte ich an zu prüfen, ob es angemessen ist, den Verbleib von Patientenunterlagen durch eine Nachweisführung organisatorisch zu kontrollieren.

In einer Anfrage wurde meine Stellungnahme zu einer organisatorischen Regelung erbeten: In einem Klinikum war eine „Zentrale Rechnungserfassung" eingerichtet worden. Jede Postsendung, die nicht mit dem Vermerk „persönlich" versehen ist und die eine Rechnung enthalten könnte, wird seitdem durch die Poststelle des Klinikums geöffnet, um alle Rechnungen möglichst vollständig und umgehend der Zentralen Rechnungserfassung zuleiten zu können. Die an mich gerichtete Frage betraf die Zulässigkeit des zentralen Öffnens der Postsendungen.

Mir erscheint es für den internen Postablauf grundsätzlich hinnehmbar, daß eine Postsendung, die nicht mit dem Vermerk „persönlich" oder mit einem vergleichbaren Vermerk versehen ist, durch die Poststelle des Klinikums geöffnet wird. Allerdings muß in einem Klinikum ergänzend geregelt sein, daß auch Schreiben, die in geeigneter Weise als Arztbriefe gekennzeichnet sind, ungeöffnet an die entsprechende Person bzw. Stelle weitergeleitet werden. Dabei sollten in einem Klinikum auch Briefe, die z. H. eines Arztes adressiert sind, wie Arztbriefe behandelt und daher ungeöffnet weitergeleitet werden. Es sollte zusätzlich festgelegt werden, daß Schreiben, die versehentlich oder wegen mangelnder Kenntlichmachung in der Anschrift geöffnet wurden, unmittelbar in einem verschlossenen Umschlag an den Empfänger weiterzuleiten und nicht auf den Dienstweg zu geben sind.

6.5.2 Vertraulichkeit von Gesprächen

Eine Reihe von Fällen hat mich bereits veranlaßt, zur Frage des unbefugten Mithörens von Gesprächen vertraulichen Inhalts Stellung zu nehmen und auf die Rechtsvorschriften, nach denen der Schutz dieser Gespräche zu gewährleisten ist, hinzuweisen. Entsprechende Darlegungen enthalten einige meiner Tätigkeitsberichte.

Ein Bürger machte mich jetzt auf eine Beeinträchtigung der Datensicherheit in der Psychologischen Beratungsstelle einer Stadt aufmerksam, die er bei einem Besuch festgestellt hatte. Er schilderte, daß er wegen zu dünner Wände bzw. Türen (einfacher Rigips/Glastüren) Gespräche aus den Nachbarzimmern deutlich mitverfolgen konnte.

Bei der Ortsbesichtigung in der Psychologischen Beratungsstelle stellten meine Mitarbeiter folgendes fest: Selbst bei einem Gespräch, das nur in mittlerer Lautstärke in einem Beratungszimmer geführt wird, ist auf dem Flur ein Mithören noch aus einigen Metern Entfernung einwandfrei möglich. Auch im Nachbarzimmer kann ein solches Gespräch weitgehend verfolgt werden.

Im Hinblick auf die aus Artikel 4 Abs. 2 der Landesverfassung Nordrhein-Westfalen folgende Verpflichtung, personenbezogene Daten gegen unbefugte Kenntnisnahme durch Dritte zu schützen, muß die Stadt besondere Sorgfalt darauf verwenden zu verhindern, daß vertrauliche Gespräche in den Zimmern der Psychologischen Beratungsstelle von Unbefugten mitgehört werden können. Insbesondere ist im Hinblick auf die besondere Empfindlichkeit der geführten Gespräche sicherzustellen, daß es anderen Besuchern der Beratungsstelle nicht möglich ist, die in den Beratungszimmern geführten Gespräche mitzuverfolgen.

Bei einem abschließenden Gespräch wurde erörtert, daß die derzeitige Situation in Bezug auf die Möglichkeit des Mithörens von Gesprächen in der Psychologischen Beratungsstelle einer Änderung bedarf. Es wurde u.a. die Möglichkeit besprochen, ein Ingenieurbüro einzuschalten, um festzustellen, welche Maßnahmen geeignet und angemessen sind, um die Vertraulichkeit von Gesprächen zu gewährleisten.

6.5.3 Wahrung des Sozialgeheimnisses

Zahlreiche Eingaben haben mir gezeigt, daß auch die Sozialleistungsträger ihrer Verpflichtung zur Wahrung des Sozialgeheimnisses nicht immer in der gebotenen Weise nachkommen.

So hatte ich bei einem auf Grund einer Beschwerde durchgeführten Informations- und Kontrollbesuch bei einem Leistungsträger festgestellt, daß die in Bearbeitung befindlichen Akten offen in Regalen oder auf dem Aktenbock aufbewahrt wurden. Das externe Reinigungspersonal war zwar auf das Datengeheimnis verpflichtet, hatte aber nach Dienstschluß unbeaufsichtigt Zugang zu den Diensträumen und damit Gelegenheit, von dem Inhalt der Akten Kenntnis zu nehmen.

In anderen Fällen beschwerten sich Bürger darüber, daß bei ihrer Vorsprache im Sozialamt alle Türen zu den angrenzenden Räumen, in denen sich weitere Sachbearbeiter befanden, offenstanden. In einem Fall hatte sich sogar der Sachbearbeiter aus dem Nebenzimmer unaufgefordert in das Gespräch eingemischt.

Aus dem Gebot, das Sozialgeheimnis zu wahren (§ 35 Abs. 1 Satz 1 SGB I a. F.) ergibt sich die Verpflichtung der Leistungsträger, die technischen und organisatorischen Maßnahmen (einschließlich Dienstanweisungen) zu treffen, um sicherzustellen, daß die Sozialdaten nur Befugten zugänglich sind und nur an diese, nicht an Dritte weitergegeben werden. Dritte sind auch

andere, nicht mit der Sachbearbeitung im konkreten Einzelfall befaßte Mitarbeiter, da das Sozialgeheimnis auch innerhalb des Leistungsträgers gilt.

Diesen Anforderungen wurde in den genannten Fällen nicht entsprochen.

Indem das Reinigungspersonal nach Dienstschluß unbeaufsichtigt Zugang zu den Diensträumen hatte, war nicht sichergestellt, daß personenbezogene Daten nur Befugten zugänglich waren. Dies stellte einen Verstoß gegen das Sozialgeheimnis dar, und zwar unabhängig davon, ob tatsächlich Einblick in die Akten genommen wurde. Unbeachtlich war auch, daß das Reinigungspersonal auf die Geheimhaltung verpflichtet war. Eine Geheimhaltungsverpflichtung auf seiten des Datenempfängers wirkt lediglich als Schranke gegen eine unbefugte Weiteroffenbarung an Dritte, kann aber eine Befugnis zur (Erst-)offenbarung an ihn als Datenempfänger nicht begründen.

Falls die Reinigung der Diensträume weiterhin in Abwesenheit der in den Räumen tätigen Mitarbeiter erfolgen soll, muß entweder für eine ständige Aufsicht gesorgt oder sichergestellt werden, daß sich sämtliche Akten mit personenbezogenen Daten in sicher verschlossenen Schränken befinden.

Die Verpflichtung zur Wahrung des Sozialgeheimnisses gebietet es bei Vorsprache von Antragstellern auch, sowohl offenstehende Türen zu den angrenzenden Räumen zu schließen als auch andere Mitarbeiter, die für die Bearbeitung der jeweiligen Sache nicht konkret zuständig sind, zum Verlassen des Raumes anzuhalten. Dies gilt auch für den Vertreter eines Sachbearbeiters, da bei Anwesenheit des zuständigen Bearbeiters der Vertretungsfall nicht gegeben ist. Etwas anderes läßt sich ausnahmsweise dann vertreten, wenn das Verhalten eines Besuchers bei früheren Vorsprachen - z. B. besonders aggressives Auftreten - bei dem zuständigen Sachbearbeiter Angst vor tätlichen Übergriffen ausgelöst hat. In einem solchen Fall wäre es aus Sicherheitserwägungen nicht zu beanstanden, wenn bei entsprechendem Betragen des Besuchers die Verbindungstür zum Nachbarzimmer geöffnet wird. Dabei ist allerdings darauf zu achten, daß dort kein anderer Besucher anwesend ist.

Durch das Zweite Gesetz zur Änderung des Sozialgesetzbuchs hat sich die Rechtslage nicht geändert, da auch nach § 35 SGB I in der nunmehr geltenden Fassung das Sozialgeheimnis zu wahren ist und nach § 78 a SGB X die erforderlichen technischen und organisatorischen Maßnahmen zu treffen sind.

6.5.4 Unterlagenvernichtung

Fragen und Hinweise im Zusammenhang mit dem Vernichten von Unterlagen stehen weiterhin im Zentrum des Interesses. Immer wieder werden mein Rat und meine Stellungnahme gesucht, und bei Kontrollbesuchen prüfe ich, ob das Verfahren zur Unterlagenvernichtung den Anforderungen gerecht wird. Öffentlich bekanntgewordene Pannen geben darüber hinaus Veranlassung zur Prüfung von Einzelfällen.

In den Arbeitsräumen einer kontrollierten Behörde sind jeweils zwei Behältnisse für zu entsorgendes Material aufgestellt. Bei dem einen der Behältnisse handelt es sich um einen Papierkorb. Dieser ist für die Aufnahme des gesamten Papierabfalls einschließlich der zu vernichtenden Unterlagen mit personenbezogenen Daten vorgesehen. Über das zweite Behältnis sollen sonstige Abfälle entsorgt werden.

Zum Reinigen der Arbeitsräume werden sowohl eigene Kräfte als auch Fremdkräfte eingesetzt. Es ist Aufgabe der Reinigungskräfte, die Behältnisse zu leeren. Dabei wird der Inhalt der Papierkörbe in einen Abfallschacht geschüttet, dessen Öffnung sich auf dem gleichen Stockwerk befindet. Der Abfallschacht endet im Keller des Gebäudes in einem Sammelbehälter.

Das Papier in dem Sammelbehälter wird in geeigneten Zeitabständen in ein Zerkleinerungsgerät gegeben. In dem Zerkleinerungsgerät wird das Papier in Streifen von etwa 2 cm Breite zerschnitten. (Bei einer Überprüfung konnten allerdings auch Stücke erheblich größerer Breite gefunden werden.) Das zerschnittene Papier wird anschließend in Ballen gepreßt. Diese Papierballen werden von einer Fremdfirma abgeholt und zu einer Papierfabrik transportiert.

Zu diesem Verfahren der Unterlagenvernichtung habe ich auf folgendes hingewiesen:

- Werden Datenträger mit personenbezogenen Daten aus Dateien oder Akten (§ 2 Abs. 1 Satz 1 DSG NW) vernichtet, handelt es sich datenschutzrechtlich um Löschung von Daten und damit um eine Phase der Datenverarbeitung (§ 3 Abs. 2 Nr. 6 DSG NW). Soweit ein Reinigungsunternehmen durch seine Arbeitskräfte Unterlagen aus den Papierkörben sammelt und zu dem Abfallschacht transportiert, führt dieses daher innerhalb einer Phase der Datenverarbeitung - innerhalb des Löschens - eine Teilaufgabe aus. Bei der Arbeit des Reinigungsunternehmens handelt es sich insoweit um Verarbeitung personenbezogener Daten im Auftrag (§ 11 DSG NW). Diese Tatsache sollte in dem Vertrag mit dem Reinigungsunternehmen in geeigneter Form zum Ausdruck gebracht werden.

- Personenbezogene Daten, die auf Unterlagen aufgezeichnet sind, die vernichtet werden, gelten erst dann als gelöscht, wenn es nicht mehr möglich ist, den Inhalt aus den vernichteten Unterlagen zu rekonstruieren. Als Hilfsmittel bei der Beurteilung der Frage, ob Unterlagen nach ihrer Zerkleinerung durch einen Aktenvernichter als vernichtet angesehen werden können, sollte die Norm DIN 32 757 (Vernichten von Informationsträgern) herangezogen werden.

  Diese Norm unterscheidet fünf Sicherheitsstufen bei der Vernichtung von Informationsträgern. Sicherheitsstufe 1 entspricht den geringsten Anforderungen und Sicherheitsstufe 5 den höchsten Anforderungen an das Vernichten. Von mir wird im allgemeinen empfohlen, Unterlagen so zu vernichten, daß nach Möglichkeit den Anforderungen der Sicherheitsstufe 4

entsprochen wird. Durch das Zerkleinern des Papiers in dem Zerkleinerungsgerät der Behörde wird dagegen ein Zustand erreicht, der noch nicht einmal den Anforderungen der Sicherheitsstufe 1 der Norm DIN 32 757 entspricht. Es kann daher nicht davon ausgegangen werden, daß die auf den Unterlagen aufgezeichneten Daten nach dem Zerkleinern des Papiers gelöscht sind. Die Papierballen enthalten daher personenbezogene Daten.

- Die Behörde ist für die Sicherung von Unterlagen mit personenbezogenen Daten verantwortlich, solange die auf diesen aufgezeichneten Daten nicht als gelöscht angesehen werden können. Diese Verantwortung endet daher bei dem derzeitigen Verfahren der Unterlagenvernichtung erst, sobald bei der Verarbeitung in der Papierfabrik ein entsprechender Zustand erreicht ist.

Während des Kontrollbesuchs wurde erörtert, daß unter Berücksichtigung dieser Hinweise das Gesamtverfahren der Vernichtung der Unterlagen mit personenbezogenen Daten überprüft werden sollte. Anregungen bei der Suche nach einer geeigneten Lösung können der von mir herausgegebenen Organisationshilfe - Unterlagenvernichtung entnommen werden. Ich habe empfohlen, das Verfahren zur Vernichtung von Unterlagen mit personenbezogenen Daten so abzuändern oder zu ergänzen, daß den Anforderungen des Datenschutzes entsprochen wird.

Bei einem anderen Kontrollbesuch stand der mit einer Fremdfirma abgeschlossene Vertrag zur Vernichtung von Unterlagen im Zentrum der Erörterung. Grundlage der Erörterung war die Organisationshilfe - Unterlagenvernichtung. Die Erörterung des Vertrages führte zu einer Reihe von Hinweisen zur Verbesserung der Datensicherheit bei der Unterlagenvernichtung. Im Hinblick auf die nur noch kurze Laufzeit des derzeitigen Vertrages waren diese Hinweise vor allem für den Abschluß des nächsten Vertrages von Bedeutung. Die kontrollierte Stelle sagte zu, den nächsten Vertrag unter Berücksichtigung der Hinweise aus der Organisationshilfe - Unterlagenvernichtung abzuschließen.

Eine öffentliche Stelle unterrichtete mich, sie habe bereits vor längerer Zeit mit einer Fremdfirma einen Vertrag über die Entsorgung der Papierabfälle mit datenschutzrelevantem Inhalt geschlossen. Durch Beschluß des Amtsgerichts sei jetzt das Konkursverfahren über das Vermögen dieser Firma eröffnet worden. Man sei in Sorge, weil möglicherweise eigene und fremde Papierabfälle noch nicht vernichtet seien und ein Zugang auf das Betriebsgelände nicht möglich sei.

In der Folgezeit stellte sich heraus, daß alle der Fremdfirma übergebenen Unterlagen vernichtet worden waren. Der aktuelle Anlaß war daher nicht mehr vorhanden. Bezüglich eines evtl. neu abzuschließenden Vertrages für die Vernichtung von personenbezogenen Unterlagen gab ich insbesondere folgende Hinweise:

- Es ist bei der Vertragsgestaltung darauf zu achten, daß zu vernichtende Unterlagen vor Abschluß der Vernichtung nicht in das Eigentum Dritter übergehen.
- Der Vertrag sollte die Verpflichtung für den Auftragnehmer enthalten, daß die Unterlagen bis zu deren Vernichtung nicht mit fremden Unterlagen vermischt werden dürfen. Die Frage des Auseinandersortierens in einem evtl. Konkursfall des Auftragnehmers entsteht bei entsprechender Vertragsregelung nicht.
- Jede ordnungsgemäß durchgeführte Vernichtung sollte vom Auftragnehmer schriftlich bestätigt werden.

Diese und auch weitere Hinweise für eine unter dem Gesichtspunkt der Datensicherheit angemessene Vertragsgestaltung bei der Vernichtung von personenbezogenen Unterlagen kann die öffentliche Stelle in meinem 11. Tätigkeitsbericht (S. 151 bis 155) sowie in den Abschnitten A und D der Organisationshilfe - Unterlagenvernichtung finden.

Von einer Tageszeitung wurden mir Unterlagen übergeben, die auf einem Schrottplatz gefunden worden waren. Die Unterlagen enthielten personenbezogene Kfz-Dokumente verschiedenster Art.

Eine eingehende Klärung des Vorfalls ergab, daß die Unterlagen durch den Bediensteten eines Straßenverkehrsamts beim Transport auf einen Behälter mit entwerteten Kfz-Kennzeichen gelegt und dann irrtümlich mit diesen Kennzeichen entsorgt worden waren. Um die Datensicherheit beim Umgang mit personenbezogenen Unterlagen besser zu gewährleisten, habe ich empfohlen vorzuschreiben, daß Vorgänge, die noch aufzubewahren sind, nicht - auch nicht kurzzeitig - während des Transports mit für die Vernichtung bestimmten Schriftstücken oder Objekten zusammengefaßt werden dürfen.

Einer Pressemitteilung entnahm ich, daß ein Umschlag mit Mikrofilmen eines Kreditinstituts auf der Straße gefunden worden war. Die gefundenen Mikrofilme betrafen, wie ich bei der Überprüfung des Vorfalls feststellte, Unterlagen, die zur Vernichtung bestimmt waren. Der Vorfall, der nicht endgültig aufgeklärt werden konnte, gab zu einer eingehenden Überprüfung der getroffenen Sicherheitsmaßnahmen Veranlassung. Das Kreditinstitut hat Ablauf und Überwachung der Unterlagenvernichtung inzwischen neu organisiert.

6.5.5 Versendung von Unterlagen

Die Anfrage einer Stadt, die Möglichkeiten ermitteln wollte, Abgabenbescheide kostengünstiger zu versenden, veranlaßte mich, bei der Deutschen Bundespost Postdienst die Handhabung von „Infopost" zu klären.

Die Deutsche Bundespost Postdienst teilte mir dazu mit, daß nicht nur das Einlieferungspostamt berechtigt ist, Infopost für Kontrollzwecke zu öffnen, sondern auch das Zustellpostamt und der zustellende Postbeamte. Für mich

ist nicht erkennbar, durch welche Vereinbarung mit dem Einlieferungspostamt die Rechte des Zustellpostamtes und des zustellenden Postbeamten eingeschränkt werden können. Nach meinem derzeitigen Kenntnisstand gehe ich daher davon aus, daß die Versendung von Abgabenbescheiden mit personenbezogenen Daten als Infopost unzulässig ist.

Ein Bürger beschwerte sich, er habe von der Stadt einen Bußgeldbescheid für eine Verkehrsordnungswidrigkeit erhalten, der nur an den äußeren Rändern geschlossen war. Der mittlere Teil sei unverschlossen und für jedermann einsehbar gewesen. Der Bescheid sei auch nicht in einem Umschlag zum Versand gebracht worden.

Die Stadt teilte mir dazu mit, Erstellung und Versand dieser Bescheide erfolgten DV-gestützt. Ein mir als Beispiel übersandter Formularsatz bestand aus zwei Teilen, die an einer Perforation getrennt werden konnten. Der Formularsatz war zwar an den Rändern einwandfrei geschlossen, so daß der im Innern stehende Text erst nach dem Öffnen hätte gelesen werden können. Durch ein Falten entlang der Perforation war diese aber beschädigt. Dadurch wurde eine Einsichtnahme in den Inhalt des Bußgeldbescheids durch Dritte möglich.

Nach § 10 Abs. 1 Satz 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. Werden personenbezogene Daten in nicht-automatisierten Dateien oder in Akten verarbeitet, sind Maßnahmen zu treffen, um insbesondere den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern (§ 10 Abs. 3 DSG NW).

Nach meiner Beobachtung und nach der Feststellung des betroffenen Bürgers ging ich davon aus, daß der Bußgeldbescheid bereits bei leichter Beanspruchung während des Transports aufreißen konnte und dann nicht mehr ordnungsgemäß verschlossen war. Der Bußgeldbescheid genügte damit nicht den Anforderungen nach § 10 Abs. 3 DSG NW. Daher habe ich der Stadt empfohlen, durch geeignete Maßnahmen - etwa durch Änderung am Material oder an der Perforation - sicherzustellen, daß bei der Versendung von Bußgeldbescheiden eine angemessene Datensicherheit gewährleistet ist.

Ein Bürger machte mich darauf aufmerksam, daß die Versendung von personenbezogenen Unterlagen - z. B. Einladungen zu Prüfungen sowie deren Ergebnisse - durch die Industrie- und Handelskammer an seinen Ausbildungsbetrieb ohne den Zusatz „Personalabteilung" in der Anschrift erfolge. Ohne diesen Zusatz im Adreßfeld würden seine personenbezogenen Unterlagen von der Poststelle des Betriebes geöffnet, so daß nicht berechtigte Personen wie etwa Angestellte der Poststelle oder Boten die Möglichkeit zur Kenntnisnahme erhielten. Mit dem Zusatz „Personalabteilung" in

der Anschrift würden die Schreiben dagegen ungeöffnet an die Personalabteilung seines Ausbildungsbetriebs weitergeleitet.

Die um Stellungnahme gebetene Industrie- und Handelskammer unterrichtete mich, daß sie künftig alle Schreiben, die Prüfungsunterlagen enthalten, gut sichtbar mit dem Stempelaufdruck „Personalangelegenheit/Vertraulich" kennzeichnen wird. Ich gehe davon aus, daß durch diese Maßnahme in Zukunft eine angemessene Datensicherheit bei der Versendung von Prüfungsunterlagen gewährleistet wird.

Düsseldorf, den 23. Februar 1995

Maier-Bode

Anlagen

Anlage 1 (zu 3.1.1)

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994

zum Ausländerzentralregistergesetz

(gegen die Stimme Bayerns)

Das Ausländerzentralregister beim Bundesverwaltungsamt in Köln existiert seit 40 Jahren ohne gesetzliche Grundlage. Derzeit stehen den verschiedenen Benutzern des Registers Daten zu mindestens 8 Millionen Ausländern, die sich in der Bundesrepublik aufhalten oder aufgehalten haben, zur Verfügung. Gespeichert sind neben Daten zur Identifizierung und weiteren Beschreibung der Person insbesondere Angaben zum Meldestatus, Aufenthaltsrecht und Asylverfahren.

Die Datenschutzbeauftragten des Bundes und der Länder haben immer wieder darauf hingewiesen, daß die Führung eines derartigen Registers ohne gesetzliche Regelung mit dem vom Grundgesetz Deutschen wie Ausländern gleichermaßen garantierten Recht auf informationelle Selbstbestimmung unvereinbar ist. Sie begrüßen daher, daß mit dem am 2. März 1994 vom Bundeskabinett beschlossenen Entwurf für ein Ausländerzentralregistergesetz eine gesetzliche Grundlage geschaffen werden soll.

Zwar enthält dieser Gesetzentwurf gegenüber früheren Entwürfen eine Reihe datenschutzrechtlicher Verbesserungen, Bedenken bestehen jedoch weiterhin: Die Datenschutzbeauftragten wenden sich insbesondere dagegen, daß das Ausländerzentralregister nicht nur als Informations- und Kommunikationssystem für die mit der Durchführung ausländer- und asylrechtlicher Vorschriften betrauten Behörden dienen, sondern darüber hinaus als Informationsverbund für Aufgaben der Polizei, Strafverfolgungsorgane und Nachrichtendienste zur Verfügung stehen soll.

Die Funktionserweiterung wird deutlich durch die Speicherung von Erkenntnissen der Sicherheitsbehörden zu Ausländern in das Register. So soll der INPOL-Fahndungsbestand des BKA, soweit er Ausschreibungen zur Festnahme und zur Aufenthaltsermittlung von Ausländern enthält, in das Ausländerzentralregister übernommen werden. Gleiches gilt für die vorgesehene Speicherung von Angaben zu Personen, bei denen Anhaltspunkte für den Verdacht bestehen, daß sie im einzelnen bezeichnete Straftaten planen, begehen oder begangen haben. Diese Informationen dienen nicht einem Informationsbedarf zur Erfüllung ausländerbehördlicher Aufgaben, sondern - worauf die Entwurfsbegründung hinweist - der Kriminalitätsbekämpfung. Für diese Zwecke stehen den Sicherheitsbehörden aber eigene Informationssysteme zur Verfügung. Nach Auffassung der Datenschutz-

beauftragten dürfen deshalb derartige Erkenntnisse nicht in das Register aufgenommen werden.

Die im Entwurf vorgesehenen Voraussetzungen, unter denen u. a. für Polizeibehörden, Staatsanwaltschaften und Nachrichtendienste automatisierte Abrufverfahren eingerichtet werden können, stellen keine wirksamen Vorkehrungen für eine Begrenzung der Abrufe dar. Besonders problematisch ist der geplante automatisierte Zugriff durch die Nachrichtendienste auf einen - wenn auch reduzierten - Datensatz. Für die Dienste ist in den jeweiligen bereichsspezifischen Gesetzen der automatisierte Abruf aus anderen Datenbeständen ausgeschlossen. Die Erforderlichkeit derartiger Abrufe ist in keiner Weise belegt. Die Datenschutzbeauftragten sprechen sich deshalb dafür aus, zumindest auf den automatisierten Abruf durch Nachrichtendienste zu verzichten.

Anlage 2 (zu 3.1.2)

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994

zu Art. 12 Verbrechensbekämpfungsgesetz zur Trennung von Polizei und Nachrichtendiensten

Geheimdienstliche Informationsmacht und polizeiliche Exekutivbefugnisse müssen strikt getrennt bleiben. Die Datenschutzbeauftragten des Bundes und der Länder stellen mit Besorgnis Entwicklungen fest, die die klare Trennungslinie zwischen Nachrichtendiensten und Polizeibehörden weiter zu verwischen drohen. Dies betrifft vor allem den Einsatz des Bundesnachrichtendienstes nach dem Verbrechensbekämpfungsgesetz:

- Der BND erhält danach bei der Fernmeldeaufklärung auch Befugnisse, die auf eine gezielte Erhebung von Daten für polizeiliche Zwecke hinauslaufen können. Deshalb ist bei dem Vollzug des Gesetzes darauf zu achten, daß nicht gezielt Informationen gesammelt werden, die vom Auftrag des BND nicht umfaßt werden.

- Zwischen nachrichtendienstlichen Vorfelderkenntnissen und polizeilichen Zwangsmaßnahmen ist ein Filter erforderlich, der vor allem Unbeteiligte vor überzogenen Belastungen schützt.

Die Datenschutzbeauftragten fordern, für die Zusammenarbeit von Nachrichtendiensten und Polizei in der Durchführung und Gesetzgebung das Trennungsgebot strikt zu beachten. Dies gilt auch bei der Fernmeldeaufklärung des BND. Eine wirksame Kontrolle durch den Datenschutzbeauftragten in diesem sensiblen Bereich ist auch nach der Rechtssprechung des Bundesverfassungsgerichts sicherzustellen.

Anlage 3 (zu 3.1.8)

Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 15. April 1993

zum Entwurf eines Gesetzes zur Umsetzung des Föderalen Konsolidierungsprogramms - FKPG -

Der Gesetzentwurf sieht Regelungen vor, die eine mißbräuchliche Inanspruchnahme von Sozialleistungen verhindern sollen und von erheblicher datenschutzrechtlicher Bedeutung sind.

Über die bisher gesetzlich vorgesehene Einzelfallprüfung hinaus würde durch den Gesetzentwurf ermöglicht, daß insbesondere die Daten aller Sozialhilfeempfänger, also auch derjenigen, bei denen kein Anhaltspunkt für falsche Angaben oder Verletzungen von Mitteilungspflichten besteht, ohne weiteres pauschal mit den Datenbeständen der Renten- und der Arbeitslosenversicherung abgeglichen werden. Darüber hinaus soll nach dem Regierungsentwurf der On-line-Abruf von Daten aus einer unbegrenzten Vielzahl von Dateien anderer Verwaltungsbereiche ohne Rücksicht auf die jeweilige Sensibilität dieser Daten möglich sein.

Im Bereich der Arbeitslosenversicherung soll die erst zum 1.1.1993 in Kraft getretene, datenschutzgerechte Vorschrift über die Erhebung von Daten bei Außenprüfungen ohne erkennbaren sachlichen Grund durch eine Vorschrift ersetzt werden, die wichtige Grundsätze des Persönlichkeitsschutzes nicht berücksichtigt.

Im einzelnen weisen die Datenschutzbeauftragten - unter Einbeziehung der Empfehlungen der Ausschüsse des Bundesrates vom 8.4.1993, Drucksache 121/2/93 - auf folgendes hin:

Artikel 9 Nr. 29 (§ 117 Bundessozialhilfegesetz - BSHG -)

1. **§ 117 Abs. 1 BSHG**

   Nach der Begründung zu § 117 Abs. 1 BSHG (Regierungsentwurf) - allerdings nicht nach dem Wortlaut der Vorschrift - soll der Leistungsmißbrauch über einen Datenabgleich mit der Bundesanstalt für Arbeit (BA) und der gesetzlichen Rentenversicherung aufgedeckt werden. Irgendein Anlaß für diesen Datenabgleich muß nicht gegeben sein. Ein solches, die Glaubwürdigkeit aller Sozialhilfeempfänger in Zweifel ziehendes Vorgehen ist allenfalls dann verhältnismäßig und damit vertretbar, wenn verifizierbare Erkenntnisse darüber vorliegen, daß ein erheblicher Anteil der Sozialhilfeempfänger der schon jetzt bestehenden Verpflichtung, den Sozialhilfeträgern Leistungen der BA und das Eingehen von Beschäftigungsverhältnissen mitzuteilen, nicht nachkommt. Der Gesetzesbegründung lassen sich solche Feststellungen nicht entnehmen.

Die Zwecktauglichkeit dieses Abgleichs erscheint zudem zweifelhaft, da etwa Nebeneinkünfte von Sozialhilfeempfängern, für die keine Sozialabgaben entrichtet wurden, auch der Sozialversicherung nicht bekannt sind.

Die Ausschüsse des Bundesrates haben nunmehr empfohlen, von dem pauschalen Datenabgleich abzusehen, sowie eine Zweckbindungs- und eine Löschungsregelung einzuführen. Die Datenschutzbeauftragten begrüßen diese Empfehlung.

2. **§ 117 Abs. 2 BSHG**

Die Bundesratsausschüsse haben empfohlen, § 117 Abs. 2 BSHG des Regierungsentwurfs, insbesondere wegen der Unklarheiten des Gesetzestextes, zu streichen. In der Begründung verweisen sie auf die Regelungen von Datenübermittlungen aus anderen Verwaltungsbereichen in den jeweiligen bereichspezifischen Vorschriften.

Die Datenschutzbeauftragten begrüßen die Empfehlungen der Bundesratsausschüsse schon wegen der fehlenden Normenklarheit des Regierungsentwurfs.

Artikel 13 Nr. 20 (§§ 150 a und 150 b Arbeitsförderungsgesetz - AFG -)

a) Es ist unverständlich, daß die Neuregelung der §§ 19 a und 132 a Abs. 1 a AFG, die erst am 1.1.1993 in Kraft getreten sind, schon wenige Monate danach wieder aufgehoben und durch neue Regelungen ersetzt werden sollen. Gegen eine solche Notwendigkeit spricht auch die einschlägige Presseinformation der BA vom 18.3.1993, in der betont wird,

„... die von Jahr zu Jahr zunehmende Zahl der aufgedeckten Verstöße zeige, daß das rechtliche und administrative Instrumentarium immer besser greife."

b) Entgegen der in den §§ 132 a Abs. 1 a und 19 a AFG enthaltenen Regelung sieht § 150 a AFG keinen Datenkatalog dahingehend mehr vor, welche Daten im Rahmen der Prüfungen zulässigerweise erhoben werden können. Weil in den in § 150 a AFG zu regelnden Fällen Unverdächtige in den Datenabgleich einbezogen werden, ist es erforderlich, den Eingriff auf das unbedingt notwendige Maß zu beschränken. Dazu ist weiterhin erforderlich, daß im ersten Schritt nur die hierfür unbedingt notwendigen Daten abgeglichen werden. Der Datenkatalog ist um so dringender, als die neue Vorschrift über Außenprüfungen nach § 150 a AFG eine Erweiterung gegenüber den bisherigen Vorschriften bringt.

c) Es ist ferner unerläßlich, daß die erhobenen Daten auch weiterhin der - derzeit in § 132 a Abs. 1 a Satz 3 AFG normierten - Zweckbindung unterliegen.

d) § 150 a Abs. 5 AFG erweitert die nach dem geltenden Recht bestehende Auskunftspflicht von Arbeitgeber und Arbeitnehmer auf **jedermann**. Dies erscheint überzogen, nachdem im Bereich der Datenerhebung für Steuerzwecke eine Auskunftspflicht Dritter nur besteht, „wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziel führt oder keinen Erfolg verspricht" (§ 93 Abs. 1 AO).

Anlage 4 (zu 3.2.4)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993

zu regelmäßigen Datenübermittlungen an die öffentlich-rechtlichen Rundfunkanstalten und die Gebühreneinzugszentrale (GEZ)

(gegen die Stimme Bayerns und bei Stimmenthaltung Sachsens)

Die öffentlich-rechtlichen Rundfunkanstalten drängen seit langem auf die Schaffung einer Rechtsgrundlage für die regelmäßige Übermittlung von Meldedaten aller Einwohner an die gemeinsame Gebühreneinzugszentrale (GEZ). Sie verweisen dazu auf bereits bestehende Regelungen in den Ländern Hessen und Nordrhein-Westfalen. Auf Bitten der Konferenz der Regierungschefs der Länder hat deshalb nunmehr der zuständige Arbeitskreis der Innenministerkonferenz einen Musterentwurf für eine bundesweite Lösung im Melderecht erarbeitet. Der Entwurf sieht vor, daß künftig alle Meldebehörden in der Bundesrepublik im Fall der Anmeldung, Abmeldung oder des Todes eines volljährigen Einwohners bis zu acht Kerndaten an die GEZ übermitteln dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen eine derartige Regelung insbesondere aus folgenden Gründen ab:

Die Regelung könnte im Ergebnis zu einem bundesweiten Melderegister bei Volljährigen führen. Sie könnte außerdem gegen das verfassungsrechtlich garantierte Verhältnismäßigkeitsprinzip verstoßen. Den Rundfunkanstalten stünde möglicherweise der unkontrollierte Zugriff auf Millionen personenbezogener Daten volljähriger Einwohner der Bundesrepublik zu, obwohl es für die Rundfunkanstalten nur von Interesse ist, welcher Einwohner bei ihnen gebührenpflichtig ist und bislang seine Gebührenpflicht nicht angemeldet hat. Das vorgesehene generelle Übermittlungsverfahren kennt keine Unterscheidung zwischen erforderlichen und nicht erforderlichen Daten, sondern überläßt diese Unterscheidung der GEZ. Über die Frage, ob ein Volljähriger überhaupt gebührenpflichtig ist, geben die Meldedaten keine Auskunft. Das muß nach wie vor im herkömmlichen Verfahren durch Befragung ermittelt werden.

Die Datenschutzbeauftragten des Bundes und der Länder sind bereit, an geeigneten und verfassungskonformen Lösungen der Landesregierung zur Sicherung des Gebührenaufkommens der Rundfunkanstalten mitzuwirken.

Anlage 5 (zu 3.2.6 und 5.6.5)

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994

Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen

Angesichts der aktuellen Diskussion über die innere Sicherheit weisen die Datenschutzbeauftragten des Bundes und der Länder darauf hin, daß umfangreiche polizeiliche Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten, insbesondere im technischen Bereich, gesetzlich verankert worden sind.

Zum Kreis der Betroffenen zählen dabei nicht nur Personen, gegen die Verdachtsgründe vorliegen, sondern auch nichtverdächtige Kontakt- und Begleitpersonen und Unbeteiligte, deren Schutz nach Auffassung der Datenschutzbeauftragten besonders wichtig ist.

Vor diesem Hintergrund schlagen die Datenschutzbeauftragten vor, den derzeitigen Erkenntnisstand über die Erforderlichkeit polizeilicher Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten sowie ihre Auswirkungen auf die Rechte der Betroffenen durch folgende Maßnahmen zu verbessern:

1. Die Datenschutzbeauftragten teilen die von einigen Innenministern vertretene Auffassung, daß bloße Angaben über Einsatzzahlen der besonderen Befugnisse zur Datenerhebung nur einen begrenzten Aussagewert haben. Aufschluß über die tatsächliche Praxis, ihre Erforderlichkeit und Verhältnismäßigkeit läßt sich nur durch Überprüfung und Auswertung der einzelnen Einsätze gewinnen. Hierzu müssen unter Beteiligung der Datenschutzbeauftragten und der Wissenschaft, insbesondere der Kriminologie und des Polizeirechts, objektive und nachprüfbare Auswertungskriterien entwickelt werden.

   Die Datenschutzbeauftragten begrüßen daher die Initiative für eine sog. Rechtstatsachensammlung, die Erhebungen zu polizeilichen Ermittlungsmethoden und Eingriffsbefugnissen durchführen soll. Sie schlagen vor, in diese Rechtstatsachensammlung insbesondere Angaben über den Anlaß einer Datenerhebung mit besonderen Mitteln, die Örtlichkeit und die Dauer der Maßnahme, den Umfang der überwachten Gespräche, den betroffenen Personenkreis sowie die Anzahl der ermittelten, verurteilten, aber auch der entlasteten Personen einzubeziehen. Derartige Aufstellungen wären nicht nur für elektronische Überwachungsmethoden, sondern auch für Observationen, den Einsatz verdeckter Ermittler und V-Personen sowie für Rasterfahndungen denkbar.

2. Einige Polizeigesetze verpflichten dazu, zu überprüfen, ob es notwendig ist, bestehende Dateien weiterzuführen oder zu ändern. Dabei soll nicht

nur darauf eingegangen werden, ob die Anwendungen, d. h. die Dateien, weiterhin erforderlich sind, sondern auch auf ihren Nutzen sowie auf ihre Schwachstellen und Mängel. Ferner sind Vorschläge zu machen, wie festgestellte Defizite beseitigt oder minimiert werden können.

3. Die Datenschutzbeauftragten gehen davon aus, daß sie bei den Überlegungen zur Rechtstatsachensammlung rechtzeitig beteiligt und die jeweiligen Materialien und Zwischenergebnisse mit ihnen erörtert werden.

Anlage 6 (zu 4.2.4)

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. August 1994

zu dem Vorschlag der Kommission der Europäischen Union für eine Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, daß die Europäische Union eine allgemeine Regelung für die Gemeinschaftsstatistik trifft, weisen allerdings darauf hin, daß die datenschutzrechtliche Entwicklung bei der Europäischen Union mit dem Aufbau der europäischen Statistik keineswegs Schritt gehalten hat.

Sie stellen mit Besorgnis fest, daß der vorliegende Vorschlag einer EG-Statistikverordnung die nationalen datenschutzrechtlichen Grundsätze und wesentliche Standards des Statistikrechts weitgehend nicht berücksichtigt. Sie fordern daher zur Wahrung des Rechts der Betroffenen auf informationelle Selbstbestimmung mit Nachdruck, daß die Bundesregierung ihre Bedenken gegen diesen Vorschlag geltend macht und diese bei den Beratungen auf europäischer Ebene zum Tragen bringt.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen ausdrücklich den Beschluß des Deutschen Bundesrates vom 8. Juli 1994 (BR-Drs. 283/94 - Beschluß -).

Gegen den vorgelegten Vorschlag einer Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik (EG-Statistikverordnung) erheben sie insbesondere die folgenden datenschutzrechtlichen Bedenken:

1. In Art. 1 sollte als die zuständige Gemeinschaftsdienststelle unmißverständlich das Statistische Amt der Europäischen Gemeinschaften (EUROSTAT) bestimmt werden, weil die erforderlichen rechtlichen, administrativen, technischen und organisatorischen Maßnahmen - insbesondere zur Sicherung der Zweckbindung der zu statistischen Zwekken erhobenen Daten sowie zur Wahrung der statistischen Geheimhaltung - bei dieser Stelle bereits aufgrund der EG-Übermittlungsverordnung

1588/90 vom 11. Juni 1990 getroffen werden können. Eine jederzeit revidierbare Organisationsentscheidung der Kommission darüber, welche Dienststelle der Europäischen Union für statistische Aufgaben zuständig ist, birgt dagegen die Gefahr, daß Daten an unterschiedliche Stellen der Kommission zu unterschiedlichen Zwecken übermittelt werden.

Zugleich sollte EUROSTAT zumindest einen der Selbständigkeit der Statistischen Ämter in der Bundesrepublik Deutschland vergleichbaren organisationsrechtlichen Status erhalten, der die unter dem Gesichtspunkt der Objektivität und Neutralität gebotene Eigenständigkeit bei der Aufgabenerfüllung garantiert. Dies könnte anläßlich der für 1996 vorgesehenen Revision des Vertrages über die Europäische Union geschehen.

2. Das mehrjährige statistische Programm sollte nicht wie in Art. 3 vorgesehen von der Kommission beschlossen werden. Die grundlegenden Entscheidungen über die Bürger belastende Datenerhebungen sollten dem Rat mit Zustimmung des Europäischen Parlaments vorbehalten bleiben. Dabei sollte der Planungscharakter des Programms in den Vordergrund gestellt werden.

3. Art. 5 sollte festlegen, daß statistische Einzelmaßnahmen durch einen Rechtsakt gemäß dem Verfahren nach Art. 189 b EG-Vertrag angeordnet werden. Dies gilt auch für die statistische Auswertung von Daten, die bei den administrativen Stellen bereits vorliegen (sog. Sekundärstatistik). Die im Vorschlag vorgesehene generelle Befugnis der Kommission, statistische Einzelmaßnahmen zu regeln, ist viel zu weitgehend.

4. Die in Art. 12 vorgesehene Übertragung der Befugnis zur Organisation der Verbreitung der statistischen Daten auf die Kommission widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag, aus dem folgt, daß grundsätzlich die Mitgliedstaaten nach ihrem nationalen Recht zur Verbreitung der statistischen Daten zuständig sind. Ferner sollte in Art. 12 festgelegt werden, daß an Stellen außerhalb der statistischen Gemeinschaftsdienststelle nur nicht-vertrauliche statistische Daten übermittelt werden dürfen.

5. Der in Art. 13 gegenüber der Definition in der EG-Übermittlungsverordnung 1588/90 neu definierte Begriff „statistische Geheimhaltung" muß präzisiert werden. Dazu gehört insbesondere, daß festgelegt wird, unter welchen Voraussetzungen statistische Daten vertraulich sind und nicht nur als vertraulich gelten. Dies gilt um so mehr, als im Verordnungsvorschlag dieser Begriff nicht nur in Art. 13, sondern auch in Art. 9 Abs. 2 - allerdings mit einem anderen Begriffsinhalt - definiert wird. Der Begriff „statistische Geheimhaltung" sollte an einer Stelle in der Verordnung und so definiert werden, daß er Art. 2 Nr. 1 der EG-Übermittlungsverordnung 1588/90 und damit den derzeit geltenden nationalen Begriffsbestimmungen entspricht. Dies stände auch im Einklang mit dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag.

6. Gemäß dem Grundsatz der Subsidiarität sollte - ebenso wie die Befugnis zur Verbreitung statistischer Ergebnisse (Art. 11 Abs. 1) - auch die Festlegung der Zuständigkeit für die Durchführung der statistischen Einzelmaßnahmen (Art. 7) den Mitgliedstaaten überlassen bleiben.

7. Auch die in Art. 16 vorgesehene generelle Zugangsregelung einzelstaatlicher Stellen und der Gemeinschaftsdienststelle zu Registern der Verwaltung widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag. Dieser gebietet hier, daß - jedenfalls grundsätzlich - die Mitgliedstaaten zu bestimmen haben, in welcher Weise sich die für die Erstellung der Gemeinschaftsstatistik zuständigen nationalen Stellen Daten beschaffen. Damit ist aber nicht zu vereinbaren, daß auch Stellen der Kommission unmittelbar Zugang zu nationalen Verwaltungsregistern haben sollen.

   Ferner bleibt unklar, ob die nach Art. 16 erhobenen Daten Erhebungs- oder Hilfsmerkmale sein sollen. Im übrigen darf über Art. 16 ein Zugang zu solchen personenbezogenen Daten, die nach nationalem Recht einer besonderen Geheimhaltung, z. B. dem Steuer- oder auch dem Sozialgeheimnis unterliegen, nicht eröffnet werden.

8. Die Regelung des Art. 17 ist mißglückt. Allem Anschein nach soll hier eine weitgehende Ausnahmeregelung von der statistischen Geheimhaltung zugunsten von Forschungsinstituten, einzelner Forscher und von für die Erstellung von Nicht-Gemeinschaftsstatistiken zuständigen Stellen vorgesehen werden, die die Möglichkeit eröffnet, die in diesem Bereich geltenden strengeren nationalen Regelungen zu umgehen. Außerdem würde von der für EUROSTAT geltenden EG-Übermittlungsverordnung 1588/90 abgewichen werden. Art. 17 sollte deshalb so gefaßt werden, daß die nationalen Zugangsregelungen für Einrichtungen mit der Aufgabe der unabhängigen wissenschaftlichen Forschung nicht umgangen werden können.

9. Der Vorschlag der Kommission sieht weder eine alsbaldige Trennung und Aufbewahrung von Erhebungs- und Hilfsmerkmalen noch eine alsbaldige Löschung personenbezogener Hilfsmerkmale vor. In der Bundesrepublik Deutschland dagegen gehören entsprechende Regelungen (vgl. § 12 BStatG) zum Kernbereich des Statistikrechts. Im Volkszählungsurteil hat das Bundesverfassungsgericht ihnen grundrechtssichernde Bedeutung beigemessen.

10. Schließlich fehlt es für die Organe der Europäischen Union noch immer an einer unabhängigen und effektiven Datenschutzkontrollinstanz, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der Europäischen Union in seinen Rechten verletzt zu sein.

Anlage 7 (zu 5.9.6)

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994

zu Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten von Bund und Ländern verfolgen die zunehmende Verwendung von Chipkarten im Gesundheits- und Sozialwesen mit kritischer Aufmerksamkeit.

Chipkarte als gesetzliche Krankenversicherungskarte

Die Krankenversicherungskarte, die bis Ende des Jahres in allen Bundesländern eingeführt sein wird, darf nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten. Die Datenschutzbeauftragten überprüfen, ob

- die Krankenkassen nur die gesetzlich zulässigen Daten auf den Chipkarten speichern

  und

- die Kassenärztlichen Vereinigungen dafür sorgen, daß nur vom Bundesamt für Sicherheit in der Informationstechnik zertifizierte Lesegeräte und vom Bundesverband der Kassenärztlichen Vereinigungen geprüfte Programme eingesetzt werden.

Chipkarte als freiwillige Gesundheitskarte

Sogenannte „Gesundheitskarten", etwa „Service-Karten" von Krankenversicherungen und privaten Anbietern, „Notfall-Karten", „ Apo(theken)-Cards" und „Röntgen-Karten" werden neben der Krankenversicherungskarte als freiwillige Patienten-Chipkarte angeboten und empfohlen. Während die Krankenversicherungskarte nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten darf, kann mit diesen „Gesundheitskarten" über viele medizinische und andere persönliche Daten schnell und umfassend verfügt werden.

Gegenüber der konventionellen Ausweiskarte oder einer Karte mit einem Magnetstreifen ist die Chipkarten-Technik ungleich komplexer und vielfältig nutzbar. Damit steigen auch die Mißbrauchsgefahren bei Verlust, Diebstahl oder unbemerktem Ablesen der Daten durch Dritte. Anders als bei Ausweiskarten mit Klartext können Chipkarten nur mit technischen Hilfsmitteln gelesen werden, die der Betroffene in der Regel nicht besitzt. So kann er kaum kontrollieren, sondern muß weitgehend darauf vertrauen, daß der Aussteller der Karte und sein Arzt nur die mit ihm vereinbarten Daten im Chip speichern, das Lesegerät auch wirklich alle gespeicherten Daten anzeigt und der Chip keine oder nur eindeutig vereinbarte Verarbeitungsprogramme enthält.

Die Freiwilligkeit der Entscheidung für oder gegen die Gesundheitskarte mit Chipkarten-Technik ist in der Praxis bisweilen nicht gewährleistet. So wird ein faktischer Zwang auf die Entscheidungsfreiheit des Betroffenen ausgeübt, wenn der Aussteller - etwa ein Krankenversicherungsunternehmen oder eine

Krankenkasse - mit der Einführung der Chipkarte das bisherige konventionelle Verfahren erheblich ändert, z. B. den Schriftwechsel erschwert oder den Zugang zu Leistungen Karten-Inhabern vorbehält bzw. erleichtert.

So stellt beispielsweise eine Kasse ihren Mitgliedern Bonuspunkte in Aussicht, wenn sie auf sog. Aktionstagen der Kasse Werte wie Blutzucker, Sauerstoffdynamik, Cholesterol sowie weitere spezielle medizinische Daten ohne ärztliche Konsultation messen und auf der Karte speichern und aktualisieren lassen. In Abhängigkeit von der Veränderung dieser Werte wird von der Kasse gegebenenfalls ein Arztbesuch empfohlen. Die Vergabe solcher Bonuspunkte widerspricht dem Prinzip der Freiwilligkeit bei der Erhebung der Daten für die Patienten-Chipkarte. Der Effekt wird noch verstärkt, indem die Kasse die „Möglichkeit einer Beitragsrückerstattung" in Aussicht stellt. Die Datenschutzbeauftragten des Bundes und der Länder sehen in dieser Art der Anwendung der Chipkarten-Technik das Risiko eines Mißbrauchs, solange der Inhalt und die Nutzung der Daten nicht mit den zuständigen Fachleuten - wie den Medizinern - und den Krankenkassen abgestimmt ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält für den Einsatz und die Nutzung freiwilliger Patienten-Chipkarten zumindest - vorbehaltlich weiterer Punkte - die Gewährleistung folgender Voraussetzungen für erforderlich:

- Die Zuteilung einer Gesundheitskarte und die damit verbundene Speicherung von Gesundheitsdaten bedarf der schriftlichen Einwilligung des Betroffenen. Er ist vor der Erteilung der Einwilligung umfassend über Zweck, Inhalt und Verwendung der angebotenen Gesundheitskarte zu informieren.
- Die freiwillige Gesundheitskarte darf nicht - etwa durch Integration auf einem Chip - die Krankenversichertenkarte nach dem Sozialgesetzbuch verdrängen oder ersetzen.
- Die Karte ist technisch so zu gestalten, daß für die einzelnen Nutzungsarten nur die jeweils erforderlichen Daten zur Verfügung gestellt werden.
- Der Betroffene muß von Fall zu Fall frei und ohne Benachteiligung - z. B. gegenüber dem Arzt, der Krankenkasse oder der Versicherung - entscheiden können, die Gesundheitskarte zum Lesen der Gesundheitsdaten vorzulegen und ggf. den Zugriff auf bestimmte Daten zu beschränken. Er muß ferner frei entscheiden können, wer welche Daten in seinen Datenbestand übernehmen darf. Der Umfang der Daten, die gelesen oder übernommen werden dürfen, ist außerdem durch die gesetzliche Aufgabenstellung bzw. den Vertragszweck der Nutzer beschränkt.
- Der Kartenaussteller muß sicherstellen, daß der Betroffene jederzeit vom Inhalt der Gesundheitskarte unentgeltlich Kenntnis nehmen kann.
- Der Betroffene muß jederzeit Änderungen und Löschungen der gespeicherten Daten veranlassen können.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dafür aus, daß der Gesetzgeber dies durch bereichspezifische Rechtsgrundlagen sicherstellt.

Anlage 8 (zu 5.15.1)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993

zum Integrierten Verwaltungs- und Kontrollsystem (InVeKoS)

Die vom Ministerrat der EG 1992 beschlossene Reform der gemeinsamen Agrarpolitik sieht die Angleichung der gemeinschaftlichen Preise für bestimmte Kulturpflanzen an den Weltmarkt vor und gewährt auf Antrag als Ausgleich für die dadurch bedingten Einkommenseinbußen flächen- und tierbezogene Zuwendungen an die Erzeuger. Zur Verhinderung einer mißbräuchlichen Verwendung von Fördermitteln hat die EG die Mitgliedstaaten dabei zur Einführung eines „Integrierten Verwaltungs- und Kontrollsystem (InVeKoS)" verpflichtet. Diese haben danach integrierte Datenbanken mit Angaben über Flurstücke, deren kulturartige Nutzung sowie den Tierbestand einzurichten und in einem Mindestumfang entsprechende Kontrollen durchzuführen.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder hat die EG mit dem „Integrierten Verwaltungs- und Kontrollsystem" den Landwirtschaftsverwaltungen der Länder ein Überwachungssystem verordnet, das dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot, widersprechen kann. Insbesondere legt das EG-Recht für die Kontrolldichte nur ein Mindestmaß an Kontrollen, jedoch keine Obergrenze fest.

Zur Vermeidung unverhältnismäßiger Einschränkungen des informationellen Selbstbestimmungsrechts der betroffenen Landwirte fordern daher die Datenschutzbeauftragten des Bundes und der Länder,

- ortsunabhängige Überwachungsmöglichkeiten (Fernerkundung mittels Satellit oder Flugzeug) nicht für eine flächendeckende Totalüberwachung einzusetzen, sondern auf den von der EG geforderten Stichprobenumfang zu beschränken;
- bei der Nutzung des Kontrollsystems InVeKoS und der darin gespeicherten personenbezogenen Daten den Grundsatz der Verhältnismäßigkeit und insbesondere der Zweckbindung zu beachten;
- nur dezentrale Datenbanken in den einzelnen Bundesländern einzurichten (keine Euro- oder Zentraldatenbank über Landwirte!), und an zentrale Datenbanken keine personenbezogenen Daten zu übermitteln;
- zu beachten, daß die EG-Verordnungen zu InVeKoS keine Rechtsgrundlage für eine Erweiterung der Nutzung enthalten (z. B. zu Kontrollzwecken bei anderen landwirtschaftlichen Förderungsmaßnahmen oder außerhalb des landwirtschaftlichen Bereichs, z. B. zur Besteuerung).

Stichwortverzeichnis

Die fettgedruckten Zahlen weisen auf den jeweiligen Tätigkeitsbericht, die übrigen Zahlen auf die Seiten hin.

B

C

G

H