# Der Landesbeauftragte für den Datenschutz Nordrhein-Westfalen

# 11. Tätigkeitsbericht

# Elfter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Nordrhein-Westfalen

für die Zeit vom 1. Januar 1991
bis zum 31. Dezember 1992

Herausgeber: Der Landesbeauftragte
für den Datenschutz Nordrhein-Westfalen
Reichsstraße 43, 4000 Düsseldorf 1
ISSN 0179-2431
Druck: satz+druck gmbh, Düsseldorf

Gedruckt auf chlorfrei gebleichtem Papier

# Gliederung

## Anlagen

# 1. Vorbemerkung

Die Ausstattung der Behörden und öffentlichen Einrichtungen in Nordrhein-Westfalen mit moderner Informations- und Kommunikationstechnik setzt sich beschleunigt fort. Der PC am Arbeitsplatz, die Dezentralisation der automatisierten Datenverarbeitung und ihre zunehmende Vernetzung sind die Stichworte für diese Entwicklung. Damit stellen sich nicht nur immer wieder neue Probleme, sondern es wird die noch wachsende Bedeutung des Datenschutzes deutlich. Eine spezielle Verankerung des Rechtes eines jeden auf Schutz seiner personenbezogenen Daten im Grundgesetz liegt daher heute näher als je zuvor, auch wenn das Bundesverfassungsgericht bekanntlich festgestellt hat, daß sich schon aus den Artikeln 1 und 2 des Grundgesetzes das Menschenrecht auf informationelle Selbstbestimmung ergibt. Für das Land Nordrhein-Westfalen muß jedenfalls positiv vermerkt werden, daß seine Landesverfassung das Grundrecht auf Datenschutz bereits seit 1978 festgeschrieben hat.

Die Öffnung der Grenzen, besonders aber die Schaffung des europäischen Binnenmarktes haben großen Einfluß auf die Belange des Datenschutzes. Es ist jetzt schon abzusehen, daß sich daraus auch Veränderungen in unserem Datenschutzrechtssystem ergeben werden. Im Zuge dieser Entwicklung wird es darauf ankommen, gemeinsame europäische Regelungen auf möglichst hohem Niveau zu finden. Die Mitgliedstaaten müssen weiterhin in der Lage sein, den nationalen Besonderheiten – etwa durch strengere Vorschriften – Rechnung zu tragen.

In der Datenschutzgesetzgebung bestehen nach wie vor erhebliche Lücken. Es fehlen bereichspezifische gesetzliche Regelungen vor allem im Justizbereich, aber beispielsweise auch im Schulwesen und im Gesundheitswesen. Soweit gesetzgeberische Initiativen ergriffen werden, ist eine Tendenz zu oft weitreichenden Regelungen erkennbar, durch die das Recht auf informationelle Selbstbestimmung vermehrt eingeschränkt wird. Als Beispiel sei hingewiesen auf die Gesetzgebung zur Bekämpfung der organisierten Kriminalität – wobei dieser Begriff schon unscharf ist – und das in diesem Rahmen immer wieder geforderte verdeckte Abhören und Aufzeichnen des gesprochenen Wortes in und aus Privatwohnungen (vgl. unten S. 31).

Besorgniserregend ist, mit welchem Nachdruck auch maßgebliche Behördenvertreter in diesem Zusammenhang von „überzogenem Datenschutz" sprechen. In Zeitungsartikeln wird über einen „Luxus an Individualrechten" philosophiert, den wir uns „heute nicht mehr leisten können". Der stellvertretende Leiter eines in Nordrhein-Westfalen gelegenen Zollfahndungsamtes wird mit den Worten zitiert: „Wir müssen mal etwas weg von diesen Verbrecherschutzgesetzen". Konkrete Nachweise dafür, inwiefern Datenschutzregelungen die Verbrechensbekämpfung ernstlich am Erfolg hindern, bleiben bei solchen Vorwürfen durchweg aus.

Natürlich erfordert der Datenschutz mitunter schwierige Lernprozesse und organisatorische Vorkehrungen oder Umstellungen. Letztlich dient dies aber

dem verfassungsmäßig vorgegebenen Ziel, die Menschenwürde zu achten und jedem einen garantierten Freiraum zu erhalten, in den nur eingegriffen werden darf, wenn es im überwiegenden Allgemeininteresse wirklich erforderlich ist. Im Rechtsstaat sind nicht alle Mittel zulässig, die den Behörden bei der Aufgabenerfüllung nützlich sein können.

In meinem 10. Tätigkeitsbericht hatte ich die Lage des Datenschutzes mit einem großen Haus verglichen, das schon bewohnt wird, gleichzeitig aber auch noch Baustelle ist. Es ist zunehmend darauf zu achten, daß keine Schwachstellen und Risse in das Bauwerk kommen und vorhandene Lücken geschlossen werden; denn wenn es nachhaltig hereinregnet, kommt allzu leicht der Schwamm ins Haus.

Der nachfolgende Bericht beschreibt zunächst allgemein das Tätigwerden meiner Dienststelle im Berichtszeitraum. Sodann werden in besonderen Abschnitten die Aufnahme eines speziellen Grundrechts auf Datenschutz in das Grundgesetz und der grenzüberschreitende Datenverkehr insbesondere auf europäischer Ebene behandelt. In dem Abschnitt über den Datenschutz in einzelnen Bereichen werden in einer Auswahl die vielfältigen Datenschutzprobleme dargestellt, mit denen ich mich im Berichtszeitraum sowohl im Rahmen der Vorbereitung von gesetzlichen Regelungen und von Verwaltungsvorschriften als auch im alltäglichen Verwaltungsgeschehen befaßt habe. Fragen der technischen und organisatorischen Seite des Datenschutzes, vor allem der Datensicherheit, werden im letzten Abschnitt abgehandelt. Das Stichwortverzeichnis gibt Hinweise nicht nur auf den vorliegenden, sondern auch auf meinen 9. und 10. Tätigkeitsbericht.

Den Mitarbeiterinnen und Mitarbeitern meiner Dienststelle danke ich für ihren engagierten und kenntnisreichen Einsatz für die Belange des Datenschutzes und die fundierte Mitwirkung beim Zustandekommen dieses Berichts.

# 2. Allgemeines

## 2.1 Schwerpunkte der Tätigkeit

Die Bearbeitung der zahlreichen **Eingaben** von Bürgerinnen und Bürgern bildete erneut einen Schwerpunkt meiner Tätigkeit. Neben den schriftlichen Eingaben erreichten mich im Berichtszeitraum vermehrt telefonische Auskunftsersuchen. Themenschwerpunkte wie die Meldedatenübermittlung an die GEZ, die Ermittlung des Elternbeitrages für Kindergärten sowie die Erhebung von Einkommens- und Vermögensdaten nicht unterhaltspflichtiger Ehegatten durch die Sozialämter waren für mich besonderer Anlaß für einen intensiven Gedankenaustausch mit den betroffenen Stellen. Die im Einzelfall vorgetragenen Bedenken, Hinweise und Anregungen der Bürgerinnen und Bürger boten mir breite Argumentationsmöglichkeiten. Sie erleichterten mir das Eintreten für eine datenschutzgerechte Lösung, bisweilen allerdings erst gegen zunächst nachhaltigen Widerstand der betroffenen Stellen.

Erfreulicherweise ist andererseits auch die Zahl an mich gerichteter **Beratungsersuchen** öffentlicher Stellen, die selbst daran interessiert waren, datenschutzrechtlich schwierige Fragen schon frühzeitig mit mir abzuklären, gestiegen.

Einen weiteren Schwerpunkt meiner Tätigkeit in den letzten beiden Jahren bildeten **Stellungnahmen** zu einer Vielzahl von Gesetz- und Verordnungsentwürfen auf Bundes- und Landesebene. Darunter fielen u. a. das Verfassungsschutzgesetz, die Gemeindeordnung, das Melderechtsrahmengesetz, das Gesetz über Tageseinrichtungen für Kinder, das Gesundheitsdatenschutzgesetz, das Sechste Gesetz zur Änderung dienstrechtlicher Vorschriften, die Abgabenordnung, das Umweltinformationsgesetz sowie die Gewerbeordnung. Nähere Ausführungen zu den dabei zum Teil aufgetretenen Schwierigkeiten enthalten die folgenden Abschnitte. Außerdem habe ich gegenüber dem Landtag Nordrhein-Westfalen Bedenken und Anregungen zu datenschutzrechtlich bedeutsamen Themen wie dem Lauschangriff, der Datenübermittlung der Einwohnermeldeämter an die GEZ, dem Gesetz über Tageseinrichtungen für Kinder sowie dem Datenschutz in Krankenhäusern vorgetragen.

Darüber hinaus wurden im Berichtszeitraum zahlreiche **Kontroll-, Beratungs- und Informationsbesuche** vor Ort durchgeführt. So wurden u. a. Einwohnermeldeämter, Polizeibehörden, Gesundheitsämter, Hochschulen, Schulen, Finanzämter, Straßenverkehrsämter sowie kommunale Datenverarbeitungszentralen aufgesucht.

Einem Teil dieser Besuche lag eine geänderte Informations-/Kontrollpraxis insoweit zugrunde, als Gegenstand meiner Feststellungen ein bestimmter Sachverhalt war, der in einem Querschnittsvergleich bei mehreren gleichartigen Behörden jeweils an einem Tag gezielt überprüft wurde. Die Behörden waren zuvor über den Zeitpunkt meines Besuches und den Schwerpunkt der Prüfung unterrichtet worden. Der Besuch endete mit der Erörterung der

Ergebnisse im Rahmen eines Abschlußgespräches. Dadurch konnte der Austausch schriftlicher Informationen erheblich reduziert werden. Einigen Stellen wurde eine Kontrollmitteilung übersandt, teilweise wurde eine schriftliche Stellungnahme der Behörde vereinbart.

Die dargestellte Kontrollpraxis war für beide Seiten von Vorteil. Zum einen ermöglichte sie fundierte Erkenntnisse hinsichtlich des untersuchten Sachverhalts. Soweit neue Verwaltungsvorschriften geschaffen bzw. vorhandene ergänzt werden sollten, war es mir möglich, vielfältige Argumentationshilfen zu geben. Die Beschränkung auf einen Kontrollschwerpunkt ermöglichte mir außerdem, meine Präsenz vor Ort auf eine größere Anzahl meiner Kontrolle unterliegender Stellen zu erstrecken. Der Umstand, daß der Informationscharakter des zuvor bekannt gegebenen Kontrollgegenstandes im Vordergrund des Besuches stand, wirkte sich positiv auf die Gesprächsatmosphäre aus. Bei zahlreichen Behörden stieß ich auf großes Interesse und die Bereitschaft, mich in meinen Anliegen zu unterstützen. Allerdings würde ich es begrüßen, wenn auch die in meinen Tätigkeitsberichten gegebenen Hinweise und Empfehlungen in stärkerem Maße von den betroffenen Stellen wahrgenommen und beachtet werden.

## 2.2 Durchsetzungsmöglichkeiten

Im allgemeinen wird dem Datenschutz von den öffentlichen Stellen im Rahmen der Aufgabenerfüllung zunehmende Aufmerksamkeit eingeräumt. Verfeinerte Datenschutzvorschriften und ein im Laufe der Jahre kontinuierlich gewachsenes Datenschutzbewußtsein tragen wesentlich dazu bei. Deutliches Zeichen hierfür sind die vielen Beratungsersuchen aus den Verwaltungen bei mir, die oft auch mit praxisgerechten Verbesserungsvorschlägen verbunden sind. Besonders positive Entwicklungen lassen sich bei Behörden und Einrichtungen feststellen, die eine wirkungsvolle interne Datenschutzkontrolle eingerichtet haben. Zur Vervollständigung des Bildes muß allerdings auch gesagt werden, daß im Berichtszeitraum wieder in großer Anzahl Datenschutzverstöße aufgetreten sind.

Es gibt aber auch manche Problemfelder, in denen der notwendige Fortschritt des Datenschutzes seit langer Zeit verzögert wird. In einzelnen Fällen sind meinen Bemühungen um die Durchsetzung des informationellen Selbstbestimmungsrechts sogar Hindernisse in den Weg gestellt worden.

So muß festgestellt werden, daß datenschutzgerechte Lösungen in einer Reihe von in früheren Tätigkeitsberichten angesprochenen, nach wie vor aktuellen Fragen immer noch ausstehen. Darunter fallen insbesondere

- das Fehlen verfassungskonformer bereichspezifischer Datenschutzregelungen im Justizbereich,
- die illegale Mithörmöglichkeit des Polizeifunks durch beliebige Dritte,
- die Aufzeichnung von Notrufen (110, 112) ohne Rechtsgrundlage,
- der Schutz von Zeugen in Straf- und Bußgeldverfahren,

- die Regelung eines allgemeinen Akteneinsichtsrechts im Sozialleistungsbereich,
- der Umfang der Datenerhebung bei der Aufnahme in das Krankenhaus,
- die Datenerhebung und weitergabe im Rahmen amtsärztlicher Untersuchungen,
- die Auswertung unzulässiger Kontrollmitteilungen durch die Finanzbehörden,
- die zeitlich unbegrenzte Speicherung und Verwertung früherer Straftaten in Führerscheinangelegenheiten.

Die Hindernisse, die meiner Kontrolltätigkeit gelegentlich entgegengestellt wurden, werden an folgenden Beispielen deutlich:

- Das Justizministerium verwehrte es mir in zwei Fällen, rechtzeitig zu datenschutzrechtlich bedeutsamen Vorhaben Stellung zu nehmen, die zwar auf Bundesebene vorbereitet wurden, aber konkret auf Landesebene umzusetzen sind (vgl. unten S. 30/31).

  Die mir gesetzlich auferlegte – auch präventive – Kontrollaufgabe gegenüber der Landesregierung kann ich nur erfüllen, wenn mir rechtzeitig Kenntnis von datenschutzrelevanten Entwürfen gegeben wird. Das gilt auch für bundesgesetzliche bzw. länderübergreifende Vorhaben, deren Vollzug den Landes- und Kommunalbehörden obliegt. Eine frühzeitige Beteiligung ermöglicht mir, ggf. nach Erfahrungsaustausch mit anderen Datenschutzkontrollbehörden auf eine datenschutzgerechte Regelung hinzuwirken und damit zu vermeiden, daß Mängel nachträglich mit oft größerem Aufwand beseitigt werden müssen. Die in diesem Zusammenhang geäußerte Auffassung des Justizministeriums, ich müsse abwarten, bis meine Beratung von den obersten Landesbehörden gewünscht werde, verkennt den Umfang der Kontrollbefugnis des Landesbeauftragten für den Datenschutz.

- Das Ministerium für Arbeit, Gesundheit und Soziales forderte mich im Zusammenhang mit der Ermittlung und Offenbarung der Namen von „streikverdächtigen" Zahnärzten (vgl. unten S. 65/66) energisch auf, es bei seinen (nach meiner Prüfung mit einem Datenschutzverstoß verbundenen) Bemühungen „uneingeschränkt" zu unterstützen und rügte, daß ich mich in dieser Sache unmittelbar an die Krankenkassenverbände gewandt hatte, ohne zunächst das Ministerium zu unterrichten.

  Hierin zeigt sich, daß auch eine oberste Landesbehörde zuweilen die Datenschutzkontrolle hinsichtlich ihrer Aufgaben und Befugnisse nachhaltig verkennt und damit behindert.

- Es gelingt nicht immer, Datenschutzbelange, in denen keine Meinungsverschiedenheit zwischen der Landesregierung und mir besteht, im nachgeordneten Bereich auch durchzusetzen. So haben eine Stadt und ein Kreisgesundheitsamt auf meine Beanstandung erklärt, meiner jeweils mit dem zuständigen Ministerium abgestimmten Rechtsauffassung werde

nicht gefolgt. In einem anderen Fall weigerte sich eine Behörde, mein Auskunftsersuchen, das ich auf Grund einer Eingabe übersandt hatte, zu beantworten, obwohl das zuständige Ministerium hierzu eine ausdrückliche Weisung erteilt hatte.

Wenn es sich hier auch nur um Einzelvorfälle handelt, muß ihnen doch konsequent mit den geeigneten Aufsichtsmitteln nachgegangen werden.

- Meine Kontrolltätigkeit wird aber auch beeinträchtigt, wenn ein Beschäftigter des öffentlichen Dienstes von seinem Vorgesetzten gerügt wird, weil er sich mit datenschutzrechtlichen Bedenken an mich wendet. Nachdem ein Oberstadtdirektor von meiner Einschaltung erfahren hatte, teilte er dem Petenten u. a. mit: „Es fällt negativ auf die Musikschule und damit auf die Stadt zurück, wenn der Datenschutzbeauftragte des Landes als Angehöriger einer fremden Behörde durch Ihre Aussage erfährt, daß Sie als städtischer Mitarbeiter und als Musikpädagoge nicht in der Lage sind, einen einfachen Vordruck auszufüllen und den Zweck von Beurteilungen zu erkennen ... Wenn Sie auch in Zukunft Bedenken haben, an einer Schule zu arbeiten, die ihre Schüler beurteilt, so könnten Sie dieses Problem durch eine Aufgabe Ihres Beschäftigungsverhältnisses lösen."

  Ich sehe im Inhalt dieser Äußerung eine Maßregelung des Betroffenen. Niemand darf deswegen benachteiligt oder gemaßregelt werden, weil er sich an den Landesbeauftragten für den Datenschutz wendet (§ 25 Abs. 2 DSG NW). Ich habe daher dem Schulträger empfohlen, die Maßregelung zu löschen bzw. für den Fall, daß das Schreiben zur Personalakte genommen wurde, diese entsprechend zu bereinigen.

Im übrigen kann ich feststellen, daß in den meisten Fällen der nach wie vor zahlreichen Verstöße gegen datenschutzrechtliche Vorschriften, zu denen es im Berichtszeitraum in der Verwaltungspraxis gekommen ist, meine Empfehlungen angenommen worden sind. In 22 dieser Fälle war allerdings eine Behebung der Mängel entsprechend meinen Empfehlungen nicht sichergestellt, so daß ich vom Mittel der förmlichen Beanstandung Gebrauch machen mußte. Folgende Sachverhalte waren hierbei betroffen:

- Weitergabe von Unterschriftenlisten beschwerdeführender Bürgerinnen und Bürger an andere Behörden und private Dritte,

- ungerechtfertigte Veröffentlichung von Namen und Anschriften betroffener Einzelpersonen in Bekanntmachungen der Tagesordnungen von Ratssitzungen,

- Bekanntgabe der Namen betroffener Bürgerinnen und Bürger trotz fehlender Erforderlichkeit an Rats- und Ausschußmitglieder, Zuhörer öffentlicher Sitzungen und die Presse,

- Bekanntgabe der persönlichen Gründe eines Bürgers, ein Wahlehrenamt nicht zu übernehmen, an die Fraktionen des Rates,

- Einrichtung eines ADV-Verfahrens „Fehlbelegerabgabe/Wohnraumüberwachung" mit automatisiertem Zugriff des Kreises auf die Daten der Einwohnermeldeämter,
- Übermittlung der Verfahrensdaten zur Zahlung einer Geldbuße an gemeinnützige Einrichtungen nach Einstellung des Strafverfahrens,
- Fehlen baulicher Maßnahmen im Standesamt zum Ausschluß des Mithörens Dritter,
- Weigerung einer Kreispolizeibehörde, einem Auskunftsersuchen nach § 26 Abs. 1 DSG NW ausreichend nachzukommen,
- Gewährung von Akteneinsicht in Personalakten und ehrengerichtlichen Verfahrensakten von Rechtsanwälten zur Erstellung einer Doktorarbeit,
- Übermittlung der Namen der Bediensteten an Dritte durch eine unverschlüsselte Zeiterfassungsanlage,
- Fortschreibung der anläßlich der Vorsorgeuntersuchung im Kindergarten erhobenen Daten mit anläßlich weiterer schulärztlicher Untersuchungen erhobenen Daten,
- Aufforderung des Gesundheitsamtes zur Unterrichtung über die auf Grund des Ergebnisses der Vorsorgeuntersuchung im Kindergarten eingeleiteten weiteren Maßnahmen des Hausarztes,
- übermäßige Datenerhebung bei der Bereitstellung eines Kindergartenplatzes,
- Erhebung zweckfremder Angaben im Rahmen der Einschulungsuntersuchung,
- Offenbarung der ärztlichen Schweigepflicht unterliegender Daten durch den Amtsarzt an nicht zu seinen berufsmäßig tätigen Mitarbeitern zählende Sachbearbeiter des Gesundheitsamtes,
- Weiteroffenbarung dem Zweckbindungsgebot unterliegender Sozialdaten aus Sozialgerichtsakten abgeschlossener Verfahren für wissenschaftliche Zwecke,
- Verwendung der den Krankenkassen zu Abrechnungszwecken übermittelten Versichertendaten für Zwecke der aktiven Gesundheitsberatung,
- Offenbarung von Sozialdaten gegenüber einem unberechtigten Dritten,
- unzulässige Erhebung, Erfassung und Offenbarung der Namen an einem sog. Warnstreik beteiligter Zahnärzte,
- unzutreffende Unterrichtung der Eltern über ihre Rechte im Zusammenhang mit der Glaubhaftmachung ihrer Einkommensangaben zur Festsetzung des Kindergartenbeitrages,
- Erhebung und Übermittlung der Daten von Hundekäufern, die ihren Wohnsitz in einer anderen Gemeinde haben,

- Weigerung, die bestehende erhebliche Beeinträchtigung der Datensicherheit bei der Aufbewahrung von Patientendaten früher als in drei bis vier Jahren durch eine bauliche Maßnahme zu beseitigen.

Soweit dem Verstoß gegen datenschutzrechtliche Vorschriften über den Einzelfall hinausgehende Bedeutung zukommt, verweise ich auf die ausführliche Darstellung im nachfolgenden Berichtsteil. Dabei soll allerdings nicht unerwähnt bleiben, daß nach meinem Eindruck in einigen Fällen eine Beanstandung vermeidbar gewesen wäre, wenn nicht die betroffenen Stellen auf Grund teilweise datenschutzfremder Erwägungen auf ihrem Standpunkt beharrt und so eine Beanstandung geradezu herausgefordert hätten.

## 2.3 Öffentlichkeitsarbeit

Öffentlichkeitsarbeit ist für mich eine willkommene Möglichkeit, Ratsuchenden zu helfen und das Datenschutzbewußtsein der Bürgerinnen und Bürger wie auch der öffentlichen Stellen zu festigen. Daher habe ich mich ihr wiederum mit besonderem Interesse gewidmet.

Im Berichtszeitraum erreichten mich zahlreiche Einladungen zur Teilnahme an **Fortbildungs-, Informations- und Diskussionsveranstaltungen**. Zu den Zuhörern gehörten Bürgerinnen und Bürger, die sich für die datenschutzrechtlichen Aspekte aktueller politischer Themen interessierten, Fortbildungsgruppen, denen an einer Einführung in den Datenschutz lag sowie Angehörige bestimmter Berufsgruppen, denen die Ziele des Datenschutzes mit besonderem Bezug auf die jeweils betroffenen Bereiche vermittelt wurden. Angesichts des Gewinns, den beide Seiten aus derartigen Veranstaltungen ziehen, habe ich versucht, dem Interesse im Rahmen der personellen Möglichkeiten meiner Dienststelle nachzukommen.

Die von mir vorgehaltenen **Informationsbroschüren** wurden weiterhin in großer Zahl angefordert. Aufgrund vermehrter Anfragen zum Thema „Datensicherheit" habe ich die entsprechenden Auszüge aus meinen bisherigen Tätigkeitsberichten in einem Sammelband Datensicherheit zusammengefaßt herausgegeben und einem breiten Empfängerkreis zur Verfügung gestellt. Im Hinblick auf die steigende Zahl der Anfragen zur Datensicherheit beim Vernichten von Unterlagen habe ich eine Organisationshilfe „Unterlagenvernichtung" entwickelt, die insbesondere nach ihrer Vorstellung in der Fachpresse einen großen Anklang gefunden hat. Ich freue mich, daß ich zum Thema „Datensicherheit" zahlreiche Anfragen auch von Behördenmitarbeiterinnen und -mitarbeitern, denen die Aufgaben eines internen Datenschutzbeauftragten übertragen wurden, erhielt. Sie erlauben mir, meine Empfehlungen dort anzubringen, wo sie unmittelbar umgesetzt werden können. Gleiches gilt für die Möglichkeit der Veröffentlichung datenschutzrechtlicher Beiträge in Fachzeitschriften, von der ich wiederum Gebrauch gemacht habe.

Themen von aktueller Bedeutung haben außerdem vielfältige Kontakte zu den **Medien** ausgelöst. Insbesondere Datenübermittlungen der Einwohnermeldeämter an die GEZ, der Lauschangriff, die Datenerhebung zwecks Festsetzung der Kindergartenbeiträge, die Einführung der Chipkarte im

Gesundheitswesen, die aktive Gesundheitsberatung durch Krankenkassen, der Arbeitnehmerdatenschutz und die Programmviren waren Gegenstand von Interviews gegenüber Presse, Rundfunk und Fernsehen. Die zahlreichen Eingaben und Anrufe nach Veröffentlichungen belegen, daß gerade die Selbstbestimmung über ihre eigenen Daten wichtiges Anliegen vieler Bürgerinnen und Bürger ist.

## 2.4 Dateienregister

Mit Runderlaß des Innenministeriums vom 12.08.1992 (MBl. NW. 1992 S. 1256) wurden die „Hinweise zur Anmeldung der Dateien beim Landesbeauftragten für den Datenschutz Nordrhein-Westfalen" vom 31.03.1981 (SMBl. NW. 20026) aufgehoben. Dies hat bei den speichernden Stellen des Landesbereichs zu einer erheblichen Verunsicherung geführt. Mehrfach haben mich Anfragen erreicht, bei denen die Anrufer davon ausgingen, daß es nunmehr nicht mehr erforderlich sei, mir **Dateibeschreibungen** vorzulegen.

Nach § 23 Abs. 1 DSG NW ist die speichernde Stelle verpflichtet, dem Landesbeauftragten für den Datenschutz die Beschreibung aller automatisiert geführten Dateien, in denen personenbezogene Daten gespeichert sind, mit den Angaben der Dateibeschreibung (§ 8 Abs. 1) vorzulegen. Der Landesbeauftragte für den Datenschutz führt ein Register dieser Dateien (Dateienregister).

Gemäß § 1 Abs. 1 DRegVO NW ist die Beschreibung automatisiert geführter Dateien meiner Dienststelle unverzüglich vorzulegen. Für bereits zum Register gemeldete Dateien finden die Vorschriften des § 8 Abs. 1 und des § 23 Abs. 1 DSG NW sowie der Verordnung erstmals in Fällen eintretender Veränderungen Anwendung (§ 35 Abs. 3 DSG NW, § 2 Abs. 2 DRegVO NW). Somit hat sich durch die Aufhebung des o. a. Runderlasses an der Verpflichtung der speichernden Stellen, mir die Beschreibung automatisiert geführter Dateien vorzulegen, nichts geändert.

Nach § 7 DSG NW haben die obersten Landesbehörden, die Gemeinden und Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen jeweils für ihren Bereich die Ausführung des Datenschutzgesetzes Nordrhein-Westfalen sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen.

Leider wird diese Verpflichtung von den Adressaten häufig nicht oder nur unvollständig wahrgenommen. Dies zeigt sich zum einen daran, daß die mir vorgelegten Dateibeschreibungen teilweise erhebliche Mängel aufweisen. So war ich etwa gezwungen, einer obersten Landesbehörde nahezu die gesamten Meldungen aus dem nachgeordneten Bereich zurückzusenden. Wegen der Fehlerhaftigkeit war es mir nicht möglich, sie in dieser Form in das von mir geführte Dateienregister aufzunehmen. Die oberste Landesbehörde hatte die Fehlerhaftigkeit der Meldungen nicht bemerkt, obwohl die nachgeordneten Stellen die Meldungen dort zuvor vorgelegt hatten.

In Spalte 6 des Meldevordrucks sind oftmals die einzelnen Arten der Daten, die tatsächlich gespeichert werden, nicht benannt. In Spalte 7 fehlen bei regelmäßig empfangenen Daten vielfach die Angaben zur Herkunft der Daten; es ist teilweise nicht ersichtlich, ob eine regelmäßige Übermittlung stattfindet (Spalte 8). Die Angabe zur Rechtsgrundlage der Datenverarbeitung in Spalte 9 der Meldung ist häufig unrichtig oder fehlt ganz.

Ich empfehle deshalb insbesondere den obersten Landesbehörden, ihren nachgeordneten Behörden Hilfestellungen bei der Abgabe der Meldungen in Form von **Anleitungen** zu geben. Nach meiner Kenntnis ist dies bisher leider nur durch zwei Ministerien geschehen, und auch dort nur für den Bereich jeweils eines Referates.

Auch ist festzustellen, daß noch immer nicht alle speichernden Stellen ihrer gesetzlichen Anzeigepflicht nachgekommen sind. Diese Stellen müssen unverzüglich dafür Sorge tragen, daß noch ausstehende Meldungen zum Dateienregister nachgeholt werden.

Der Umfang des Registers hat weiterhin stark zugenommen. Es war daher erforderlich, das bislang praktizierte manuelle Abhefteverfahren auf eine automatisierte Führung umzustellen. Das Dateienregister wird z. Z. auf ein elektronisches Informations- und Dokumentationssystem übernommen. Die umfangreichen Arbeiten hierzu sind inzwischen angelaufen und werden voraussichtlich noch einen erheblichen Arbeits- und Zeitaufwand erfordern. Nach erfolgter Umstellung werde ich auch in größerem Umfang in der Lage sein, Auswertungen bzw. vergleichende Überprüfungen der zum Dateienregister angemeldeten Dateien vorzunehmen.

## 2.5 Zusammenarbeit im Datenschutz

Die **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** hat im Berichtszeitraum in sechs Sitzungen wiederum eine Reihe wesentlicher aktueller Datenschutzfragen behandelt und u. a. nachstehende Entschließungen und Beschlüsse gefaßt:

- zu dem Vorschlag der EG-Kommission für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten,
- zu Telekommunikation und Datenschutz,
- zum Datenschutz im Recht des öffentlichen Dienstes,
- zur geplanten Datei „Gewalttäter Sport",
- zum Arbeitnehmerdatenschutz,
- zum Grundrecht auf Datenschutz,
- zur Neuregelung des Asylverfahrens,
- zum Datenschutz bei internen Telekommunikationsanlagen,
- zum Gesundheitsstrukturgesetz,
- zur Chipkarte als elektronischer Krankenversicherungskarte,
- zum Lauschangriff.

Die Arbeitskreise Steuerverwaltung und Statistik haben weiterhin unter meinem Vorsitz getagt. Der Arbeitskreis Steuerverwaltung hat sich besonders mit der Novellierung der Abgabenordnung befaßt. Im Arbeitskreis Statistik wurden vorrangig die mit der fortschreitenden politischen und wirtschaftlichen Integration innerhalb der Europäischen Gemeinschaft verbundenen Auswirkungen auf das Recht der amtlichen Statistik in der Bundesrepublik Deutschland, insbesondere das Statistikgeheimnis, behandelt.

Die von der Konferenz der Datenschutzbeauftragten eingerichtete Arbeitsgruppe „Öffentliche Unternehmen" hat sich unter meinem Vorsitz mit der durch die Novellierung des Bundesdatenschutzgesetzes entstandenen Problematik beschäftigt, in welchen Fällen Vereinigungen von juristischen Personen des öffentlichen Rechts, die privatrechtlich organisiert sind, als öffentliche Stellen zu gelten haben. In die Beratung von Abgrenzungskriterien ist auch der „Düsseldorfer Kreis" einbezogen.

Die **Internationale Konferenz** der Datenschutzbeauftragten hat im Oktober 1991 in Straßburg und im Oktober 1992 in Sydney getagt. Im Vordergrund standen bei diesen Zusammenkünften die Bemühungen um eine Verbesserung des Datenschutzes im grenzüberschreitenden Datenverkehr.

# 3. Grundrecht auf Datenschutz

Das Grundrecht auf Datenschutz (Recht auf informationelle Selbstbestimmung) leitet sich aus der in Artikel 1 Abs. 1 des Grundgesetzes garantierten Menschenwürde und dem Grundrecht auf freie Entfaltung der Persönlichkeit (Artikel 2 Abs. 1) ab. Dies ist durch das Bundesverfassungsgericht in seinem Volkszählungsurteil aus dem Jahre 1983 klargestellt und in späteren Entscheidungen immer wieder bestätigt worden. Die im Zuge der Herstellung der deutschen Einheit gebildete Kommission Verfassungsreform befaßte sich u. a. mit der Frage der Aufnahme eigener datenschutzrechtlicher Bestimmungen in das Grundgesetz. Der Arbeitsausschuß 2 der Kommission Verfassungsreform des Bundesrates erarbeitete dazu einen Formulierungsvorschlag für ein eigenständiges Grundrecht auf Datenschutz und eine Verankerung der unabhängigen Datenschutzkontrolle im Grundgesetz.

Ich habe die Aufnahme des Rechts auf informationelle Selbstbestimmung als eigenständige Regelung in das Grundgesetz befürwortet.

Zwar birgt eine solche Regelung die Gefahr einer inhaltsändernden oder doch einschränkenden Ausgestaltung oder Auslegung. Für eine Aufnahme in das Grundgesetz spricht jedoch, daß das Recht auf informationelle Selbstbestimmung als besonderes Grundrecht bereits Eingang in mehrere Landesverfassungen gefunden hat. Die Aufnahme in weitere Landesverfassungen ist geplant. In Nordrhein-Westfalen hat sich die Festschreibung des Grundrechts auf Schutz der personenbezogenen Daten schon seit dem Jahre 1978 bewährt. Da es sich bei dem Grundrecht auf informationelle Selbstbestimmung um ein Menschenrecht handelt, sollte es auf Dauer nicht nur in den einzelnen Landesverfassungen – mit unterschiedlichem Wortlaut – ausdrücklich geregelt, sondern im Grundgesetz deutlich erkennbar verankert werden. Damit würde auch dem Gesichtspunkt der Normenklarheit Rechnung getragen.

In diesem Zusammenhang halte ich es für bedeutsam, daß gemäß Artikel 19 Abs. 1 Satz 2 des Grundgesetzes ein Gesetz, das ein Grundrecht einschränkt, das Grundrecht unter Angabe des Artikels nennen muß (sog. Zitiergebot). Durch eine eigene Regelung des Grundrechts auf Datenschutz im Grundgesetz könnte die Schutzfunktion des Zitiergebots hergestellt werden.

In Artikel 77 a der Verfassung des Landes Nordrhein-Westfalen ist die unabhängige Datenschutzkontrolle bereits seit 1978 verankert. Diese Regelung ist für die Verwirklichung des Grundrechts auf Datenschutz von entscheidender Bedeutung und hat sich im Alltag bewährt. Ich habe mich daher dafür ausgesprochen, daß eine unabhängige Datenschutzkontrolle auch im Grundgesetz abgesichert wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit den genannten Fragen auseinandergesetzt. Sie hat außerdem die

Möglichkeit der Aufnahme eines Rechts auf Informationsfreiheit in das Grundgesetz erörtert. Sie faßte bei Gegenstimme des Bayerischen Datenschutzbeauftragten eine Entschließung, in der der vom Deutschen Bundestag und Bundesrat eingesetzten Gemeinsamen Verfassungskommission ein konkreter Formulierungsvorschlag für das Grundrecht auf Datenschutz unterbreitet wurde (vgl. Anlage 1, S. 160/161).

# 4. Grenzüberschreitender Datenverkehr

## 4.1 Vorschlag der EG-Kommission für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten

Der mit Blick auf die Vollendung des EG-Binnenmarktes zum 1. Januar 1993 vorgelegte Vorschlag für eine allgemeine Richtlinie des Rates wurde im Berichtszeitraum in den zuständigen EG-Gremien intensiv beraten. Das Europäische Parlament verabschiedete am 11. März 1992 fast 120 Änderungsanträge zum ursprünglichen Entwurf aus dem Jahre 1990. Die Kommission der Europäischen Gemeinschaften reagierte darauf mit dem geänderten Entwurf vom 15. Oktober 1992.

Die **Neufassung** verzichtet auf die formelle Unterscheidung zwischen den für den öffentlichen und den privaten Bereich geltenden Regelungen. Besonderheiten des öffentlichen Bereichs sind nicht mehr in einem eigenen Kapitel, sondern im Zusammenhang der einzelnen Vorschrift geregelt. Außerdem ist für bestimmte Verarbeitungen, die nicht geeignet sind, die Rechte und Freiheiten der betroffenen Personen zu beeinträchtigen, keine oder nur eine vereinfachte Meldepflicht bei der Kontrollbehörde vorgesehen.

Positiv anzumerken ist, daß die Neufassung an Übersichtlichkeit und Verständlichkeit gewonnen hat. Dies sowie die Vereinfachung einzelner Verfahrensweisen dürfte die praktische Handhabung erleichtern und zu mehr Akzeptanz in der Öffentlichkeit führen. Ich begrüße außerdem, daß die im ersten Entwurf enthaltene globale Befreiung gemeinnütziger Einrichtungen von den Bestimmungen der Richtlinie nicht mehr vorgesehen ist. Die Rechte der Bürger dürften nicht mehr garantiert sein, wenn verschiedenste Organisationen von jeder Verpflichtung ausgenommen würden.

Außerdem ist in der Neufassung klarer geregelt, welche einzelstaatliche Rechtsvorschrift auf die Verarbeitung Anwendung findet. Nach dem ursprünglichen Vorschlag bestimmte sich die territoriale Zuständigkeit nach dem Standort der Datei. Eine Datei kann jedoch – insbesondere im Fall von Datenbanken und Netzen – auf mehrere Mitgliedstaaten verteilte Standorte haben. Nach der Neufassung richtet sich die Zuständigkeit nach dem Ort, an dem der Verantwortliche ansässig ist. Hat dieser seinen Sitz nicht im Gemeinschaftsgebiet, benutzt aber dort seine automatisierte Datenverarbeitung, gilt das Recht des Staates, in dessen Hoheitsgebiet sich diese Verarbeitung befindet.

Ich bedauere demgegenüber, daß der neue Entwurf in einigen wesentlichen Punkten auf eine Korrektur der früheren Fassung verzichtet und Regelungen enthält, die unzureichend bzw. ergänzungsbedürftig sind. So ist der Anwendungsbereich weiterhin auf die Verarbeitung personenbezogener Daten in Dateien beschränkt. Bei Weitergabe personenbezogener Daten in Drittländer gibt sich der Entwurf mit einem „angemessenen" Schutz im Zielland zufrieden. Auch wenn die Angemessenheit des Schutzniveaus nunmehr definiert ist, ist

ein wirksamer Schutz des Betroffenen nur gewährleistet, wenn im Empfängerland zumindest ein dem EG-Standard gleichwertiges Datenschutzniveau besteht.

Unter Berücksichtigung der unterschiedlichen Datenschutzstandards in den Partnerländern muß jedes Land die Möglichkeit behalten, sein nationales Datenschutzniveau fortzuentwickeln. Nach dem neuen Entwurf können die Mitgliedstaaten lediglich „die Voraussetzungen näher bestimmen, unter denen die Verarbeitung personenbezogener Daten zulässig ist". Dieser Wortlaut reicht nicht aus. Es sollte vielmehr klargestellt werden, daß die Richtlinie einen Mindeststandard enthält, der der Schaffung strengerer nationaler Regelungen insbesondere in spezifischen Bereichen nicht entgegensteht.

Nach dem Entwurf verabschiedet die EG-Kommission im Rahmen einer abgeleiteten Rechtsetzungsbefugnis die „erforderlichen technischen Modalitäten und die notwendigen Maßnahmen, um die einheitliche Anwendung der Bestimmungen dieser Richtlinie zu gewährleisten". Um auszuschließen, daß die Kommission die Möglichkeit erhält, umfassend in alle Datenbereiche ihrer Mitgliedstaaten einzugreifen, müssen ihre Rechtsetzungsbefugnisse eindeutig begrenzt werden.

Nach der Neufassung bestimmen die Mitgliedstaaten in ihren Rechtsvorschriften, „unter welchen Bedingungen eine nationale Kennziffer oder jedes andere Kennzeichen allgemeiner Bedeutung verwendet werden darf". Unter Berücksichtigung der deutschen Rechtslage muß klargestellt werden, daß auf eine derartige Regelung auch verzichtet werden kann.

Die Richtlinie muß bis zum 1. Juli 1994 in nationales Recht umgesetzt sein. Bereits vorhandene Verarbeitungen müssen den neuen Regelungen spätestens ab 1. Juli 1997 entsprechen.

Insgesamt bewerte ich den geänderten Vorschlag als weiteren Schritt in Richtung eines harmonisierten Datenschutzes in Europa. Er wird Einfluß nehmen auf die künftige Datenschutzgesetzgebung und -praxis in der Bundesrepublik Deutschland. Dies begründet Vorteile – die Partner können aus den Erfahrungen der anderen Länder lernen und erfahren durch sie Unterstützung bei der Durchsetzung ihrer Forderungen –, aber auch die Notwendigkeit, kritisch zu reflektieren, in welchen Bereichen den jeweiligen deutschen Gegebenheiten durch die Beibehaltung bzw. Fortentwicklung der nationalen Regelungen Rechnung getragen werden soll.

## 4.2 Grenzüberschreitender Datenverkehr in einzelnen Bereichen

### 4.2.1 Vorschlag der EG-Kommission für eine ISDN-Datenschutzrichtlinie

Mit ihrem Richtlinienvorschlag zum Datenschutz in digitalen Telekommunikationsnetzen vom 18. Juli 1990 reagierte die EG-Kommission auf bereits früher erhobene Forderungen der europäischen Datenschutzbeauftragten

nach einer einheitlichen Datenschutzregelung für das **grenzüberschreitende ISDN.**

Der Vorschlag enthielt zahlreiche datenschutzfreundliche Regelungen: So sah er die generelle Verkürzung der Zielnummer im Einzelentgeltnachweis des Anrufers um die letzten vier Ziffern vor. Den Anrufer sollte ein Signal erreichen, wenn die Möglichkeit besteht, daß seine Rufnummer beim Angerufenen angezeigt wird. Außerdem wurde dem Anrufer prinzipiell das Recht eingeräumt, die Rufnummernanzeige im Einzelfall auf Knopfdruck zu unterdrücken.

Zwischenzeitlich wurde der Vorschlag überarbeitet. Die modifizierte Fassung sieht allerdings neben einigen positiv zu wertenden Änderungen eine Verkürzung der Zielnummer im Einzelentgeltnachweis des Anrufers nicht mehr vor.

Auch wenn die Richtlinie nicht mehr rechtzeitig zum Beginn des Europäischen Binnenmarktes am 1. Januar 1993 verabschiedet werden konnte, begrüße ich das in den Entwürfen zum Ausdruck gekommene hohe Schutzniveau als wichtigen Teilbereich des Grundrechtsschutzes im entstehenden Europäischen Wirtschaftsraum.

### 4.2.2 Europol

Mit Europol, dem geplanten Europäischen Kriminalamt, hat sich der Europäische Rat für eine EG-weite zentrale Polizeieinrichtung entschieden, der die Koordinierung von Informationen und Erkenntnissen zur Bekämpfung des grenzüberschreitenden organisierten Verbrechens übertragen werden soll. In einer ersten Aufbaustufe von Europol soll eine gemeinsame Zentrale zur Bekämpfung der Rauschgiftkriminalität (EDU-Europol) errichtet werden. Obgleich die Notwendigkeit der Schaffung einer rechtlichen Grundlage für die Arbeit von EDU-Europol anerkannt ist, soll die EDU-Europol bereits vor Erlaß einer europäischen Konvention im Rahmen einer Übergangslösung tätig werden. Von deutscher Seite wurde insoweit der Austausch von Verbindungsbeamten aus allen 12 EG-Staaten vorgeschlagen, die jeweils mittels Datensichtgerät direkten Zugang zu ihren nationalen polizeilichen Informationssystemen haben, sofern diese für die Bekämpfung der Rauschgiftkriminalität von Bedeutung sind. Der Vorteil einer solchen Zusammenarbeit wird in der räumlichen Nähe der um Auskunft ersuchenden und auskunfterteilenden Verbindungsbeamten und der hierdurch gesteigerten Effektivität des gemeinsamen Informationsaustausches gesehen.

Nicht zu übersehen sind indes auch die bereits durch diese Übergangslösung vor der Schaffung erforderlicher Rechtsgrundlagen für die EDU-Europol aufgeworfenen datenschutzrechtlichen Probleme. Insbesondere die Verwendung der Informationen sowie die eigenständige Nutzungs- und Übermittlungskompetenz des Bundeskriminalamts bezüglich der polizeilichen Informationssysteme der Länder aufgrund der sogenannten Zentralstellenfunktion des Bundeskriminalamts stehen hier zur Diskussion. Ich werde daher in Abstimmung mit den Datenschutzbeauftragten des Bundes und der Länder die datenschutzrechtlichen Fragen der dargestellten Übergangslösung an das Innenministerium des Landes Nordrhein-Westfalen herantragen. Es wird da-

für Sorge zu tragen sein, daß ohne rechtliche Grundlage Datenverarbeitung auch im Rahmen der Übergangslösung nicht über die nach geltendem Recht zulässige Zusammenarbeit auf bilateraler Ebene bzw. im Rahmen von Interpol hinausgehen wird. Eine datenschutzrechtliche Bewertung des bislang erst in groben Zügen konzipierten Europol kann verständlicherweise derzeit noch nicht erfolgen.

### 4.2.3 EG-Statistiken

Mit fortschreitender politischer und wirtschaftlicher Integration innerhalb der Europäischen Gemeinschaft zeigt sich die Tendenz, die erforderliche Harmonisierung von Statistiken im EG-Bereich zunehmend durch Rechtsakte der Gemeinschaft zu erreichen. Hierbei läßt die aktuelle Entwicklung des europäischen Statistiksystems erwarten, daß in den nächsten Jahren vielfältige Informationen und Einzelangaben, die der statistischen Geheimhaltung (§ 16 BStatG) unterliegen, an das für die Statistik in der EG zuständige Statistische Amt der Europäischen Gemeinschaften (EUROSTAT) übermittelt werden.

Die hiermit verbundenen Auswirkungen auf das Recht der amtlichen Statistik in der Bundesrepublik Deutschland, insbesondere das Statistikgeheimnis, sind zwar heute noch nicht vollständig absehbar, jedoch besteht nach den derzeitigen Erkenntnissen Anlaß, die bereits im 10. Tätigkeitsbericht (S. 34) erhobene Forderung nach einer wirksamen unabhängigen Datenschutzkontrolle bei den zuständigen Organen der EG mit Nachdruck zu vertreten. Dies ist vor dem Hintergrund zu sehen, daß nach Artikel 3 Abs. 2 der Verordnung des Rates der Europäischen Gemeinschaft vom 11. Juni 1990 (Amtsblatt der EG Nr. L 151/1) die einzelstaatlichen Vorschriften über das Statistikgeheimnis nicht gegen die Übermittlung vertraulicher statistischer Daten an das Statistische Amt der Europäischen Gemeinschaften geltend gemacht werden können, soweit diese Übermittlung in einem eine Gemeinschaftsstatistik regelnden Rechtsakt der Gemeinschaft vorgesehen ist. Derartige Rechtsakte, die die Errichtung von Einzelregistern und hiermit verbundene Datenanforderungen vorsehen, sind zu erwarten.

Nur beispielhaft ist auf einen Vorschlag der Kommission hinzuweisen, nach dem eine Verordnung des Rates über die innergemeinschaftliche Koordinierung des Aufbaus von Unternehmensregistern für statistische Zwecke (CS/92/6) erlassen werden soll. Die auf Grund dieser Verordnung zu übermittelnden Informationen eröffnen im EG-Bereich weitgehende Zusammenstellungen von Daten für statistische Zwecke. Damit werden etwa die Regelungen über Adreßdateien nach § 13 BStatG, nach denen nur begrenzte einzelne Dateien für bestimmte Statistiken zulässig sind, durch höherrangiges EG-Recht insoweit außer Kraft gesetzt. Umso dringlicher ist die Schaffung einer mit effektiven Kontrollmöglichkeiten ausgestatteten Datenschutzinstanz bei den zuständigen Organen der EG.

# 5. Datenschutz in einzelnen Bereichen

## 5.1 Einwohnerwesen

### 5.1.1 Melderegister

Zum Entwurf eines Ersten Gesetzes zur Änderung des **Melderechtsrahmengesetzes** – MRRG – (Stand: 03.01.1992) habe ich eine Stellungnahme abgegeben. Darin habe ich vor allem betont, daß das Verfahren zur Bestimmung von Haupt- und Nebenwohnung unter Beachtung des Rechts auf informationelle Selbstbestimmung der Betroffenen neu zu regeln ist. Außerdem habe ich meine erheblichen Bedenken gegen die fortbestehende Regelung der Hotel- und Krankenhausmeldepflicht deutlich gemacht.

Ebenso sollte im Rahmen der Novellierung des Melderechtsrahmengesetzes ein weiteres grundsätzliches Problem gelöst werden. Nach geltendem Recht sind **Datenübermittlungen** vom Einwohnermeldeamt **zu anderen Verwaltungsstellen** für Kreise einerseits und kreisfreie Städte andererseits unterschiedlich geregelt. Eine Angleichung ist hier nach meiner Auffassung im Interesse einer einheitlichen, für die betroffenen Bürgerinnen und Bürger überschaubaren Handhabung geboten.

Zudem bedarf es einer Klarstellung im Gesetz, daß die Übermittlung von **Wählerdaten an politische Parteien** (§ 22 MRRG, § 35 Abs. 1 MG NW) nicht alle wahlberechtigten Bürgerinnen und Bürger umfassen darf, sondern, wie es der Wortlaut der Vorschrift schon jetzt verlangt, lediglich einzelne Wählergruppen, z. B. Jungwähler, Senioren (vgl. 10. Tätigkeitsbericht, S. 5, 40 bis 43). Der Bundesrat hat inzwischen einen entsprechenden Änderungsvorschlag zu § 22 Abs. 1 Satz 1 MRRG eingebracht, dem die Bundesregierung bereits zugestimmt hat. Ich gehe deshalb davon aus, daß das Innenministerium des Landes Nordrhein-Westfalen seine entgegenstehende Auffassung nicht weiter aufrecht erhält.

Die Datenübermittlung an **Adreßbuchverlage** sollte von der Einwilligung der betroffenen Bürgerinnen und Bürger abhängig gemacht werden, wie dies beim Zugang zu den ebenfalls für Werbezwecke genutzten Datenbeständen der Kraftfahrzeughalter beim Kraftfahrt-Bundesamt und den Datenbeständen der Telefonkunden bei der Deutschen Bundespost TELEKOM in Abänderung der bisherigen Verfahren bereits geregelt ist.

Nachdem im Jahre 1992 das Meldegesetz des Landes Nordrhein-Westfalen – MG NW – nunmehr seit zehn Jahren in Kraft ist, muß es auch aus der Sicht des Datenschutzes als Mangel empfunden werden, daß das Innenministerium von der Ermächtigung des § 38 MG NW, die zur Durchführung dieses Gesetzes erforderlichen **Verwaltungsvorschriften** zu erlassen, bisher keinen Gebrauch gemacht hat. Auch von den Einwohnermeldeämtern wird das Fehlen der Verwaltungsvorschriften häufig beklagt, wie ich im Rahmen von Kontrollbesuchen und Beratungsersuchen erfahren habe.

Ein besonderes datenschutzrechtliches Problem ist die Praxis einiger Universitäts- und Hochschulstädte in Nordrhein-Westfalen, den **Hauptwohnsitz** von Studentinnen und Studenten gegen ihren erklärten Willen dorthin zu verlegen, obwohl sie selbst nur in diesen Städten ihre Nebenwohnung nehmen wollen. Dies wird von Betroffenen als „Zwangsausbürgerung" aus ihren Heimatgemeinden in diese Städte empfunden. Dabei setzen sich diese Städte auch über Feststellungen der Heimatgemeinden hinweg, die Hauptwohnung der Betroffenen sei dort, und melden die Betroffenen auch gegen den Willen der Heimatgemeinde um.

Wer dieser Zwangsummeldung entgehen will, hat die Umstände seiner Ausbildung und sein Privatleben umfassend gegenüber der Universitäts- und Hochschulstadt offenzulegen. Er hat etwa einen Nachweis über die von ihm belegten Veranstaltungen (Lehrveranstaltungen, Vorlesungen, Proseminare, Seminare, Kolloquien und Übungen) zu führen, einen Nachweis der von ihm angegebenen Vereinstätigkeit oder ehrenamtlichen Arbeit mit Bestätigung der einzelnen Termine, einen Nachweis über die regelmäßigen Heimfahrten, ggf. Vorlage eines Dienst- bzw. Arbeitsvertrages, sowie eine genaue Auflistung der Aufenthaltszeiten in der Universitätsstadt und am Heimatort. Betroffene haben diese Praxis als einen Schritt in Richtung Überwachungsstaat und hin zum „gläsernen Bürger" bezeichnet. Das von mir hierzu befragte Innenministerium legt Wert auf die Feststellung, daß Nachprüfungen durch die Städte zu diesem Zweck nicht zu einer unverhältnismäßigen Ausforschung der persönlichen Lebensverhältnisse der Betroffenen führen dürfen. Zulässig sei lediglich eine Plausibilitätsprüfung. Hiergegen verstößt freilich die dargestellte Praxis.

Verstöße gegen Vorschriften über den Datenschutz könnten vermieden werden, wenn festgelegt wird, daß bis zur Altersgrenze von 27 Jahren die Hauptwohnung von Personen, die sich in der Ausbildung befinden, in der Regel die vorwiegend benutzte Wohnung in der Heimatgemeinde ist. Für Studentinnen und Studenten, die eine Fach- oder Fachhochschule für die öffentliche Verwaltung besuchen, enthält der Runderlaß des Innenministeriums vom 21.05.1985 – I C 3/41.303 – (MBl. NW. 1985 S. 863) zur Bestimmung der Hauptwohnung unter Nr. 1.122 bereits die Festlegung, daß von der Bestimmung der Wohnung am Ort der Ausbildungsstätte zur Hauptwohnung im allgemeinen abgesehen werden sollte.

Auf Anfrage einer Gemeinde war zu prüfen, ob es nach § 35 Abs. 3 MG NW zulässig ist, Daten von Alters- und Ehejubilaren an die Bürgermeisterinnen und Bürgermeister ausländischer **Partnerstädte** zu übermitteln, damit von dort aus Anlaß der Jubiläen schriftlich gratuliert werden kann. Das von mir um eine Stellungnahme gebetene Innenministerium vertritt hierzu die Auffassung, daß Empfänger von Melderegisterauskünften nach § 35 Abs. 3 MG NW nicht nur inländische, sondern ebenso ausländische Stellen sein können. Es bestünden deshalb gegen eine derartige Datenübermittlung keine grundsätzlichen Bedenken. Dabei werde allerdings unterstellt, daß ein eingelegter Wider-

spruch der Betroffenen beachtet wird und schutzwürdige Belange (§ 7 MG NW) im Einzelfall nicht entgegenstehen.

Nach § 7 Satz 1 MG NW dürfen schutzwürdige Belange der Betroffenen durch die Verarbeitung oder sonstige Nutzung personenbezogener Daten nicht beeinträchtigt werden. Zwar mögen es manche Betroffene begrüßen, Glückwünsche zu ihrem Jubiläum von Vertretern der ausländischen Partnerstadt zu erhalten. Andere dagegen können es als Belästigung empfinden. Wieder andere können sogar äußerst erschrocken darüber sein, daß ihre personenbezogenen Daten „nun auch schon" in das Ausland übermittelt werden. Man kann auch nicht von jeder Altersjubilarin und jedem Altersjubilar erwarten, daß sie wissen, welche Partnerstädte ihre Wohngemeinde hat.

Unter Zugrundelegung der Auffassung des Innenministeriums ist deshalb bei Berücksichtigung der schutzwürdigen Belange der Betroffenen nach meiner Auffassung eine Übermittlung der gewünschten Daten an eine ausländische Partnerstadt nur mit Einwilligung der Betroffenen zulässig.

Die Wahrung des **Adoptionsgeheimnisses** nach § 1758 BGB bei der Übermittlung der Meldedaten von Kindern, die in einem Adoptionspflegeverhältnis stehen, an öffentlich-rechtliche Religionsgesellschaften bereitete in den vergangenen Jahren in der Praxis oft Schwierigkeiten und gab auch erneut Anlaß zu zahlreichen Bürgereingaben. Die Meldebehörde ist zur Wahrung des Adoptionsgeheimnisses verpflichtet. Aus diesem Grund wird bei den Meldedaten des zur Adoption vorgesehenen Kindes eine Auskunftssperre eingetragen. Nach § 32 Abs. 1 MG NW darf die Meldebehörde einer öffentlich-rechtlichen Religionsgesellschaft zur Erfüllung ihrer Aufgaben bestimmte Daten ihrer Mitglieder übermitteln. Zu diesen Daten gehören auch Übermittlungssperren, denen der Hinweis auf die Wahrung des Adoptionsgeheimnisses zuzuordnen ist. Es kommt nach meinen Erfahrungen häufig vor, daß der Hinweis auf die Wahrung des Adoptionsgeheimnisses bei den öffentlich-rechtlichen Religionsgesellschaften nicht oder nicht ausreichend beachtet wird. So werden diese Daten immer wieder für caritative Zwecke verwendet, wie etwa in Listen für Haussammlungen aufgenommen. Dadurch droht die Gefahr, daß die beabsichtigte Annahme des Kindes aufgedeckt wird.

Rechtlich zufriedenstellend ist in diesem Zusammenhang die Rechtslage in Bayern. Nach § 13 Abs. 1 der Bayerischen Meldedatenübermittlungsverordnung hat eine Datenübermittlung u. a. an öffentlich-rechtliche Religionsgesellschaften dann zu unterbleiben, wenn im Melderegister eine Auskunftssperre wegen Adoptionspflege gespeichert ist. Zur Klarstellung halte ich die Aufnahme einer entsprechenden Vorschrift in die Meldedatenübermittlungsverordnung des Landes Nordrhein-Westfalen für dringend geboten.

Auf Grund der Vielzahl von Fällen, in denen die öffentlich-rechtlichen Religionsgesellschaften die Übermittlungssperren nicht beachten, scheidet nach meiner Auffassung, die von einer Reihe von Gemeinden und Kreisen geteilt wird, schon jetzt eine Übermittlung derartiger Datensätze im Hinblick auf § 7 MG NW wegen Beeinträchtigung der schutzwürdigen Belange des Kindes

aus. Das Innenministerium, das ich seit längerem um eine Stellungnahme gebeten hatte, hat sich bisher noch nicht geäußert. Im Interesse der betroffenen Kinder ist eine schnelle Abhilfe geboten.

### 5.1.2 Gesetzwidrige Datenverarbeitungsprogramme

Bereits in meinem 10. Tätigkeitsbericht (S. 36/37) habe ich dargestellt, daß in einer Gemeinde das Einwohnermelderegister mit Hilfe eines Programms automatisiert geführt wurde, das nicht den gesetzlichen Vorgaben entsprach. Eine von mir daraufhin landesweit vorgenommene stichprobenweise Überprüfung der in den Einwohnermeldeämtern eingesetzten ADV-Programme hat ergeben, daß lediglich in einem einzigen Fall das eingesetzte Programm in den überprüften Punkten beanstandungsfrei war. In den anderen Fällen sind Programmänderungen erforderlich.

Als Mangel war vor allem wiederum festzustellen, daß die gesetzliche Verpflichtung aus § 11 Abs. 2 und 3 MG NW i.V.m. § 1 Abs. 1 DVO MG NW, die dort genannten Daten und Hinweise in einen **gesonderten Bestand** zu überführen und im aktuellen Bestand zu löschen, programmtechnisch nicht zu verwirklichen war. Erschwerend kam wiederum hinzu, daß die Bediensteten des Einwohnermeldeamtes auf die Gesetzwidrigkeit des eingesetzten Programms seit Jahren hingewiesen hatten, ohne daß die jeweilige Stadt beim Programmhersteller oder beim Rechenzentrum auf eine Programmänderung gedrängt hätte.

Schwerwiegende datenschutzrechtliche Bedenken bestehen auch gegen die programmtechnische Ausgestaltung der **Anzeige von Auskunftssperren** im Programm. Wenn etwa beim ersten Aufruf des mit einem Sperrvermerk versehenen Datensatzes die Angaben einer einfachen Melderegisterauskunft (§ 34 Abs. 1 MG NW) zusammen mit dem Vermerk „Auskunftssperre" erfolgen, bestand im Zusammenhang mit den räumlichen Gegebenheiten in den kontrollierten Einwohnermeldeämtern für den Auskunftssuchenden durchaus die Möglichkeit, trotz bestehender Auskunftssperre die gewünschte Auskunft durch einfaches Ablesen vom Bildschirm zu erhalten. Durch einen Zwischenbildschirm, der nur den Hinweis „Auskunftssperre" enthält, ist dieses Problem auf einfache Weise zu lösen und in anderen Programmen auch bereits gelöst worden.

In einigen Programmen wurden als „Auskunftssperre" auch die **Widersprüche** nach § 35 MG NW bezeichnet. Dies führt in der Praxis dazu, daß die Auskunft über eine Person generell verweigert wird, obwohl die Betroffenen etwa lediglich der Übermittlung ihrer Daten an einen Adreßbuchverlag widersprochen haben. Auch insoweit ist es notwendig, die Programme den gesetzlichen Vorgaben (Auskunftssperre § 34 Abs. 5, 6, 7, § 7 MG NW; Widerspruch § 35 Abs. 1, 2, 3, 4 MG NW) anzupassen.

Als weiteres schwerwiegendes Versagen eines eingesetzten Programms habe ich festgestellt, daß in einer Gemeinde bei der Weitergabe von Einwohnerdaten an einen **Adreßbuchverlag** eine fehlerhafte Auswahl getroffen

wurde und so die Daten von mehreren hundert Personen weitergegeben wurden, die dem ausdrücklich widersprochen hatten.

Bereits durch das Programm sollte sichergestellt sein, daß **Suchvermerke** (§ 3 Abs. 2 Nr. 6 MG NW) im Einwohnermelderegister entsprechend der gesetzlichen Vorgabe nicht länger als zwei Jahre gespeichert werden. Ohne die programmtechnische Regelung des Problems bleiben solche Datensätze offenbar beliebig lange gespeichert.

Als besonders schwerwiegender Datenschutzverstoß ist ein Programmfehler zu bewerten, bei dem die Wahrung des **Adoptionsgeheimnisses** nicht mehr gewährleistet ist. Dies ist dann der Fall, wenn das Programm sowohl bei Aufruf des alten als auch des neuen Familiennamens die bisherige und die neue Identität zusammen offenlegt.

Zu einer unzulässigen Datenverarbeitung führte auch ein Programm, das als Bestandteil der **Adresse** stets das Datum „Name des Wohnungs- und Hauseigentümers" aufführte. Diese Angaben wurden auch im Wege des Datenträgeraustausches weitergegeben, so u. a. an die GEZ. Im Datensatz für das Meldewesen ist zwar im Feld „Anschrift" auch der Name des Wohnungsgebers bzw. der Wohnungsgeberin vorgesehen, aber nicht generell, sondern nur dann, wenn dies zur Adressierung erforderlich, d. h. unbedingt notwendig ist. Im Regelfall entfällt daher diese Angabe. Auf meinen Hinweis hat die Gemeinde die Löschung der Angaben veranlaßt und vorgesorgt, daß künftig diese Daten nicht mehr gespeichert werden.

Je nach Schwere der festgestellten Programmfehler und der Schnelligkeit ihrer Beseitigung durch den Programmhersteller bleibt für die datenverarbeitende Stelle die Frage zu prüfen, mit welchen Maßnahmen für die Zwischenzeit die Datenschutzrechte der Betroffenen zu gewährleisten sind. Dies kann im Extremfall auch dazu führen, daß das eingesetzte Programm gegen das Programm eines anderen Herstellers ausgetauscht werden muß.

### 5.1.3 Vernichtung fehlerhafter Pässe und Personalausweise

Schon in meinem 10. Tätigkeitsbericht (S. 39/40) habe ich feststellen müssen, daß zahlreiche Paß- und Personalausweisbehörden reklamierte fehlerhafte Ausweisdokumente nicht wie vorgeschrieben an die Bundesdruckerei zurücksenden. Zwar hatte das Innenministerium mit Erlaß vom 12. September 1989 – I B 3/38.232/40.321 – die Regierungspräsidenten gebeten, die Paß- bzw. Personalausweisbehörden der jeweiligen Bezirke auf die einschlägigen Bestimmungen hinzuweisen. Eine mir nunmehr zugegangene Auflistung der Bundesdruckerei hat aber gezeigt, daß durch den Erlaß eine wesentliche Verbesserung der Praxis nicht erreicht wurde. Statt der im Jahre 1990 überprüften 66 Gemeinden sind nunmehr 63 Gemeinden betroffen, davon 10 Gemeinden zum wiederholten Male.

Da nach meiner Einschätzung eine Wiederholung der Vorfälle für die Zukunft nicht ausgeschlossen werden kann, habe ich zur Vermeidung weiterer Verstöße gegen die Vorschriften des Paß- und Personalausweisrechts unter Hinweis auf § 7 DSG NW dem Innenministerium empfohlen, mit der Bundes-

druckerei ein Verfahren zu vereinbaren, das zuverlässig solche Fehler ausschließt. Das Innenministerium hält diese Empfehlung für „nicht realisierbar und verfahrenstechnisch nicht möglich".

## 5.2 Wahlen

Vom Innenministerium bin ich für die Beratung der unabhängigen Kommission für Rechts- und Verwaltungsvereinfachung des Bundes (Waffenschmidt-Kommission) um eine Stellungnahme zur Frage der **öffentlichen Auslegung des Wählerverzeichnisses** gebeten worden.

Nach meiner Auffassung würde allein ein Verzicht auf die Auslegung des Wählerverzeichnisses den Erfordernissen des Datenschutzes voll Rechnung tragen. Der seinerzeit bestehende rechtspolitische Zweck für die Auslegung des Wählerverzeichnisses war, Wahlberechtigten zu ermöglichen festzustellen, ob sie im Wählerverzeichnis eingetragen sind. Diese Kontrolle ist heute dadurch gewährleistet, daß alle im Wählerverzeichnis Eingetragenen eine schriftliche Wahlbenachrichtigung erhalten. Auch zu dem Zweck die Prüfung zu ermöglichen, ob andere Personen zu Unrecht eingetragen oder nicht eingetragen sind, erscheint die Auslegung des Verzeichnisses als entbehrlich.

Bei der derzeit gesetzlich möglichen Offenlegung alphabetisch geordneter Wählerverzeichnisse werden die melderechtlichen Auskunftssperren (§ 34 Abs. 5 bis 7 MG NW) nicht berücksichtigt. Eine Umgehung der melderechtlichen Auskunftssperren durch Einblicknahme in das Wählerverzeichnis ist daher auf Grund der geltenden Rechtslage möglich. Dies bedeutet eine nicht hinnehmbare Beeinträchtigung der betroffenen Bürgerinnen und Bürger. Soweit nicht auf die Auslegung des Wählerverzeichnisses vollständig verzichtet wird, sollten daher bei derartigen Wählerverzeichnissen die Wahlberechtigten mit Auskunftssperren in dem auszulegenden Exemplar von Amts wegen unkenntlich gemacht werden, wie bisher schon auf Antrag der Wahlberechtigten ihr Geburtsdatum.

Bei Wählerverzeichnissen, die nach Ortsteilen, Straßen und Hausnummern gegliedert werden, ist aus der Sicht des Datenschutzes äußerst bedenklich, daß damit etwa die Langzeitpatientinnen und patienten in Landeskrankenhäusern aufgelistet und der Neugier ihrer Mitmenschen preisgegeben werden. Gerade in diesem Bereich sollte dem Recht auf informationelle Selbstbestimmung der Betroffenen besonders Rechnung getragen werden, da das Wählerverzeichnis über seine Zweckbestimmung hinaus das Datum des Aufenthalts in einer derartigen Einrichtung offenbart und zusätzlich je nach Spezialisierungsgrad der Klinik auch konkrete Rückschlüsse auf die Art der Erkrankung zuläßt. Wegen dieser häufig sehr sensiblen Daten der Betroffenen sollte, soweit nicht von der Auslegung des Wählerverzeichnisses ganz abgesehen wird, vorher die Einwilligung der Betroffenen eingeholt werden. Bei Verweigerung der Einwilligung sollten die Daten von Amts wegen in dem zur Auslegung bestimmten Exemplar unkenntlich gemacht werden.

Ich habe angeregt, insoweit für die nächsten Wahlen im Lande Nordrhein-Westfalen einen ausreichenden Datenschutz sicherzustellen. Eine Stellungnahme des Innenministeriums zu meinen Vorschlägen ist bisher nicht ergangen.

## 5.3 Ausländerwesen

### 5.3.1 Neufassung des Ausländergesetzes

Erste Erfahrungen mit den Datenverarbeitungsvorschriften des Gesetzes über die Einreise und den Aufenthalt von Ausländern im Bundesgebiet (Ausländergesetz – AuslG) in der Praxis zeigen, daß das Gesetz aus der Sicht des Datenschutzes als dringend nachbesserungsbedürftig bezeichnet werden muß (vgl. 10. Tätigkeitsbericht, S. 16).

### 5.3.2 Verwaltungsvorschriften zum Ausländergesetz

Zu bedauern ist besonders, daß offenbar zeitnah mit einem Inkrafttreten der Verwaltungsvorschriften zum Ausländergesetz nicht gerechnet werden kann. Im Vorgriff haben deshalb verschiedene Länder, so auch Nordrhein-Westfalen, zu einzelnen Vorschriften des Ausländergesetzes vorläufige Hinweise erlassen, um den erheblichen Unsicherheiten in der Praxis etwa bei der Anwendung des § 76 AuslG zu begegnen.

Dieser Zustand ist unbefriedigend. Er führt im Ergebnis dazu, daß einzelne Behörden oder auch ganze Behördenbereiche selbständig entscheiden, welche Vorschriften des Ausländergesetzes sie für sich als verbindlich ansehen und deshalb anwenden und welche sie nicht akzeptieren und deshalb nicht anwenden. Damit wird die Verbindlichkeit der Regelungen des Ausländergesetzes unterlaufen und zur Disposition der einzelnen Behörde bzw. des einzelnen Bediensteten gestellt. Aus der Sicht des Datenschutzes ist die gegenwärtige Situation für die betroffenen Ausländerinnen und Ausländer so nicht hinnehmbar.

In diesem Zusammenhang ist darauf hinzuweisen, daß es zumindest angreifbar ist, durch Verwaltungsvorschriften im Gesetz geregelte, aber nicht erforderlich erscheinende Einschränkungen des Rechts auf informationelle Selbstbestimmung der Ausländerinnen und Ausländer zu relativieren oder wieder rückgängig zu machen. Gegen den Versuch, durch Verwaltungsvorschriften die verbindlichen gesetzlichen Regelungen des Ausländergesetzes teilweise für nicht anwendbar zu erklären, bestehen verfassungsrechtliche Bedenken. Eine Verwerfungskompetenz über Gesetze steht der Verwaltung nicht zu.

### 5.3.3 Asylverfahrensgesetz

Für die Beratung des Gesetzes zur Neuregelung des Asylverfahrens (Asylverfahrensgesetz – AsylVfG) hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28. April 1992 bei Gegenstimme des Bayerischen Datenschutzbeauftragten eine Entschließung gefaßt. Die Konferenz empfahl Änderungen des Gesetzentwurfs zur Neuregelung des Asylverfahrens, insbesondere zu den Regelungen über die erkennungsdienstliche

Behandlung von Asylbewerbern zur Sicherung der Identität und über die Nutzung der dabei gewonnenen erkennungsdienstlichen Unterlagen zur Strafverfolgung und zur Gefahrenabwehr (vgl. Anlage 2, S. 161/162). Den Bedenken der Konferenz hat der Bundesgesetzgeber durch das Asylverfahrensgesetz vom 26. Juni 1992 (BGBl. I S. 1126) nicht Rechnung getragen.

Leider ist festzuhalten, daß das **Ausländerzentralregister** immer noch ohne ausreichende Rechtsgrundlage arbeitet. Im Hinblick auf die große Zahl dort gespeicherter personenbezogener Daten aller Ausländerinnen und Ausländer kann dies nicht länger hingenommen werden. Dies erscheint um so gravierender, wenn das Ausländerzentralregister nicht auf den Nachweis beschränkt wird, daß eine bestimmte Ausländerbehörde über eine bestimmte Ausländerin bzw. einen bestimmten Ausländer Unterlagen besitzt, sondern zu einem bundesweiten zentralen Informations- und Kommunikationssystem bis hin zu einem gesonderten polizeilichen Fahndungssystem über Ausländerinnen und Ausländer ausgebaut wird.

### 5.3.4 Wahlen zum Ausländerbeirat

Eine Reihe von Gemeinden haben datenschutzrechtliche Bedenken vorgetragen, zur Vorbereitung und Durchführung von Wahlen zum Ausländerbeirat auf die im Melderegister und beim Ausländeramt gespeicherten Daten der Ausländerinnen und Ausländer zurückzugreifen. Diese Bedenken werden von mir geteilt.

Wie die Regelungen in § 3 Abs. 2 Nr. 1 MG NW und § 35 Abs. 1 MG NW zeigen, ist die Verwendung von Daten aus dem Melderegister zum Zwecke der Durchführung von Wahlen erkennbar bereichspezifisch abschließend geregelt. Aus den Vorschriften des Meldegesetzes wird deutlich, daß als Wahlen, für die Meldedaten verwendet werden sollen, nur Parlaments- und Kommunalwahlen in Betracht kommen. Die entsprechenden Aufgabenzuweisungsnormen zur Durchführung der Wahlen in der Gemeindeverwaltung finden sich in den jeweiligen entsprechenden Wahlgesetzen und -ordnungen. Die Verwendung der Meldedaten zur Wahl eines Ausländerbeirates ist danach bisher im Meldegesetz nicht vorgesehen. Eine entsprechende Satzungsregelung der Gemeinde wäre nach meiner Auffassung insoweit wegen Verstoßes gegen höherrangiges Landesrecht unzulässig.

Gleiches gilt für die Verwendung von Daten aus dem Ausländeramt zur Durchführung von Wahlen zum Ausländerbeirat. Die Verwendung von Ausländerdaten zu derartigen Wahlzwecken ist, etwa im Hinblick auf die Offenlegung des Wählerverzeichnisses, ein schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung der ausländischen Mitbürgerinnen und Mitbürger, die eine bereichspezifische Verwendungsregelung erforderlich macht. Diese fehlt im derzeit geltendem Ausländergesetz. Ein Rückgriff auf die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen scheidet daher aus.

Unter Vermeidung von Verstößen gegen Vorschriften über den Datenschutz können deshalb Wahlen zum Ausländerbeirat bei Nutzung von Melde- und

Ausländerdaten derzeit nur durchgeführt werden, wenn die Betroffenen zuvor in die Datenverarbeitung eingewilligt haben oder wenn sie auf Grund einer Aufforderung sich selbst in sog. Wählerlisten eingetragen und die erforderlichen Angaben selbst gemacht haben.

### 5.3.5 Einkommensangaben bei Erteilung eines Sichtvermerks

Die bereits in meinem 10. Tätigkeitsbericht (S. 44) behandelte Frage, ob im Zusammenhang mit der Erteilung von Aufenthaltserlaubnissen in Form von Sichtvermerken die bewilligende Behörde Daten über die Höhe des Einkommens der Einladenden erheben darf, war nach Inkrafttreten des Ausländergesetzes erneut unter Beachtung der Regelung des § 84 AuslG zu überprüfen.

Nach meiner Auffassung kann auf § 84 AuslG die Erhebung von Daten über das Einkommen der Betroffenen nicht gestützt werden. Wie sich aus § 84 Abs. 2 Satz 1 AuslG normenklar ergibt, bedarf die Verpflichtung nach Abs. 1 Satz 1 der Schriftform. Die Frage, ob die Verpflichtungserklärung durch das Einkommen auch gedeckt ist, stellt sich nach dem Ausländergesetz nicht. Das Ausländergesetz enthält danach weder eine Befugnisnorm für die Ausländerbehörde, entsprechende Daten über das Einkommen beim Betroffenen zu erheben und ggf. die für die Richtigkeit der Angaben erforderlichen Nachweise zu fordern, noch normiert es eine Verpflichtung der Einladenden, über die schriftliche Erklärung nach § 84 Abs. 2 Satz 1 AuslG hinaus noch Angaben zu ihrem Einkommen und ggf. zu ihren Arbeitgebern zu machen.

Das Innenministerium hat mir hierzu mitgeteilt, daß es sich meiner Argumentation nicht verschließen könne. Es beabsichtige daher, die Ausländerbehörden zu bitten, von der Erfassung des Nettoeinkommens abzusehen.

## 5.4 Bau-, Wohnungs- und Liegenschaftswesen

### 5.4.1 Baulückenkataster

In verschiedenen Gemeinden sind Versuche unternommen worden, durch Veröffentlichung sog. „Baulückenkataster" vorhandene Wohnflächenreserven in Baulücken bzw. mindergenutzten Grundstücken zu mobilisieren und so Impulse für die private Bauwirtschaft zu geben, die mit zu einer Verbesserung der jeweiligen Wohnungsmarktsituation führen sollten. Die Verfahrensgestaltung in den einzelnen Gemeinden war recht unterschiedlich. Aus der Sicht des Datenschutzes ist zum Baulückenkataster deshalb nur auf einige Grundsätze hinzuweisen.

Die Bekanntgabe personenbezogener Daten durch Veröffentlichung eines Baulückenkatasters bedarf als Eingriff in das Recht der betroffenen Grundstückseigentümerinnen und -eigentümer auf informationelle Selbstbestimmung einer gesetzlichen Grundlage. Eine solche liegt nicht vor.

Mit dem Baugesetzbuch (BauGB) sowie dem Maßnahmengesetz zum Baugesetzbuch (BauGBMaßnG) hat der Gesetzgeber Regelungen in den Bereichen Bauleitplanung und Wohnungsbauförderung geschaffen und den

zuständigen Behörden ein entsprechendes bereichspezifisches Instrumentarium zur Aufgabenerfüllung an die Hand gegeben. Soweit es städteplanerisch nicht gewollte Baulücken zu schließen gilt bzw. dringender Wohnbedarf der Bevölkerung durch bauliche Nutzung der Baulücken zu decken ist, hat der Gesetzgeber mit den Möglichkeiten des Baugebots auch aus Gründen des dringenden Wohnbedarfs der Bevölkerung, ggf. sogar nach Durchführung eines Enteignungsverfahrens (vgl. § 176 BauGB, § 8 Abs. 1 und 3 BauGBMaßnG), eine gesetzgeberische Wertung getroffen, wie diesen Mißständen zu begegnen ist.

Dabei hat er jedoch keine Aufgabenzuweisungsnorm geschaffen, wonach die Gemeinden neben der Bauleitplanung mit den dafür vorgesehenen Mitteln auch die Aufgabe zu erfüllen haben, bauwilligen Interessenten die Auswahl von Baulücken als Baugrundstücke durch Aufstellen eines „Baulückenkatasters" in Katalogform zu erleichtern, um dadurch den privatwirtschaftlichen Markt für Baulücken zu aktivieren.

Fehlt es den Gemeinden somit an einer Zuweisungsnorm für die beschriebene Aufgabe, so läßt sich die Veröffentlichung der personenbezogenen Daten in einem Baulückenkataster nur mit schriftlicher Einwilligung der Betroffenen gemäß § 4 Satz 1 Buchstabe b DSG NW vornehmen. Die Veröffentlichung eines „Baulückenkatasters" begegnet nur dann keinen datenschutzrechtlichen Bedenken, wenn der Eigentümer oder die Eigentümerin in Kenntnis der Umstände schriftlich eingewilligt hat.

### 5.4.2 Bauakten

Im Zusammenhang mit dem Wunsch eines Rechtsnachfolgers, bei einem bebauten Grundstück wegen einer beabsichtigten Umbaumaßnahme in die Bauakte seines Rechtsvorgängers Akteneinsicht zu nehmen, war ich gezwungen, grundlegend zur Führung von Bauakten Stellung zu nehmen. In der Bauakte waren die bautechnischen Daten, die von dem Bauamt als „objektbezogene Daten" bezeichnet wurden, der persönliche Schriftverkehr des Rechtsvorgängers mit dem Bauamt und ein Beschwerdevorgang von Hausbewohnern über den Rechtsnachfolger zusammengefaßt.

Die von der Gemeinde als „objektbezogen" bezeichneten Daten sind gleichwohl für die datenschutzrechtliche Bewertung als personenbezogen einzustufen, da nach § 3 Abs. 1 DSG NW personenbezogene Daten auch Einzelangaben über sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person sind. Dieser Datenbestand ist in seiner Gesamtheit, wenn er von den anderen Unterlagen getrennt ist, im Hinblick auf das Verlangen nach Akteneinsicht datenschutzrechtlich anders zu behandeln als die übrigen genannten Unterlagen.

Auf das Verlangen nach Akteneinsicht durch den Rechtsnachfolger ist § 18 DSG NW nicht anzuwenden, da der Vorgang, in den eingesehen werden soll, nicht zu seiner Person gespeicherte Daten enthält bzw. nicht enthalten darf. Der Rechtsnachfolger ist in diesem Zusammenhang vielmehr als Dritter anzusehen, an den personenbezogene Daten, soweit nicht bereichspezifi-

sche Regelungen bestehen, nur unter den Voraussetzungen des § 16 DSG NW übermittelt werden dürfen. Eine danach zulässige Übermittlung könnte allerdings auch in der Form der Akteneinsichtgewährung erfolgen.

Soweit der Rechtsnachfolger geltend macht, wegen einer geplanten Umbaumaßnahme Akteneinsicht nehmen zu müssen, ist deshalb zu prüfen, ob insoweit ein rechtliches (§ 16 Abs. 1 Buchstabe c DSG NW) oder ein berechtigtes Interesse (§ 16 Abs. 1 Buchstabe d DSG NW) vorliegt. Nach meiner Auffassung dürfte hinsichtlich der „objektbezogenen" Daten in der Regel kein Grund zu der Annahme bestehen, daß das Geheimhaltungsinteresse des Rechtsvorgängers als Betroffener überwiegt (§ 16 Abs. 1 Buchstabe c). Soweit das Ergebnis der Überprüfung das Vorliegen lediglich eines berechtigten Interesses ergeben würde, wäre die Gewährung von Akteneinsicht nur zulässig, wenn der Rechtsvorgänger als Betroffener dieser Datenübermittlung nicht widersprochen hat (§ 16 Abs. 1 Buchstabe d). In diesem Fall ist der Rechtsvorgänger als Betroffener über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck in geeigneter Weise zu unterrichten.

Unverständlich war, wie in der Bauakte des Rechtsvorgängers ein Beschwerdevorgang über den Rechtsnachfolger geführt wurde. Eine derartige Vermischung von Datenbeständen erscheint unzulässig. Derartige Vorgänge sind, soweit sie zulässigerweise aufzubewahren sind, gesondert zu führen. Eine fehlerhafte Zusammenführung von Daten in einem Vorgang kann einem ansonsten berechtigten Auskunftsverlangen nicht entgegengehalten werden. Auf meine Anregung hin hat die Gemeinde mitgeteilt, daß das Bauordnungsamt bereits damit begonnen habe, die Unterlagen mit „objektbezogenen" Daten in einem gesonderten Ordner der Bauakte zu führen bzw., falls dies im Einzelfall noch nicht geschehen ist, entsprechend zu verfahren, wenn sich ein Rechtsnachfolger melden sollte. Für den Beschwerdevorgang wurde ebenfalls eine besondere Akte angelegt.

### 5.4.3 Lagepläne für Zwangsversteigerung

Durch eine Gemeinde wurde ich auf die Praxis eines Amtsgerichts aufmerksam gemacht, das bei der Anforderung der Lagepläne von Liegenschaften, für die eine Zwangsversteigerung angeordnet ist, jeweils eine Ausfertigung des Anordnungsbeschlusses über die Zwangsversteigerung beigefügt hatte. Aus diesem Anordnungsbeschluß, der mit dem Anschreiben offen versandt wurde, war für die Gemeinde genau zu erkennen, wer gegen wen und warum die Zwangsversteigerung betreibt.

Die Übersendung eines Anordnungsbeschlusses mit allen darin enthaltenen sensiblen personenbezogenen Daten ist weder zur Aufgabenerfüllung des Katasteramtes noch des Amtsgerichts erforderlich. Das Katasteramt benötigt zur Erledigung des Verlangens des Amtsgerichts nach einer Lageskizze des Beschlagnahmeobjektes lediglich die Grundstücksdaten, das Aktenzeichen des Amtsgerichts sowie die Angabe des Verwendungszwecks.

Zur Vermeidung von Verstößen gegen den verfassungsrechtlichen Grundsatz der Erforderlichkeit habe ich daher angeregt, zukünftig auf die Übersendung des Anordnungsbeschlusses an das Katasteramt zu verzichten und lediglich die zur Aufgabenerfüllung des Katasteramtes erforderlichen Daten zu übermitteln. Das Amtsgericht hat mitgeteilt, daß es meiner Anregung folgen wird.

## 5.5 Kommunalwesen

Das Innenministerium hat mir den Referentenentwurf des Gesetzes zur Änderung der Kommunalverfassung zur Stellungnahme übersandt. Zur darin enthaltenen **Novellierung der Gemeindeordnung** habe ich aus der Sicht des Datenschutzes Stellung genommen.

Der Entwurf enthält selbst nur wenige bereichspezifische Datenschutzregelungen. Dies wird damit begründet, daß das allgemeine Datenschutzrecht, also insbesondere das DSG NW ausreicht, um die Bürgerinnen und Bürger vor einer uneingeschränkten Weitergabe persönlicher Daten an Dritte zu schützen. Als Sachverhalte, die einer bereichspezifischen Datenschutzregelung zugeführt werden, sind aufgezählt das Akteneinsichtsrecht der Ratsmitglieder, die Datenpreisgabe in öffentlichen Sitzungen, Datenweitergabe an Mitarbeiterinnen und Mitarbeiter von Fraktionen sowie die Verpflichtung zur Offenlegung der wirtschaftlichen und persönlichen Verhältnisse der Ratsmitglieder. Nach meiner Auffassung besteht aber über die bisher im Referentenentwurf vorgesehenen Datenschutzregelungen hinaus ein erheblich weiterer bereichspezifischer Regelungsbedarf.

Das gesetzgeberische Vorhaben, die Kommunalverfassung zu ändern, sollte dazu genutzt werden, das **Verhältnis zwischen Verwaltung und Rat** in datenschutzrechtlicher Hinsicht insgesamt normenklar zu regeln. So ist bisher keine Regelung erkennbar, welche Instanz den Datenschutz für den Bereich des Rates im Sinne von § 7 DSG NW sicherstellt. Bei zunehmendem Einsatz von automatisierter Datenverarbeitung im Rat und insbesondere in den Fraktionen ist zudem nicht erkennbar, welche Instanz die Anforderungen zur Datensicherheit gemäß § 10 Abs. 1 Satz 1 DSG NW für die Rats- und Fraktionsarbeit gewährleistet.

Bei Ausscheiden einer **Fraktion** ist auch nicht geregelt, was mit den von ihr gespeicherten personenbezogenen Daten geschieht. Ein ungelöstes Problem ist der bei den Fraktionen im Laufe der Ratsarbeit entstehende Mischdatenbestand aus Daten, die dem Bereich der Parteiarbeit zuzurechnen sind, und Daten, die aus der Ratsarbeit stammen. Nach der Rechtslage wäre es eine unzulässige Zweckänderung, wenn personenbezogene Daten aus der Ratsarbeit von der ausscheidenden Fraktion „mitgenommen" und für Zwecke der Parteiarbeit genutzt würden.

Aber auch bei Fraktionen, die über mehrere Wahlperioden im Rat vertreten sind, wird hinsichtlich der Verarbeitung personenbezogener Daten nicht deutlich, welche Daten wie lange zu welchem Zweck aufzubewahren, welche Daten wann unter welchen Sicherungsmaßnahmen zu löschen sind und welche Instanz die ordnungsgemäße Einhaltung der Regelungen der

Datenverarbeitung überwacht. Die Bürgerinnen und Bürger, die sich an eine Fraktion mit einem Anliegen wenden, können deshalb kaum noch abschätzen, wer was wann und wie lange über sie weiß.

Als besonders bedenklich ist einzustufen, daß immer wieder personenbezogene Daten aus Vorgängen, die dem Rat zur Beratung und Entscheidung vorliegen, ohne Rechtsgrundlage an **private Dritte** und die **Presse** weitergegeben werden. Solche Fälle waren in der Vergangenheit mit den mir zur Verfügung stehenden Mitteln in der Regel nicht abschließend aufklärbar. Gerade in diesem Punkt sollte nach meiner Auffassung durch die Novellierung der Kommunalverfassung eine Änderung erreicht werden.

## 5.6 Rechtswesen

### 5.6.1 Behinderung vorbeugender Datenschutzkontrolle

Durch einen anderen Landesbeauftragten für den Datenschutz bin ich darauf aufmerksam gemacht worden, daß das Bundesministerium der Justiz in einem Schreiben an die Landesjustizverwaltungen verschiedene Fragen aufgeworfen habe, die im Zusammenhang mit Überwachungsmaßnahmen im **Funktelefon-Netz C** stehen. Diese Fragen besitzen erhebliche datenschutzrechtliche Bedeutung. So soll durch Erfassen der Daten über Aufenthaltsbereiche von Mobiltelefonen die Erstellung von „Bewegungsbildern" der Anschlußinhaber möglich sein.

Das Justizministerium, das ich um Überlassung einer Kopie der entsprechenden Unterlage zur Durchführung einer eigenen datenschutzrechtlichen Prüfung gebeten hatte, hat mein Auskunftsverlangen abgelehnt. Da diese Fragen bundesweite Maßnahmen sowie mögliche bundesgesetzliche Regelungen beträfen, das Schreiben des Bundesministeriums der Justiz im übrigen als VS-NfD gekennzeichnet sei, halte das Justizministerium es für sachgerecht, von einer Weitergabe der Informationen abzusehen. Der weiteren Begründung der Ablehnung ist zu entnehmen, daß das Justizministerium es zur Voraussetzung für die Überlassung der von mir erbetenen Unterlagen macht, daß es im jeweiligen Fall erkennen kann, inwiefern in diesem Zusammenhang eine Rechtsverletzung möglich wäre.

Eine vorbeugende Datenschutzkontrolle (§ 22 Abs. 1 DSG NW) sowie eine Zusammenarbeit mit anderen Datenschutzbeauftragten (§ 22 Abs. 5 DSG NW) ist mir bei dieser Haltung des Justizministeriums nicht (mehr) möglich.

In einem anderen Fall hatte ich das Justizministerium um Übersendung des Entwurfs zur Änderung der **Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten** (RiVASt) gebeten. Nach über einem Monat erreichte mich die Aufforderung des Justizministeriums „für eine kurze Begründung dieser Bitte, die mir ermöglicht, eine entsprechende Entscheidung über die Übersendung zu treffen". Auf Grund des Hinweises auf meine Kontrollbefugnis nach § 22 Abs. 1 DSG NW erhielt ich nach dann bereits über zwei Monaten eine andere Unterlage übersandt, als sie von mir erbeten war. Eine Stellungnahme zu den Richtlinien, wie von mir ursprünglich beabsichtigt

und gegenüber dem Justizministerium auch angekündigt, war dann aus zeitlichen Gründen nicht mehr möglich. Als Unterlage wurde nicht das zur Diskussion gestellte Papier übersandt, sondern das Ergebnis der Diskussion, der bereits zwischen dem Bundesministerium der Justiz und den Landesjustizverwaltungen abgestimmte Entwurf. Die Abstimmung erfolgte in den zwei Monaten, die das Justizministerium für die Bearbeitung meines Auskunftsverlangens benötigte. Auch durch zeitliche Verzögerung kann eine rechtzeitige Datenschutzkontrolle ausgeschlossen werden.

An diesen Fällen wird die Auffassung des Justizministeriums deutlich, daß offenbar der Landesbeauftragte für den Datenschutz bei der Vorbereitung von datenschutzrelevanten Regelungen durch den Bund nicht informiert werden soll, obwohl das Land an der Gestaltung solcher Regelungen mitwirkt und deren Ausführung auch später im Landesbereich erfolgt. Unter diesen Voraussetzungen sehe ich derzeit zumindest in Teilen eine wirksame vorbeugende Datenschutzkontrolle im Bereich des Justizministeriums als nicht (mehr) möglich an. Datenschutzkontrolle darf sich aber nicht auf nachgehende Überprüfung beschränken, sondern muß auch im Vorfeld tätig werden, um Datenschutzverletzungen von vornherein zu vermeiden.

### 5.6.2 Strafsachen

In meinem 10. Tätigkeitsbericht (S. 17/18) hatte ich bereits auf ein Mißverhältnis bei der Gesetzgebung im Bereich der Justiz hingewiesen. Einerseits werden umfangreiche gesetzgeberische Aktivitäten entfaltet, mit denen das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger zunehmend eingeschränkt wird. Andererseits ist fast zehn Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts immer noch nicht absehbar, wann die Datenverarbeitung im Justizbereich allgemein und umfassend entsprechend den Forderungen dieses Urteils auf normenklare gesetzliche Grundlagen gestellt wird. Dieser Trend wird deutlich an dem **Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität** (OrgKG) vom 15. Juli 1992, das inzwischen in Kraft getreten ist. Die gegen den Gesetzentwurf vorgebrachten Bedenken der Datenschutzbeauftragten des Bundes und der Länder sind nicht berücksichtigt worden. Das Gesetz enthält eine Fülle von weitreichenden Eingriffsbefugnissen, ohne hinreichend normenklar die Voraussetzungen und Folgen zu regeln.

Zusätzlich sollen, wie eine breite Diskussion in der Öffentlichkeit zeigt, nunmehr auch das Abhören und Aufzeichnen des gesprochenen Wortes in und aus Wohnungen (sog. **Lauschangriff**) gesetzlich verankert werden. Hierzu haben die Datenschutzbeauftragten des Bundes und der Länder mit Ausnahme des Bayerischen Datenschutzbeauftragten in einer Entschließung vom 1./2. Oktober 1992 auf die verfassungsrechtliche Problematik und die sehr grundsätzlichen Bedenken hingewiesen (vgl. Anlage 3, S. 162/163).

Mir war bekanntgeworden, daß das Justizministerium des Landes Schleswig-Holstein neue Richtlinien für die **Zusammenarbeit der Justizbehörden mit**

**den Medien** in Kraft gesetzt hat, die einen deutlich verbesserten Datenschutz enthielten. So ist festgelegt, daß die Nennung der Namen von Verfahrensbeteiligten (Beschuldigten, Opfern, Zeugen) ohne deren Zustimmung unterbleibt. Bei Jugendlichen ist ihre und die Zustimmung der gesetzlichen Vertreter notwendig. Es sollen auch alle Angaben, die zur Identifizierung von Verfahrensbeteiligten geeignet sein könnten, unterbleiben. Derartige Vorschriften fehlen in den Richtlinien für die Zusammenarbeit mit der Presse für Nordrhein-Westfalen. Auf meine Frage, ob und wann mit einer entsprechenden Überarbeitung der nordrhein-westfälischen Richtlinien zu rechnen sei, hat mir das Justizministerium mitgeteilt, daß es dazu gegenwärtig keine Veranlassung sähe.

Aus konkretem Anlaß war die Frage zu prüfen, ob und inwieweit nach einer zulässigen **Aktenüberlassung an Dritte** die Verpflichtung der öffentlichen Stelle weiterbesteht, hinsichtlich dieser Akten einen ausreichenden Datenschutz zu gewährleisten. In dem zugrunde liegenden Fall hatte ein Rechtsanwalt über einen längeren Zeitraum auf dem Rücksitz seines Pkw mehrere Akten eines umfangreichen Strafverfahrens in einer Weise befördert, daß zumindest beim Parken des Fahrzeugs am Straßenrand der Name des Betroffenen und das Aktenzeichen des Verfahrens für jeden Passanten deutlich lesbar waren.

Diese Datenübermittlung an beliebige Passanten war selbstverständlich unzulässig. Auch unter dem Gesichtspunkt der Datensicherung scheidet der Rücksitz eines Fahrzeugs als sicherer Aufbewahrungsort für Verfahrensakten mit derart sensiblen Daten aus. Nach meiner Auffassung hat die Staatsanwaltschaft, die die Akten herausgegeben hatte, eine bleibende Verantwortung für einen datenschutzkonformen Umgang bei der Überlassung von Akten mit personenbezogenen Daten an Dritte. Wenn feststeht, daß mit den Akten nicht ordnungsgemäß umgegangen worden ist und für die Zukunft ein verändertes Verhalten nicht erreicht werden kann, besteht insoweit für die Staatsanwaltschaft als speichernde Stelle die Verpflichtung, für Abhilfe zu sorgen. Auf meine Bitte hin hat die Staatsanwaltschaft das Rechtsanwaltsbüro aufgefordert, die Akten aus dem Pkw zu entfernen bzw. so abzulegen, daß Unbefugte keinen Einblick nehmen können. Der Rechtsanwalt ist dieser Aufforderung nachgekommen.

### 5.6.3 Zwangsvollstreckung

Ein Bürger hatte mich auf das Vorgehen eines **Gerichtsvollziehers** aufmerksam gemacht, der seiner Meinung nach unter Verletzung des Datenschutzes eine **Computeranlage** und Disketten **gepfändet** hatte. Der Gerichtsvollzieher hatte eine Personalcomputeranlage bestehend aus einem Rechner, Diskettenlaufwerk, einer Tastatur, einem Bildschirm, einem Drucker sowie einem Modem und die dazugehörige auf Disketten abgespeicherte Software beschlagnahmt und im Wege des Vermieterpfandrechts an den Vermieter übergeben. Durch Übergabe der Disketten an den Vermieter sind die darauf enthaltenen Daten an ihn übermittelt worden. Eine Rechtsgrundlage für die

Übermittlung personenbezogener Daten des Betroffenen durch den Gerichtsvollzieher an den Vermieter ist nicht ersichtlich.

Es ist zu fragen, ob nicht bei Disketten, die die Bezeichnung wie etwa „Briefe" oder „Haushaltsdaten, Privatdaten" tragen, bereits eine Unpfändbarkeit nach § 811 Nr. 10 und 11 ZPO auf Grund des Inhalts besteht. Es bleibt in diesem Zusammenhang zudem zu prüfen, ob gebrauchte Disketten, soweit sie nicht erkennbar Original-Software enthalten, von einer Pfändung durch den Gerichtsvollzieher generell auszunehmen sind, da gebrauchte Disketten in der Regel keinen Marktwert haben dürften. Weiter ist zu überlegen, ob nicht bei Pfändung eines Personalcomputers mit Festplatte, dem Betroffenen Gelegenheit gegeben werden muß, die auf der Festplatte vorhandenen Daten auf Diskette zu nehmen und die personenbezogenen Daten auf der Festplatte zu löschen. Im Hinblick darauf, daß die Zwangsvollstreckung in EDV-Sachen – Hard- und Software – offenbar erst in jüngster Zeit zunimmt und die entsprechende Rechtsprechung in der Zwangsvollstreckung noch nicht gefestigt ist, ist zudem zu überlegen, ob den Gerichtsvollziehern für die Zwangsvollstreckung in Datenverarbeitungsanlagen und Disketten Hilfen, etwa in Form einer Dienstanweisung oder eines Erlasses, an die Hand zu geben sind.

Auf meine Bitte um eine entsprechende Stellungnahme hat mir das Justizministerium mitgeteilt, es könne eine in naher Zukunft liegende abschließende Stellungnahme nicht in Aussicht stellen.

### 5.6.4 Grundbuch

Anläßlich der Novellierung der Grundbuchordnung im Jahre 1985 haben Datenschutzbeauftragte bereits vorgeschlagen, zur besseren Wahrung der Rechte der betroffenen Grundstückseigentümer und dinglich Berechtigten Einsichtnahmen in Grundakten und Grundbücher zu protokollieren. Begründung hierfür war, daß vielfach Datenschutzverstöße nicht aufklärbar waren, da mangels Protokollierung nicht feststellbar war, wer in die Grundbuchakten Einsicht genommen hatte. Seinerzeit wurde die Angelegenheit nach Erörterung zwischen den Justizministerien des Bundes und der Länder unter Hinweis auf die verfahrenstechnischen Schwierigkeiten nicht weiter verfolgt.

Nunmehr hat das Abgeordnetenhaus von Berlin im Rahmen eines Gesetzes zur Ausführung des Gerichtsverfassungsgesetzes (AG GVG) eine Regelung getroffen, die dem Anliegen der **Protokollierung von Einsichtnahmen**, das auch ich unterstütze, umfassend Rechnung trägt. Die Regelung betrifft neben den Grundbuchämtern auch andere Bereiche der Justiz (§ 21 Abs. 5 AG GVG Berlin).

Im Gesetz ist festgelegt, daß bei Einsicht in Akten die Tatsache der Datenweitergabe in den Akten zu vermerken ist. Diese gesetzliche Regelung wird noch durch eine Verfügung ergänzt, die festlegt, daß die Eintragungen ausschließlich von den Geschäftsstellenbediensteten auszuführen sind. Die Listen über erfolgte Grundbucheinsichten sind bei nachfolgenden Einsichtnahmen jeweils aus den Akten herauszunehmen, denn sie erhalten ihrerseits geschützte personenbezogene Daten der jeweiligen vorhergehenden Ein-

sichtnehmenden. Ausnahmen hiervon gelten lediglich für dinglich Berechtigte, da die Protokollierungspflicht gerade ihren Schutz bezweckt. Sie sollen jederzeit durch die Einsicht in die vorbezeichneten Listen in die Lage versetzt werden zu erkennen, an wen ihre im Grundbuch gespeicherten Daten übermittelt worden sind.

Aus der Sicht des Datenschutzes halte ich es für zwingend erforderlich, auch für Nordrhein-Westfalen eine entsprechende Regelung zu schaffen. Die Feststellung und Überprüfung von Datenschutzverstößen sollte auch in diesem Bereich möglich sein. Bereiche, die wegen fehlender Protokollierung faktisch kontrollfrei sind, sind mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar.

Das Justizministerium hat mir hierzu mitgeteilt, daß es derzeit keine Notwendigkeit sehe, entsprechend den Berliner Vorstellungen im Rahmen eines Gesetzes zur Ausführung des Gerichtsverfassungsgesetzes eine ausdrückliche Regelung zu treffen, daß die Einsichtnahmen im Grundbuch protokolliert werden.

### 5.6.5 Strafvollzug

Im Bereich des Strafvollzugs wurden wiederum eine Reihe von Datenschutzfragen an mich herangetragen.

Bei meiner Kontrolltätigkeit habe ich mehrfach festgestellt, daß sich Datenschutzprobleme, die in einer Justizvollzugsanstalt schon gelöst worden sind, in einer anderen wiederholen. Eine **Dienstanweisung für Datenschutz** im Justizvollzugsbereich, die unter Berücksichtigung der unterschiedlichen Vollzugsarten den Bediensteten im Umgang mit dem Recht auf informationelle Selbstbestimmung der Gefangenen eine Handlungshilfe bietet, könnte hier wesentliche Verbesserungen bewirken. Die Dienstanweisung müßte insbesondere Vorgaben enthalten für den im Vollzug zu findenden Ausgleich zwischen dem Recht auf informationelle Selbstbestimmung der Gefangenen, dem Vollzugsziel, dem Recht auf informationelle Selbstbestimmung der Justizvollzugsbediensteten, den Sicherheitsinteressen der Bediensteten, den schutzwürdigen Belangen Dritter außerhalb der Anstalten, den personellen Möglichkeiten und den baulichen Gegebenheiten der Anstalten.

Als Schritt in die richtige Richtung bewerte ich deshalb, daß es mir im Rahmen eines Kontrollbesuchs bei einer Justizvollzugsanstalt gelungen ist, daß die anstehenden Datenschutzprobleme in einer **Hausverfügung** geregelt werden. Darin wird u. a. festgelegt, daß die Zellenbelegungskladden in den Abteilungskanzeln, die die Angaben Name, Vorname, Geburtsdatum, sowie die Gefangenenbuchnummer aller auf der Abteilung befindlichen Gefangenen enthalten, nunmehr so aufbewahrt werden, daß die Mitgefangenen diese Daten nicht mehr beliebig ablesen können. Bei der Postkontrolle in den Abteilungskanzeln ist dafür Sorge zu tragen, daß grundsätzlich kein Gefangener die Möglichkeit hat, Anschrift oder Absender einer Postsendung zu erkennen. Zettel, die Zusatzinformationen für Schon- oder Krankenkost, sowie den Namen des Gefangenen enthalten, sind nicht mehr an den Zellen-

türen anzubringen, sondern in den Abteilungskanzeln aufzubewahren. Gespräche der Bediensteten untereinander über Gefangene sind so zu führen, daß Unbefugte nicht mithören können. Auch für die Abwicklung privater Besuche in der Justizvollzugsanstalt wurde ein Verfahren gefunden, das dem Recht auf Datenschutz der Besucherinnen und Besucher sowie des Gefangenen Rechnung trägt.

Für die Fertigung einer Diplomarbeit erhielt ein Student die Erlaubnis des Justizministeriums, in einer **Justizvollzugsanstalt** zu **fotografieren**. Ein Betroffener hat sich dagegen gewandt, gegen seinen Willen in Anstaltskleidern vor der offenen Haftraumtür fotografiert zu werden.

Das Justizministerium hat sich hierzu auf seine Richtlinien für die Zusammenarbeit mit der Presse berufen. Danach sind Aufnahmen von Gefangenen nur zulässig, wenn gewährleistet ist, daß diese nicht erkennbar sind und die Erreichung des Vollzugsziels nicht gefährdet wird. Sollen Gefangene in einer Weise fotografiert werden, daß sie vom Betrachter der Aufnahme identifiziert werden können, so ist außer der schriftlichen Zustimmung des Gefangenen die Erlaubnis des Präsidenten des Vollzugsamtes einzuholen. Alle Personen, denen die Herstellung von Aufnahmen in Vollzugseinrichtungen gestattet wird, werden auf diese Vorschriften hingewiesen. Der Anstaltsleiter achtet auf deren Einhaltung.

Nach der von mir eingeholten Stellungnahme zeigen die in der Vollzugsanstalt aufgenommenen Fotos lediglich Teilansichten (kopflose Körper, Unterarme und dgl.) einiger Gefangener, so daß eine Zuordnung dieser Fotos zu einem bestimmten Gefangenen nicht möglich ist. Nach meiner Auffassung verlangen es die Datenschutzrechte der Gefangenen, daß alle in der Anstalt aufgenommenen Fotos einschließlich der Negative der Vollzugsanstalt zur Prüfung vorgelegt werden, ob Rechte der Gefangenen betroffen sein könnten. Demgegenüber hat es das Justizministerium für ausreichend angesehen, daß lediglich die zur Verwendung bestimmten Fotos durch den zuständigen Referenten des Justizministeriums überprüft werden.

Durch eine Eingabe bin ich auf die Praxis der **Postnachsendung** einer Justizvollzugsanstalt aufmerksam gemacht worden, die eingehende Post ehemaliger Insassen, die lediglich in eine andere Anstalt verlegt worden waren, mit dem Vermerk „unbekannt verzogen" an den Absender zurückzusenden. Nunmehr ist festgelegt, daß die Post innerhalb des Vollzugsbereichs weiterzuleiten ist, wenn ein Gefangener zwar in eine andere Anstalt verlegt worden ist, sich aber weiterhin im Vollzug befindet.

In einer **Gefangenenpersonalakte** waren auf einer Liste persönliche Daten von Bediensteten des Justizvollzugsbereichs enthalten, die im Falle der Entlassung des Gefangenen aus der Haft schutzbedürftig sind. Hierzu gehören z. B. Fälle, in denen der Gefangene in der Vergangenheit Repressalien angedroht hatte. Im Rahmen eines Strafverfahrens war eine solche Akte von der Staatsanwaltschaft als Beweismittel beigezogen, dem Gericht vorgelegt und den Verteidigern in Ablichtung zur Verfügung gestellt worden. Die Ablichtung der Liste ist dem Gefangenen von seinen Verteidigern überlassen

worden. Wie das Justizministerium mir auf meine Anfrage mitgeteilt hatte, vermochte es einen Verstoß gegen Bestimmungen des Datenschutzes insoweit nicht zu erkennen.

Nach meiner Auffassung bestehen gegen die Aufbewahrung einer derartigen Liste in der Gefangenenpersonalakte erhebliche datenschutzrechtliche Bedenken. Eine Rechtsgrundlage für die listenförmige Speicherung der Daten Bediensteter, die bei der Entlassung eines Gefangenen gefährdet und hierüber zu unterrichten sind, in der Gefangenenpersonalakte ist nicht zu erkennen. Wie der Vorfall zeigt, besteht die Gefahr, daß bei Aufnahme einer Liste gefährdeter Personen in die Gefangenenpersonalakte die Möglichkeit der Kenntnisnahme durch den Gefangenen geschaffen wird.

Nach § 10 DSG NW haben die Justizvollzugsanstalten die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine den Vorschriften des Datenschutzgesetzes entsprechende Verarbeitung der Daten sicherzustellen. Werden personenbezogene Daten in Akten verarbeitet, sind Maßnahmen zu treffen, um insbesondere den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern. Dies scheint mir bei den gemäß Nr. 58 Abs. 2 Vollzugsgeschäftsordnung geführten Gefangenenpersonalakten nicht gewährleistet zu sein.

Zur Vermeidung weiterer Verstöße gegen Vorschriften über den Datenschutz habe ich daher dem Justizministerium empfohlen, die Gefangenenpersonalakten mit Unterordnern, wie z. B. einem Sicherheitsordner, führen zu lassen. Hierdurch wäre es den Gerichten auch möglich, ihre Ersuchen auf Herausgabe von Gefangenenpersonalakten auf den Umfang zu beschränken, der für ihre Aufgabenerfüllung erforderlich ist. Das Justizministerium hat mitgeteilt, daß es meiner Empfehlung nicht folgen wird. Die Wiederholung eines derartigen Vorfalls erscheint daher nicht ausgeschlossen.

### 5.6.6 Häftlingsüberwachung

Es bestand Anlaß, die von der Ständigen Konferenz der Innenminister und -senatoren der Länder am 3. Mai 1991 beschlossenen Maßnahmen zur Bekämpfung des Terrorismus gegenüber dem Justizministerium aufzugreifen. Die darin vorgesehene Unterstützung der Justiz bei der Häftlingsüberwachung durch die Polizei und den Verfassungsschutz begegnet datenschutzrechtlichen Bedenken, da es im Strafvollzugsgesetz an einer Rechtsgrundlage für ein Tätigwerden von Polizei und Verfassungsschutz im Justizvollzugsbereich fehlt. Nach § 155 Strafvollzugsgesetz (StVollzG) sind die Aufgaben der Justizvollzugsanstalt grundsätzlich von Justizvollzugsbediensteten wahrzunehmen. § 34 StVollzG regelt die Verwertung der im Rahmen der Häftlingsüberwachung gewonnenen Daten abschließend und sieht vor, daß Kenntnisse aus der Überwachung der Besuche oder des Schriftwechsels ausschließlich verwertet werden dürfen, wenn dies aus Gründen der Behandlung geboten ist, um die Sicherheit oder Ordnung der Anstalt zu wahren oder Straftaten oder Ordnungswidrigkeiten zu verhüten, zu unterbinden oder zu verfolgen.

Ich habe daher das Justizministerium gebeten, zu den im einzelnen aufgeführten Bedenken Stellung zu nehmen. An Stelle der erbetenen Stellungnahme hat das Justizministerium meine Anfrage jedoch im Hinblick auf den Entwurf eines Vierten Gesetzes zur Änderung des Strafvollzugsgesetzes, das eine datenschutzrechtliche Ergänzung dieses Gesetzes beinhalten soll, dem Bundesministerium der Justiz zugesandt und ihn um Prüfung der Vereinbarkeit der in Frage stehenden Bestimmungen mit den Vorstellungen der für den Verfassungsschutz zuständigen Behörden des Bundes und der Länder gebeten. Auch ein Jahr später enthielt sich das Justizministerium einer eigenen Stellungnahme mit dem Hinweis, ihm lägen keine Erkenntnisse zu dem o. g. Gesetzesvorhaben vor. Auf meine weitere Nachfrage, zu welchem Ergebnis die Prüfung meiner Bedenken, sei es auf Bundes-, sei es auf Landesebene, geführt hat, teilt mir das Justizministerium mit, dies sei ihm nicht bekannt. Im übrigen weist mich das Justizministerium darauf hin, daß

> „die Frage des Ob, Wann und Wie dieser Prüfung durch den Bundesminister der Justiz nicht Ihrer Kontrolle im Sinne von § 22 Abs. 1 DSG NW unterliegt und mithin auch nicht dem Bereich Ihrer Aufgabenerfüllung im Sinne von § 26 DSG NW zuzuordnen ist".

Wie das Justizministerium in diesem Zusammenhang seine eigene Zuständigkeit und Verantwortlichkeit für eine rechtswidrige Datenverarbeitung im Strafvollzugsbereich verneint und meine Kontrollzuständigkeit verkennt, wird daran deutlich, daß es meine Frage, wie es selbst die von mir aufgezeigten Bedenken der in seinem Bereich praktizierten Häftlingsüberwachung bewertet, wie folgt beantwortet:

> „Von einer eigenen Bewertung der in Ihrem Schreiben vom 19.07.1991 (26.8.11) angeführten Bedenken habe ich, da sie nicht ein dem hiesigen Ressort entstammendes Papier, sondern eine der ständigen Konferenz der Innenminister und -senatoren der Länder entstammende Entschließung zum Gegenstand haben, Abstand genommen."

### 5.6.7 Bewährungshelfer

Ein Bewährungshelfer hat sich an mich gewandt und um Beratung zu datenschutzrechtlichen Fragen im Zusammenhang mit einem **Bewährungsplan** gebeten. Im Rahmen der Überprüfung zeigte sich, daß Bewährungshelferinnen und Bewährungshelfer zwar in erheblichem Umfang sensible personenbezogene Daten aus fast allen Lebensbereichen ihrer Probanden und auch dritter Personen verarbeiten, mit der Lösung der damit im Zusammenhang stehenden datenschutzrechtlichen Probleme allerdings weitgehend allein gelassen sind. Es bestehen weder ausreichende normenklare Rechtsgrundlagen noch erläuternde Verwaltungsvorschriften. Auch im Wege der Rechts- und Fachaufsicht scheinen klärende Hinweise zur Lösung von Datenschutzfragen eher selten zu sein.

Soweit der Proband durch den vorgelegten Bewährungsplan verpflichtet wurde, zum Zwecke der Durchführung der Bewährungsaufsicht dem Bewährungshelfer auf Verlangen **Auskunft** zu erteilen über Wohnsitz und Arbeits-

stelle, Wechsel des Wohnsitzes und der Arbeitsstelle, sowie Einhaltung der Auflagen, Weisungen, Anerbieten und Zusagen, ist für eine derartige Datenerhebung eine Rechtsgrundlage nicht erkennbar. Sie läßt sich weder aus § 56 d StGB noch dem Gesetz über die Bewährungshelfer entnehmen. Im Hinblick auf den Charakter der Bewährung (§ 56 StGB) dürfte für den Probanden jedoch eine Obliegenheit vorliegen, diese Angaben zu machen. Bei einer Weigerung dürfte in der Regel ein Widerrufsgrund nach § 56 f StGB vorliegen. Der Umfang der in diesem Zusammenhang zu erhebenden Daten steht nicht im Belieben des jeweiligen Bewährungshelfers, sondern ist an den Verfassungsgrundsätzen der Verhältnismäßigkeit und Erforderlichkeit zu messen. Außerdem sind die Aufklärungspflichten gemäß § 12 Abs. 2 DSG NW zu beachten.

Soweit der Bewährungsplan eine Beschränkung der **Berichtspflicht gegenüber dem Gericht** vorsah, war diese Regelung nach meiner Auffassung nicht mit dem Wortlaut des § 56 d Abs. 3 Satz 3 StGB in Einklang zu bringen. Nach dieser Vorschrift hat der Bewährungshelfer über die Lebensführung des Verurteilten in Zeitabständen zu berichten, die das Gericht bestimmt. Es bestehen Zweifel, ob die Verwendung des Begriffs „Lebensführung" den Anforderungen des Bundesverfassungsgerichts in seinem Volkszählungsurteil an eine normenklare gesetzliche Grundlage für eine derartige Datenverarbeitung noch entspricht.

Aus der Sicht des Datenschutzes ist die Berichtspflicht aus Satz 3 unter Beachtung der Vorschrift des § 56 f StGB auszulegen. Insoweit ist die Übermittlung von Daten an das Gericht nur in dem Umfange zur Aufgabenerfüllung des Gerichts erforderlich, wie es für die Prüfung und Entscheidung über einen möglichen Widerruf relevant sein kann. In den Fällen, in denen diese Voraussetzungen fehlen, könnte ein Bericht nach Satz 3 sich in dem Hinweis auf das Fehlen relevanter Erkenntnisse erschöpfen. Festzuhalten bleibt, daß darüber hinaus Angaben an das Gericht, die für dessen Tätigwerden lediglich dienlich oder nützlich sein können, nur mit Einwilligung des Probanden übermittelt werden dürfen.

Datenschutzrechtliche Bedenken bestehen auch dagegen, daß der Bewährungshelfer ohne Wissen und vorherige rechtliche Aufklärung und Einwilligung des Probanden und ggf. betroffener Dritter, wie Ehepartner, Eltern, Geschwister, Freunde, Kollegen, Arbeitgeber, Vermieter, Gläubiger, Ärzte etc. anvertraute personenbezogene Daten in seiner Geschäftsakte erfaßt und speichert. Insoweit fehlt es an einer gesetzlichen Grundlage. Eine derartige Datenverarbeitung dürfte sich in der Regel auch nicht aus dem Bewährungsbeschluß ergeben. Eine **Verarbeitung personenbezogener Daten Dritter** bedarf daher in jedem Einzelfall der Einwilligung des Probanden (Ausnahme: § 13 Abs. 2 DSG NW) und der Einwilligung der jeweils betroffenen Dritten.

Einer Stellungnahme des Justizministeriums entnehme ich, daß es mit mir der Ansicht ist, daß in die Akten der Bewährungshelferinnen und Bewährungshelfer insgesamt nur die Daten aufzunehmen sind, die zur Erfüllung der Aufgaben notwendig sind.

Datenschutzrechtlich bedenklich war weiter, daß der Bewährungsplan zwar ein umfassendes **Akteneinsichtsrecht** des Probanden vorsah, im Gegensatz zu § 18 Abs. 3 DSG NW jedoch nicht die schutzwürdigen Belange Dritter berücksichtigte.

Zur **Verschwiegenheitspflicht** der Bewährungshelferinnen und Bewährungshelfer bin ich mit dem Justizministerium der Auffassung, daß bei der Mitteilung von Angaben im Rahmen der Bewährungsaufsicht gegenüber dem Gericht/der Gnadenstelle kein „unbefugtes" Offenbaren im Sinne von § 203 StGB vorliegt, wenn auch insoweit der Grundsatz der Erforderlichkeit beachtet wird.

Aus der Sicht des Datenschutzes wünschenswert wäre es, wenn im Interesse einer landesweit einheitlichen Handhabung der Bewährungsaufsicht das Justizministerium **Richtlinien für die Arbeit der Bewährungshilfe** erlassen würde, die auch die Datenverarbeitung der Bewährungshelferinnen und Bewährungshelfer im Hinblick auf die bestehenden Rechtsgrundlagen klarstellend auslegt. Bewährungspläne auf der Grundlage dieser Richtlinien dürften ein geeignetes Mittel sein, um das Recht auf informationelle Selbstbestimmung der Probanden und auch Dritter im Einzelfall zu gewährleisten. Das Justizministerium vertritt hierzu die Auffassung, im Hinblick auf die Fachaufsicht über die Bewährungshelferinnen und Bewährungshelfer durch das jeweils zuständige Gericht/die jeweils zuständige Gnadenstelle seien keine Verwaltungsbestimmungen zu treffen. Nach meiner Auffassung bedeutet aber der Erlaß derartiger Hinweise keinen Eingriff in die richterliche Unabhängigkeit.

## 5.7 Polizei

### 5.7.1 Arbeitsgrundlagen

Mit Runderlaß des Innenministeriums vom 19.04.1991 (MBl. NW. S. 697) wurden die **Verwaltungsvorschriften** zu dem seit 01.05.1990 gültigen **Polizeigesetz Nordrhein-Westfalen** (PolG NW) erlassen. Meine Bedenken, die ich bereits im 9. Tätigkeitsbericht (S. 35) und 10. Tätigkeitsbericht (S. 23) gegen die Entwürfe zum Gesetz zur Fortentwicklung des Datenschutzes im Bereich der Polizei und der Ordnungsbehörden aufgezeigt habe, konnten nur zum Teil durch klarstellende Auslegung in diesen Verwaltungsvorschriften ausgeräumt werden. In Teilbereichen hätte die datenschutzgerechte Handhabung der gesetzlichen Vorschriften durchaus gesteigert werden können, wenn der norminterpretierenden und ermessenssteuernden Funktion der Verwaltungsvorschriften mehr Gewicht beigemessen worden wäre. Leider ist das Innenministerium zum überwiegenden Teil nicht bereit gewesen, meinen Anmerkungen zu den Verwaltungsvorschriften zum Polizeigesetz zu folgen und entsprechende Änderungen und Hinweise einzuarbeiten.

Nach Inkrafttreten des Polizeigesetzes am 1. Mai 1990 entsprechen die **Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen** (KpS-Richtlinien), zumindest soweit sie Regelungen des Datenschutzes und der polizeilichen Datenverarbeitung enthalten, insgesamt nicht

mehr der geltenden Rechtslage. Die Richtlinien sind in vielen Punkten überholt, in anderen Punkten stehen sie zur geltenden Rechtslage im Widerspruch und in einigen Punkten hat sich die polizeiliche Datenverarbeitungspraxis bereits so verselbständigt, daß sie weder der geltenden Rechtslage noch den Richtlinien entspricht. Als Folge der Abweichung der Verwaltungsvorschrift von den zugrunde liegenden Rechtsvorschriften entstehen in der polizeilichen Praxis verschiedene Datenschutzprobleme und Datenschutzverstöße, die durch eine Überarbeitung der KpS-Richtlinien zu vermeiden wären. Hiervon habe ich mich bei einer Reihe von Kontrollbesuchen im Polizeibereich überzeugt. Auf meine Anfrage hin hat das Innenministerium mitgeteilt, daß in der ersten Jahreshälfte 1993 mit einem Entwurf bundeseinheitlich aktualisierter Rahmenrichtlinien zu rechnen ist.

Bei den Informations- und Kontrollbesuchen im Bereich der Polizei haben sich Datenschutzprobleme grundsätzlicher Art bei der Datenverarbeitung im Zusammenhang mit der **Führung von Kriminalakten** herausgestellt. Es bedarf unbedingt einer Überarbeitung des der Führung von Kriminalakten zugrunde liegenden Runderlasses des Innenministeriums vom 21. März 1988 (MBl. NW. S. 472), um den Datenschutz in den an dieser Stelle nur stichwortartig aufgezeigten Bereichen zu verbessern:

- technische und organisatorische Sicherung der Kriminalakten auf Grund baulicher Gegebenheiten,
- Zugangsbeschränkung zur Kriminalaktenhaltung,
- Trennung der Zentralen Jugendschutzdatei und der Kriminalakten über Polizeibeamte der eigenen Behörde vom übrigen Kriminalaktenbestand,
- Zugriffsbeschränkungen auch außerhalb der normalen Dienstzeit,
- Dokumentation der Einsichtnahme in Kriminalakten,
- Nachprüfbarkeit der Entscheidung, wer, aus welchen Gründen die Anlage einer Kriminalakte, die Länge der Laufzeit bzw. die Prüftermine, eine Speicherung im Kriminalaktennachweis des Landes oder des Bundes oder die Vergabe der personengebundenen Hinweise im polizeilichen Informationssystem INPOL veranlaßt hat,
- sachgerechte Bestimmung des Aussonderungsdatums und der Aussonderungsfrist einer Kriminalakte,
- Vergabe von personengebundenen Hinweisen, z. B. „geisteskrank" ohne nachprüfbare ärztliche Feststellung oder „BTM-Konsument" bei Drogenhändlern oder „Prostitution" an Prostituierte, zu denen auf freiwilliger Grundlage eine Kriminalakte mit erkennungsdienstlichen Unterlagen angelegt worden ist,
- Bereinigung des Altaktenbestands, der nicht einmal mehr den überarbeitungsbedürftigen KpS-Richtlinien entspricht,
- landesweite zweijährige Speicherung von Personen unter 14 Jahren mit dem personengebundenen Hinweis „gefährdete Minderjährige".

Das Innenministerium wertet die aufgezeigten Datenschutzprobleme noch aus und sieht sich derzeit nicht in der Lage, hierzu Stellung zu nehmen.

Lediglich zu dem bereits im 8. Tätigkeitsbericht (S. 30) behandelten Problem, daß die Polizeibehörden ihre Kriminalakten nach wie vor nahezu unabhängig von dem Ausgang der Verfahren bei der Justiz führen (**Rückmeldung Justiz – Polizei**), hat das Innenministerium im Einvernehmen mit dem Justizministerium inzwischen Stellung genommen. Leider wird darin jede Initiative, die zur Aktualisierung der polizeilichen Datensammlungen einerseits und damit dem Recht Betroffener auf Löschung unzutreffender und somit unzulässigerweise gespeicherter Daten andererseits dienen würde, mit dem Hinweis auf den Gesetzentwurf der Bundesregierung über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (Justizmitteilungsgesetz) zum jetzigen Zeitpunkt abgelehnt. Trotz meiner anläßlich der Kontroll- und Informationsbesuche gewonnenen Erkenntnisse zu der mangelhaften Unterrichtung der Polizei durch die Justiz über den Ausgang von Strafverfahren halten das Innenministerium und das Justizministerium wegen der zu erwartenden gesetzlichen Regelung und angesichts der bestehenden, sich in der Praxis allerdings nicht bewährenden Informationsmöglichkeiten der Polizei nach Nr. 11 der Anordnung über Mitteilungen in Strafsachen (MiStra) Abhilfemaßnahmen z. Z. für nicht geboten.

### 5.7.2 Informationssysteme

Im Berichtszeitraum hatte ich verschiedentlich Anlaß, mich mit der Speicherung personenbezogener Daten in polizeilichen Informationssystemen auseinanderzusetzen.

Zu meiner Anfrage nach der Speicherpraxis im Zusammenhang mit **Verstößen gegen § 218 StGB** hat das Innenministerium erklärt, daß Daten über Frauen, gegen die wegen einer Straftat nach § 218 Abs. 1 i.V.m. Abs. 3 StGB ermittelt wurde, ab sofort nicht mehr in Kriminalpolizeiliche personenbezogene Sammlungen aufzunehmen sind. Von ihrer Speicherung in polizeilichen Informationssystemen ist abzusehen. Da diese Daten in den kriminalpolizeilichen Sammlungen bzw. in polizeilichen Informationssystemen nicht listenmäßig zu recherchieren sind, wurde weiter verfügt, daß diese Daten auf Antrag der Betroffenen, ansonsten von Amts wegen zu löschen sind, wenn sie im Rahmen der laufenden Sachbearbeitung festgestellt werden.

Ebenfalls gelöscht wurden die **Daten von Palästinensern**, die zwecks vorbeugender Verbrechensbekämpfung während des Golfkrieges zur Polizei vorgeladen und deren Daten nach Übermittlung durch die Landespolizeibehörden seitens des Bundeskriminalamts länderübergreifend in der Arbeitsdatei PIOS-Innere Sicherheit (APIS) weit über das Ende des Golfkrieges hinaus gespeichert worden waren. Im Zuge der Überprüfung der Speicherung stellten sich die Anhaltspunkte für eine Speicherung, daß nämlich die Betroffenen sich möglicherweise an terroristischen Gewalttaten beteiligten, Gewalttäter unterstützten oder sachdienliche Hinweise geben könnten, als zu vage für eine bis 1994 vorgesehene Speicherung zum Zwecke der Gefahrenab-

wehr heraus. Die mehrfach geäußerten Bedenken der Datenschutzbeauftragten haben dazu geführt, daß die Erforderlichkeit der Speicherung auch seitens des Landeskriminalamts und des Innenministeriums verneint wurde.

Demgegenüber wurde seitens des Innenministeriums Nordrhein-Westfalen im Rahmen der Innenministerkonferenz der Einrichtung einer **Verbunddatei „Vermißte, unbekannte Tote, unbekannte hilflose Personen"** zugestimmt, auf die die Landespolizeibehörden bei den Ermittlungen im Zusammenhang mit diesem Personenkreis on-line Zugriff nehmen können. Die Erforderlichkeit der umfangreichen Verwendung von personengebundenen Hinweisen, der Speicherung von Namen Unbeteiligter sowie der möglichen Motive für ein Verschwinden der betreffenden Person („Streuner", „Abenteurer") wird gleichwohl noch begründet werden müssen, um die bestehenden datenschutzrechtlichen Bedenken auszuräumen.

Ebenfalls wird noch die Geeignetheit und Erforderlichkeit der von der Innenministerkonferenz beschlossenen **Verbunddatei „Gewalttäter Sport"** zu begründen sein, die den Polizeibehörden bei der Gefahrenabwehr im Zusammenhang mit Sportveranstaltungen dienen soll. Bislang ist dies trotz Aufforderung der Datenschutzbeauftragten des Bundes und der Länder durch die Polizei nicht hinreichend geschehen. Zur Begründung herangezogene Sachverhalte scheinen wegen ihrer Vereinfachung an den polizeipraktischen Erfordernissen vorbeizugehen. Sie lassen zudem völlig offen, wie die auf Namen potentieller Gewalttäter aufbauende Datei sinnvoll genutzt werden kann, wenn vor Ort die betreffenden Personen zunächst einmal mit all den bekannten praktischen Schwierigkeiten identifiziert werden müssen, bevor polizeitaktische Entscheidungen getroffen werden können.

Anders verhält es sich mit der **Zentralen Informationsstelle Sporteinsätze** (ZIS) beim Landeskriminalamt Nordrhein-Westfalen, die seit dem 03.02.1992 den Informationsaustausch der Landespolizeibehörden bei sportlichen Großveranstaltungen sicherstellen soll. Gegen die systematische und umfassende Unterrichtung der Polizeibehörden über die für die Beurteilung der Sicherheitsaspekte bei Fußballspielen nötigen Informationen, für die nach polizeilicher Einschätzung keine personenbezogenen Daten gebraucht werden, bestehen keine durchgreifenden datenschutzrechtlichen Bedenken. Da entgegen der Aussage des Innenministeriums anläßlich der Fußball-Europameisterschaft 1992 jedoch personenbezogene Daten seitens der ZIS verarbeitet worden sind, habe ich insoweit eine datenschutzrechtliche Prüfung eingeleitet.

### 5.7.3 Nutzung polizeilicher Informationssysteme

Wie bereits an früherer Stelle bemerkt (vgl. 10. Tätigkeitsbericht, S. 64/65), wird geradezu regelmäßig von betroffenen Bürgerinnen und Bürgern der Verdacht geäußert, daß Polizeibeamte **für private Zwecke** unbefugt personenbezogene Daten im Informationssystem der Polizei abfragen. Das Beispiel eines Polizeibeamten, der Angaben über sich selbst im polizeilichen Informationssystem abfragt und mir einen entsprechenden Ausdruck seiner Abfrage zur datenschutzrechtlichen Überprüfung der Speicherung seiner Daten zu-

sendet, trägt nicht dazu bei, den verschiedentlich von Betroffenen geäußerten Eindruck zu beseitigen, bei den polizeilichen Informationssystemen handele es sich um einen „Selbstbedienungsladen". Dies wird insbesondere darauf zurückzuführen sein, daß bei derartigen Abfragen lediglich das Terminal, von dem abgefragt wurde, und der Terminalbenutzer, nicht aber der die Abfrage veranlassende Beamte namentlich dokumentiert wird. Eine derartige Dokumentation, die aus Sicht der Polizei aus arbeitsökonomischen Gründen nicht ausgeweitet werden könne, minimiert das Risiko der Entdeckung unzulässiger Abfragen. So konnte in einem Fall einem Polizeibeamten, dessen Ehefrau in einem Zivilrechtsstreit Angaben über eine dritte Person machte, die offensichtlich nur aus dem polizeilichen Informationssystem stammen konnten, nicht nachgewiesen werden, daß er die am Tage vor der Gerichtsverhandlung von einem Terminal der Dienststelle durchgeführte Abfrage auch tatsächlich veranlaßt hatte.

Ähnlich stellt sich das Problem bei Abfragen im **Zentralen Verkehrsinformationssystem** (ZEVIS) dar. Weder die nach § 30 a Abs. 3 und § 36 Abs. 6 des Straßenverkehrsgesetzes (StVG) vorgesehene Grundprotokollierung eines jeden Abrufs noch die nach § 30 a Abs. 4 und § 36 Abs. 7 StVG vorgesehene stichprobenweise **Zusatzprotokollierung** für Abrufe aus dem zentralen Fahrzeugregister sowie aus dem Verkehrszentralregister ermöglichen eine Identifizierung aller abfragenden Personen. Ich habe daher das Innenministerium um Prüfung gebeten, inwieweit sich eine in den Bundesländern Bayern und Schleswig-Holstein bereits praktizierte Zusatzprotokollierung bei jeder ZEVIS-Abfrage auch in Nordrhein-Westfalen realisieren ließe. Ferner habe ich das Innenministerium gebeten, sich auf Bundesebene für die auch vom Bundesbeauftragten für den Datenschutz aufgestellte Forderung einzusetzen, daß bei der Zusatzprotokollierung die Angabe der Abfrageanlässe differenzierter durch einen von sechs auf zehn Abfragefälle erweiterten Katalog möglich ist. Auch wenn diese Maßnahmen keinen umfassenden Schutz vor mißbräuchlicher Nutzung des Zentralen Verkehrsinformationssystems bieten können, verbessern sie doch in angemessener Form die Möglichkeit, einem etwaigen Mißbrauch an Hand der vorhandenen Dokumentation nachzugehen und entfalten somit präventive Wirkung. In seiner Antwort kündigt das Innenministerium an, sich um eine „angemessene Zusatzprotokollierung" zu bemühen und sich für eine weitergehende Differenzierung der Abfrageanlässe einzusetzen.

Nach wie vor nicht hinreichend geregelt ist ferner der Zugriff der Polizei auf die Daten aus dem **örtlichen Fahrzeugregister**. Bereits in meinem 6. Tätigkeitsbericht (S. 132) habe ich grundsätzliche datenschutzrechtliche Bedenken gegen die Anwendung der sog. Schlüssellösung geltend gemacht, die es der Polizei ermöglichte, in den Räumen der Kfz-Zulassungsstelle außerhalb der üblichen Dienstzeiten Zugriff auf diese Daten zu nehmen. Anläßlich eines Informationsbesuchs bei einer Zulassungsstelle habe ich nunmehr festgestellt, daß es durchaus Praxis ist, den Polizeibehörden seitens der Zulassungsstelle den Gesamtbestand des örtlichen Fahrzeugregisters regelmäßig auf Mikrofiche zur Verfügung zu stellen. Mangels gesetzlicher Grundlage halte

ich dieses für datenschutzrechtlich unzulässig. Das Innenministerium teilt meine Auffassung. Es hat inzwischen die Einstellung dieser Datenübermittlung veranlaßt.

Das Problem unzulässiger **On-line-Zugriffe** der Polizei auf **andere Datenbestände** als die des Einwohnermeldeamts bzw. der Zulassungsstelle ist demgegenüber noch nicht gelöst. Wie ich in Erfahrung gebracht habe, ist es einigen Kreispolizeibehörden möglich, auf die Datenbestände der Führerscheinstelle on-line Zugriff zu nehmen, obwohl die erforderliche gesetzliche Grundlage im Sinne von § 9 Abs. 1 DSG NW für derartige Zugriffe auf das Führerscheinregister nicht vorhanden ist. Mangels gesetzlicher Grundlage ist daher der Zugriff der Kreispolizeibehörden auf das Führerscheinregister ebenso unzulässig wie die Unterhaltung der On-line-Verbindung durch die die Führerscheindaten zur Verfügung stellende Straßenverkehrsbehörde. Zu dieser Problematik hat das Innenministerium noch nicht Stellung genommen.

### 5.7.4 Informationssammlungen

Eine Reihe von polizeilichen Informationssammlungen, die neben den zulässigerweise geführten polizeilichen Informationssystemen angelegt worden waren, hat mir im Berichtszeitraum Anlaß zu einer datenschutzrechtlichen Überprüfung gegeben. Auf die „Säuferliste" und die „Wahllichtbildvorlage" soll hier beispielhaft eingegangen werden.

Die bei einer Kreispolizeibehörde geführte „**Säuferliste**" stellte sich als eine dem Streifenbefehl beigefügte Liste mit personenbezogenen Daten mutmaßlicher Alkoholsünder im Straßenverkehr dar, die sich zu einem Teil aus mitunter recht vagen Hinweisen aus der Bevölkerung, zum anderen aus dienstlichen Erkenntnissen bzw. aus Aussagen der in die Liste aufgenommenen Personen zusammensetzte. Eine Überarbeitung der Liste und die Löschung von Daten einzelner Betroffener erfolgte nach Darstellung der Kreispolizeibehörde in bestimmten Abständen, spätestens nach sechs Monaten. Zweck der Liste sei es gewesen, gezielte Kontrollen der aufgelisteten Verkehrsteilnehmer vorzunehmen, über die „Erkenntnisse" zu Trinkgewohnheiten und Fahrtrouten, zu benutzten Parkplätzen und vermuteten Verhaltensweisen, z. B. bei einer evtl. Verkehrskontrolle, gesammelt und zum Teil mehr als 14 Monate aufbewahrt wurden. Der Nachweis, daß mit Hilfe dieser Liste Alkoholsündern im Straßenverkehr wirksam entgegengetreten wurde, konnte erwartungsgemäß nicht geführt werden. Meine datenschutzrechtlichen Bedenken gegen den Einsatz einer derartigen Liste gründen sich im wesentlichen darauf, daß sie zu einem großen Teil nur auf Mutmaßungen und Verdächtigungen (Dorfklatsch) beruhte und gerade nicht der erforderlichen zeitnahen gezielten Überprüfung und Abklärung der besonderen Gefahren diente, die von Alkoholsündern im Straßenverkehr ausgehen. Vielmehr war sie für die zufällige Kontrolle dieser Verkehrsteilnehmer vorgesehen, soweit es der übliche Streifendienst überhaupt ermöglichte. Mitunter dauerte es viele Wochen, ohne daß eine Überprüfung an Hand der Liste vorgenommen wurde. Dieses zur Erfüllung einer polizeilichen Aufgabe völlig ungeeignete Mittel, das im übrigen nach Angaben des Innenministeriums bei keiner anderen Polizei-

behörde des Landes vorgehalten wird, kann daher eine Verarbeitung personenbezogener Daten in der vorliegenden Form nicht rechtfertigen. Nach Prüfung meiner datenschutzrechtlichen Bedenken hat das Innenministerium deshalb auch durch Runderlaß klargestellt, daß Listen der hier in Frage stehenden Art nicht verwendet werden dürfen. Das Innenministerium ist mit mir der Auffassung, daß es dagegen rechtlich unbedenklich wäre, den Einsatzaufträgen die zur Erfüllung dieser Aufträge notwendigen Daten für den Einzelfall beizufügen. Dies kann allerdings nur im Hinblick auf Personen zulässig sein, bei denen auf Grund von gesicherten, aktuellen Erkenntnissen zu erwarten ist, daß sie unter Alkoholeinwirkung oder nach Entzug der Fahrerlaubnis ein Fahrzeug im Straßenverkehr führen werden. Durch diese Änderung des Verfahrens wird somit eine zeitnahe und gezielte Kontrolle des betroffenen Personenkreises möglich, womit anschaulich der Nachweis geführt wird, daß Datenschutz nicht „Tatenschutz" ist, sondern zur Verbesserung der vorbeugenden Bekämpfung von Straftaten durch die Polizei beiträgt.

Dies habe ich auch in meiner Antwort auf zahlreiche Eingaben von besorgten Bürgerinnen und Bürgern zum Ausdruck gebracht, die in Unkenntnis der näheren Zusammenhänge in der „Säuferliste" ein wirksames Instrumentarium für die polizeiliche Arbeit gesehen haben. Die weitere Reaktion dieser Bürgerinnen und Bürger zeigt mir, daß Mißverständnisse in Bezug auf den Datenschutz offensichtlich ausgeräumt werden konnten.

Der Oberkreisdirektor der zuständigen Kreispolizeibehörde hat erst auf ausdrückliche Weisung des Innenministeriums die Verwendung der „Säuferlisten" auf den Polizeiwachen in seinem Kreisgebiet eingestellt. Bisher hat er sich zudem geweigert, die weiteren in diesem Zusammenhang bestehenden Datenschutzfragen zu beantworten. Eine deshalb von mir nach § 24 Abs. 1 Nr. 1 DSG NW gegenüber dem Innenministerium ausgesprochene Beanstandung hat auch nach mehreren Monaten nicht zu dem Ergebnis geführt, daß der Oberkreisdirektor seiner gesetzlichen Verpflichtung nach § 26 DSG NW vollständig nachkommt.

Durch das Beratungsersuchen einer Kreispolizeibehörde bin ich auf die unter datenschutzrechtlichen Aspekten ebenfalls bedenkliche Nutzung einer polizeilichen Datensammlung, der sog. **Wahllichtbildvorlage**, aufmerksam geworden. Hierbei werden in der Regel aus der zulässigerweise geführten Lichtbildvorzeigekartei der Polizei Lichtbilder von Personen, die vormals erkennungsdienstlich behandelt worden sind, zusammengestellt und Zeugen zur Auswahl vorgelegt. Soweit diese Lichtbilder aus der Lichtbildvorzeigekartei dazu genutzt werden, einen unbekannten Täter zu ermitteln oder eine bestimmte Person als Täter zu identifizieren, ist die Vorlage der Lichtbilder gegenüber Zeugen nach § 14 PolG NW oder § 81 c StPO zulässig. Sofern die Vorlage der Lichtbilder einer Person, die als Täter erkennbar nicht in Frage kommen kann, jedoch nur erfolgt, um Zeugen neben dem Lichtbild des zu überführenden Täters eine Wahl unter mehreren Lichtbildern zu ermöglichen, halte ich diese Wahllichtbildvorlage mangels Rechtsgrundlage ohne Einwilligung der Betroffenen für nicht zulässig. Ich gebe insoweit zu bedenken, daß

auch eine Wahlgegenüberstellung von Zeuge und Täter und weiteren Personen nach § 58 Abs. 2 StPO nicht ohne Einwilligung der sich zur Gegenüberstellung zur Verfügung stellenden Personen zulässig ist. In der von mir angeforderten rechtlichen Beurteilung dieser Wahllichtbildvorlage teilt das Innenministerium grundsätzlich meine Rechtsauffassung. Eine Regelung der Wahllichtbildvorlage ist gleichwohl noch nicht erfolgt. Vielmehr hat das Innenministerium das Justizministerium, dieses wiederum das Bundesministerium der Justiz und die anderen Justizverwaltungen um Stellungnahme gebeten. Diese Stellungnahmen stehen noch aus. Neben den rechtlichen Möglichkeiten sollte allerdings auch der Vorschlag einer Kreispolizeibehörde geprüft werden, den Polizeibehörden eine Auswahl computerunterstützt hergestellter Phantombilder zur Verfügung zu stellen. Hierdurch ließen sich die aufgezeigten rechtlichen Probleme mit einem geringen tatsächlichen Aufwand von vornherein vermeiden.

### 5.7.5 Informationsbeschaffung

Die Presseberichterstattung zur Ausstattung der Autobahnpolizei mit **Videoabstandsmeßanlagen** (VAMA) habe ich zum Anlaß für eine Prüfung bei einem zuständigen Regierungspräsidenten – Verkehrsüberwachungsbereitschaft – genommen. Dabei habe ich festgestellt, daß durch den Einsatz der Videokameras zur Abstandsmessung personenbezogene Daten sowohl von Verkehrsteilnehmern, die eine Ordnungswidrigkeit oder Straftat begehen, als auch von denen, die vorschriftsmäßig einen überwachten Autobahnabschnitt durchfahren, erhoben werden. Vor allem bei auffälligen Fahrzeugen, wie beschrifteten Lastkraftwagen und Personenkraftwagen, werden Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter, jedenfalls aber bestimmbarer natürlicher Personen erhoben. Auch die Lesbarkeit der Nummernschilder und die Erkennbarkeit der Fahrzeuginsassen auf den Videofilmen dürfte, soweit nicht jetzt schon möglich, nur von der Qualität der eingesetzten Aufnahme- und Auswertegeräte abhängig sein. Die Datenerhebung geschieht durch verdeckt aufgestellte Beobachtungsposten und Einsatzfahrzeuge. Insgesamt lassen sich grundlegende Unterschiede zu den bisherigen Radarüberwachungen und Abstandskontrollen feststellen. Die gegenüber diesen Verfahren nicht von der Hand zu weisenden Vorteile für die polizeiliche Arbeit können allerdings nicht darüber hinweghelfen, daß es für diese Maßnahme der Datenerhebung keine Rechtsgrundlage in der Strafprozeßordnung gibt. Auch die Grundsätze zum Übergangsbonus lassen sich zur Rechtfertigung dieses Verfahrens nicht heranziehen, da es sich um ein neues, durch Kombination von umfassender Videografie und einzelner Fotografie gestaltetes Verfahren handelt. Der von mir im Interesse einer datenschutzgerechten Lösung geführte Schriftverkehr mit dem Innenministerium in dieser Sache ist noch nicht abgeschlossen. Das Innenministerium ist auf meine rechtlichen Bedenken ohne nähere Begründung nicht eingegangen, obgleich weder die Rechtsgrundlage für das Verfahren noch nähere datenschutzrechtliche Bestimmungen z. B. für die Aufbewahrung, Löschung und Nutzung der Videoaufnahmen vorhanden sind.

Lediglich hinsichtlich der Versendung von in diesem Verfahren gewonnenen **Frontalidentifizierungsfotos** hat sich das Innenministerium dahingehend eingelassen, daß nur solche Fotos im Rahmen des Ordnungswidrigkeitenverfahrens versandt werden, auf denen der Fahrzeugführer abgebildet ist, nicht jedoch weitere im Fahrzeug befindliche Personen. Eine verbindliche Vorgabe im Rahmen des Runderlasses zur Videoabstandsmeßanlage fehlt indes zu diesem Punkt. Darauf mögen die Bürgereingaben an mich zurückzuführen sein, wonach es nach wie vor Polizeibehörden gibt, die von der ihnen zur Verfügung stehenden technischen Ausstattung keinen Gebrauch machen, Bildausschnitte von Frontalidentifizierungsfotos herzustellen und zu versenden. Festzuhalten bleibt allerdings auch, daß erfreulicherweise die Initiative für eine landesweit gültige Regelung, lediglich Bildausschnitte im Ordnungswidrigkeitenverfahren zu verwenden, von einer vor Ort zuständigen Polizeibehörde ausging.

Noch nicht hinreichend beantwortet ist die von mir gegenüber dem Innenministerium aufgegriffene Frage, zu welchen polizeilichen Zwecken es erforderlich sein soll, im Rahmen der Bearbeitung sog. **Kennzeichenanzeigen** im Ordnungswidrigkeitenverfahren die Daten von Kraftfahrzeughaltern grundsätzlich im Fahndungsbestand des polizeilichen Informationssystems INPOL abzugleichen. Dabei ist zu berücksichtigen, daß die Betroffenen bei durch das Videoabstandsmeßverfahren oder durch eine Radarkontrolle festgestellten Verstößen anders als bei einer Verkehrskontrolle ohnehin in der Regel nicht angehalten werden und die von den Betroffenen begangenen Ordnungswidrigkeiten somit zum Teil schon Wochen zurückliegen. Diese Praxis einiger Polizeibehörden, deren Hintergrund sich weder auf gesetzliche Vorgaben noch auf im Erlaßwege getroffene Regelungen stützen kann, stellt sich mir mangels einer nachvollziehbaren Darlegung ihrer Erforderlichkeit durch das Innenministerium als unzulässige, weil unverhältnismäßige Datenverarbeitung dar.

Demgegenüber ließ sich im Zusammenhang mit der Einführung neuer **Vordrucksätze für Unfallanzeigen** der Polizei der Umfang der insoweit zu verarbeitenden personenbezogenen Daten auf das erforderliche Maß reduzieren. Das bei den Vordrucken vorgesehene Durchschreibverfahren mit insgesamt fünf Ausfertigungen für verschiedene Adressaten wurde vom Innenministerium auf meine Empfehlung hin so überarbeitet und mit vorgeschwärzten Feldern versehen, daß die jeweiligen Empfänger auch tatsächlich nur die für sie bestimmten Daten in dem für ihre Aufgabenerfüllung erforderlichen Maße erhalten.

### 5.7.6 Informationsweitergabe

Wegen ihrer in der Regel besonderen Sensibilität verdient die Weitergabe polizeilicher Informationen, sei es in den privaten Bereich, sei es an öffentliche Stellen, datenschutzrechtlich verstärkte Beachtung.

So stellt beispielsweise die im Auftrag der Landespolizeidienststellen vom Bundeskriminalamt beabsichtigte regelmäßige Übermittlung von

**Kfz-Sachfahndungsdaten** aus dem polizeilichen Informationssystem INPOL an Kfz-Hersteller und an den HUK-Verband zwecks Abgleich mit den bei den Kfz-Herstellern in automatisierter Form gespeicherten Daten eine Nutzung der Sachfahndungsdaten durch Private dar, deren Rechtsgrundlage nicht erkennbar ist. Zu bedenken ist, daß die Sachfahndungsdatei in INPOL bisher geführt wurde, um – ggf. aus dem privaten Bereich stammende – Informationen durch die Polizei überprüfen zu können. Der Umstand, daß die Landespolizeien diesen Abgleich nunmehr dem privaten Bereich ermöglichen wollen, wirft zum einen die Frage nach der Rechtsgrundlage, zum anderen nach der Sicherung der Einhaltung erforderlicher Datenschutzbestimmungen durch die privaten Empfänger auf. Der lapidare Hinweis durch das Bundeskriminalamt, die geschädigten Kfz-Eigentümer hätten bereits durch ihre Anzeigeerstattung zum Ausdruck gebracht, daß sie der Tataufklärung bzw. der Rückführung ihres Fahrzeugs höheres Gewicht beimessen als dem Schutz ihrer in diesem Zusammenhang offenbarten Daten, vermag meine Bedenken nicht auszuräumen. Insoweit würde es naheliegen, die Kfz-Eigentümer im Zusammenhang mit der Anzeigeerstattung um die schriftliche Einwilligung in die beabsichtigte Datenübermittlung zu bitten. In Verkennung des Umstands, daß das Bundeskriminalamt den Kfz-Sachfahndungsbestand lediglich im Auftrag der Länderpolizeien führt, hält das Innenministerium die Zuständigkeit des Bundeskriminalamts und damit keinen Handlungsbedarf auf Länderebene für gegeben..

Um eine unter datenschutzrechtlichen Aspekten bedenkliche Weitergabe polizeilicher Informationen in den privaten Bereich handelt es sich auch in den Fällen, in denen Polizeibehörden die **Daten von Opfern** einer Straftat **an den Täter** übermitteln, in der Absicht, diesem die Möglichkeit zur Entschuldigung und Wiedergutmachung zu geben. Ich verkenne zwar nicht, daß aus kriminologischer Sicht die Konfrontation des Täters mit seinem Opfer, z. B. bei einer Körperverletzung, eine gewisse spezialpräventive Wirkung auf den Täter ausüben und gerade bei jugendlichen Straftätern Wiederholungen verhindern helfen kann. Es kann aber nicht angehen, daß diese erneute Begegnung von Täter und Opfer für das Opfer völlig überraschend kommt, weil die Polizei dem Täter ohne Kenntnis und vorherige Einwilligung des Opfers die Kontaktaufnahme mit dem Opfer ermöglicht hat. Hiergegen bestehen die bereits in meinem 10. Tätigkeitsbericht (S. 54 bis 56) geäußerten Bedenken gegen die Angaben von Zeugen- und Anzeigeerstatteranschriften in der Anklageschrift, im Strafbefehl oder im Bußgeldbescheid. Weitere Eingaben im Berichtszeitraum verdeutlichen die Betroffenheit und Besorgnis von Bürgerinnen und Bürgern, die die Preisgabe der Privatanschrift gegenüber dem Täter auslöst.

Eine gemäß § 28 Abs. 2 PolG NW zulässige Datenübermittlung durch die Polizei an andere, für die Gefahrenabwehr zuständige öffentliche Stellen (hier: Straßenverkehrsamt) sehe ich in der Meldung von **Fahrerlaubnisinhabern**, die ein Kraftfahrzeug unter offensichtlichem **Drogeneinfluß** führen oder deren Drogenkonsum in anderem Zusammenhang bekannt wird. Die Voraussetzungen des § 28 Abs. 2 PolG NW, daß die Kenntnis dieser Daten zur Aufgabenerfüllung des Empfängers, des Straßenverkehrsamts, für den Be-

reich der Gefahrenabwehr erforderlich erscheint, wird seitens der Polizei gestützt auf das Gutachten „Krankheit und Kraftverkehr" des Gemeinsamen Beirates für Verkehrsmedizin beim Bundesministerium für Verkehr und beim Bundesministerium für Jugend, Familie und Gesundheit (Heft 67/85 der Schriftenreihe des Bundesministeriums für Verkehr, S. 19). Danach beeinträchtigt der Konsum von Rauschmitteln die Fahrtauglichkeit in schwerwiegender Weise nicht nur während des akuten Rauschzustands sondern bei Einnahme sog. Halluzinogene auch nach dem Abklingen der akuten Rauschsymptomatik und einem symptomfreien Intervall (sog. Echo-Rausch, „Flashback"). Folgerichtig wird daher der Straßenverkehrsbehörde die Entscheidung über die Entziehung der Fahrerlaubnis oder deren Einschränkung sowie die Erteilung von Auflagen hierzu seitens der Polizei zu ermöglichen sein.

Hingegen waren datenschutzrechtliche Bedenken in einem anderen Fall zu erheben, in dem die Polizei personenbezogene **Daten einer Zeugin** sowie Erkenntnisse aus ihrer Aussage bei der Polizei in einem Strafermittlungsverfahren gegen einen Privatclubbesitzer **an das Finanzamt** übermittelt hatte. Obwohl die Zeugin vor ihrer Vernehmung nicht auf ihr Auskunftsverweigerungsrecht nach § 163 a Abs. 5 i.V.m. § 55 Abs. 2 StPO hingewiesen worden war, wurde die in der Aussage erwähnte Erwerbstätigkeit der Zeugin in dem Privatclub dem Finanzamt mitgeteilt, um überprüfen zu lassen, ob die Zeugin ihre erzielten Einnahmen auch versteuert hat. Rechtswidrig gespeicherte Daten, die unter Verstoß gegen zwingend vorgeschriebene Hinweispflichten erhoben wurden, sind gemäß § 32 Abs. 2 Nr. 2 PolG NW jedoch zu löschen und nicht auch noch, wie hier geschehen, an andere Behörden zu übermitteln. Auf meine Anregung hin hat sich die betreffende Polizeibehörde hierzu bereiterklärt.

Ebenfalls Einvernehmen konnte bei der polizeilichen Informationsweitergabe im Zusammenhang mit wichtigen Ereignissen innerhalb des Polizeibereichs erzielt werden. Hinsichtlich der bereits in meinem 10. Tätigkeitsbericht (S. 66) aufgezeigten Praxis der Polizei, bei wichtigen Ereignissen eine Vielzahl von öffentlichen Stellen durch Meldungen zu informieren (sog. **WE-Meldung**), hat das Innenministerium entsprechend seiner Ankündigung den Runderlaß über Meldungen wichtiger Ereignisse geändert. Es ist meiner Empfehlung gefolgt und hat WE-Meldungen, die Polizeibeamte in dienst- oder personalrechtlicher Hinsicht betreffen können, in ihrer Kennzeichnung Personalsachen gleichgestellt. Insbesondere der Empfängerkreis innerhalb der unterrichteten Behörde ist danach bei Eingang der WE-Meldung festzulegen („direkt auf den Tisch"). Leider ist nicht ausdrücklich geregelt, daß derartige WE-Meldungen innerhalb der Behörde möglichst im verschlossenen Umschlag zu versenden sind.

### 5.7.7 Polizeiorganisation

Schon in meinem 9. Tätigkeitsbericht (S. 56 bis 58) und 10. Tätigkeitsbericht (S. 69/70) hatte ich Anlaß, auf die **interne Datenschutzkontrolle** in den einzelnen Kreispolizeibehörden einzugehen. Im Zuge der angestrebten Neuorganisation der Kreispolizeibehörden stellt sich die Frage einer effizien-

ten internen Kontrolle erneut. Die Vorstellungen des Innenministeriums, die datenschutzrechtliche Kontrollinstanz einem Sachgebiet „Datenschutz" zu übertragen, überzeugen mich in diesem Zusammenhang in der bisher vorgesehenen Form jedoch nicht. Es ist nicht zu erkennen, wie eine Datenschutzkontrollinstanz effektiv institutionalisiert sein soll, wenn sie in einem gegenüber allen übrigen Sachgebieten gleichrangigen Dezernat eingerichtet ist, über kein spezielles Instrumentarium zur Durchsetzung datenschutzrechtlicher Belange, wie etwa direktes Vortragsrecht oder regelmäßige Berichterstattung bei der Behördenleitung, verfügt und im übrigen weisungsabhängig im Verwaltungsaufbau organisiert ist. Vielmehr sehe ich bei einer solchen Lösung eine faktische Abschottung der Kontrollinstanz von der Behördenleitung organisatorisch festgeschrieben, obwohl allein die Behördenleitung auf der Grundlage der durch die Kontrollen erlangten Erkenntnisse verbindliche Weisungen für die gesamte Dienststelle treffen kann. Dies muß, wie ich zuletzt in meinem 10. Tätigkeitsbericht (S. 141/142) für den kommunalen Bereich dargestellt habe, nicht heißen, daß eine effektive Datenschutzkontrolle nur durch einen behördeninternen Datenschutzbeauftragten geleistet werden kann. Ich habe dem Innenministerium empfohlen, die hier genannten Kriterien im Interesse der Effektivität auch für die in einem Sachgebiet eingegliederte Datenschutzkontrollinstanz zu schaffen.

Bleibt die Wirksamkeit der zukünftigen behördeninternen Datenschutzkontrollinstanz im Polizeibereich abzuwarten, so steht hinsichtlich der **baulichen Maßnahmen in Polizeiwachen** fest, daß nach eigenen Angaben des Innenministeriums in ca. 200 Polizeistationen mit weniger als 50 Bediensteten im engeren Wachbereich, in Polizeiwachen mit durchgehendem Wechseldienst und in Polizeiautobahnwachen ausreichender Datenschutz nicht sichergestellt ist. Die Verarbeitung personenbezogener Daten über Funk, Terminal und Telefon sowie im direkten Kontakt mit Besuchern dieser Stellen ist nur in der Weise möglich, daß unbefugte Dritte, insbesondere nicht zur Behörde gehörende Personen, die Daten mitlesen oder mithören können. In der bereits im 10. Tätigkeitsbericht (S. 68) erwähnten angeforderten Stellungnahme ging das Innenministerium im Mai 1991 zunächst davon aus, daß eine Trennung von Wachraum- und Fernmeldebetrieb in keinem Verhältnis zum angestrebten Erfolg der umfassenden Datensicherung stünde, da sie sich nicht durch kurzfristig realisierbare Maßnahmen bewirken ließe. Dieser eher pauschalen Weigerung, davon Abstand zu nehmen, beim Ausbau von Polizeiwachen offenbar noch heute nach den „vorläufigen Grundsätzen für Raumgrößen und die technische Ausstattung vom 27.10.1978" vorzugehen, folgte nach einer gemeinsamen Besprechung im November 1991 die Zusage des Innenministeriums, generelle Perspektiven des baulichen Datenschutzes in Polizeiwachen aufzuzeigen. Diese liegen mir allerdings immer noch nicht vor.

Neben dem eher herkömmlichen Problem der baulichen Ausstattung von Polizeibehörden muß der Einführung neuer Informations- und Kommunikationstechnik im Polizeibereich besondere Aufmerksamkeit aus Sicht des Datenschutzes zukommen. Ich habe daher sechs Polizeibehörden, bei denen versuchsweise eine **automatisierte Vorgangsverwaltung** (AVV) eingeführt

wurde, Informationsbesuche abgestattet und festgestellt, daß mit der AVV die ordnungsgemäße Erfassung, Bearbeitung und Verwaltung (Registratur) von Ermittlungsvorgängen (Strafanzeigen, Ersuchen, Berichte etc.), die bei der Polizei ein vielfältiges System von Tagebüchern, Haftbüchern, Indizes, Karteien und Sammlungen erfordert, effektiver bewältigt werden kann. Die AVV sieht dafür eine rechnergestützte Erfassung und Auswertung aller zur Verwaltung eines Ermittlungsvorgangs erforderlichen Daten vor, die zur Unterstützung der polizeilichen Arbeit im direkten Zugriff oder in Form von Listenauswertungen zur Verfügung gehalten werden müssen. Eine Rechnervernetzung oder ein automatisierter Datenaustausch zwischen den mit der AVV ausgestatteten Behörden besteht nicht. Da nach den neueren Planungen seitens des Innenministeriums eine Ausstattung sämtlicher Kreispolizeibehörden mit moderner Informations- und Kommunikationstechnik, insbesondere für die Textverarbeitung auf PCs, im Rahmen des sog. Wach- und Wechseldienstprogramms vorgesehen ist, und noch nicht abzusehen ist, wie die AVV angesichts des entstehenden Medienbruchs in der bisherigen Form integriert oder abgelöst wird, habe ich von einer abschließenden datenschutzrechtlichen Bewertung der AVV bislang abgesehen. Es wird jedoch weiterhin wichtig sein, die Einführung moderner Informations- und Kommunikationstechnik im Bereich der Polizei daraufhin zu überprüfen, ob das Recht auf informationelle Selbstbestimmung des Einzelnen, der aus welchem Grund auch immer mit der Polizei in Berührung kommt, durch die Automatisierung der Verarbeitung seiner Vorgangsdaten nicht in unvertretbarem Maße beeinträchtigt wird. Hierbei wird zu berücksichtigen sein, welch hohen organisatorischen und personellen Aufwandes es bedarf, um automatisiert geführte Datenbestände zu pflegen und zutreffende Daten vorzuhalten.

Dies zeigen mir nicht zuletzt die Eingaben von Bürgerinnen und Bürgern sowie die Beratungsersuchen von Dienststellen, die Hinweise darauf enthalten, daß die vom Landeskriminalamt ausgegebenen **Warnlisten zur Löschung** bestimmter personenbezogener Daten, insbesondere personengebundener Hinweise, im INPOL-System nach Ablauf der Speicherfrist nicht rechtzeitig abgearbeitet werden konnten. Andererseits habe ich ebenfalls feststellen müssen, daß durchaus vorhandene organisatorische Maßnahmen schlichtweg auf Grund menschlicher Versäumnisse nicht greifen und z. B. die Löschung eines Datensatzes im polizeilichen Informationssystem nicht in allen Datengruppen veranlaßt wird. Hier bleibt mir nur anzumahnen, daß alle Bediensteten einer Behörde in regelmäßigen Abständen auf die einschlägigen Dienstanweisungen und das nötige Maß an Sorgfalt im Umgang mit personenbezogenen Daten hingewiesen werden.

### 5.7.8 Rechtsansprüche gegenüber der Polizei

Auf ein gesteigertes Datenschutzbewußtsein dürfte es zurückzuführen sein, daß Bürgerinnen und Bürger zur Wahrung ihres Rechts auf informationelle Selbstbestimmung vermehrt die ihnen zustehenden Rechtsansprüche gegenüber öffentlichen Stellen, insbesondere der Polizei, geltend machen. Gerichtet sind die Ansprüche in der Regel auf **Auskunft** über bei der Polizei gespeicherte

Daten Betroffener und auf Vernichtung von kriminalpolizeilichen Sammlungen und erkennungsdienstlichen Unterlagen. Auf Grund der zahlreichen Eingaben habe ich feststellen müssen, daß die Polizeibehörden in der Praxis den Ansprüchen der Betroffenen in Verkennung der Rechtslage nicht immer in der gebotenen Form Rechnung tragen. Vor allem § 18 DSG NW, der auch für Polizeibehörden die Auskunftserteilung an Betroffene über ihre gespeicherten Daten zur Regel, die Auskunftsverweigerung hingegen zur Ausnahme erklärt, wird mitunter seitens der Polizeibehörden in seinem Grundsatz zunächst verkehrt, wenn es Betroffenen um Auskunft aus kriminalpolizeilichen Sammlungen geht. Auf meine Empfehlungen im Einzelfall wurden jedoch bislang regelmäßig die verweigerten Auskünfte erteilt.

Ein gewisses Maß an Unsicherheit sowohl auf Seiten der Betroffenen als auch auf Seiten der Polizei ist demgegenüber bei den Ansprüchen auf **Vernichtung** von kriminalpolizeilichen Sammlungen und erkennungsdienstlichen Unterlagen zu verzeichnen. Der Umstand, daß in kriminalpolizeilichen Sammlungen sog. Merkblätter auch zu Strafverfahren geführt werden dürfen, die für Betroffene mit einem Freispruch oder einer Einstellung nach § 170 Abs. 2 bzw. 153/153 a StPO endeten, macht es erforderlich, näher auf den gesetzlichen Zweck der kriminalpolizeilichen Sammlungen gemäß § 24 Abs. 2 PolG NW einzugehen. Danach kann die Polizei die im Rahmen der Verfolgung von Straftaten gewonnenen personenbezogenen Daten auch zum Zwecke der Gefahrenabwehr speichern. Nach Nr. 1.2 der KpS-Richtlinien (vgl. oben 5.7.1, 2. Spiegelstrich) ist es Zweck der gespeicherten Unterlagen, bei Ermittlungen die Aufklärung des Sachverhalts zu unterstützen und die Feststellung von Verdächtigen zu fördern sowie Hinweise zur Gefahrenabwehr zu geben. Gegen eine solche Speicherung bestehen keine durchgreifenden datenschutzrechtlichen Bedenken. Dies gilt nach der ständigen Rechtsprechung der Verwaltungsgerichte sogar dann, wenn Betroffene nicht verurteilt worden sind, sofern der dem Ermittlungs- und Strafverfahren zugrunde liegende Verdacht nicht vollständig ausgeräumt worden ist.

## 5.8 Verfassungsschutz

### 5.8.1 Entwurf eines Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen

Das Innenministerium hatte im Berichtszeitraum einen ersten Entwurf des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vorgelegt. Hierzu habe ich sowohl schriftlich als auch im Rahmen von Besprechungen mit Vertretern der Verfassungsschutzbehörde Stellung genommen. Ziel meiner Verbesserungsvorschläge war es, die praktische Handhabung des Gesetzes auf der Grundlage der Verfassung rechtlich einwandfrei zu gewährleisten. Insgesamt sind jedoch eine Reihe meiner Bedenken zu verschiedenen Regelungen des Gesetzentwurfs, insbesondere der Generalklausel zu den Befugnissen, den Sicherheitsüberprüfungen und dem Auskunftsrecht Betroffener, bestehen geblieben. Meine im 10. Tätigkeitsbericht (S. 74) geäußerte Hoffnung, daß die dem Datenschutz gegenüber aufgeschlossene Haltung und

Praxis der Verfassungsschutzbehörde auch Eingang in das zu erwartende Verfassungsschutzgesetz Nordrhein-Westfalen finden wird, erfüllt auch der überarbeitete und als Drucksache 11/4743 dem Landtag vorgelegte Gesetzentwurf nicht. Hierzu habe ich mich daher nochmals in einer ausführlichen Stellungnahme (vgl. Vorlage 11/1896) geäußert.

### 5.8.2 Geheimschutzgesetz Nordrhein-Westfalen

Im Berichtszeitraum hatte ich Gelegenheit, zu dem Entwurf eines Geheimschutzgesetzes für das Land Nordrhein-Westfalen, Stand: 20.12.1991, und eines Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen, Stand: 01.12.1991, Stellung zu nehmen. Nachdem ich meine datenschutzrechtlichen Überlegungen und Vorschläge dem Innenministerium gegenüber umfassend aufgezeigt hatte, wurde mir der überarbeitete Entwurf eines Geheimschutzgesetzes, Stand: 27.04.1992, übersandt. Es ist zu begrüßen, daß dieser Entwurf im Hinblick auf die notwendigen Datenschutzregelungen deutlich verbessert worden ist und einen erheblichen Teil meiner Vorschläge nunmehr berücksichtigt. Da dem Entwurf eine Begründung nicht beigefügt war, ist allerdings nicht nachvollziehbar, aus welchen Gründen meine übrigen Vorschläge zur Verbesserung des Datenschutzes nicht übernommen worden sind. Im Hinblick auf den zwischenzeitlich im Landtag eingebrachten Entwurf eines Verfassungsschutzgesetzes wäre zudem am ehesten in Erwägung zu ziehen gewesen, den Entwurf eines Geheimschutzgesetzes im Verfassungsschutzgesetz in einen eigenen Abschnitt einzuarbeiten, um auf diese Weise die Mitwirkung der Verfassungsschutzbehörde bei Sicherheitsüberprüfungen auf eine gesetzliche Grundlage zu stellen. Die Durchführung von Sicherheitsüberprüfungen, gestützt auf die derzeit vorgesehenen Regelungen im Entwurf eines Verfassungsschutzgesetzes, wäre nach meiner Auffassung unzulässig.

Bei meinen Vorschlägen handelt es sich im wesentlichen um folgende Punkte, die an dieser Stelle lediglich stichwortartig angesprochen werden können:

- normenklare Regelung der Folgen einer verweigerten Einwilligung Betroffener in die Sicherheitsüberprüfung,
- Bestellung eines eigenen Geheimschutzbeauftragten für die Sicherheitsüberprüfung im Bereich der Verfassungsschutzbehörde,
- Interessenkollision bei der Bestellung des Leiters einer kleineren Dienststelle zum Geheimschutzbeauftragten für die Sicherheitsüberprüfung,
- Umschreibung des Vorliegens eines Sicherheitsrisikos in der Person des Betroffenen,
- Pflicht Betroffener zu wahrheitsgemäßen Angaben über Daten Dritter,
- Belehrung Betroffener über die Folgen der Verweigerung von Angaben,
- Voraussetzung für das Absehen von einer einfachen oder erweiterten Sicherheitsüberprüfung,

- nähere Regelungen der Datenerhebung bei Sicherheitsüberprüfungen durch die Verfassungsschutzbehörde,
- Erforderlichkeit einer Reihe von Angaben zur Sicherheitserklärung,
- Regelung der Bewertung und Übermittlung „sicherheitserheblicher" Erkenntnisse, insbesondere Anhörung des Betroffenen zu Erkenntnissen,
- Qualität der Angaben für die Aufnahme in die Sicherheitsakte,
- Voraussetzung für ein Auskunftsrecht und für die Löschung von Angaben in der Sicherheitsakte,
- Speicherung von „weichen" Daten sowie Daten von Lebenspartnern in automatisierten Dateien,
- Voraussetzung der Ausnahmegenehmigung bei Reisebeschränkungen.

Eine nochmalige Bearbeitung des Entwurfs eines Geheimschutzgesetzes ist insoweit aus datenschutzrechtlicher Sicht erforderlich. Sie bleibt ebenso abzuwarten, wie die gesetzgeberischen Aktivitäten des Bundesgesetzgebers, der seinerseits den Entwurf eines Sicherheitsüberprüfungsgesetzes des Bundes, Stand: 15.04.1992, erarbeitet hat. Hiervon wird abhängen, ob – wie aus datenschutzrechtlicher Sicht wünschenswert – Nordrhein-Westfalen alsbald sein eigenes Gesetzgebungsvorhaben abschließt oder ob auch insoweit die Absicht verfolgt wird, wie beim Verfassungsschutzgesetz Nordrhein-Westfalen mit eigenen Vorstellungen hinter bundesrechtlichen Regelungen zurückzustehen.

### 5.8.3 Elektronisches Textkommunikationsverfahren (ELKOM)

Im Berichtszeitraum habe ich Kenntnis von dem elektronischen Textkommunikationsverfahren ELKOM erhalten, über das die Erstellung, Bearbeitung von Texten und deren kryptisierte Versendung an die Verbundteilnehmer des nachrichtendienstlichen Informationssystems NADIS über das vorhandene NADIS-Leitungsnetz und die entsprechenden Datenendgeräte möglich ist. Im Rahmen eines Informationsbesuchs bei der Verfassungsschutzbehörde Nordrhein-Westfalen stellte sich heraus, daß seitens der Verfassungsschutzbehörde bei ELKOM die ausschließliche Kommunikationsfunktion des Systems im Vordergrund gesehen wird. Da aber zumindest in dem Eingangs- und Ausgangsbereich des Systems eine durch automatisierte Verfahren auswertbare Sammlung von Daten zu ein- und ausgehenden Dokumenten aufgebaut wird, handelt es sich bei ELKOM um eine Datei im Sinne des § 3 Abs. 4 Buchstabe a DSG NW. Sie ermöglicht eine Verarbeitung, insbesondere Auswertung und Übermittlung personenbezogener Daten, bei der die Mitteilungsflüsse im nachhinein nicht ohne weiteres nachvollziehbar dokumentiert sind und auch im übrigen offenbleibt, inwieweit Benachrichtigungs- und Auskunftsansprüchen Betroffener Rechnung getragen werden kann. Der Bundesbeauftragte für den Datenschutz, der für das Bundesamt für Verfassungsschutz den Dateibegriff des § 3 Abs. 2 Nr. 1 BDSG zugrunde zu legen hat, teilt meine Auffassung zur Dateiqualität von ELKOM. Gleichwohl verneinen sowohl das Bundesamt für Verfassungsschutz als auch die Verfas-

sungsschutzbehörde Nordrhein-Westfalen die Dateieigenschaft von ELKOM und damit die Notwendigkeit einer Dateibeschreibung im Sinne des § 8 DSG NW. Die datenschutzrechtliche Überprüfung ist insoweit noch nicht abgeschlossen.

## 5.9 Sozialwesen

### 5.9.1 Zweites Gesetz zur Änderung des Sozialgesetzbuchs

Die am 1. Juni 1991 in Kraft getretene Neufassung des Bundesdatenschutzgesetzes machte wegen ihrer unmittelbaren Auswirkung auf die Datenschutzvorschriften des Sozialgesetzbuchs deren umfassende Überarbeitung erforderlich. Zum einen waren die zahlreichen Verweisungen auf das Bundesdatenschutzgesetz durch Neuparagraphierung unrichtig geworden, zum anderen erstreckt sich der Regelungsgehalt des Bundesdatenschutzgesetzes nunmehr auch auf die Datenverarbeitung in Akten. Des weiteren war dem Umstand Rechnung zu tragen, daß das Sozialgesetzbuch bislang nur einzelne Phasen der Datenverarbeitung regelt – wie die Datenerhebung lediglich im Rahmen der Mitwirkungspflicht des Betroffenen sowie die Offenbarung und die Löschung von Sozialdaten –, daß aber die Regelung sämtlicher Phasen der Datenverarbeitung auch im Sozialleistungsbereich im Hinblick auf ihren Eingriffscharakter verfassungsrechtlich geboten ist.

Dementsprechend hat das Bundesministerium für Arbeit und Sozialordnung einen Gesetzentwurf zur Änderung von Vorschriften des Sozialgesetzbuchs über die Zahlung des Gesamtsozialversicherungsbeitrages und den Schutz der Sozialdaten sowie zur Änderung anderer Vorschriften (Zweites Gesetz zur Änderung des Sozialgesetzbuchs – 2. SGBÄndG ) vorgelegt, der inzwischen zwar mehrmals überarbeitet worden ist, aus datenschutzrechtlicher Sicht aber noch Mängel aufweist.

Bereits in meinem 9. Tätigkeitsbericht (S. 29) hatte ich darauf hingewiesen, daß die Datenschutzbeauftragten des Bundes und der Länder es für erforderlich halten, dem großzügigen Datenaustausch innerhalb des Sozialleistungsbereichs (§ 69 SGB X) durch Zweckbindung engere Grenzen zu ziehen. Diese Forderung ist im Gesetzentwurf unberücksichtigt geblieben, so daß die Betroffenen auch künftig nicht überblicken können, „wer was wann und bei welcher Gelegenheit über sie weiß" – ein verfassungsrechtlich bedenklicher Zustand.

Einen Verstoß gegen das Transparenzgebot stellt die Ausweitung der bisher engen Erhebungs- bzw. Mitwirkungsregelungen (§§ 60 bis 65 SGB I) dar, indem nach dem Entwurf die Sozialleistungsträger ermächtigt werden sollen, Daten weitgehend ohne Mitwirkung des Betroffenen zu erheben.

Soweit der Gesetzentwurf die Verarbeitung oder Nutzung von Sozialdaten für die Wahrnehmung von Disziplinarbefugnissen gestattet, widerspricht dies dem besonderen Schutzcharakter der Sozialdaten, weil deren Verwendung für einen derartigen Zweck keinerlei sozialrechtliche Außenwirkung, sondern solche dienstrechtlicher Art entfaltet. Das Disziplinarverfahren ist Bestandteil

des Beamtenrechts, also Verwaltungsrecht und damit – anders als die Wahrnehmung von Aufsichts-, Kontroll- und Rechnungsprüfungsaufgaben (vgl. § 35 Abs. 1 Satz 2 SGB I) – nicht Aufgabe im Sinne des Sozialgesetzbuchs. Dieser Tatbestand läßt sich nicht „hinwegdefinieren", indem der Gesetzgeber eine Verarbeitung zur Wahrnehmung von Disziplinarbefugnissen als vom Zweck der Erhebung gedeckt deklariert.

Kritik verdient der Gesetzentwurf auch insofern, als er dem Gebot der informationellen Gewaltenteilung nicht konsequent Rechnung trägt. Zum einen wird die Weitergabe innerhalb der speichernden Stelle der Datenverarbeitungsphase „Nutzen" zugeordnet, obwohl sie ihrem Wesen nach ein Übermittlungsvorgang ist; zum anderen orientiert sich die Definition der speichernden Stelle nur partiell und ansatzweise an dem im Datenschutzrecht geltenden funktionalen Stellenbegriff.

Insbesondere auf diese gewichtigen Bedenken habe ich das Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen (MAGS) hingewiesen, damit diese im weiteren Gesetzgebungsverfahren Berücksichtigung finden.

### 5.9.2 Gesundheitsstrukturgesetz

Angesichts der dramatischen Kostenentwicklung in allen Bereichen der Krankenversicherung ist unter großem Zeitdruck das Gesetz zur Sicherung und Strukturverbesserung der gesetzlichen Krankenversicherung (Gesundheitsstrukturgesetz) beraten und beschlossen worden. Dieses Gesetz, das am 01.01.1993 in Kraft getreten ist, bringt die bislang tiefgreifendsten Veränderungen im System der Krankenversicherung. Es soll eine sofortige Kostenbegrenzung bewirken und durch strukturelle Maßnahmen die Finanzierbarkeit der gesetzlichen Krankenversicherung langfristig sichern.

Die Unabweisbarkeit dieser gesetzgeberischen Zielsetzung darf jedoch nicht dazu führen, daß das rechte Augenmaß für die im Verfassungsrang stehenden Persönlichkeitsrechte der Versicherten wie auch für die sie schützende ärztliche Schweigepflicht verlorengeht. Eine solche Gefahr birgt vor allem der vorgesehene verstärkte Einsatz automatisierter Datenverarbeitung in sich. Die Datenschutzbeauftragten des Bundes und der Länder haben im Laufe der Gesetzesberatungen in ihrer Entschließung vom 1./2. Oktober 1992 zum Gesundheitsstrukturgesetz gegenüber dem Regierungsentwurf Verbesserungen des Persönlichkeitsschutzes der Krankenversicherten vorgeschlagen (vgl. Anlage 4, S. 163/164).

### 5.9.3 Verfahren bei der Ermittlung des Elternbeitrages für Kindergärten

Das Verfahren bei der Ermittlung des Elternbeitrages für Kindergärten nach dem Gesetz über Tageseinrichtungen für Kinder (GTK) hat zahlreiche Proteste der Elternschaft ausgelöst. Die Betroffenen wandten sich insbesondere dagegen, daß von ihnen verlangt wurde,

- ihre derzeitige Erwerbstätigkeit genau zu bezeichnen,

- den die verschiedenen Einkommensarten und ggf. Daten nicht Unterhaltspflichtiger enthaltenden Einkommens-/Lohnsteuerbescheid vorzulegen, anstatt ihnen die Art und Weise der Glaubhaftmachung ihrer Angaben zum Elterneinkommen freizustellen,
- die Angaben zur Einkommenshöhe generell glaubhaft zu machen,
- die sog. „Berechnungshilfe" für die Ermittlung des Elterneinkommens ausgefüllt dem Jugendamt zu übersenden.

Zur Ermittlung des Elternbeitrages hatte das MAGS einen Musterfragebogen entwickelt, der von den örtlichen Trägern der öffentlichen Jugendhilfe weitgehend übernommen wurde. In diesem Fragebogen wurde unter „Angaben zur Person" die genaue Bezeichnung der derzeitigen Erwerbstätigkeit verlangt. Außerdem wurden die Eltern darauf hingewiesen, daß sie auf Verlangen (des Trägers) ihre Angaben zu den positiven Einkünften glaubhaft zu machen hätten, z. B. durch Vorlage des Steuerbescheides oder einer Verdienstbescheinigung des Arbeitgebers oder sonstiger geeigneter Unterlagen. Nicht der Glaubhaftmachung dienende Angaben, beispielsweise die Einkünfte von Ehegatten, die mit dem Kind nicht verwandt sind, könnten unleserlich gemacht werden.

Zudem enthielt der Musterfragebogen sowohl den Hinweis, daß die Betroffenen im einzelnen zur Berechnung ihrer positiven Einkünfte eine seitenlange „Berechnungshilfe", die eine genaue Darlegung der positiven Einkünfte enthält, ausfüllen und mit der Erklärung zum Elterneinkommen abgeben könnten, als auch den Hinweis, daß die Angaben in der Erklärung überprüft werden können.

Gegen das Verlangen nach Angabe der genauen Bezeichnung der derzeitigen Erwerbstätigkeit hatte ich Bedenken geäußert, weil diese Angabe keine zuverlässigen Erkenntnisse über die Summe der positiven Einkünfte vermittelt, auf die aber das Gesetz abhebt. Diese Angabe ist überdies bedenklich, weil damit spekulativ von der sozialen auf die wirtschaftliche Stellung geschlossen wird, obwohl die mit gewissen Erwerbstätigkeiten verbundene Vorstellung von der Einkommenshöhe den tatsächlichen Verhältnissen durchaus widersprechen kann. Es gibt z. B. zahlreiche Erwerbstätigkeiten, die von vornherein keinerlei Rückschlüsse auf das Einkommen zulassen (z. B. Gastwirt, Handelsvertreter), sowie die Möglichkeit, Einkommen zu erzielen, ohne erwerbstätig zu sein.

Nach § 17 Abs. 3 Satz 1 GTK ergibt sich die Höhe der Elternbeiträge aus der Anlage zu diesem Gesetz, die aber nur die Angabe des Jahreseinkommens in einer Summe vorsieht. Dies bedeutet, daß für eine Überprüfung der Angaben der Personensorgeberechtigten auch nur der Nachweis des Gesamteinkommens in einer Summe, nicht jedoch, wie dies im Steuerbescheid bzw. in der Berechnungshilfe der Fall ist, aufgegliedert nach den einzelnen Einkommensarten zu erbringen ist. Durch die den Personensorgeberechtigten nahegelegte Beifügung des Steuerbescheides oder Rückgabe der Berechnungshilfe gelangen somit mehr Daten zur Kenntnis des örtlichen Trägers der

öffentlichen Jugendhilfe, als dieser zu seiner Aufgabenerfüllung nach § 17 GTK benötigt.

Zwar wurde in dem Musterfragebogen darauf hingewiesen, daß nicht der Glaubhaftmachung dienende Angaben unleserlich gemacht werden können. Das hierzu angeführte Beispiel machte jedoch nicht hinreichend deutlich, daß auch die einzelnen Einkommensarten zu den „nicht der Glaubhaftmachung dienenden Angaben" gehören und damit (z. B. im Steuerbescheid) ebenfalls unleserlich gemacht werden dürfen. Dies wurde nicht nur von den Personensorgeberechtigten, sondern, wie mir die von den Gemeinden verwendeten Vordrucke gezeigt haben, auch von diesen nicht erkannt. Dort wurden in vielen Fällen ausdrücklich – wenn auch zum Teil auf freiwilliger Basis – Angaben zu den einzelnen Einkommensarten erhoben. Auch zur Feststellung, ob Verluste mit positivem Einkommen ausgeglichen wurden, reicht die Kenntnis der einzelnen Beträge aus, um so das Rechenwerk nachvollziehen zu können; die Offenlegung der einzelnen Einkommensarten ist dazu nicht erforderlich.

Dementsprechend hat die Rückgabe der Berechnungshilfe, auch wenn sie freigestellt wird, zu unterbleiben. Die Berechnungshilfe kann zwar den Personensorgeberechtigten als Orientierungshilfe zur Verfügung gestellt werden. Dabei muß aber deutlich gemacht werden, daß sie nicht für den Jugendhilfeträger bestimmt ist.

Zu Mißverständnissen hat auch der Hinweis geführt, daß die Angaben in der Erklärung zum Elterneinkommen überprüft werden können. Durch diese Formulierung wurde bei Betroffenen der unzutreffende Eindruck erweckt, als wäre der örtliche Träger der öffentlichen Jugendhilfe berechtigt, etwa durch Rückfrage bei Dritten die Richtigkeit der Angaben zu überprüfen. Nach § 17 Abs. 5 GTK kann der örtliche Jugendhilfeträger lediglich verlangen, daß die Angaben zur Einkommenshöhe glaubhaft gemacht werden. Hat er Zweifel an der Richtigkeit der Angaben, so ist er darauf verwiesen, sich an den Betroffenen zu wenden und ihm Gelegenheit zu geben, die entstandenen Zweifel zu zerstreuen. Gelingt es dem Betroffenen nicht, die Zweifel auszuräumen, also seine Angaben zur Einkommenshöhe glaubhaft zu machen, so hat er den höchsten Elternbeitrag zu leisten (§ 17 Abs. 5 Satz 2 GTK). Diese insoweit normenklare gesetzliche Grundlage läßt keinen Raum für eine Nachprüfung der Angaben zur Einkommenshöhe am Betroffenen vorbei, etwa in Anwendung der Amtshilfevorschrift des § 21 Abs. 4 SGB X.

Das MAGS hielt entgegen meiner Auffassung die genaue Bezeichnung der derzeitigen Erwerbstätigkeit für zweckdienlich, weil auf diese Weise gleichsam als „Vorstufe der Glaubhaftmachung" in einer Vielzahl von Fällen (z. B. öffentlicher Dienst, regional-spezifische Arbeitgeber) eine weitere Kontrolle der Angaben zur Einkommenshöhe durch den örtlichen Jugendhilfeträger entbehrlich würde. Dieser Zielvorstellung war – datenschutzrechtlich noch vertretbar – zu entsprechen, indem den Personensorgeberechtigten, die freiwillig ihren Beruf angeben und damit erklären, daß sie aus dieser Tätigkeit ihre Einkünfte erzielen, der Verzicht auf weitere Glaubhaftmachung in Aus-

sicht gestellt werden sollte. Dementsprechend wurde in den Vordruck bei den Angaben zu den positiven Einkünften ein entsprechender Hinweis aufgenommen und bei den Angaben zur Person des Sorgeberechtigten auf die genaue Bezeichnung der derzeitigen Erwerbstätigkeit verzichtet.

Meinen Bedenken gegen die Rückgabe der Berechnungshilfe ist das MAGS gefolgt, indem die Berechnungshilfe nicht mehr als „Anlage" zur verbindlichen Erklärung zum Einkommen, sondern nur noch als „Berechnungshilfe zur verbindlichen Erklärung zum Einkommen" bezeichnet wird. Außerdem enthält sie eingangs den Hinweis: „Diese Berechnungshilfe ist für Sie bestimmt und verbleibt bei Ihren Unterlagen". Zudem hat das MAGS meiner Empfehlung folgend die Möglichkeit der Überprüfung der Angaben zum Einkommen ersetzt durch die wörtliche Wiedergabe des § 17 Abs. 5 GTK.

Nachdem das MAGS seinen Musterfragebogen entsprechend überarbeitet und den örtlichen Trägern der öffentlichen Jugendhilfe über die Landesjugendämter zur Verwendung empfohlen hatte, erreichten mich nur noch vereinzelt Beschwerden von Eltern.

Allerdings mußte ich gegenüber einer Stadt als Verstoß gegen das informationelle Selbstbestimmungsrecht förmlich beanstanden, daß sie es unterließ, die Eltern darüber aufzuklären, daß die Vorlage des Einkommensteuerbescheides nur **eine** unter mehreren Möglichkeiten der Glaubhaftmachung des Elterneinkommens ist, und es damit den Eltern nicht freistellte, unter Verwendung welcher Unterlagen sie ihre Angaben glaubhaft machen. Der Stadtdirektor hatte in einer Presseerklärung erläutert, daß und warum die Vorlage des Steuerbescheides aus seiner Sicht die einfachste Lösung gerade auch für die Eltern sei. Dabei wurde jedoch der unzutreffende Eindruck erweckt, als könnte alternativ nur der vom MAGS entwickelte Fragebogen verwendet werden; dieser sei so umfangreich und kompliziert wie eine Steuererklärung.

Meiner Empfehlung, diese von Mißverständnissen geprägte Fehlinformation zu korrigieren und entsprechend der aus dem informationellen Selbstbestimmungsrecht folgenden Aufklärungspflicht die Leser der Presseerklärung nunmehr zutreffend über ihre Rechte im Zusammenhang mit der Glaubhaftmachung ihrer Einkommensangaben zu unterrichten, ist der Stadtdirektor nicht gefolgt.

### 5.9.4 Ärztliche Bescheinigung als Voraussetzung für den Kindergartenbesuch

Eltern wandten sich dagegen, daß sie für die Aufnahme ihres Kindes in den Kindergarten eine Bescheinigung ihres Hausarztes beibringen mußten, die neben Angaben zur Person Angaben zum allgemeinen Gesundheitszustand, zu bisherigen Krankheiten und Behinderungen sowie über Größe, Gewicht, Aussehen, Körperbau, Zähne, Schutzimpfungen, Untersuchungsbefund und Krankheitsbezeichnungen enthielt.

Die Bereitstellung eines Kindergartenplatzes ist eine Sozialleistung, für die personenbezogene Daten nur erhoben werden dürfen, soweit ihre Kenntnis

zu deren Erfüllung erforderlich ist (§ 62 Abs. 1 des Kinder- und Jugendhilfegesetzes). Dabei sind an die Erforderlichkeit strenge Anforderungen zu stellen. Das Erforderlichkeitsprinzip zwingt die öffentliche Verwaltung, sich bei der Datenerhebung auf das zur rechtmäßigen Erfüllung ihrer Aufgaben unerläßliche Minimum zu beschränken. Es genügt daher nicht, wenn eine Angabe zur Aufgabenerfüllung nur dienlich oder, etwa zur Abrundung des Bildes oder als Hintergrundinformation, nützlich ist. Sie muß vielmehr zur Aufgabenerfüllung unerläßlich sein, so daß ohne ihre Kenntnis die Leistung nicht gewährt werden kann. Demnach dürften für die Bereitstellung eines Kindergartenplatzes Angaben wie Name, Vorname, Wohnanschrift und Geburtstag des Kindes, Name und Vorname des Vaters und der Mutter sowie Angaben darüber, wie die Eltern während des Tages zu erreichen sind, genügen. Keinesfalls ist hierfür die Kenntnis medizinischer Daten erforderlich.

Für jedes Kind muß allerdings durch ärztliche Untersuchung nachgewiesen werden, daß einer Aufnahme in die Tageseinrichtung aus ärztlicher Sicht nichts entgegensteht (§ 15 Abs. 2 GTK). Aus dem Zweck der Vorschrift ergibt sich, daß Kinder im Kindergarten vor übertragbaren Krankheiten geschützt werden sollen. Deshalb kann von den Erziehungsberechtigten nur die Vorlage einer Bescheinigung verlangt werden, aus der sich ergibt, daß das Kind ärztlich untersucht worden ist und nicht an einer übertragbaren Krankheit leidet. Eine Verpflichtung der Erziehungsberechtigten, den Arzt von der Schweigepflicht zu entbinden, damit dieser berechtigt ist, weitergehende medizinische Daten zu offenbaren, ist dieser Vorschrift nicht zu entnehmen. Die Richtlinien des MAGS vom 30. Juni 1982, auf die sich der Jugendhilfeträger berufen hat, können die fehlende gesetzliche Grundlage für die Erhebung derartiger Daten nicht ersetzen, da es sich hierbei lediglich um Verwaltungsvorschriften handelt, die im übrigen die Betroffenen nicht binden.

Da der Jugendhilfeträger nicht bereit war, entsprechend meiner Empfehlung von den Erziehungsberechtigten lediglich die Vorlage einer Bescheinigung zu verlangen, aus der hervorgeht, daß das Kind ärztlich untersucht worden ist und ob aus ärztlicher Sicht seiner Aufnahme in die Tageseinrichtung nichts entgegensteht, mußte ich diese Datenerhebung im Übermaß als Verstoß gegen den verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz förmlich beanstanden.

### 5.9.5 Check-up-Untersuchung

Durch einen Pressebericht wurde mir bekannt, daß eine AOK bei 830 Versicherten, die an einer **Untersuchung zur Früherkennung von Krankheiten** (Check-up-Untersuchung) teilgenommen hatten, eine Umfrage durchgeführt hat. Dabei wurde insbesondere nach dem Anlaß für die Untersuchung, nach den Ratschlägen des Arztes und der Zufriedenheit des Versicherten mit dem Check-up gefragt. Auf dem Fragebogen war zur Unterscheidung von Geschlecht und Altersgruppen die Mitgliedsnummer vermerkt.

In § 284 Abs. 1 Satz 1 SGB V ist abschließend geregelt, für welche Zwecke der Krankenversicherung die Krankenkassen personenbezogene Daten ihrer

Versicherten erheben und erfassen dürfen. Zu anderen als den dort genannten Zwecken dürfen die Daten nur verwendet werden, soweit dies durch Rechtsvorschriften des Sozialgesetzbuchs angeordnet oder erlaubt ist (§ 284 Abs. 3 SGB V). Die Auswertung der abgerechneten Krankenscheine zwecks Gewinnung des für die Umfrage in Betracht kommenden Versichertenkreises läßt sich keinem der im Gesetz genannten Zwecke der Krankenversicherung zuordnen.

Ebensowenig kann ihre Verwendung damit gerechtfertigt werden, daß die Versicherten gehalten sind, durch eine gesundheitsbewußte Lebensführung sowie frühzeitige Beteiligung an gesundheitlichen Vorsorgemaßnahmen den Eintritt von Krankheiten zu vermeiden, und den Krankenkassen die gesetzliche Aufgabe obliegt, ihren Versicherten allgemein wie auch im Einzelfall durch Aufklärung, Beratung und Leistungen zu helfen und auf gesunde Lebensverhältnisse hinzuwirken (§ 1 SGB V). Eine derartig allgemeine Beschreibung von Aufgaben der Krankenkassen und Verpflichtungen der Versicherten kann Eingriffe in deren informationelles Selbstbestimmungsrecht über die bereichspezifischen Befugnisnormen hinaus nicht rechtfertigen. Zudem erscheint zweifelhaft, ob sich das hier praktizierte Verfahren mit dem Anonymisierungsgebot vereinbaren läßt (§ 92 Abs. 4 Satz 3 SGB V).

Die AOK hat sich meiner Rechtsauffassung zwar nicht angeschlossen, aber erklärt, sie beabsichtige die Wiederholung einer derartigen Umfrage bei ihren Versicherten nicht. Im Hinblick darauf habe ich von einer förmlichen Beanstandung abgesehen.

### 5.9.6 Aktive Gesundheitsberatung

Krankenkassen gehen offenbar vermehrt dazu über, die ihnen zu Abrechnungszwecken übersandten Krankenscheine im Hinblick auf bestimmte Erkrankungen (z. B. Suchtkrankheiten, psychische Erkrankungen, Adipositas, Diabetes) auszuwerten, um die Versicherten gezielt zu beraten. So hatte der bei einer AOK speziell für die Betreuung von Sucht- und psychisch Kranken zuständige Sozialarbeiter einem Versicherten von sich aus einen Termin für einen Hausbesuch vorgeschlagen. Eine IKK hatte ihre an Diabetes leidenden Versicherten zu einer Fahrradtour eingeladen.

Die Auswertung der der Krankenkasse zu Abrechnungszwecken übersandten Krankenscheine für eine **gezielte** Gesundheitsberatung der Versicherten ist nach den hier allein in Betracht kommenden Befugnisvorschriften des Gesundheitsreformgesetzes nicht zulässig, da zu den in § 284 Abs. 1 Satz 1 SGB V abschließend genannten Zwecken der Krankenversicherung die Beratung von Versicherten nicht gehört und die Verwendung von Versichertendaten für Beratungszwecke auch nicht durch das Sozialgesetzbuch angeordnet oder erlaubt ist (§ 284 Abs. 3 SGB V).

Die Krankenkassen haben ihre Versicherten **allgemein** über Gesundheitsgefährdungen und über die Verhütung von Krankheiten aufzuklären und darüber zu beraten, wie Gefährdungen vermieden und Krankheiten verhütet werden können (§ 20 Abs. 1 Satz 1 SGB V). Unter einer allgemeinen Aufklä-

rung und Beratung kann nach dem Wortsinn nur eine generelle, nicht eine auf den einzelnen Versicherten und den Einzelfall abgestellte individuelle Information verstanden werden. Eine Verpflichtung zur gezielten individuellen Beratung ergibt sich zwar aus dem Anspruch des Versicherten gegenüber den Leistungsträgern auf Beratung über seine Rechte und Pflichten nach dem Sozialgesetzbuch (§ 14 Satz 1 SGB I). Dabei muß jedoch die Initiative vom Versicherten ausgehen, indem er seine Krankenkasse um Beratung ersucht. Die Krankenkasse darf dem Versicherten keine Beratung von sich aus aufdrängen, geschweige denn, ihm einen Termin für einen Hausbesuch vorschlagen.

Der Krankenkasse bleibt es freilich unbenommen, ihre Versicherten von sich aus auf die Möglichkeit der Teilnahme an Beratungsgesprächen hinzuweisen. Dies muß aber in allgemeiner Form geschehen, etwa bei öffentlichen Werbeaktionen, durch Presseveröffentlichungen oder in Mitgliederzeitschriften. Die Krankenkassen sind demgegenüber nicht befugt, aktive Gesundheitsberatung zu betreiben, indem sie sich gezielt an einzelne ausgewählte Versicherte wenden.

Soweit die Krankenkassenverbände das Vorgehen ihrer Mitgliedskassen mit einem Hinweis auf § 17 SGB I und die Vorschriften des Gesetzes über die Angleichung der Leistungen zur Rehabilitation (RehaAnglG) zu rechtfertigen versuchen, geht dies fehl. § 17 SGB I enthält lediglich Verfahrensregelungen als Richtschnur für die Leistungsträger bei der Gewährung von Sozialleistungen nach dem Sozialgesetzbuch. Derartige Vorschriften können Eingriffe in das informationelle Selbstbestimmungsrecht über die bereichspezifischen Befugnisnormen des SGB V hinaus nicht rechtfertigen.

Auf die Vorschriften des RehaAnglG kann schon deshalb nicht abgehoben werden, weil nach den Umständen nicht von vornherein davon ausgegangen werden kann, daß es sich bei dem angesprochenen Kreis der Versicherten um Personen handelt, die körperlich, geistig oder seelisch behindert sind oder denen eine solche Behinderung droht (§ 1 RehaAnglG). Unabhängig davon handelt es sich bei der Beratungspflicht nach dem RehaAnglG um eine bereichspezifische Regelung, die als Vorläufer des § 14 SGB I anzusehen ist, dessen Regelungsgehalt, wie oben dargelegt, den Krankenkassen ein derartiges Tätigwerden nicht gestattet.

Somit bleibt festzuhalten, daß der Gesetzgeber mit gezielter Gesundheitsberatung verbundene Eingriffe in das informationelle Selbstbestimmungsrecht nicht zugelassen hat. Es ist allein Sache des Arztes, dem sich der Patient im Vertrauen auf dessen Verschwiegenheitspflicht offenbart hat, notwendige Behandlungsmaßnahmen einzuleiten und durchzuführen.

Da eine Krankenkasse meiner Empfehlung, auf die Möglichkeit von Beratungsgesprächen nicht gezielt unter Verwendung von Versichertendaten, sondern nur in allgemeiner Form hinzuweisen, nicht gefolgt ist, habe ich deren Vorgehen förmlich beanstandet.

Meiner Rechtsauffassung ist das MAGS entgegengetreten, und zwar insbesondere unter Hinweis auf die Rechtsprechung des Bundessozialgerichts, das eine Beratung von Amts wegen für zulässig oder sogar geboten gehalten habe.

Richtig ist, daß das Bundessozialgericht in zahlreichen Entscheidungen einen Anspruch des Versicherten auf hinreichende Beratung von Amts wegen aus Anlaß eines (Leistungs-)Antrages anerkannt und auf die vertragsähnlichen Nebenpflichten aus dem öffentlich-rechtlichen Versicherungsverhältnis nach dem Grundsatz von Treu und Glauben gegründet hat. Diese Rechtsprechung, die – soweit ersichtlich – ausnahmslos von einem bereits bestehenden unmittelbaren Verwaltungskontakt des Betroffenen zu seinem Leistungsträger ausgeht, ist in Fällen einer von der Krankenkasse ausgehenden Gesundheitsberatung nicht einschlägig. Der Versicherte sucht hier zu Behandlungszwecken seinen Arzt auf, ein Verwaltungskontakt zur Krankenkasse besteht insoweit nicht und wird von dem Betroffenen auch nicht ohne weiteres gewünscht.

Im übrigen vermag das MAGS nicht zu erkennen, wieso in dem von mir beanstandeten Fall dem Versicherten eine Beratung aufgedrängt wird. Eine Beratung gegen den Willen des Betroffenen sei schon der Natur der Sache nach nicht möglich. Beratung könne vielmehr nur dann erfolgen, wenn der Betroffene mitwirke, d. h. beratungswillig sei. Nehme der Versicherte das Angebot zur Beratung nicht an, unterbleibe die Beratung. Nehme er dagegen das Beratungsangebot an, liege darin zugleich die konkludente Geltendmachung seines Beratungsanspruchs. Die Beratung erfolge auf Antrag des Versicherten. Auf die Frage, ob eine Beratung auch von Amts wegen zulässig sei, komme es daher in diesem Zusammenhang nicht an.

Das MAGS verkennt hierbei, daß eine Beratung des Versicherten diesem bereits aufgedrängt wird, indem die Krankenkasse von sich aus an den Betroffenen herantritt und ihm damit die Entscheidung abverlangt, ob er das Beratungsangebot der Krankenkasse annimmt oder ablehnt.

### 5.9.7 Chipkarte statt Krankenschein

Auf erhebliches Interesse der Öffentlichkeit stieß die vorgesehene Ersetzung des herkömmlichen Krankenscheines durch die sog. Chipkarte. Deren hohe Speicherkapazität hat vor allem Befürchtungen geweckt, daß auf diesem Wege mehr Informationen, insbesondere medizinische Daten wie die Diagnosen an die Krankenkassen gelangen könnten.

Das Gesundheitsreformgesetz von 1989 hatte vorgesehen, den herkömmlichen Krankenschein bis zum 01.01.1992 durch eine Magnetstreifenkarte zu ersetzen; deren Einführung ist jedoch an verschiedenen Widerständen insbesondere der Kassenärzte gescheitert.

Soweit nunmehr angestrebt wird, die technisch weitaus leistungsfähigere Chipkarte als **Krankenversichertenkarte** nach dem Sozialgesetzbuch einzuführen, ist dies nur dann nicht zu beanstanden, wenn sich die Speicherung im

Chip auf die vom Gesetzgeber als Inhalt der Krankenversichertenkarte zugelassenen Angaben (§ 291 Abs. 2 SGB V) beschränkt, nämlich

- Bezeichnung der ausstellenden Krankenkasse,
- Familienname und Vorname des Versicherten,
- Geburtsdatum,
- Anschrift,
- Krankenversichertennummer,
- Versichertenstatus,
- Tag des Beginns des Versicherungsschutzes,
- bei befristeter Gültigkeit der Karte das Datum des Fristablaufs.

Deshalb muß der Versuchung, unter Ausnutzung der weitaus größeren Speicherkapazität der Chipkarte auch unzulässige Daten darin aufzunehmen, durch geeignete Vorkehrungen begegnet werden. Keinesfalls dürfen bei Einführung einer Chipkarte medizinische Informationen, auch nicht auf freiwilliger Grundlage, auf der gesetzlich vorgeschriebenen Krankenversichertenkarte gespeichert werden.

Andererseits sollte es dem Versicherten unbenommen bleiben, sich eine zweite Chipkarte zu beschaffen, auf der die von ihm wegen besonderer gesundheitlicher Risiken für erforderlich erachteten Informationen gespeichert sind. In der hierzu erforderlichen Einwilligungserklärung, die schriftlich zu erfolgen hat, müssen die vom Versicherten benannten Datenarten ausdrücklich aufgeführt sein. Eine zweckfremde Nutzung der Daten durch Dritte ist gesetzlich zu unterbinden. Damit wäre berechtigten Interessen der Versicherten Rechnung getragen, ohne daß sie befürchten müssen, den Krankenkassen könnten unzulässigerweise ärztliche Daten bekanntwerden.

Darüber hinaus bleibt datenschutzrechtlich zu fordern, daß der Inhalt der Chipkarte für den Versicherten transparent und überprüfbar ist. Hierzu müßten die Krankenkassen und Ärzte verpflichtet werden, Lesegeräte vorzuhalten, mit deren Hilfe der Versicherte den Inhalt seiner Krankenversichertenkarte (Pflichtkarte und evtl. freiwillige Karte) nachprüfen kann. Zudem muß technisch sichergestellt sein, daß alle in der Chipkarte gespeicherten Daten für den Versicherten sichtbar werden, also keine Daten vor ihm versteckt werden können.

Im Hinblick auf das Gefährdungspotential der Speicherkapazität der Chipkarte gehe ich in Übereinstimmung mit dem Bundesbeauftragten für den Datenschutz und dem Bundesministerium für Gesundheit davon aus, daß – zunächst für die Einführungsphase – nur zertifizierte Hard- und Software eingesetzt werden darf.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher am 1./2. Oktober 1992 den in der Anlage 5, S. 164, wiedergegebenen Beschluß zur Chipkarte als elektronischer Krankenversicherungskarte gefaßt.

### 5.9.8 Ermittlung und Offenbarung der Namen von „streikverdächtigen" Zahnärzten

Am 27. Juni 1992 hielten der Kassenzahnärztlichen Vereinigung Nordrhein (KZV) angehörende Zahnärzte aus Protest gegen das Gesundheitsstrukturgesetz ihre Praxen zu den regulären Sprechstunden nicht geöffnet. Presseberichten zufolge beabsichtigte das MAGS, gegen die an diesem sog. **Warnstreik** beteiligten Zahnärzte Disziplinarmaßnahmen durch die KZV zu erzwingen. Zu diesem Zweck forderte das MAGS die Krankenkassen auf, die Namen der betreffenden Zahnärzte festzustellen und ihm über die Landesverbände zu übermitteln.

Dieses Verfahren war datenschutzrechtlich unzulässig. § 284 Abs. 1 SGB V regelt bereichspezifisch und abschließend, welche personenbezogenen Daten die Krankenkassen für Zwecke der Krankenversicherung erheben und erfassen dürfen, soweit sie dafür erforderlich sind. Die Erhebung und Erfassung der Namen von Kassenzahnärzten, die an dem sog. Warnstreik teilgenommen haben, durch die Krankenkassen läßt sich keinem der im Gesetz aufgeführten Zwecke zuordnen. Dabei ist unerheblich, ob die Krankenkassen die Daten – auf welche Weise auch immer – von Amts wegen oder auf Anstoß von Versicherten erhoben haben oder ob sie ihnen durch Hinweise von Versicherten bekanntgeworden sind. Unzulässig erfaßte personenbezogene Daten sind zu löschen (§ 79 Abs. 1 Satz 1 SGB X i.V.m. § 20 Abs. 2 Nr. 1 BDSG). Sie stehen für eine Offenbarung gegenüber dem MAGS nicht zur Verfügung.

Eine Offenbarung wäre nach § 69 Abs. 1 Nr. 1 SGB X nur dann zulässig, wenn sie zur rechtmäßigen Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch erforderlich ist. Zwar sieht der Wortlaut dieser Vorschrift nicht ausdrücklich vor, daß die Aufgabenerfüllung rechtmäßig sein muß. Die Rechtmäßigkeit ist jedoch eine derart selbstverständliche Voraussetzung jeden Verwaltungshandelns, daß auch ohne ausdrückliche Festlegung im Gesetz eine Offenbarung nur unter dieser Voraussetzung als zulässig angesehen werden kann. Zur rechtmäßigen Aufgabenerfüllung gehört auch, daß nur personenbezogene Daten offenbart werden, die der offenbarenden Stelle zulässigerweise bekanntgeworden sind.

Der Hinweis der Landesverbände auf den „gesetzlichen Sicherstellungsauftrag" der gesetzlichen Krankenkassen ging fehl. Zum einen enthält das Gesetz in § 72 Abs. 1 Satz 1 SGB V, wonach Zahnärzte und Krankenkassen zur Sicherstellung der kassenzahnärztlichen Versorgung der Versicherten zusammenwirken, lediglich einen generalklauselartigen Hinweis auf die gemeinsame Selbstverwaltung, die in den nachfolgenden Vorschriften konkret geregelt ist. Danach handelt für die Zahnärzte die KZV, für die Krankenkassen treten deren Landesverbände auf.

Aus diesem durch Kooperation geprägten Regelwerk ergibt sich auch nicht andeutungsweise die Befugnis der Krankenkassen, durch Erhebung, Erfassung und Offenbarung personenbezogener Daten von Kassenzahnärzten in deren informationelles Selbstbestimmungsrecht einzugreifen, zumal dies

durch die abschließende Spezialvorschrift des § 294 Abs. 1 Satz 1 SGB V ausgeschlossen ist.

Zum anderen hat der Gesetzgeber nicht den Krankenkassen, sondern der KZV den Sicherstellungsauftrag erteilt, und zwar als Sicherstellungsmonopol dergestalt, daß allein die KZV die kassenzahnärztliche Versorgung sicherzustellen hat. Demgemäß darf sie auch Einzelangaben über die persönlichen und sachlichen Verhältnisse der Zahnärzte erheben und erfassen, soweit dies für die Sicherstellung der kassenzahnärztlichen Versorgung erforderlich ist; und sie allein hat die Erfüllung der den Kassenzahnärzten obliegenden Pflichten zu überwachen und diese, soweit notwendig, unter Anwendung der gesetzlich vorgesehenen Maßnahmen zur Erfüllung ihrer Pflichten anzuhalten.

Den Vorschriften des SGB V ist nicht zu entnehmen, daß die Krankenkassen berechtigt sind, gesetzlich der KZV zugewiesene Aufgaben gleichsam an sich zu ziehen, wenn nach ihrer Auffassung die KZV ihrer Verpflichtung aus dem Sicherstellungsauftrag nicht angemessen nachkommt.

Auch der Auffassung des MAGS, die „umfassende Unterrichtungsverpflichtung" der Krankenkassen über deren Landesverbände gegenüber ihm als Aufsichtsbehörde (§ 88 SGB IV) gestatte diesen, die Namen der an dem sog. Warnstreik beteiligten Zahnärzte zu erheben und an das MAGS zu übermitteln, konnte nicht gefolgt werden. Eine im Wege der Aufsicht zu sanktionierende Rechtsverletzung durch die Krankenkassen stand hier ersichtlich nicht in Rede. Vielmehr sollten die Krankenkassen dem MAGS Daten zur Verfügung stellen, damit dieses die KZV anweisen konnte, gegen die betreffenden Zahnärzte Disziplinarmaßnahmen einzuleiten. Dabei handelte es sich um Daten, die die Krankenkassen für ihre Aufgabenerfüllung nach dem Sozialgesetzbuch nicht benötigen und daher, wie oben dargelegt, nicht erheben, speichern und übermitteln dürfen.

Da die Krankenkassenverbände an ihrer Auffassung festhielten und die Namen der an dem sog. Warnstreik beteiligten Zahnärzte an das MAGS übermittelt haben, mußte ich diesen Verstoß gegen das Sozialgeheimnis förmlich beanstanden. Zu dessen Folgenbeseitigung war es geboten, die dem MAGS offenbarten Daten von ihm zurückzufordern und unverzüglich zu löschen.

### 5.9.9 Weitergabe durch Dritte erstellter Arztberichte

Durch die Anfrage einer Kassenärztlichen Vereinigung wurde mir bekannt, daß Krankenkassen die Vertragsärzte auffordern, die von Dritten, nämlich Krankenhäusern und Kurkliniken über ihre Patienten erstellten Entlassungsberichte, Arztbriefe oder Kurberichte an den Medizinischen Dienst der Krankenkassen zu übersenden. Hierfür fehlt es an einer gesetzlichen Grundlage, die es dem Arzt gestattet, einer solchen Aufforderung nachzukommen. Die an der kassen- und vertragsärztlichen Versorgung teilnehmenden Ärzte sind verpflichtet und befugt, die für die Erfüllung der Aufgaben der Krankenkassen sowie der Kassenärztlichen Vereinigungen notwendigen Angaben, die aus der Erbringung, der Verordnung sowie der Abgabe von Versicherungslei-

stungen entstehen, aufzuzeichnen und in den gesetzlich geregelten Fällen den Krankenkassen mitzuteilen (§ 294 SGB V). Allerdings bezieht sich diese Verpflichtung und Befugnis nur auf Angaben über Leistungen, die der Arzt selbst erbracht hat. Bei den in den Krankenhausentlassungsberichten enthaltenen Angaben handelt es sich jedoch um Leistungen, deren Erbringer der Krankenhausarzt ist. Auskunftsverpflichtet und -befugt ist insoweit nur das Krankenhaus, das dabei die Vorschriften der §§ 301, 276 Abs. 4 SGB V zu beachten hat.

### 5.9.10 Angaben zu Einkommens- und Vermögensverhältnissen nicht unterhaltspflichtiger Ehegatten

Auf heftigen Widerstand der Betroffenen stößt die nach wie vor weit verbreitete Praxis der Sozialämter, im Rahmen der Gewährung von Sozialhilfe nicht nur von dem unterhaltspflichtigen Angehörigen, sondern auch von seinem nicht unterhaltspflichtigen Ehegatten Angaben über dessen Einkommens- und Vermögensverhältnisse zu verlangen.

Schon in meinem 8. Tätigkeitsbericht (S. 61) habe ich ausgeführt, daß für dieses Verlangen der Sozialämter keine gesetzliche Grundlage besteht. Demgegenüber berufen sich die Sozialämter auf das Urteil des Verwaltungsgerichtshofs Baden-Württemberg vom 14.03.1990 – 6 S – 1575/89 . Das Gericht folgert aus dem Begriff der Einkommens- und Vermögens**verhältnisse**, daß hier nicht nur die dem Unterhaltspflichtigen unmittelbar zufließenden Einkünfte und die ihm selbst unmittelbar zuzuordnenden Vermögensgegenstände gemeint seien, sondern alle Umstände, die Umfang und Höhe des Einkommens oder Vermögens des Unterhaltspflichtigen mitbestimmen können. Dazu könnten insbesondere auch Unterhaltsleistungen eines mit dem Unterhaltspflichtigen in Haushaltsgemeinschaft lebenden Ehegatten an ihn zählen. Da in der ehelichen Lebensgemeinschaft nach dem geltenden Unterhaltsrecht jeder Ehegatte gegenüber dem anderen zugleich Unterhaltsberechtigter und Unterhaltsverpflichteter sei, könnten die Einkommens- und Vermögensverhältnisse eines Ehegatten ohne Einbeziehung der entsprechenden Verhältnisse des anderen Ehegatten überhaupt nicht beurteilt werden.

Diese Auffassung kann ich nicht teilen. Auf diese Weise würde an den Unterhaltsvorschriften des Bürgerlichen Gesetzbuchs (§§ 1601, 1605) vorbei faktisch eine Unterhaltspflicht für **nicht unterhaltspflichtige Angehörige** begründet. Die Auskunftspflicht des in gerader Linie Verwandten bezieht sich auf Einkünfte und Vermögen, nicht auf andere Umstände, insbesondere besteht keine Auskunftspflicht bezüglich des Einkommens von Ehepartnern oder Kindern des Verwandten (vgl. Palandt, 43. Aufl. § 1605 Anm. II).

Meine Auffassung wird durch ein Urteil des Amtsgerichts München vom 21. Juni 1989 – 352 C 11355/89 , das mir ein Betroffener zugeleitet hat, gestützt. Darin heißt es:

> „Eine Unterhaltsverpflichtung der Beklagten gegenüber ihrem Vater kann nur aus ihrem eigenen bereinigten Einkommen hergeleitet werden, ... Ein fiktiver Unterhaltsanspruch gegen den Ehemann kann nicht

dazu dienen, das Einkommen der Beklagten zu erhöhen. Zu Recht vertritt die Beklagte die Ansicht, daß Unterhaltszahlungen nicht dazu dienen, den Unterhaltsberechtigten seinerseits wieder unterhaltsverpflichtet zu machen, sondern daß sie zur Bestreitung des Lebensunterhaltes dienen. Eine andere Auffassung würde auch den §§ 1360, 1360 a BGB widersprechen, wonach der allein- bzw. besserverdienende Ehegatte seinem Ehepartner einen angemessenen Unterhalt zu gewähren hat. Dies umfaßt alles, was nach den Verhältnissen der Ehegatten erforderlich ist, um die Kosten des Haushalts zu bestreiten und die persönlichen Bedürfnisse der Ehegatten und den Lebensbedarf der gemeinsamen unterhaltsberechtigten Kinder zu befriedigen. Dieser angemessene Unterhalt ist aber nicht dafür einzusetzen, daß der Ehepartner einem dritten Unterhaltsberechtigten Unterhalt zu gewähren hat."

Diesen Ausführungen kann ich nur beipflichten. Auch die Erörterung der Problematik im Kreise der Datenschutzbeauftragten des Bundes und der Länder hat ergeben, daß für Ehegatten und sonstige Angehörige eines Unterhaltspflichtigen keine Auskunftspflicht besteht. Der Unterhaltspflichtige ist daher auf die Freiwilligkeit der Angaben hinzuweisen. Im übrigen ist mir bekanntgeworden, daß die zuständigen obersten Landesbehörden in Niedersachsen, Sachsen-Anhalt, Schleswig-Holstein, Saarland und Bayern diese Auffassung teilen. Ich habe daraufhin das MAGS ebenfalls um Stellungnahme gebeten.

Meiner Empfehlung, den vom Sozialamt verwendeten Vordruck meinen Bedenken entsprechend zu ändern, ist ein Oberstadtdirektor inzwischen gefolgt, indem er nunmehr das von der Vordruckkommission beim Landkreistag Nordrhein-Westfalen überarbeitete Vordruckmuster „Auskunft über Einkommens- und Vermögensverhältnisse" (Landkreistag/Städtetag NW 11.91) verwendet. Dieses ist mit dem Hinweis versehen, daß die Angaben in den gerasterten Feldern – hierzu gehören alle Angaben zum Ehegatten, zu den im Haushalt des Pflichtigen lebenden Kindern und sonstigen Personen, Miete und finanzielle Belastungen – freiwillig sind. Außerdem wird auf die Folgen der Nichtangabe dieser Daten sowie darauf hingewiesen, daß der Ehegatte ebenfalls unterschreiben muß, wenn seine Person betreffende Daten mitgeteilt werden, ohne daß er unterhaltspflichtig ist.

Es ist nicht einzusehen, weshalb dieses datenschutzrechtlich korrekte Vordruckmuster nicht landesweit Verwendung findet.

### 5.9.11 Einsicht in Sozialgerichtsakten abgeschlossener Verfahren für wissenschaftliche Zwecke

Noch immer verkennen Gerichte die Tragweite der bereits seit 1981 geltenden Vorschriften zum Schutz der Sozialdaten. So mußte ich förmlich beanstanden, daß der Präsident eines Sozialgerichts einem Wissenschaftler für eine rechtstatsächliche Studie zur Frage der Umstellung von Rahmen- auf Wertgebühren in der Sozialgerichtsbarkeit Einsicht in Gerichtsakten abge-

schlossener Verfahren, allerdings mit Ausnahme ärztlicher Atteste und Gutachten, gewährt hatte.

Sämtliche einem Sozialleistungsträger im Rahmen seiner Aufgabenerfüllung nach dem Sozialgesetzbuch bekanntgewordenen personenbezogenen Daten unterliegen bei ihm dem Sozialgeheimnis. Er darf diese Daten nur unter den im Gesetz abschließend geregelten Voraussetzungen (§§ 67 bis 77 SGB X) offenbaren. Danach ist er befugt, zur Durchführung eines mit der Aufgabenerfüllung nach dem Sozialgesetzbuch zusammenhängenden gerichtlichen Verfahrens dem Sozialgericht die hierfür erforderlichen Daten zu offenbaren. Das Sozialgericht darf die ihm für das jeweilige gerichtliche Verfahren offenbarten Daten nur an diesen Zweck gebunden verwenden (§ 78 SGB X). Eine Weiteroffenbarung zu wissenschaftlichen Zwecken durch Gewährung von Akteneinsicht stellt demnach eine unzulässige Datenverwendung dar. Dieses strenge **Zweckbindungsgebot** wird durch die „im übrigen" bestehende Verpflichtung des Datenempfängers, die Daten in demselben Umfang geheimzuhalten wie die offenbarenden Stellen, nicht etwa in der Weise durchbrochen, daß dem Datenempfänger die gesetzlichen Offenbarungsbefugnisse eröffnet werden. Normadressat dieser Offenbarungsbefugnisse sind die Sozialleistungsträger, nicht das Sozialgericht.

Der Präsident des Sozialgerichts hielt mir unter Berufung auf das Urteil des Landessozialgerichts Essen vom 21.07.1982 – L VIII J 18/80 – entgegen, daß für das sozialgerichtliche Verfahren die geltende Prozeßordnung maßgebend sei. Akteneinsicht werde in die Verfahrensakten des Gerichts, nicht in die Verwaltungsakten der Sozialleistungsträger gewährt. Im übrigen sei sichergestellt, daß der Wissenschaftler, der sich nur für die Klageanträge interessiere, keinen weiteren Einblick in die Akten nehme.

Bereits in meinem 4. Tätigkeitsbericht (S. 68) und in meinem 9. Tätigkeitsbericht (S. 65) habe ich dargelegt, daß das zitierte Urteil des Landessozialgerichts Essen die Rechtslage verkennt. Der Gesetzgeber hat im Zweiten Kapitel des Zehnten Buches des Sozialgesetzbuchs abschließende Regelungen für die Befugnis zur Offenbarung von Sozialdaten getroffen. Andere Vorschriften, insbesondere des gerichtlichen Verfahrens greifen daneben nicht durch.

Im übrigen könnte das Sozialgerichtsgesetz hier schon deshalb keine Anwendung finden, weil Einsicht nicht in Akten laufender, sondern abgeschlossener Verfahren gewährt wurde. Insoweit handelt es sich um einen Vorgang der Verwaltung, nicht der Rechtspflege.

Zudem steht der Anwendung der Sozialdatenschutzvorschriften hier nicht entgegen, daß dem Sozialgericht im Zeitpunkt der Offenbarung durch den Leistungsträger die Daten bereits – zumindest teilweise – auf Grund des Klageantrages bekannt sind. Gegenstand des Sozialdatenschutzes sind nach geltendem Recht nicht mehr „Geheimnisse", sondern „personenbezogene Daten" schlechthin. Es kommt deshalb nicht mehr darauf an, ob die Daten nur einem begrenzten Personenkreis bekannt und deshalb geschützt oder als „offenkundige Tatsachen" nicht geschützt sind. Somit gelangen in die gericht-

liche Hauptakte regelmäßig schon deshalb Sozialdaten, weil der Sozialleistungsträger in seiner Klageerwiderung zumindest Namen und Anschrift des Betroffenen sowie die Tatsache seiner Beziehung zum Sozialleistungsträger gegenüber dem Gericht offenbart.

Soweit im Schrifttum vereinzelt die Auffassung zur Diskussion gestellt worden ist, der verlängerte Sozialdatenschutz gelte nicht für die Schriftsätze der Beteiligten (also auch des Leistungsträgers) in der gerichtlichen Hauptakte, ist dies ohne Widerhall geblieben; im übrigen läßt die insoweit normenklare gesetzliche Regelung für eine derartige Betrachtungsweise keinen Raum.

Unerheblich ist auch, daß sich der Wissenschaftler nur dafür interessiert, welche Klageanträge gestellt werden. Das Sozialgericht verletzt seine Wahrungspflicht bereits dann, wenn es dem Wissenschaftler die Gerichtsakte insgesamt zugänglich macht, so daß dieser – worauf allein abzuheben ist – die Möglichkeit hat, Einblick in die gesamte Akte zu nehmen. Unter diesen Umständen kann überhaupt nicht „sichergestellt" werden, daß der Wissenschaftler Einblick nur in die Klageanträge nimmt. Jedenfalls reicht eine entsprechende Zusicherung des Wissenschaftlers nicht aus.

## 5.10 Gesundheitswesen

### 5.10.1 Gesundheitsdatenschutzgesetz

Die Verwirklichung des Vorhabens einer umfassenden Regelung des Datenschutzes im Gesundheitswesen ist inzwischen durch die Vorlage eines überarbeiteten Referentenentwurfs des MAGS einen entscheidenden Schritt näher gerückt.

Die Schaffung bereichspezifischer Vorschriften zum Datenschutz im Gesundheitswesen ist zu begrüßen; sie entspricht einer seit langem erhobenen Forderung der Datenschutzbeauftragten. Der nunmehr vorliegende Referentenentwurf berücksichtigt bereits einige wesentliche Vorschläge, die ich im Rahmen einer Ressortbesprechung zu dem Vorentwurf unterbreitet hatte. Da jedoch aus datenschutzrechtlicher Sicht weitere Änderungen und Ergänzungen geboten sind, habe ich dem MAGS insbesondere vorgeschlagen,

- im Gesetzeswortlaut selbst klarzustellen, daß nicht zweckdienliche Angaben auch mit Einwilligung weder erhoben noch gespeichert werden dürfen (§ 4 Abs. 3);
- zu präzisieren, daß nur gesetzlich normierte Auskunfts- und Meldepflichten als Ergebnis der gebotenen Rechtsgüterabwägung die ärztliche Schweigepflicht durchbrechen (§ 5 Abs. 1 Satz 1);
- entsprechend dem verfassungsrechtlichen Gebot der informationellen Gewaltenteilung die Weitergabe von Patientendaten von einer Organisationseinheit an eine andere innerhalb der Einrichtung oder öffentlichen Stelle der Übermittlung gleichzustellen (§ 5 Abs. 1 Satz 2);
- zum Schutz der der ärztlichen Schweigepflicht unterliegenden Patientendaten beim Empfänger ein Zweckbindungsgebot vorzusehen (§ 5 Abs. 2);

- normenklar zu regeln, daß nur die mit der Aufgabenerfüllung nach diesem Gesetz jeweils betrauten Ärzte die Daten ihrer Patienten für eigene wissenschaftliche Forschungsvorhaben nutzen dürfen (§ 6 Abs. 1 Satz 1);
- eine Durchbrechung der ärztlichen Schweigepflicht durch Zulassung der Datenverarbeitung im Auftrag an strenge Voraussetzungen und Kontrollen zu binden (§ 7);
- den Auskunftsanspruch des Betroffenen auch auf die Herkunft der Daten zu erstrecken und beim Akteneinsichtsrecht zwischen Gesundheitsamtsakten und Krankenhausakten zu differenzieren sowie einen unmittelbaren Anspruch des Patienten auf Akteneinsicht im Hinblick auf das informationelle Selbstbestimmungsrecht auch in den Fällen vorzusehen, in denen wegen einer zu befürchtenden unverhältnismäßigen Beeinträchtigung der Gesundheit des Patienten eine Vermittlung des Akteninhalts durch den Arzt vorausgegangen ist (§ 9);
- die Weitergabe bei der amtsärztlichen Untersuchung erhobener Einzelergebnisse (Anamnese, Befunde, Diagnose) nur in den wenigen Ausnahmefällen zuzulassen, in denen die Kenntnis von Einzelergebnissen in dem Sinne unabweisbar ist, daß ohne sie die anstehende Entscheidung nicht getroffen werden kann (§ 24 Abs. 3 Satz 2);
- wegen Unvereinbarkeit mit Artikel 4 Abs. 2 Satz 2 der Landesverfassung von Regelungen abzusehen, die die Anwesenheit Dritter bei der (zahn)ärztlichen Untersuchung von Schülern zulassen (§ 25 Abs. 2);
- von einer Vorschrift abzusehen, die es dem Gesundheitsamt gestattet, ihm gelegentlich seiner Aufgabenerfüllung bekanntgewordene Daten behandelnder Ärzte an die für standes-, berufs- oder kassenarztrechtliche Verstöße zuständigen Stellen zu übermitteln, da eine derartige Übermittlungsbefugnis zum einen den Rahmen dieses Gesetzes sprengt und hier systemfremd erscheint, zum anderen mit einer Durchbrechung der ärztlichen Schweigepflicht verbunden wäre, ohne daß hierfür ein anerkennenswerter Rechtfertigungsgrund ersichtlich ist (§ 26);
- ein Akteneinsichtsrecht auch für Maßregelvollzugspatienten vorzusehen (§ 27).

### 5.10.2 Einschulungsuntersuchung

Im Rahmen meiner Informations- und Kontrollbesuche bei Gesundheitsämtern habe ich festgestellt, daß in Einzelfällen für die Einschulungsuntersuchung weiterhin der Vordruck „Angaben für den Schularzt" mit Fragen zu Schwangerschaft und Geburtsverlauf sowie zur Familienanamnese der Großeltern, Eltern und Geschwister hinsichtlich bestimmter Krankheiten verwendet wird, obgleich das MAGS eine Familien- und Sozialanamnese für überzogen hält, wie ich in meinem 10. Tätigkeitsbericht (S. 87/88) ausgeführt habe.

Dem Einwand, die erbetenen Angaben seien zu erheben, weil der Schularzt auch die Aufgabe habe, Schäden von dem Kind abzuwenden, kann nicht gefolgt werden. Die Feststellung des für die Beurteilung der Schulfähigkeit

aus medizinischer Sicht allein maßgeblichen körperlichen Ist-Zustandes gestattet lediglich die Erhebung der hierfür erforderlichen Daten. Somit hat sich der Umfang der Datenerhebung anläßlich der Einschulungsuntersuchung an der Feststellung, ob das Kind an einer die Schulfähigkeit beeinträchtigenden gesundheitlichen Störung leidet, nicht aber an deren Pathogenese zu orientieren. Insoweit unterscheidet sich die Aufgabenerfüllung des Schularztes von der eines behandelnden Arztes. Ich habe daher die Weiterverwendung des Vordrucks „Angaben für den Schularzt" förmlich beanstandet.

### 5.10.3 Sozialpsychiatrischer Dienst der Gesundheitsämter

Förmlich beanstanden mußte ich, daß ein Kreisgesundheitsamt sich weigerte, die Klienten des Sozialpsychiatrischen Dienstes, die auf Grund von Hinweisen durch Dritte im Wege der **vorsorgenden Hilfe** zu den regelmäßigen Sprechstunden eingeladen wurden, ausdrücklich auf die Freiwilligkeit ihres Erscheinens sowie auf die Rechtsvorschrift für die Abhaltung der Sprechstunden hinzuweisen.

Das informationelle Selbstbestimmungsrecht gebietet, den Klienten zu Beginn einer freiwilligen Beratung über seine Rechte und Pflichten zu unterrichten, damit er in die Lage versetzt wird, selbst frei zu entscheiden, ob er eine Beratung in den Sprechstunden des Gesundheitsamtes wünscht. Voraussetzung hierfür ist, daß der Betroffene die Rechtsgrundlage für das Tätigwerden des Gesundheitsamtes kennt und darüber unterrichtet wird, daß seine Teilnahme freiwillig ist. Der Oberkreisdirektor war der Ansicht, das Einladungsschreiben sei inhaltlich so abgefaßt, daß eine Einladung erkennbar werde; deshalb habe auf die Freiwilligkeit des Erscheinens nicht besonders hingewiesen werden müssen. Zudem sei es nicht ratsam, die zu betreuenden schwierigen Patienten auf das PsychKG mit seinen einzelnen Paragraphen hinzuweisen.

Diesen Einwänden kann nicht gefolgt werden. Dem aus dem informationellen Selbstbestimmungsrecht folgenden Transparenzgebot kann nur dadurch entsprochen werden, daß für den Betroffenen explizit und nicht nur vom Inhalt her erkennbar wird, daß die Entscheidung, ob er der Einladung folgt oder nicht, allein bei ihm liegt. Dies läßt sich auf einfache und unmißverständliche Weise dadurch erreichen, daß in dem Einladungsschreiben ausdrücklich auf die Freiwilligkeit der Teilnahme hingewiesen wird.

Die Verpflichtung zur Bekanntgabe der Rechtsvorschrift für die Durchführung der Sprechstunden (§ 8 Abs. 1 Satz 1 PsychKG) gegenüber dem Betroffenen besteht uneingeschränkt und unabhängig vom Krankheitsbild.

Zwar wird das Kreisgesundheitsamt die Klienten des Sozialpsychiatrischen Dienstes künftig unter Angabe der Rechtsgrundlage und unter ausdrücklicher Bezeichnung des Anschreibens als „Einladung" zu den Sprechstunden einladen. Diese Verfahrensänderungen genügen jedoch den gesetzlichen Anforderungen nicht. Da die Betroffenen keinerlei Zwangsmaßnahmen nach dem PsychKG unterliegen, muß auf jeden Fall der unzutreffende Eindruck vermieden werden, als bestehe für sie eine Verpflichtung zur Teilnahme. Deshalb ist

es unerläßlich, die Betroffenen ausdrücklich, und zwar unter Verwendung des Wortes „freiwillig", darüber aufzuklären, daß ihnen die Teilnahme an den Sprechstunden freisteht.

### 5.10.4 Vergabe von Schreibarbeiten durch Krankenhausärzte

Bedenken bestehen gegen die zunehmende Vergabe von Schreibarbeiten für den ärztlichen Dienst kommunaler Krankenhäuser an private Schreibbüros.

Die auf vom Arzt besprochenen Kassetten und in Krankenberichten festgehaltenen Patientendaten (Arztbriefe, Befunde) unterliegen sowohl den Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen als auch der **ärztlichen Schweigepflicht**.

Es kann dahingestellt bleiben, ob es sich bei der Vergabe von Schreibarbeiten aus dem ärztlichen Bereich an ein privates Schreibbüro um die Übermittlung personenbezogener Daten oder um Datenverarbeitung im Auftrag handelt und inwieweit die Vergabe danach zulässig ist. Jedenfalls verbietet die ärztliche Schweigepflicht eine Offenbarung personenbezogener Daten von Patienten an ein privates Schreibbüro.

Die ärztliche Berufsordnung (BO) gebietet dem Arzt, über das, was ihm in seiner Eigenschaft als Arzt anvertraut oder bekanntgeworden ist, zu schweigen. Zur Offenbarung ist er befugt, soweit er von der Schweigepflicht entbunden worden ist oder soweit die Offenbarung zum Schutze eines höheren Rechtsguts erforderlich ist (§ 2 Abs. 4 BO). Beide Voraussetzungen liegen nicht vor. Ebensowenig kann der Inhaber oder Angestellte des Schreibbüros als „berufsmäßig tätiger Gehilfe" des Arztes (§ 203 Abs. 3 Satz 1 StGB) angesehen werden, weil seine Tätigkeit nicht in einem unmittelbaren inneren Zusammenhang mit der ärztlichen Berufsausübung steht.

Eine Vergabe von Schreibarbeiten aus dem ärztlichen Bereich an ein privates Schreibbüro ist deshalb nur mit Einwilligung des Patienten zulässig, die aus Beweissicherungsgründen schriftlich erfolgen sollte.

### 5.10.5 Übermittlung der Religionszugehörigkeit durch Krankenhäuser an Seelsorger

Der Besuch eines Gemeindebeauftragten der Pfarrei seines Wohnortes hat einen stationär behandelten Patienten veranlaßt, Erkundigungen darüber einzuholen, woher der Kirche sein Krankenhausaufenthalt bekannt war. Dabei hat sich herausgestellt, daß die im Krankenhaus tätigen Seelsorger auf Anfrage Kenntnis von dem stationären Aufenthalt eines Patienten erhalten, wenn der Patient die entsprechende Religionszugehörigkeit bei der Aufnahme angegeben hat. Unter dieser Voraussetzung werden dem zuständigen Krankenhausseelsorger Name, Vorname, Geburtsdatum, Wohnort, Straße, Aufnahmedatum und Station des Patienten übermittelt. Im vorliegenden Fall hatte der Seelsorger des Krankenhauses die personenbezogenen Daten des Betroffenen an die Pfarrgemeinde seines Wohnortes weitergegeben.

Die Religionsgesellschaften legen im Rahmen ihrer verfassungsrechtlich garantierten Autonomie ihre Aufgaben und Ziele selbst fest. Damit können sie

auch bestimmen, daß die seelsorgerische und karitative Betreuung der in einem Krankenhaus aufgenommenen Gemeindemitglieder zu den Aufgaben ihrer Pfarrgemeinde gehört. Allein diesem Zweck dient auch die Erhebung der Religionszugehörigkeit durch das Krankenhaus, das diese Angabe für seine eigene Aufgabenerfüllung nicht benötigt. Bei der Übermittlung muß allerdings sichergestellt werden, daß bei den Empfängern ausreichende Datenschutzmaßnahmen getroffen werden. Insbesondere muß bei der Pfarrgemeinde gewährleistet sein, daß die haupt- oder ehrenamtlichen Mitglieder der Gemeinde die von dem Krankenhaus übermittelten Daten nur zur Erfüllung der genannten Aufgaben nutzen und keinem Dritten zugänglich machen (§ 15 i.V.m. § 14 Abs. 1 Satz 1 DSG NW).

Unter diesen Voraussetzungen bestehen keine durchgreifenden Bedenken gegen die Übermittlung der Namen der in einem Krankenhaus aufgenommenen Gemeindemitglieder an ihre Pfarrgemeinde. Das Arztgeheimnis steht dem nicht entgegen, da die Angaben über die Aufnahme in das Krankenhaus und über die Religionszugehörigkeit dem Krankenhaus nicht von einem Arzt übermittelt, sondern bei dem Patienten selbst erhoben worden sind.

Eine rechtliche Verpflichtung des Patienten zur Angabe seiner Religionszugehörigkeit besteht nicht. Das Krankenhaus hat deshalb bei der Erhebung auf die Freiwilligkeit der Angabe hinzuweisen (§ 12 Abs. 2 Satz 3 DSG NW). Wenn ein Patient eine seelsorgerische oder karitative Betreuung nicht wünscht, hat er die Möglichkeit, die Angabe der Religionszugehörigkeit zu verweigern. Somit entscheidet der Patient durch die Preisgabe oder Nichtpreisgabe selbst darüber, ob seine Konfession an die Religionsgesellschaft weitergegeben werden darf. Aus der Sicht des Datenschutzes halte ich es dabei für erforderlich, die Patienten vor der Angabe ihrer Religionszugehörigkeit über die Möglichkeit der Übermittlung ihrer Namen an den Seelsorger der jeweiligen Religionsgesellschaft ins Bild zu setzen.

## 5.11 Personalwesen

### 5.11.1 Arbeitnehmerdatenschutz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich im Berichtszeitraum eingehend mit Fragen des Arbeitnehmerdatenschutzes befaßt, nachdem dessen gesetzliche Regelungsbedürftigkeit in jüngerer Zeit offenkundig geworden ist (vgl. auch meinen 10. Tätigkeitsbericht, S. 19). Die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. März 1992 (s. Anlage 6, S. 165 bis 167) weist hierzu auf die datenschutzrechtlich bedeutsamen Gesichtspunkte hin.

### 5.11.2 Sechstes Gesetz zur Änderung dienstrechtlicher Vorschriften

Die Landesregierung bereitet die Anpassung des Landesbeamtengesetzes (LBG) und des Landesrichtergesetzes an die durch verschiedene Bundesgesetze veränderten rahmenrechtlichen Vorgaben des Beamtenrechtsrahmengesetzes und Regelungen des Bundesbeamtengesetzes vor. Den Schwerpunkt des hierzu vorliegenden Entwurfs eines Sechsten Gesetzes zur

Änderung dienstrechtlicher Vorschriften bildet dabei die Neuregelung des Personalaktenrechts, deren vorrangiges Anliegen es sein soll, das Persönlichkeitsrecht des Beamten im Rahmen einer effektiven Verwaltung der Personalakten zu stärken. Aus datenschutzrechtlicher Sicht erscheinen jedoch einige Änderungen und Ergänzungen geboten. Deshalb habe ich zu dem Gesetzentwurf, auch im Hinblick auf die Ausführungen in meinem 10. Tätigkeitsbericht (S. 90 bis 95), gegenüber dem Innenministerium vorgeschlagen,

- die gesetzlichen Voraussetzungen für die Versetzung eines Beamten wegen Dienstunfähigkeit in den Ruhestand durch eine Regelung zu ergänzen, die vorsieht, daß mit der Anordnung der Untersuchung des Beamten in der Regel nur die Übermittlung des Ergebnisses der medizinischen oder psychologischen Untersuchung und der dabei festgestellten Risikofaktoren/Beeinträchtigungen der Dienstfähigkeit verlangt werden darf (§ 45 Abs. 1 LBG);
- wegen des mit einer Akteneinsicht von Beauftragten des Dienstherrn verbundenen schwerwiegenden Eingriffs in das informationelle Selbstbestimmungsrecht des Beamten sowie im Hinblick darauf, daß dabei jeweils mehr Daten preisgegeben werden, als für die Teilzuständigkeit des Beauftragten erforderlich ist, diesem Personenkreis nur dann Zugang zur Personalakte zu gewähren, wenn seine Beteiligung an Personalentscheidungen zur Wahrnehmung besonderer Belange gesetzlich vorgesehen ist und der Beamte eingewilligt hat (§ 102 Abs. 3 Satz 2 LBG);
- in den die freie Heilfürsorge der Polizeivollzugsbeamten sowie deren Dienstunfähigkeit regelnden Vorschriften die Aufgaben und Befugnisse des Polizeiarztes im Bereich der freien Heilfürsorge und der Untersuchungen im Rahmen der Verwendungsfähigkeit der Polizeivollzugsbeamten festzulegen und abzugrenzen. Dabei ist insbesondere die hierfür erforderliche Datenverarbeitung des Polizeiarztes unter Berücksichtigung des Grundsatzes der Abschottung der im Rahmen der Gewährung freier Heilfürsorge gewonnenen von denjenigen personenbezogenen Daten, die bei der Feststellung der Verwendungsfähigkeit der Polizeivollzugsbeamten erhoben werden, gesetzlich zu verankern (§ 189 Abs. 2 und § 194 LBG).

### 5.11.3 Drittes Gesetz zur Änderung des Personalvertretungsgesetzes

Die Landesregierung beabsichtigt eine umfangreiche Novellierung des Personalvertretungsgesetzes für das Land Nordrhein-Westfalen (LPVG). Hierzu habe ich Anregungen gegeben und zum Teil Bedenken geäußert.

- Wegen in der praktischen Anwendung aufgetretener Unklarheiten sollte der Begriff der „Sammlungen von Personaldaten" in der geltenden Fassung (§ 65 Abs. 3 Satz 1) gesetzlich näher erläutert werden.
- Unter Hinweis auf die Ausführungen in meinem 10. Tätigkeitsbericht (S. 102/103) habe ich die Schaffung normenklarer und nach Möglichkeit abschließender bereichspezifischer, den Umgang mit personenbezogenen Daten durch den Personalrat regelnder Vorschriften angeregt (§ 65

Abs. 4). In den danach zu treffenden Regelungen sollten nach meiner Auffassung insbesondere folgende Gesichtspunkte berücksichtigt werden:

Art und Dauer der Speicherung von in Beteiligungsverfahren übermittelten personenbezogenen Daten der Beschäftigten,

Behandlung von Vorgängen des Personalrats mit personenbezogenen Daten,

Voraussetzungen für eine zulässige Datenerhebung, -übermittlung und -nutzung durch den Personalrat,

Art und Dauer der Aufbewahrung von Tagesordnung und Niederschrift; Verwendung der Niederschrift,

Festlegung erforderlicher organisatorischer und technischer Maßnahmen zur Datensicherheit sowie

Sicherstellung der Kontrolle durch den Dienststellenleiter.

- Hinsichtlich der in den Sondervorschriften für Lehrkräfte enthaltenen Regelungen über die Sammelerörterung zwischen der Leitung der Dienststelle und allen betroffenen Personalvertretungen habe ich angeregt, den Begriff der allgemeinen schulformübergreifenden Angelegenheiten in der Gesetzesbegründung klarzustellen. Damit soll eine unzulässige, durch den Gesetzeswortlaut nicht gedeckte Weitergabe personenbezogener Daten betroffener Lehrkräfte an nicht zu beteiligende Personalräte vermieden werden. Das Innenministerium hat mir mitgeteilt, daß es diese Anregung nicht aufgreifen wird.
- Im übrigen habe ich gegen die Regelung, daß bei Versetzungen von Lehrkräften an eine Schule oder ein Studienseminar der bei der abgebenden Dienststelle gebildete Personalrat dem bei der aufnehmenden Dienststelle gebildeten Personalrat Gelegenheit zur Äußerung gibt, erhebliche datenschutzrechtliche Bedenken erhoben, die ich auch nach Erörterung mit dem Innenministerium aufrechterhalten muß. Es ist nicht erkennbar, daß im Hinblick auf dieses Beteiligungsverfahren der Personalräte untereinander eine Abwägung zwischen einem etwaigen dienstlichen Interesse hieran und dem hiermit verbundenen Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen vorgenommen worden ist, so daß diese Regelung dem Verfassungsgebot der Verhältnismäßigkeit widersprechen dürfte. Die zur Beschleunigung von Lehrerversetzungsverfahren gedachte Regelung erscheint auch nicht zwingend erforderlich, weil die notwendigen Mitbestimmungsverfahren nach der Rechtsprechung in beiden Dienststellen gleichzeitig durchgeführt werden können und die Dienststellenleitung notfalls eine vorläufige Regelung treffen kann (BVerwG, DÖV 1988, 602).

### 5.11.4 Disziplinarordnung

Im Rahmen der vorgesehenen Novellierung der Disziplinarordnung des Landes Nordrhein-Westfalen (DO NW) habe ich das Innenministerium auf daten-

schutzrechtliche Bedenken gegen zu weitreichende Übermittlungsvorschriften und eine unangemessene Tilgungsregelung hingewiesen. Im einzelnen habe ich vorgeschlagen,

- die Voraussetzungen für die Vorlage von Personalakten oder anderen Behördenunterlagen mit personenbezogenen Daten oder die Erteilung entsprechender Auskünfte an Disziplinarbefugnisse ausübende Behörden, an Untersuchungsführer und Disziplinargerichte im Gesetz normenklar zu regeln. Der bloße Hinweis auf die Dienstaufsicht darf nicht jede Informationsanforderung rechtfertigen;
- die Tilgungsvorschriften um eine klarstellende Regelung zu ergänzen, wonach im Falle des Freispruchs im förmlichen Disziplinarverfahren die entstandenen Vorgänge sofort aus den Personalakten zu entfernen und zu vernichten sind; denn der Betroffene kann im Falle eines Freispruchs wegen eines nicht erwiesenen Dienstvergehens beanspruchen, unmittelbar und nicht erst nach Ablauf einer bestimmten Frist als von einer Disziplinarmaßnahme nicht betroffen angesehen zu werden. Zudem würde eine auch in diesem Fall vorgesehene Tilgungsfrist sein informationelles Selbstbestimmungsrecht verletzen und ihn darüber hinaus unverhältnismäßig belasten. Hiervon unberührt bleibt das Recht des Betroffenen, einer Tilgung zu widersprechen.

### 5.11.5 Gemeinsame Geschäftsordnung

Zu der inzwischen in Kraft getretenen Neufassung der Gemeinsamen Geschäftsordnung für die Ministerien des Landes Nordrhein-Westfalen (GGO) hatte ich der Landesregierung zahlreiche Anregungen und Vorschläge zur Verbesserung des Datenschutzes unterbreitet. Bedauerlicherweise berücksichtigt die GGO meine Anregungen und Vorschläge nicht, die sich im Bereich der Personaldatenverarbeitung im wesentlichen auf folgende Gesichtspunkte bezogen haben:

- Problematik der Weitergabe personenbezogener Daten an das Organisationsreferat (Notwendigkeit einer bereichspezifischen Regelung),
- Einsichtnahme der Gleichstellungsbeauftragten in Personalakten,
- Klarstellung zur Weitergabe von Personaldaten an den Büroleitenden Beamten,
- Notwendigkeit, Schreiben mit vertraulichem Inhalt, insbesondere Schreiben in Personalangelegenheiten, mit einem entsprechenden Hinweis (Personalsache, vertraulich!) zu kennzeichnen,
- Schaffung einer ergänzenden Regelung, wonach bei der Freigabe von Akten für wissenschaftliche Zwecke hierin enthaltene sensible Personal- und Gesundheitsdaten nur mit Einwilligung des Betroffenen übermittelt werden dürfen.

Im übrigen habe ich darauf hingewiesen, daß es sich bei den Bestimmungen über Beteiligungen verschiedener Organisationseinheiten an Einzelmaßnahmen und deren Verpflichtung zu enger Zusammenarbeit nur um Auf-

gabenzuweisungsregelungen handeln kann. Soweit eine Verarbeitung personenbezogener Daten stattfindet, können solche Eingriffe in Persönlichkeitsrechte nur auf gesetzliche Vorschriften gestützt werden (§ 29 DSG NW). Die daraus folgenden Befugnisse zur Verarbeitung personenbezogener Daten von Bewerbern und Beschäftigten können klarstellend in Dienstanweisungen festgelegt werden. Ferner habe ich unter Hinweis auf die Ausführungen in meinem 10. Tätigkeitsbericht (S. 103/104) verdeutlicht, daß die Regelung, wonach die Gleichstellungsbeauftragte hinsichtlich der Akteneinsicht im Rahmen ihrer Mitwirkung bei Personalmaßnahmen Teil der personalverwaltenden Stelle ist, dem geltenden Recht widerspricht, und empfohlen, der Gleichstellungsbeauftragten zur Erfüllung ihrer Aufgaben kein Akteneinsichtsrecht, sondern nur ein Auskunftsrecht einzuräumen.

Das Innenministerium hat meine Anregung, zu den Regelungen über Beteiligungen verschiedener Organisationseinheiten an Einzelmaßnahmen und deren Verpflichtung zu enger Zusammenarbeit ergänzende Bestimmungen vorzusehen, lediglich insoweit aufgegriffen, als es im Entwurf einer Ergänzenden Geschäftsordnung (EGO) zu den jeweils klarstellungsbedürftigen Vorschriften einen gleichlautenden Hinweis darauf gegeben hat, daß bei der Zusammenarbeit mit anderen Stellen des Hauses hinsichtlich der Verarbeitung personenbezogener Daten von Bewerbern und Beschäftigten die datenschutzrechtlichen Bestimmungen, insbesondere § 29 DSG NW, zu beachten sind.

Diese pauschalen Hinweise reichen jedoch nicht aus, um den Mitarbeiterinnen und Mitarbeitern Klarheit darüber zu vermitteln, ob und inwieweit sie im jeweiligen Einzelfall zur Verarbeitung personenbezogener Daten befugt sind oder nicht. Ich habe dem Innenministerium daher empfohlen, die aus der Vorschrift für die Personaldatenverarbeitung (§ 29 DSG NW) folgenden Befugnisse in dem jeweiligen Regelungszusammenhang eindeutig und für alle Betroffenen erkennbar festzulegen. Das Innenministerium will meiner Empfehlung nicht folgen. Es könne nicht Aufgabe der EGO sein, gesetzliche Tatbestände zu kommentieren. Von den Mitarbeitern dürfe erwartet werden, daß sie ohne weitere Klarstellung die gesetzlichen Tatbestände des DSG NW beachten. Dabei übersieht das Innenministerium jedoch, daß meine Empfehlung nicht auf eine Kommentierung gesetzlicher Tatbestände, sondern darauf gerichtet ist, bestimmte, aus § 29 DSG NW folgende Datenverarbeitungsbefugnisse im jeweiligen Regelungszusammenhang der GGO festzulegen.

### 5.11.6 Beurteilungsrichtlinien

Mit Runderlaß vom 25. Mai 1991 hat das Innenministerium Richtlinien für die dienstliche Beurteilung der Beamten seines Geschäftsbereichs (BRL) bekanntgegeben, die am 1. Juni 1992 in Kraft getreten sind. Ich hatte erst nach dessen Veröffentlichung Gelegenheit zur Stellungnahme und habe zu einzelnen Regelungen die folgenden Empfehlungen gegeben:

- Im Zusammenhang mit der Bestimmung über die Erstellung eines Beurteilungsvorschlags (Erstbeurteilung) durch einen Vorgesetzten des zu

beurteilenden Beamten sollte eine Regelung getroffen werden, die sicherstellt, daß der Erstbeurteiler keine Kopie seines Beurteilungsvorschlags zurückbehält, um sich spätere Beurteilungen zu erleichtern und sich dabei nicht in Widerspruch zu seinen früheren Beurteilungen zu setzen. Dementsprechend sollten die Vorschriften über die „Geschäftsmäßige Behandlung der Beurteilungen" (Nr. 12 BRL) dahingehend ergänzt werden, daß die Fertigung von Durchschriften oder Kopien eines Beurteilungsvorschlags unzulässig ist. Dem hat das Innenministerium entgegengehalten, aus der Vorschrift über die Vernichtung von Entwürfen und Notizen nach Aufnahme in die Personalakte (Nr. 12 BRL) folge zwingend auch die Unzulässigkeit der Anfertigung von Durchschriften oder Kopien eines Beurteilungsvorschlags, da anders dem Sinn dieser Bestimmung zuwidergehandelt würde. Etwa dennoch bestehende Zweifel könnten ggf. durch gesonderten Erlaß ausgeräumt werden.

Dies befriedigt im Hinblick auf den eindeutigen Wortlaut der genannten Vorschrift nicht. Gerade weil der Beurteilungsvorschlag hierin nicht erwähnt ist, kann dies bei dem Erstbeurteiler zu der Fehlinterpretation führen, er könne ein Zweitexemplar seines Beurteilungsvorschlags zurückbehalten. Die Gefahr einer derartigen Fehlinterpretation besteht nach meiner Auffassung insbesondere, wenn der Erstbeurteiler zur Führung von Personalnebenakten befugt ist.

- Die die Schlußzeichnung (Endbeurteilung) regelnde Vorschrift, nach der der Schlußzeichnende zur Beratung weitere personen- und sachkundige Bedienstete im Rahmen einer Beurteilerbesprechung heranzieht, sollte durch die Klarstellung ergänzt werden, daß der Teilnehmerkreis der Beurteilerbesprechung auf die Leitungsebene der Behörde beschränkt bleibt. Dies hat das Innenministerium ebenfalls als nicht erforderlich erachtet und mitgeteilt, daß das Beurteilergremium beim Innenministerium vom Staatssekretär, den Abteilungsleitern und der Gleichstellungsbeauftragten gebildet werde. Entsprechendes gelte für andere Behörden des Geschäftsbereichs. Die Befugnis der Gleichstellungsbeauftragten als einer Beauftragten des Arbeitgebers, in Personalangelegenheiten mitzuwirken und Einsicht in Personalakten zu nehmen, werde anläßlich der gesetzlichen Neuregelung des Personalaktenrechts durch eine besondere Vorschrift klargestellt.

  Hierzu habe ich darauf hingewiesen, daß eine Bekanntgabe von Beurteilungsdaten an die Gleichstellungsbeauftragte datenschutzrechtlich nur dann zulässig ist, wenn der Betroffene einer normenklaren gesetzlichen Regelung entnehmen kann, daß seine Beurteilungsdaten vor Schlußzeichnung durch den Leiter der Behörde oder dessen Vertreter auch an die Gleichstellungsbeauftragte weitergegeben werden.

- Zur Wahrung des Löschungsanspruchs der Beamtin oder des Beamten (§ 19 Abs. 3 DSG NW) erscheint eine ergänzende Regelung geboten, wonach die durch eine Gegenäußerung erfolgreich angegriffene Beurteilung wie auch die Gegenäußerung selbst zu löschen sind, es sei denn, die

Beamtin oder der Beamte wünscht deren Aufbewahrung in der Personalakte. Das Innenministerium beabsichtigt eine solche Regelung nicht, stimmt mir aber in der Sache zu.

- Für das Gespräch der Schwerbehindertenvertretung mit dem Erstbeurteiler sollte zur Wahrung schutzwürdiger Belange des Betroffenen dessen Einwilligung eingeholt werden. Das Innenministerium hat hierzu unter Hinweis auf die insoweit mit den BRL inhaltlich übereinstimmenden Richtlinien zur Durchführung des Schwerbehindertengesetzes im öffentlichen Dienst im Lande Nordrhein-Westfalen erklärt, die berechtigten Belange des betroffenen Bediensteten erschienen ausreichend geschützt, wenn die Schwerbehindertenvertretung im Falle seines ausdrücklichen Widerspruchs von der Wahrnehmung seiner Interessen Abstand nehme.

  Die vorgesehene Regelung läßt sich jedoch nicht auf die Vorschriften des Schwerbehindertengesetzes (SchwbG) stützen. Insbesondere die Unterrichtungspflicht des Arbeitgebers gegenüber der Schwerbehindertenvertretung (§ 25 Abs. 2 SchwbG) rechtfertigt nicht einen Informationsaustausch zwischen Schwerbehindertenvertretung und Erstbeurteiler unter Mißachtung des informationellen Selbstbestimmungsrechts des Betroffenen. Voraussetzung für die Rechtmäßigkeit eines derartigen Datenaustauschs ist eine vorherige ausdrückliche Willensbekundung durch den Betroffenen. Als eine solche kann nach dem für die Verarbeitung personenbezogener Daten geltenden Verbot mit Erlaubnisvorbehalt nur die Einwilligung in Betracht kommen; die Widerspruchslösung scheidet aus.

### 5.11.7 Automatisiertes Verfahren für die Stellenverwaltung

Zu dem von einer interministeriellen Arbeitsgruppe erarbeiteten Konzept für ein automatisiertes Verfahren für die Stellenverwaltung in der Landesverwaltung hat das Finanzministerium meine Stellungnahme erbeten.

Das geplante ressortübergreifende Verfahren soll strukturelle Mängel des derzeitigen Verfahrens der Bewirtschaftung von Planstellen und Stellen beseitigen. Angestrebt wird hierbei nicht lediglich eine automationsunterstützte Bewirtschaftung von Planstellen und Stellen, sondern ein System, in dem zusätzlich die Personalverwaltung und die Zahlbarmachung der Bezüge integriert abgewickelt werden. Als Zielsetzung ist vorgegeben, ein Programmsystem zu entwickeln, das Maßnahmen der Stellenverwaltung vereinfacht, eine beschleunigte Bearbeitung ermöglicht sowie eine bessere Qualität der Arbeitsergebnisse gewährleistet. Das System soll in allen Geschäftsbereichen der Landesverwaltung einsetzbar sein und gleichartige Arbeitsergebnisse liefern. Die Berücksichtigung ressortspezifischer Besonderheiten soll ermöglicht und der Änderungsdienst für das ADV-Verfahren „Zahlbarmachung der Bezüge" integriert werden; zudem sollen regelmäßige, gleichartige Datenauswertungen bereitgestellt, Auswertungen im Rahmen der Dienst- und Fachaufsicht vorgesehen sowie wahlfreie Datenauswertungen in anonymisierter Form ermöglicht werden. Für den Datenkatalog, bestehend aus personen- und

stellenbezogenen Daten, sowie den Funktionskatalog, der personen- und stellenbezogene Vorgänge beinhaltet, wird ein Mindestumfang festgelegt, den die Umsetzung der Vorschriften zur Stellenverwaltung erfordert. Diese Datenbasis für die vorgesehenen Informationssysteme kann um – nicht näher erläuterte – Informationen vergrößert werden, um ressortspezifischen Besonderheiten Rechnung zu tragen.

Mit Stellendateien und -informationssystemen habe ich mich zuletzt in meinem 9. Tätigkeitsbericht (S. 73 bis 77) befaßt und auf das von der automatisierten Datenverarbeitung ausgehende Gefahrenpotential hingewiesen, das bei der Prüfung der Zulässigkeit der Datenverarbeitung in diesen Fällen besonders strenge Maßstäbe erfordert. Im Hinblick auf das automatisierte Verfahren für die Stellenverwaltung in der Landesverwaltung habe ich ebenso wie bereits die interministerielle Arbeitsgruppe darauf hingewiesen, daß das Vorhaben nur auf der Grundlage einer – bis jetzt nicht vorhandenen – bereichspezifischen Rechtsvorschrift zu verwirklichen wäre. In diesem Zusammenhang verweise ich auch auf die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. März 1992 zum Arbeitnehmerdatenschutz (s. Anlage 6, S. 165 bis 167 zu 5.11.1).

Ungeachtet noch ausstehender gesetzlicher Regelungen wie auch einer entsprechenden Rechtsverordnung zu § 9 Abs. 2 DSG NW habe ich zu dem automatisierten Verfahren für die Stellenverwaltung in der Landesverwaltung umfangreiche Hinweise zu den organisatorischen und technischen Fragen des Datenschutzes gegeben und im übrigen auf die mit diesem Verfahren einhergehende Gefahr der Entstehung von Persönlichkeitsprofilen hingewiesen, die zu einer unverhältnismäßigen Belastung der Beschäftigten führen könnten.

### 5.11.8 Mitarbeiterbefragung

Durch eine Eingabe wurde ich auf eine in einer Landesbehörde durchgeführte Mitarbeiterbefragung aufmerksam, für die eine vom Behördenleiter eingerichtete Arbeitsgruppe einen Fragebogen entwickelt hatte mit dem Auftrag, Anregungen, Vorschläge und Gedanken zum Thema „Führung und Behördenkultur" zusammenzutragen. Eine andere Landesbehörde, die mit einer ähnlichen Befragung ein „Leitbild der Behörde" erarbeiten wollte, hat hierzu, nachdem interne Bedenken gegen die Rechtmäßigkeit der Datenerhebung laut geworden waren, meine Stellungnahme erbeten.

In den Fragebogen wurden zwar überwiegend nicht tatsächliche Angaben, sondern Meinungen (weitgehend über Dritte) und Informationen über subjektive Einstellungen erbeten. Es handelte sich dabei aber um personenbezogene Daten, weil auch Angaben zu inneren Zuständen wie z. B. Einstellungen, Wünschen und Meinungen Einzelangaben über persönliche Verhältnisse natürlicher Personen sind. Zudem konnten die erhobenen Angaben – jedenfalls auf Grund der die Antworten ergänzenden Gründe, Beispiele oder Bemerkungen in Verbindung mit dem bei der Arbeitsgruppe vorhandenen Zusatzwissen – zu einer Identifizierung der Betroffenen führen, waren also bestimmbar, so

daß bei den Mitarbeiterbefragungen – ungeachtet der Formulierung im Fragebogenanschreiben einer der Behörden, die Fragebogen würden „anonym gehalten", – personenbezogene Daten erhoben wurden (§ 3 Abs. 1 DSG NW).

Die mit beiden Mitarbeiterbefragungen verfolgten Ziele sind keinem der die Verarbeitung von Personaldaten rechtfertigenden Zwecke (§ 29 Abs. 1 Satz 1 DSG NW) konkret zuzuordnen, geschweige denn dafür erforderlich. Da auch sonstige gesetzliche Vorschriften, die die Befragung gestatten könnten, nicht ersichtlich sind, wären die Befragungen allenfalls auf freiwilliger Grundlage in Betracht zu ziehen gewesen. Indessen bestehen erhebliche Zweifel, ob solche Befragungen als freiwillig angesehen werden könnten. Diesbezügliche Bedenken gründen sich vor allem darauf, daß in einem Fall den Betroffenen vorher fälschlich Anonymität zugesichert worden war, und in beiden Fällen die Betroffenen weder ausdrücklich auf die Freiwilligkeit hingewiesen noch darüber aufgeklärt worden sind, daß es sich faktisch um eine personenbezogene Erhebung handelt und was im einzelnen mit ihren Daten geschieht, so daß sie möglicherweise die Tragweite ihrer Entscheidung, an der Befragung teilzunehmen, gar nicht überblickt haben. Auf jeden Fall wurde die Befragung aber insoweit nicht auf freiwilliger Grundlage durchgeführt, als dabei weitgehend Daten (Werturteile) über Dritte (Vorgesetzte) erhoben wurden, deren Einwilligung hierzu nicht eingeholt worden ist, allerdings rechtswirksam auch nicht hätte eingeholt werden können. Denn eine solche Einwilligung wäre unter den gegebenen Umständen nicht als freiwillig anzusehen, weil sich die Betroffenen (Vorgesetzten) unter Druck gesetzt fühlen könnten und damit in ihrer Entscheidung nicht frei wären. Deshalb dürfen auch im Rahmen einer freiwilligen Befragung Angaben, die das Verhältnis oder die Einstellung der Befragten zu Dritten betreffen, generell nicht erhoben werden.

Da sich in den bereits ausgefüllten Fragebogen die Antworten zu den unzulässigen Fragen nach Einstellungen zu Dritten nicht von den übrigen Antworten trennen ließen, habe ich beiden Behördenleitern empfohlen, die bereits ausgefüllten Fragebogen umgehend zu vernichten. Außerdem habe ich empfohlen, künftig bei personenbezogenen Erhebungen von Beschäftigtendaten die Befragten hierüber sowie über den Verwendungszweck in der Weise konkret aufzuklären, daß sie überblicken können, was im einzelnen mit ihren Daten geschieht und wer davon Kenntnis erlangt, sowie auf die Freiwilligkeit der Teilnahme ausdrücklich hinzuweisen; zudem dürfen keine Angaben erfragt werden, die das Verhältnis der Befragten zu Dritten betreffen.

### 5.11.9 Speicherung und Übermittlung von Personaldaten außerhalb der Personalakte

Durch eine Presseveröffentlichung wurde mir bekannt, daß ein Oberstadtdirektor den Deutschen Bühnenverein e. V., der in Theater- und Orchesterangelegenheiten im öffentlichen und privaten Bereich beratend tätig ist, gebeten hatte, von einer neuangestellten leitenden Mitarbeiterin entwickelte konzeptionelle Vorstellungen zu ihrem Aufgabenbereich zu begutachten. Hierzu sind dem Deutschen Bühnenverein auf Anforderung Fotokopien des Bewerbungsschreibens nebst Lebenslauf und des Arbeitsvertrages durch

den Fachvorgesetzten der Betroffenen übersandt worden. Diesem waren die Bewerbungsunterlagen im vorangegangenen Bewerbungsverfahren vom Personalamt für das Bewerbungsgespräch mit der Maßgabe zur Verfügung gestellt worden, sie mit dem Personalvorschlag wieder zurückzureichen. Vor der Rücksendung der Bewerbungsunterlagen hat der Fachvorgesetzte Ablichtungen hiervon gefertigt mit der Begründung, er benötige sie u. a. für seine Empfehlung gegenüber einem Kommunalausschuß sowie für die Beurteilung der Betroffenen und der von ihr vorgelegten konzeptionellen Vorstellungen.

Daten von Bewerbern und Beschäftigten dürfen innerhalb der Verwaltung der Stadt u. a. verarbeitet werden, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses erforderlich ist (§ 29 Abs. 1 Satz 1 i.V.m. § 14 Abs. 5 DSG NW). Diese Voraussetzungen sind nach meiner Auffassung erfüllt, soweit die genannten Personalunterlagen der Betroffenen vom Personalamt an den Fachvorgesetzten zwecks Führung des Bewerbungsgesprächs und Abgabe des Personalvorschlages weitergegeben worden sind. Hingegen ist die Anfertigung von Fotokopien dieser Unterlagen durch den Fachvorgesetzten der Betroffenen und die mit dem Rückgabeverlangen des Personalamts nicht zu vereinbarende Aufbewahrung der Fotokopien schon deshalb nicht zulässig, weil die fraglichen Bewerbungsunterlagen zur Personalakte zu nehmen sind und Personalnebenakten grundsätzlich nicht geführt werden dürfen (vgl. 10. Tätigkeitsbericht, S. 98).

Die Übermittlung der genannten Personalunterlagen an den Deutschen Bühnenverein als eine nicht-öffentliche Stelle ist nur zulässig, wenn der Empfänger ein rechtliches Interesse darlegt, der Dienstverkehr es erfordert oder der Betroffene eingewilligt hat (§ 29 Abs. 1 Satz 2 DSG NW). Ein rechtliches Interesse des Empfängers lag offensichtlich nicht vor, ebensowenig die Einwilligung der Betroffenen. Auch der Dienstverkehr erforderte es nicht, dem Deutschen Bühnenverein dem Personalaktengeheimnis unterliegende Vorgänge zur Verfügung zu stellen. Unter „Dienstverkehr" sind Datenübermittlungen zu verstehen, die die öffentliche Verwaltung für den Bürger transparent machen (z. B. Bekanntgabe von Dienst- und Funktionsbezeichnung der Mitarbeiter; Dienstausweise; Herausgabe von Telefonverzeichnissen).

Ich habe dem Oberstadtdirektor empfohlen, die von dem Fachvorgesetzten gefertigten Kopien der Bewerbungsunterlagen der Betroffenen zurückzufordern und zu vernichten, ggf. durch eine entsprechende Dienstanweisung dafür Sorge zu tragen, daß in vergleichbaren Fällen der Fachbereich keine Fotokopien von Bewerbungsunterlagen fertigt und zurückbehält, sowie künftig dem Deutschen Bühnenverein von diesem angeforderte Personaldaten nur mit schriftlicher Einwilligung der Betroffenen zu übermitteln.

### 5.11.10 Verwendung von Fehlzeiten für dienstliche Beurteilungen

Für die Bediensteten einer Justizvollzugsanstalt werden Arbeitszeitkarten geführt, in die alle Dienst- und Ausfallzeiten eingetragen werden. Im Zusammenhang mit anstehenden Beurteilungen der Bediensteten, die im Hinblick

auf die Besetzung zahlreicher Beförderungsstellen notwendig wurden, sind die Fehlzeiten von Bediensteten des allgemeinen Vollzugsdienstes der letzten vier Jahre aus den Arbeitszeitkarten auf Veranlassung der Anstaltsleitung ermittelt und aufgelistet worden. Nach Gesprächen mit den Betroffenen über die Ursachen von Erkrankungen sollten diese Erkenntnisse in das Beurteilungsmerkmal „körperliches Leistungsvermögen" einfließen.

Daten von Beschäftigten dürfen verarbeitet werden, wenn dies zur Durchführung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist (§ 29 Abs. 1 Satz 1 DSG NW). Diese Voraussetzungen lagen hinsichtlich der Speicherung der Fehlzeiten in den Arbeitszeitkarten vor, denn die Leitung des allgemeinen Vollzugsdienstes muß für ihre Koordinations- und Kontrollaufgaben bezüglich der Dienstplangestaltung Kenntnis von der Abwesenheit der Justizvollzugsbediensteten haben und die Tatsache der Abwesenheit auch festhalten. Darüber hinaus gilt die Arbeitszeitkarte als Beleg für besoldungs- und vergütungsrelevante Umstände (s. RdVfg. des Justizministeriums vom 3. Dezember 1975 – 1414 – IV B.1).

Soweit sich bei der zu diesen Zwecken vorgenommenen Auswertung einer Arbeitszeitkarte Auffälligkeiten (z. B. häufige Abwesenheit wegen Krankheit) ergeben, ist es selbstverständlich zulässig, hierüber im Einzelfall mit dem Betroffenen ein Personalgespräch zu führen. Die Auswertung der Arbeitszeitkarten erfolgte nach meinen Erkenntnissen im vorliegenden Fall jedoch, um Bedienstete mit entsprechenden Auffälligkeiten überhaupt erst herauszufinden. Eine derartige „Fahndung" stellt eine unzulässige Ausforschung dar. Darüber hinaus liegt hinsichtlich der Nutzung der Daten für die Vorbereitung von Personalgesprächen im Zusammenhang mit anstehenden dienstlichen Beurteilungen eine gesetzlich nicht gedeckte Zweckänderung vor. Beschäftigtendaten dürfen nur für die gesetzlich bestimmten Zwecke verarbeitet werden (§ 29 Abs. 1 Satz 1 DSG NW). Diese Zweckbindung schließt eine Weiterverarbeitung zur Erfüllung anderer Aufgaben der speichernden Stelle schlechthin aus. Zwar können im Einzelfall für eine dienstliche Beurteilung auch krankheitsbedingte Abwesenheiten des Betroffenen insoweit berücksichtigt werden, als sie sich in seinen dienstlichen Verhältnissen auswirken (vgl. OVG Münster, DÖD 1990, 170). In einem solchen Fall ist der Betroffene jedoch als „auffallend häufig krank" bereits bekannt, so daß auch keine datenschutzrechtlichen Bedenken bestünden, mit ihm ein Personalgespräch hierüber – ggf. zu Beweiszwecken auch unter Auswertung seiner Arbeitszeitkarte – zu führen, soweit dies nicht ohnehin schon zu einem Zeitpunkt geschehen ist, als sich die krankheitsbedingte Abwesenheit noch nicht in seinen dienstlichen Verhältnissen ausgewirkt hatte. Eine derartige einzelfallbezogene Auswertung der Arbeitszeitkarte auf Grund konkreter Anhaltspunkte war jedoch im vorliegenden Fall gerade nicht festzustellen.

Ich habe dem Leiter der Justizvollzugsanstalt empfohlen, dafür Sorge zu tragen, daß die in den Arbeitszeitkarten festgehaltenen Daten nicht für die

Vorbereitung von Personalgesprächen im Zusammenhang mit anstehenden dienstlichen Beurteilungen verwendet werden.

### 5.11.11 Übermittlung personenbezogener Daten durch eine Zeiterfassungsanlage

Förmlich beanstanden mußte ich die Übermittlung personenbezogener Daten der Bediensteten durch eine Zeiterfassungsanlage, auf die ich gelegentlich eines Informations- und Kontrollbesuchs von Bediensteten angesprochen wurde und die im Erdgeschoß eines städtischen Gesundheitsamtes so eingerichtet ist, daß jeder (Bedienstete, Reinigungskräfte, Besucher) an Hand der die Namen der Mitarbeiter am oberen Ende aufweisenden Arbeitszeitkarten erkennen kann, wer im Hause anwesend bzw. abwesend ist.

Sowohl die interne Weitergabe der Beschäftigtendaten, wozu der Name sowie die Tatsache, daß der betreffende Beschäftigte anwesend bzw. abwesend ist, gehört, als auch die Übermittlung dieser Daten an Dritte ist unzulässig, weil zum einen keiner der die Personaldatenverarbeitung rechtfertigenden Zwecke (§ 29 Abs. 1 Satz 1 DSG NW) es erfordert, die Zeiterfassungsanlage so einzurichten, daß die Bediensteten des Gesundheitsamtes untereinander Kenntnis davon erhalten, wer anwesend bzw. abwesend ist, und zum anderen für die Übermittlung der Beschäftigtendaten an Personen außerhalb des öffentlichen Bereichs weder ein rechtliches Interesse der Empfänger dargelegt werden kann, noch der Dienstverkehr die Übermittlung erfordert, und eine Einwilligung der Betroffenen nicht vorliegt (§ 29 Abs. 1 Satz 2 DSG NW).

Der Oberstadtdirektor vertritt demgegenüber die Auffassung, die moderne Verwaltung habe sich mit ihren Dienstleistungen so anzubieten, daß der Besucher Aufgabenwahrnehmung und Aufgabenträger durch entsprechende Wegweiser und Beschriftung eindeutig erkennen könne, weshalb er auch unabhängig von der Zeiterfassungsanlage ohne nennenswerten Aufwand Kenntnis davon erlangen müsse, ob eine seinen Fall bearbeitende Person anwesend ist oder nicht. Durch die Art und Weise des Betriebs der Zeiterfassungsanlage finde keine über das notwendige Maß hinausgehende Datenverarbeitung statt, und schutzwürdige Belange der Mitarbeiter würden nicht derart beeinträchtigt, daß eine Änderung des Verfahrens geboten sei. Im übrigen seien die bereitgehaltenen Daten, deren Informationswert gering sei, für den interessierten Übermittlungsempfänger ohne größeren Aufwand auch auf anderem Wege zu erlangen. Die Zeiterfassungsanlage sei vor vielen Jahren mit Zustimmung der Personalvertretung eingeführt worden. Bisher hätten die Betroffenen keine Einwände erhoben. Anlagen dieser Betriebsart und -form seien in Betrieben und Verwaltungen mit gleitender Arbeitszeit durchaus üblich und akzeptiert.

Diese Einwände sind nicht stichhaltig. Die Zeiterfassungsanlage hat den erklärten Zweck, die Arbeitszeit der Beschäftigten zu erfassen. Sie hat nach ihrer Zweckbestimmung aber nicht die Funktion einer Dienstleistung für Besucher, für die im übrigen gar nicht erkennbar ist, daß die Arbeitszeitkarten

der Zeiterfassungsanlage als „Wegweiser und Beschriftung" in dem vom Oberstadtdirektor angesprochenen Sinne gedacht sind. Soweit der Oberstadtdirektor versucht, der Zeiterfassungsanlage eine solche Funktion zuzuordnen, ist dies schon deshalb ein untaugliches Mittel, weil der Besucher damit allenfalls erkennen könnte, daß der gewünschte Bedienstete abwesend ist; er könnte aber nicht feststellen, daß dieser Bedienstete, wenn er als im Hause anwesend erscheint, damit auch für den Besucher an seinem Arbeitsplatz erreichbar ist. Zudem ist für ihn nicht erkennbar, wie lange (ob nur kurzzeitig oder längerfristig) der Bedienstete abwesend ist, so daß er in jedem Fall auf zusätzliche anderweitige Auskünfte über die Dauer der Abwesenheit und etwaige Vertretungsregelungen angewiesen ist.

Für die Beurteilung der Zulässigkeit der Datenverarbeitung ist im übrigen unerheblich, ob sich der Übermittlungsempfänger die Daten auch auf anderem Wege beschaffen kann; ebensowenig darf auf den vermeintlich geringen Informationswert der Daten und demzufolge auf eine Nichtbeeinträchtigung schutzwürdiger Belange der Betroffenen abgehoben werden. Das Datenschutzrecht kennt keine belanglosen Daten, und die vom Gesetzgeber getroffene Regelung für den Umgang mit Personaldaten (§ 29 DSG NW) verbietet es der hieran gebundenen öffentlichen Verwaltung, diesen Regelungsgehalt durch Einführung des Tatbestandsmerkmals „schutzwürdige Belange" zu relativieren. Auch die Zustimmung des Personalrats ist nicht geeignet, Datenschutzverstöße zu sanktionieren, die im übrigen unabhängig davon vorliegen, ob Bedienstete Einwendungen erheben. Zudem bin ich anläßlich meines Informations- und Kontrollbesuchs von Bediensteten auf die Zeiterfassungsanlage aufmerksam gemacht worden. Daß Anlagen dieser Betriebsart und -form in Verwaltungen durchaus üblich seien, widerspricht meinen bisherigen Erkenntnissen, wäre aber zutreffendenfalls kein Rechtfertigungsgrund für die Beibehaltung derartiger Anlagen, müßte vielmehr zu deren unverzüglicher Umrüstung führen. Diese wäre durch eine nur geringfügige organisatorische Änderung zu erreichen, indem die an der Zeiterfassungsanlage angebrachten Namen der Bediensteten, etwa durch Kennummern, verschlüsselt werden. Der Oberstadtdirektor wird meinem entsprechenden Vorschlag gleichwohl unter Hinweis auf einen nicht näher erläuterten Mehraufwand nicht folgen und beabsichtigt, die Zeiterfassungsanlage in der bestehenden Form weiterzubetreiben.

### 5.11.12 Weitergabe von Personaldaten an die Gleichstellungsbeauftragte

Ein Stadtdirektor hat mich um Auskunft zu Fragen der Weitergabe personenbezogener Daten von der Personalabteilung an die von der Stadt bestellte Gleichstellungsbeauftragte und zur Zulässigkeit ihrer Teilnahme an Sitzungen des Personalausschusses gebeten. In einem vom Rat beschlossenen Aufgabenkatalog sind ihr u. a. folgende Tätigkeiten zugewiesen:

- Überwachung geschlechtsneutraler Stellenausschreibungen in der Verwaltung,

- Mitwirkung bei Bewerbungsfragen und Stellenbesetzungen innerhalb der Verwaltung,
- Unterstützung von Beschäftigten der Verwaltung bei der Wahrnehmung ihrer Interessen in Gleichstellungsfragen in Zusammenarbeit mit dem Personalrat.

Was die Weitergabe personenbezogener Daten von Beschäftigten an die Gleichstellungsbeauftragte anbelangt, so ist zunächst davon auszugehen, daß der Gleichstellungsbeauftragten, wenn ihre Funktion nicht leerlaufen soll, ein Mitwirkungsrecht bei der Durchführung von Personalmaßnahmen zustehen kann. Dieses Mitwirkungsrecht korreliert mit einer Verpflichtung der personalverwaltenden Stelle, die Gleichstellungsbeauftragte mitwirken zu lassen und ihr die dafür erforderlichen Personaldaten zur Verfügung zu stellen. Dabei sind allerdings an die Erforderlichkeit strenge Anforderungen zu stellen. Es genügt nicht, daß die Daten für die Aufgabenerfüllung nur dienlich oder nützlich sind, sie müssen vielmehr zur Aufgabenerfüllung unerläßlich sein. In diesem engen Umfang ist die Weitergabe von Personaldaten an die Gleichstellungsbeauftragte auch als Aufgabenerfüllung der personalverwaltenden Stelle bei der Durchführung personeller Maßnahmen anzusehen und damit von der die Personaldatenverarbeitung regelnden Vorschrift (§ 29 Abs. 1 Satz 1 DSG NW) gedeckt.

Zur Frage des Teilnahmerechts der Gleichstellungsbeauftragten an Sitzungen des Personalausschusses teile ich die Auffassung des Nordrhein-Westfälischen Städte- und Gemeindebundes. Hiernach obliegt dem Gemeindedirektor im Rahmen seines Organisationsrechts die Entscheidung, welche Dienstkräfte an den Sitzungen des Rates und der Ausschüsse teilnehmen. Dabei ist jedoch zu berücksichtigen, daß die Gleichstellungsbeauftragte nicht als eine mit der Bearbeitung von Personalangelegenheiten beauftragte Bedienstete anzusehen ist. Weder aus ihrer Funktion noch aus dem Aufgabenkatalog von Gleichstellungsstellen folgt zwingend, daß die Gleichstellungsbeauftragte oder Gleichstellungsstellen mit der Bearbeitung von Personalangelegenheiten beauftragt sind. Die bloße Mitwirkung an Personalmaßnahmen stellt noch keine Bearbeitung von Personalangelegenheiten dar. Der Schutz personenbezogener Daten betroffener Bediensteter erfordert es daher, daß die Gleichstellungsbeauftragte an nicht-öffentlichen Sitzungen des Personalausschusses grundsätzlich nur dann teilnehmen darf, wenn ihr die Personaldaten im Wege der Auskunft hätten bekanntgegeben werden dürfen.

Im übrigen kann der vom Rat beschlossene Aufgabenkatalog nicht dazu führen, an die Gleichstellungsbeauftragte mehr personenbezogene Daten zu übermitteln, als ihr gemessen an den gesetzlich normierten Aufgaben zustehen. Eine Erweiterung des Aufgabenkatalogs der Gleichstellungsbeauftragten durch Ratsbeschluß kann keine zusätzlichen Eingriffe in das informationelle Selbstbestimmungsrecht der Betroffenen rechtfertigen.

### 5.11.13 Informationsrechte des Personalrats über das Vorliegen einer Schwangerschaft

Wie mir bekanntgeworden ist, besteht vielfach Unklarheit darüber, ob dem Personalrat das Vorliegen einer Schwangerschaft ohne Einwilligung der Betroffenen mitgeteilt werden darf.

Die Weitergabe personenbezogener Daten von Bediensteten an den Personalrat ist immer dann problematisch, wenn sie außerhalb der im Landespersonalvertretungsgesetz (LPVG) förmlich geregelten Beteiligungsverfahren erfolgt. Das informationelle Selbstbestimmungsrecht weiblicher Bediensteter wird insbesondere beeinträchtigt, wenn Personalverwaltungen dem Verlangen des Personalrats nachkommen, Schwangerschaften von Arbeitnehmerinnen auch ohne deren Einwilligung laufend mitzuteilen. Begründet wird dieses Verlangen zuweilen damit, der Personalrat benötige diese Informationen zur Erfüllung der ihm obliegenden allgemeinen Aufgaben (§ 64 LPVG). Aus der bloßen Zuweisung allgemeiner Aufgaben an den Personalrat folgt indes nicht schon die Befugnis und erst recht nicht die Verpflichtung der Dienststellen, sensible personenbezogene Daten von Beschäftigten an diesen vorbei und ohne ihr Einverständnis an den Personalrat weiterzugeben. Hierzu bedarf es vielmehr einer im Verhältnis zu den Betroffenen normenklaren Befugnisregelung, die den Vorschriften des Landespersonalvertretungsgesetzes jedoch nicht entnommen werden kann. Dies gilt insbesondere auch im Hinblick auf die Regelung, wonach der Personalrat auf die Verhütung von Unfall- und Gesundheitsgefahren zu achten hat (§ 64 Abs. 1 Nr. 4 LPVG). Hierbei handelt es sich lediglich um eine allgemeine Aufgabenzuweisungsnorm, die als solche Eingriffe in das informationelle Selbstbestimmungsrecht nicht gestattet. Für die Bekanntgabe des Vorliegens einer Schwangerschaft an den Personalrat ohne Einwilligung der Betroffenen fehlt es an einer entsprechenden Befugnisnorm.

## 5.12 Statistik

### 5.12.1 Kinder- und Jugendhilfestatistik

Die Bestimmungen des Kinder- und Jugendhilfegesetzes (KJHG) zur Durchführung einer Kinder- und Jugendhilfestatistik haben bei verschiedenen Trägern der freien Jugendhilfe zu Unklarheiten darüber geführt, ob ihre Mitarbeiterinnen und Mitarbeiter bei der Ausfüllung der vom Landesamt für Datenverarbeitung und Statistik (LDS) verwendeten Erhebungsvordrucke nicht in Konflikt mit ihrer beruflichen Schweigepflicht geraten. Als bedenklich wurde eingewandt, daß sich die bereits bei Beratungsbeginn vorgesehene Ausfüllung des Erhebungsbogens ungünstig auf das anzubahnende Vertrauensverhältnis zwischen Berater und zu Beratendem auswirke und daß der Träger durch die ausgefüllten Erhebungsvordrucke einen Überblick über die Tätigkeit des Beraters erhalte.

Die Vorschriften des KJHG für die Kinder- und Jugendhilfestatistik stellen eine bereichspezifische normenklare Rechtsgrundlage für diese Erhebung dar. Auch bei Erfüllung der Auskunftspflicht des Trägers der freien Jugendhilfe

bleibt die Schweigepflicht der einzelnen Berater (§ 203 Abs. 1 Nr. 4 StGB) letztlich unangetastet. Diese Personen machen sich nur dann eines Verstoßes gegen die Schweigepflicht schuldig, wenn sie unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis offenbaren, das ihnen in ihrer speziellen Funktion anvertraut oder sonst bekanntgeworden ist. Die Erfüllung der statistischen Auskunftspflicht (§ 102 Abs. 2 Nr. 6 KJHG) stellt hingegen nicht bereits die Offenbarung eines fremden Geheimnisses an einen anderen dar. Die einschlägigen Erhebungsvordrucke des LDS enthalten keine Fragen, die dieser Behörde einen Rückschluß auf die Befragten ermöglichen und diese damit identifizieren könnten. Das LDS verfügt auch nicht über Zusatzwissen, mit dessen Hilfe ein entsprechender Personenbezug hergestellt werden könnte. Da die Daten über die Beratung somit anonymisiert erfaßt und verarbeitet werden, ist die Offenbarung eines fremden Geheimnisses an einen anderen ausgeschlossen. Ob sich die Ausfüllung des Erhebungsvordrucks bei Beginn der Beratung in der geschilderten Weise auswirkt, vermag ich nicht zu beurteilen. Jedenfalls werden datenschutzrechtliche Belange in diesem Fall nicht berührt, weil die Schweigepflicht des Beraters und das Statistikgeheimnis gewahrt sind. Soweit im übrigen der Träger der freien Jugendhilfe durch die Vordrucke einen Überblick über die Tätigkeit des Beraters erhält, ist dies zwangsläufige Nebenfolge der gesetzlichen Auskunftspflicht des Trägers.

### 5.12.2 Einsatz von computergestützten Erhebungsinstrumenten im Rahmen des Mikrozensus

Das Landesamt für Datenverarbeitung und Statistik erwägt im Zuge der Weiterentwicklung von Methoden der amtlichen Statistik und der Sozialforschung, bei künftigen Erhebungen nach dem Mikrozensusgesetz (MZG) tragbare Computer (Laptops) als zusätzliche Erhebungsinstrumente einzusetzen. Den zu Befragenden soll allerdings weiterhin die Wahlmöglichkeit eingeräumt werden, die Fragen mündlich gegenüber dem Interviewer oder schriftlich zu beantworten.

Bei allen Vorteilen, die der Laptop-Einsatz zur Durchführung der Erhebungen, insbesondere hinsichtlich der Zeitersparnis bieten kann, halte ich ein solches Verfahren unter dem Gesichtspunkt des Datenschutzes für problematisch. Der Gesetzgeber hat zur Erhebung von Daten im Rahmen des Mikrozensus bestimmte, fest umrissene Erhebungsmöglichkeiten vorgesehen, die in jedem Fall voraussetzen, daß als Erhebungsmittel Erhebungsvordrucke eingesetzt werden (§ 10 MZG). Nach dem eindeutigen Wortlaut des Gesetzes müssen andersartige, im konkreten Fall also auch computergestützte Erhebungsinstrumente an Stelle von Erhebungsvordrucken als ausgeschlossen angesehen werden. Da diese normenklare Regelung anläßlich der letzten Novellierung des Gesetzes unverändert geblieben ist, kann hieraus nach meiner Auffassung, die auch von anderen Landesbeauftragten für den Datenschutz geteilt wird, nur gefolgert werden, daß der Gesetzgeber andere, insbesondere technische Erhebungsmittel derzeit offenbar nicht hat zulassen wollen, zumal

diese mit besonderen Risiken verbunden sind. Ich muß daher angesichts des klaren Gesetzeswortlauts eine Befragung im Rahmen des Mikrozensus nach gegenwärtiger Rechtslage als datenschutzrechtlich bedenklich erachten, soweit diese mit computergestützten Erhebungsinstrumenten (Laptops) erfolgen soll.

## 5.13 Wissenschaft und Forschung

### 5.13.1 Aktionsprogramm „Qualität der Lehre"

Presseberichte über das Aktionsprogramm „Qualität der Lehre" haben mich veranlaßt, die datenschutzrechtlichen Auswirkungen dieses Programmes zu prüfen. Zu diesem Zeitpunkt hatte das Ministerium für Wissenschaft und Forschung des Landes Nordrhein-Westfalen (MWF) bereits mit Erlassen an die wissenschaftlichen Hochschulen und Fachhochschulen Einzelheiten zur Durchführung dieses Programmes geregelt und hierzu einen **Fragebogen** entworfen. Offensichtlich sollten neue Wege im Hochschulmanagement beschritten werden, die aber auch nachhaltige datenschutzrechtliche Auswirkungen mit sich bringen würden. Erlaß und Fragebogen sehen vor, daß im Rahmen des Aktionsprogrammes „Qualität der Lehre" die Studierenden als Adressaten und Betroffene von Lehre und Prüfungen stärker an der Gestaltung des Studien- und Prüfungsbetriebes beteiligt werden. Im Vordergrund steht eine **Beurteilung der Lehrveranstaltungen** und damit auch der Lehrenden durch die Studierenden. Das MWF hat es dabei als selbstverständlich erachtet, daß alle Lehrveranstaltungen und Lehrenden der studentischen Kritik unterzogen werden.

Nach Beratungen in der gemeinsamen Arbeitsgruppe aus Mitgliedern der wissenschaftlichen Hochschulen und des MWF hat man sich zunächst auf eine zweisemestrige Erprobungsphase in einzelnen Studiengängen geeinigt. Es werden die wesentlichen Vorgaben, wie etwa ein Musterfragebogen, eine zentrale statistische Auswertung der Fragebogen auf Fachbereichs- oder Hochschulebene, insbesondere auch eine Auswertung durch den Fachbereich, eine Darstellung des Gesamtergebnisses der Veranstaltungskritik und der daraus gezogenen Konsequenzen im „Lehrbericht" des Fachbereichs sowie eine Information der Studierenden gemacht. Der Musterfragebogen, der möglichst auch der Vergleichbarkeit der „Beurteilungsergebnisse" dienen soll, nennt sich Fragebogen für Studierende zur Beurteilung der Qualität der Lehre, bezeichnet die Lehrenden und deren Lehrveranstaltungen und enthält einen Katalog von mit einer Notenskala von „sehr gut" bis „nicht ausreichend" zu bewertenden Leistungsmerkmalen der Lehrenden wie persönliche Präsenz, Engagement, Strukturierung der Veranstaltung, Verständlichkeit, Vortragsstil, Veranschaulichung des Stoffes und Kommunikationsbereitschaft innerhalb und außerhalb der Lehrveranstaltung. Nach Auffassung des MWF sind alle Lehrenden verpflichtet, sich zur Erreichung des angestrebten Zieles einer Verbesserung der Qualität der Lehre dieser Veranstaltungskritik zu stellen und deren Auswertung durch den Fachbereich im „Lehrbericht"

auch unter Berücksichtigung ihres informationellen Selbstbestimmungsrechts hinzunehmen.

Mit dem Musterfragebogen werden personenbezogene Daten über Professoren und Hochschuldozenten verarbeitet. Die Hochschule läßt diese Daten durch die Teilnehmer der Lehrveranstaltungen erheben, die zwar selbst nicht namentlich bezeichnet werden, aber zumindest in kleinen Lehrveranstaltungen bestimmbar sind. Diese Datenerhebung ist in erster Linie als Eingriff in das Recht auf informationelle Selbstbestimmung der Lehrenden zu werten, der nur zulässig wäre, wenn die Betroffenen in die Datenerhebung eingewilligt hätten oder der Eingriff in einer normenklaren gesetzlichen Regelung vorgesehen wäre. Die gesetzliche Grundlage muß für die Betroffenen klar erkennen lassen, in welchem Umfang und zu welchem Zweck Daten über sie zur Beurteilung der Qualität ihrer Lehre erhoben und ggf. weiterverarbeitet werden dürfen.

Eine solche Regelung liegt ersichtlich nicht vor. § 29 Abs. 1 DSG NW kommt als Ermächtigungsgrundlage nicht in Betracht, weil die Datenerhebung und die vorgesehene Auswertung der Daten nicht durch die personalverwaltende Stelle, d. h. durch das Rektorat der Universität, sondern durch den Fachbereich erfolgen soll.

Dem Gesetz über die wissenschaftlichen Hochschulen des Landes Nordrhein-Westfalen kann eine solche normenklare Regelung nicht entnommen werden. Auch der von der Landesregierung vorgelegte Entwurf eines Gesetzes zur Änderung hochschulrechtlicher Vorschriften, der nach seiner Begründung vor allem auch die erforderlichen Änderungen zur Umsetzung des Aktionsprogramms „Qualität der Lehre" vorsehen soll, enthält keine Vorschrift, aus der die Lehrenden entnehmen können, daß sie verpflichtet sind, sich einer studentischen Veranstaltungskritik und einer daraus resultierenden personenbezogenen Leistungsbewertung zu stellen.

Obwohl das Innenministerium meine Bedenken gegen die Anwendung von § 29 Abs. 1 DSG NW teilt, hält das MWF an seiner Auffassung fest, auf Grund der bestehenden Rechtslage, zumindest bei entsprechenden auf die Bestimmungen der Hochschulgesetze gestützten Beschlüssen der zuständigen Gremien, könne eine die Lehrenden verpflichtende studentische Veranstaltungskritik stattfinden. Es hat aber die Frage der Ermächtigungsnorm offen gelassen und mitgeteilt, daß die jetzt erfolgte Befragung der Studierenden nur bei freiwilliger Beteiligung der Lehrenden durchgeführt worden ist.

Wenn im beabsichtigten Gesetz zur Änderung hochschulrechtlicher Vorschriften keine bereichspezifische normenklare Regelung getroffen wird, ist weiterhin davon auszugehen, daß eine gesetzliche Grundlage für eine die Lehrenden verpflichtende Teilnahme an derartigen Befragungen fehlt. Das gleiche gilt für die anschließende Auswertung der Fragebogen durch den Fachbereich; auch sie ist nur zulässig, soweit die Betroffenen eingewilligt haben. Eine „Veröffentlichung" personenbezogener Beurteilungen im Lehrbericht ist ebenfalls nur mit Einwilligung der Lehrenden möglich. Einem solchen Verfahren kann im Hinblick auf die unabhängige Stellung und das Selbstverständnis der Lehrenden

an Hochschulen nicht das Bedenken mangelnder Freiwilligkeit bei der Einwilligung entgegengehalten werden.

### 5.13.2 Aushang von Notenlisten in der Hochschule

Die andere Seite der Medaille von „Qualität der Lehre" und veröffentlichter studentischer Veranstaltungskritik ist mir in der Hochschule ebenfalls begegnet und zwar in Form von am **Schwarzen Brett** ausgehängten Listen über die Ergebnisse studentischer Leistungen. So werden etwa Ergebnislisten eines Seminars unter Angabe sowohl der Matrikelnummern als auch der Namenskürzel der Studierenden ausgehängt. Auch das ist datenschutzrechtlich nicht unproblematisch.

Selbst ohne Angabe der Namen sind Matrikelnummer und Namenskürzel personenbezogene Daten, die einer bestimmten Person (Betroffener) zugeordnet werden können. Die betroffene Person ist bestimmbar, wenn ihre Identität in Verbindung mit weiteren, außerhalb der Namensangaben liegenden Informationen bestimmt werden kann (sog. Zusatzwissen). Bereits eine kleinere Gruppe von Seminarteilnehmern, die sich untereinander kennen, oder etwa markante Namenskürzel insbesondere ausländischer Studierender (Anfangsbuchstaben z. B. Q, Y, El) lassen eine Identifizierbarkeit einzelner Studentinnen oder Studenten zu. Daher werden bei öffentlichem Aushang der Ergebnisliste nicht nur den Seminarteilnehmern selbst, sondern auch allen Personen, die Einblick in die Liste nehmen können, Leistungsdaten bekanntgegeben, sobald die Noten mit Zusatzwissen bestimmten Studentinnen oder Studenten zugeordnet werden können.

Eine solche Bekanntgabe an Dritte – sowohl Seminarteilnehmer als auch interessierte Studierende – stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Studentinnen oder Studenten dar. Ein solcher Eingriff ist nur auf Grund einer normenklaren gesetzlichen Regelung zulässig, die weder dem wissenschaftlichen Hochschulgesetz noch dem DSG NW zu entnehmen ist.

## 5.14 Schule und Kultur

### 5.14.1 Schüler- und Elterndaten

Nach wie vor ist eine normenklare gesetzliche Regelung für den Schulbereich dringend notwendig. Immer wieder verweisen Schulleiter auf die Verwaltungsvorschriften zu § 5 Abs. 4 der Allgemeinen Schulordnung (ASchO) – Richtlinien zum Schülerstammblatt – als „Rechtsgrundlage" für eine Verarbeitung personenbezogener, auch äußerst sensibler Daten wie Gesundheitsdaten oder Angaben über geistige und charakterliche Eignung von Schülerinnen und Schülern, ohne daß damit ein Grundrechtseingriff zu rechtfertigen ist. Das zeigt sich an folgenden Fällen:

In einem Fall habe ich mich mit dem Verfahren zur **Rückstellung vom Schulbesuch** befaßt. Nach Durchführung eines Schulreifetests und der Vorlage eines schulärztlichen Gutachtens hatte der Schulleiter einer Grundschule Kinder vom Schulbesuch zurückgestellt. Sie wurden nach Entscheidung

durch das Schulamt in einen Schulkindergarten eingewiesen. Zusätzlich war ein Sonderschulaufnahmeverfahren eingeleitet worden, das dann wieder eingestellt worden war.

Das Verfahren zur Rückstellung vom Schulbesuch und zur Einweisung in den Schulkindergarten wird nach § 4 Abs. 2 und § 5 Abs. 1 der Verordnung über den Bildungsgang in der Grundschule (Ausbildungsordnung gemäß § 26 b SchVG) durchgeführt. Gegen die Durchführung des Schulreifetests und der schulärztlichen Untersuchung sowie gegen die Einweisung in den Schulkindergarten bestehen aus datenschutzrechtlicher Sicht keine grundsätzlichen Bedenken. Probleme entstehen in der Praxis aber mit der in diesem Verfahren notwendigen Datenverarbeitung, weil die bereichspezifischen Datenverarbeitungsregeln fehlen. Es ist den Beteiligten letztlich nicht klar, welche im Zusammenhang mit dem Rückstellungsverfahren erhobenen Daten übermittelt und bei den einzelnen Stellen wie lange gespeichert werden dürfen.

Am Verfahren beteiligt sind im vorliegenden Fall die Grundschule, die über die Rückstellung entschieden hat, die Sonderschule, die Grundschule mit dem angegliederten Schulkindergarten sowie das Schulamt. Somit werden bei einer Reihe öffentlicher Stellen (das Gesundheitsamt soll hier außer Betracht bleiben) sehr sensible Daten über Kinder und deren Eltern bzw. Erziehungsberechtigte gespeichert, ohne daß dies in allen Fällen erforderlich ist.

Gegen eine Speicherung der Unterlagen bei der Grundschule, an der die Kinder angemeldet werden, bestehen keine datenschutzrechtlichen Bedenken, soweit sie zur Dokumentation der Rückstellung der Kinder vom Schulbesuch erforderlich ist. Auch unter Berücksichtigung einer weiteren Zurückstellung, die noch nach der Einschulung in Betracht kommen kann, dürfte aber keinesfalls eine Speicherdauer von fünf Jahren zu rechtfertigen sein. Ebensowenig kann das oftmals angeführte Argument der einfacheren verwaltungstechnischen Handhabung eine längere als die erforderliche Speicherung stützen. Es wird gerade hier verkannt, daß auch die Speicherung von personenbezogenen Daten einen Eingriff in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung bedeutet, der nur durch eine gesetzliche Regelung gerechtfertigt werden kann. Werden sensible, das Persönlichkeitsrecht der Betroffenen in besonderer Weise tangierende Daten gespeichert, kann eine schematisch für alle Fälle der Speicherung von Schüler- und Elterndaten geltende Aufbewahrungsfrist nicht hingenommen werden. Maßstab für die zulässige Dauer der Speicherung ist – wegen fehlender bereichspezifischer Regelung – die in § 13 Abs. 1 Satz 1 DSG NW vorausgesetzte Erforderlichkeit.

Außerdem erhielt und speichert die Grundschule mit dem angegliederten Schulkindergarten fast den ganzen Schriftwechsel der anderen Grundschule mit den Eltern und dem Schulamt. Dem sind u. a. Angaben über den sonderpädagogischen Förderbedarf der Kinder und die Einleitung des Sonderschulaufnahmeverfahrens zu entnehmen. Gerade im Hinblick auf die Tatsache, daß das Sonderschulaufnahmeverfahren eingestellt wurde, ist mir nicht ersichtlich, aus welchem Grund diese Schreiben übermittelt wurden und

in den Akten der Schule mit dem Schulkindergarten gespeichert werden. Zu den Akten dieser Schule wurden weiter die schulärztliche Stellungnahme sowie der gesamte Bericht des Schulleiters der anderen Grundschule über den durchgeführten Schulreifetest genommen. Zweifelhaft ist, ob diese Unterlagen übermittelt werden mußten. Nach dem Grundsatz der Erforderlichkeit hätte allenfalls die Entscheidung des Schulamtes an die Grundschule mit dem Schulkindergarten übermittelt werden dürfen.

Ein anderer Fall betraf die Übersendung des **Überweisungszeugnisses** bei einem Schulwechsel. Nach § 26 Abs. 3 ASchO erhält der Schüler beim Wechsel in eine andere Schule ein Überweisungszeugnis. Dies bedeutet, daß das Zeugnis dem Schüler bzw. den Erziehungsberechtigten auszuhändigen ist. Eine Übersendung des Zeugnisses an die aufnehmende Schule ohne Wissen der Betroffenen ist nicht vorgesehen und damit auch nicht zulässig. Es gehört nicht zu den Aufgaben der abgebenden Schule, dafür zu sorgen, daß die Aufnahme an der anderen Schule ordnungsgemäß erfolgt. Die für die Anlage des Schülerstammblattes in der aufnehmenden Schule benötigten personenbezogenen Daten sollen bei den Betroffenen direkt – etwa durch Ausfüllen des Anmeldebogens – erhoben werden. Dazu gehört grundsätzlich auch die Anforderung des Überweisungszeugnisses.

Datenschutzrechtlich problematisch erscheint mir grundsätzlich auch die **Übersendung der gesamten Schülerakte** beim Schulwechsel, insbesondere im Sonderschulbereich. Mir ist ein Fall bekanntgeworden, in dem mit Einverständnis der Schulaufsichtsbehörden der Leiter einer Sonderschule vom Leiter der aufnehmenden Schule aufgefordert wurde, beim Schulwechsel die gesamte Schülerakte zu übersenden, obwohl nach Nr. 7.1 VV zu § 5 ASchO die Unterlagen selbst nicht weitergereicht werden dürfen. Der Schulleiter der Sonderschule wurde angewiesen, die gesamte Akte zu übersenden, nachdem die Einwilligung der Erziehungsberechtigten zur Übermittlung der Akte vorlag.

Das Kultusministerium vertritt die Auffassung, es sei zwar in jedem Einzelfall zu prüfen, welche Daten der aufnehmenden Schule übermittelt werden müßten. Allerdings könne die Prüfung der Erforderlichkeit entfallen, wenn eine Einwilligung der Erziehungsberechtigten zur Übermittlung aller Daten des Schülers vorläge.

Es bestehen erhebliche datenschutzrechtliche Bedenken, in derartigen Fällen die Zulässigkeit der Übersendung der Schülerakte nur auf die Einwilligung der Erziehungsberechtigten zu stützen. Mit der Weitergabe werden nicht nur Daten über den Schüler, sondern auch Beurteilungen und Wertungen eines Lehrers, der etwa ein Gutachten erstellt hat, also Daten Dritter übermittelt. Außerdem besteht die Dokumentationspflicht der abgebenden Schule weiter. Dies und die fehlende Erforderlichkeit der Kenntnis aller Daten sprechen gegen die Zulässigkeit der Weitergabe der gesamten Akte. Deshalb können die Erziehungsberechtigten nicht über die Akte der Schule disponieren. Ich halte es besonders im Sonderschulbereich für geboten, eine Weitergabe der gesamten Schülerakte nur auf Grund einer bereichspezifischen Rechtsvorschrift zuzulassen.

Weitere Erwägungen treten hinzu. Eine wirksame Einwilligung kann durch die Erziehungsberechtigten nur erteilt werden, wenn diesen im Zeitpunkt der Erteilung der Einwilligung klar ist, auf welche Weise die Daten durch den Empfänger genutzt werden können. In der Sonderschulakte sind aber Daten enthalten, deren weitere Nutzung in der aufnehmenden Schule (insbesondere dann, wenn es sich um eine allgemeine Schule handelt) von den Erziehungsberechtigten nicht ohne besondere Kenntnisse absehbar ist. Es ist nicht auszuschließen, daß einzelne Daten, insbesondere im Hinblick auf eine unbelastete Eingliederung, für die Erziehungsberechtigten nicht erkennbare negative Auswirkungen haben können. Eine Einwilligung dürfte daher in der Regel unwirksam sein.

### 5.14.2 Lehrerdaten

Lehrerdaten werden an den Schulen in sehr unterschiedlichem Umfang verarbeitet. Während die eine Schulleitung über jede Lehrerin und jeden Lehrer eine Akte führt, in der neben einem Personalbogen u. a. Leistungsberichte, Durchschriften von Schreiben der Schulaufsichtsbehörde, Aktenvermerke und Atteste enthalten sind, wird von einer anderen Schulleitung die Sammlung von Personaldaten in diesem Umfang nicht für erforderlich gehalten. Dort gibt es weder Personalbogen noch abgeheftete Abschriften.

Mit der inzwischen vom Kultusministerium durch Erlaß umfassend geregelten Verarbeitung personenbezogener Daten der Lehrerinnen und Lehrer durch die Schulleitung (BASS 10 – 41) sind zwar datenschutzrechtliche Verbesserungen erreicht worden. Dennoch gilt auch für diese Art der Datenverarbeitung, daß eine normenklare gesetzliche Regelung besonders im Hinblick auf eine automatisierte Verknüpfung der Personaldaten mit zentralen Dateien notwendig ist. Eine derartige gesetzliche Rechtsgrundlage ist mir zum Ende des Berichtszeitraumes als Entwurf eines Gesetzes zur Änderung schulrechtlicher Vorschriften vorgelegt worden. Zu dem Gesetzentwurf werde ich eine ausführliche Stellungnahme abgeben.

Auf der Ebene der unteren Schulaufsichtsbehörden – hier der **Schulämter** – beschäftigt mich der datenschutzrechtlich zulässige Umfang der Verarbeitung von Personaldaten der Lehrerinnen und Lehrer. Im Unterschied zur Schulleitung sind die Schulaufsichtsbeamten mit dienst- und arbeitsrechtlichen Entscheidungsbefugnissen ausgestattet, die demgemäß eine größere Kenntnis an Personaldaten voraussetzen. Aber auch hier gilt es in Abgrenzung zur Einstellungs- und Beschäftigungsbehörde – dem Regierungspräsidenten als obere Schulaufsichtsbehörde – den Rahmen zulässiger Verarbeitung von Personaldaten abzustecken, weil die Berechtigung des Zugriffs auf Personaldaten nach § 29 Abs. 1 Satz 1 DSG NW nur im Rahmen der Erforderlichkeit bestehen kann.

Mir vorliegende Beispiele für die Erhebung von Personaldaten durch Schulämter zeigen, daß in unterschiedlichem Umfang Daten erhoben und gespeichert werden. Es ist mir nicht ersichtlich, für welche Aufgabenerfüllung der Schulaufsichtsbeamte Kenntnis vom Geburtsort der Lehrkraft, der generell

erfragten Staatsangehörigkeit, der Namen und Geburtsdaten ihrer Kinder sowie der Noten mit Datum und Ort der ersten und zweiten Staatsprüfung benötigt. In einem anderen Fall wurden sogar Daten über Schulbildung und der Name der Hochschule erhoben. Die datenschutzrechtliche Problematik wird mit dem Kultusministerium erörtert.

Ein Personalrat hat an mich die Frage herangetragen, ob die Erstellung personenbezogener **Zensurstatistiken** datenschutzrechtlich zulässig sei. Der Schulleiter einer Gesamtschule wies die Lehrkräfte seiner Schule an, jeweils zum Ende des ersten Schulhalbjahres von jeder unterrichteten Gruppe einen Zensurenspiegel anzufertigen und die Durchschnittsnote zu berechnen. Eine nach Jahrgängen und Fächern gegliederte Übersicht aller so erhobenen Daten wurde sogar im Lehrerzimmer ausgehängt. Jede Statistik war mit der Bezeichnung der Klasse bzw. Kursnummer versehen, so daß bei Kenntnis des Stundenplanes – der die gleichen Bezeichnungen enthielt – die jeweilige Lehrkraft identifiziert werden konnte. Durch den Aushang der Statistiken sind daher personenbezogene Daten der Lehrerinnen und Lehrer, d. h. die Art und Weise ihrer Zensurerteilung, Dritten – nämlich allen, die Zugang zum Lehrerzimmer haben – offenbart worden.

Die von mir um Stellungnahme gebetene Schulaufsichtsbehörde hat die Schulleitung der betroffenen Schule zwar aufgefordert, von einer Veröffentlichung der Statistiken im Lehrerzimmer abzusehen. Grundsätzlich hält sie aber eine Erhebung derartiger personenbezogener Statistiken für erforderlich, da diese Daten für verschiedene Konferenzen benötigt würden.

Wie mir durch eine weitere Eingabe bekanntgeworden ist, veranlaßte diese Schulaufsichtsbehörde sogar bei allen Gesamtschulen ihres Zuständigkeitsbereiches, daß mit einem Formblatt Daten für eine „flächendeckende" Zensurstatistik unter Angabe der Namen der Lehrkräfte erhoben werden. Mir erscheint zweifelhaft, ob derartige Statistiken für die Aufgabenerfüllung der Schulleitung oder des Regierungspräsidenten erforderlich sind. Es stellt sich die Frage, ob nicht auch Statistiken ohne Personenbezug ausreichen. Der Hinweis, die Statistiken würden im Rahmen verschiedener Konferenzen benötigt, sowie die Tatsache, daß sie bei der oberen Schulaufsichtsbehörde gesammelt werden, läßt vermuten, daß sie auch für Zwecke der Personalführung eingesetzt werden sollen. Wegen der grundsätzlichen Bedeutung der Angelegenheit habe ich das Kultusministerium um Stellungnahme gebeten.

Gutgemeinte Handlungen können bei Betroffenen das Gegenteil bewirken. In solchen Fällen stellt sich oft heraus, daß ein datenschutzgerechtes Verhalten der beteiligten Personen das Mißgeschick verhütet hätte:

Eine Schulsekretärin entnahm einem an den Schulleiter gerichteten Schreiben der Schulaufsichtsbehörde, daß eine Lehrerin vorzeitig in den Ruhestand treten sollte. Zur Besprechung der Modalitäten einer Verabschiedung offenbarten der Schulleiter dem Lehrerrat und die Schulsekretärin einer Reinigungskraft die bevorstehende Pensionierung. Auch das Schulverwaltungsamt wurde unterrichtet. Aber damit war die betroffene Lehrerin gar nicht

einverstanden, denn sie wollte ohne großes Aufsehen Abschied nehmen, der ihr sowieso schon schwer fiel.

Außer der Bekanntgabe der vorzeitigen Zurruhesetzung an den Schulleiter waren alle im geschilderten Fall enthaltenen Datenübermittlungen an Dritte jedenfalls zu diesen Zwecken unzulässig, weil eine Bekanntgabe ohne Einwilligung der Lehrerin nicht gerechtfertigt war. Was hätte für den Schulleiter näher gelegen, als zunächst die Lehrerin selbst zu fragen, ob sie damit einverstanden ist, daß Lehrerkollegium und Schulverwaltungsamt zur Vorbereitung einer Verabschiedung informiert werden.

### 5.14.3 Dateien an Schulen

Im Berichtszeitraum habe ich Informations- und Beratungsbesuche bei Schulen verschiedener Schularten und -stufen durchgeführt. In vielen Schulen werden bereits einige Aufgaben, insbesondere die Stundenplan- oder Zeugniserstellung mit Hilfe der automatisierten Datenverarbeitung bewältigt. In der Regel ist ein nicht vernetzter PC mit Drucker im Sekretariat, in dem Büro der Schulleitung oder einem gesonderten Raum installiert. Üblich ist allerdings immer noch die konventionelle Datenverarbeitung.

Im Bereich der Schüler- und Elterndaten werden **Schülerstammblätter**, diverse Listen, Klassenbücher sowie Suchkarteien geführt. Die Schülerstammblätter werden in der Regel klassenweise sortiert in Ordnern im Sekretariat oder einem Nebenraum aufbewahrt. Datenschutzrechtlich problematisch gestaltet sich an vielen Schulen die **Einsichtnahme** in die Schülerstammblätter durch Lehrkräfte. Erhält etwa jede Lehrkraft bei Bedarf von der Schulsekretärin den Schlüssel zu dem Schrank, in dem sich die Stammblattordner befinden, wird nicht kontrolliert, ob die Lehrkraft nur in die Unterlagen über Schüler einsieht, die sie tatsächlich unterrichtet. Ich habe daher angeregt, Lehrkräften nur das Stammblatt vorzulegen, in das sie Einsicht nehmen dürfen.

Ein weiteres Problem sehe ich in der Versendung von regelmäßigen „Änderungsmitteilungen" an die Schulen, die meist als **Serviceleistung des Schulträgers** angeboten werden. Darin werden z. B. Adressenänderungen oder der Wechsel der Erziehungsberechtigung mitgeteilt. Die Angaben in der hierfür vorgesehenen Spalte „Erziehungsberechtigung/Haushaltsvorstand" sind jedoch nicht eindeutig. Es ist für die Schule nicht erkennbar, ob es sich bei dieser Angabe um den tatsächlichen Erziehungsberechtigten des Kindes oder etwa den „Haushaltsvorstand" im steuerrechtlichen Sinn handelt. Zum einen wird die Verwendung dieser Daten regelmäßig gegen den Grundsatz, daß die Daten beim Betroffenen zu erheben sind, verstoßen. Zum anderen kann nicht ohne weiteres die Berechtigung zur Auskunftserteilung auf die Angabe „Erziehungsberechtigung/Haushaltsvorstand" gestützt werden. Hier besteht die Gefahr, daß insbesondere bei Scheidung, Wiederverheiratung oder Vormundschaft unzulässigerweise einem nicht erziehungsberechtigten Dritten Auskünfte erteilt werden. Ich halte daher die Änderungsmitteilungen über die Erziehungsberechtigten für unzulässig. Gegen die Mitteilung der

neuen Adresse bestehen dagegen zumindest bei den schulpflichtigen Kindern keine datenschutzrechtlichen Bedenken.

Ich habe auch immer wieder darauf hinweisen müssen, daß die in den Stammblattordnern abgehefteten bzw. in die Stammblätter eingelegten Unterlagen wie z. B. ärztliche Bescheinigungen oder Gutachten in verschlossenen Umschlägen aufbewahrt werden müssen.

Große datenschutzrechtliche Unsicherheit herrscht bei Datenflüssen im Zusammenhang mit den Verfahren zur Durchführung des **Lernmittelfreiheitsgesetzes** und des **Sonderschul-Aufnahmeverfahrens**. Bei diesen Verfahren sind mehrere öffentliche Stellen mit Erhebungen und Übermittlungen beteiligt.

Die von den Erziehungsberechtigten ausgefüllten Anträge nach dem **Lernmittelfreiheitsgesetz** werden über das Sozialamt an das Schulverwaltungsamt geleitet. Dieses entscheidet über die Anträge und unterrichtet die Schulen, wer Lernmittel auch ohne Leistung des Eigenanteils erhält. Damit erhält die Schule Kenntnis über die Tatsache des Sozialhilfeempfanges. Nach Nr. 2.5 der Verwaltungsvorschriften zum Lernmittelfreiheitsgesetz muß der Schulträger das Verfahren regeln und dabei dem Erfordernis des § 35 SGB I (Wahrung des Sozialgeheimnisses) Rechnung tragen. Der Schulträger muß also sicherstellen, daß durch die Ausgabe eigenanteilsfreier Lernmittel an der Schule keine unzulässige Offenbarung über Sozialhilfeleistungen erfolgt. Dies kann nur gewährleistet werden, wenn die Einziehung des Eigenanteils außerhalb der Schule organisiert, oder – falls erforderlich – die Schulsekretärin ausschließlich in ihrer Eigenschaft als Mitarbeiterin des Schulverwaltungsamtes mit der Bearbeitung betraut wird, und weder Schulleitung noch Lehrkräfte Kenntnis darüber erlangen können, wer Lernmittel ohne Leistung des Eigenanteils erhält.

Anläßlich der Überprüfung der Datenverarbeitung im Rahmen eines **Sonderschul-Aufnahmeverfahrens** habe ich festgestellt, daß einschlägige Regelungen nicht im Gesetz, sondern im Runderlaß des Kultusministeriums über das Verfahren bei der Aufnahme in Sonderschulen vom 20.12.1973 (BASS 12 – 11 Nr. 3) getroffen sind. Ich habe Zweifel, ob selbst diese Regelungen den Anforderungen des Datenschutzes genügen. Die Übermittlung der besonders sensiblen, in die Persönlichkeitsrechte der Kinder und Jugendlichen eingreifenden Daten sowie deren Speicherung bedürfen einer normenklaren bereichspezifischen Rechtsgrundlage.

Während ich an den Schulen durchaus den Eindruck gewinnen konnte, daß in den Sonderschul-Aufnahmeverfahren, in denen in besonderer Weise über das Schicksal von Kindern und Jugendlichen befunden wird, mit den Daten behutsam umgegangen wird, war dies im Bereich der unteren Schulaufsichtsbehörden nicht festzustellen. Da das Schulamt über die Aufnahme in die Sonderschule zu entscheiden hat, müssen diesem zwar zu Recht sämtliche Unterlagen, vom Schulbericht über das sonderpädagogische Gutachten bis hin zum schulärztlichen bzw. fachärztlichen Gutachten, vorgelegt werden. Neben den zuständigen Schulaufsichtsbeamten erhalten aber auch die Sach-

bearbeiter, die die Verwaltungsentscheidungen zu entwerfen haben, Einblick in die Unterlagen, die nicht nur sensible Angaben über die Kinder, sondern auch deren Eltern enthalten können. Deshalb muß ich es als datenschutzrechtlich bedenklich ansehen, wenn auf Grund der Organisation – meist nur in kreisfreien Städten – eine **klare Trennung zwischen Schulamt** als unterer Schulaufsichtsbehörde **und dem Schulverwaltungsamt** als Verwaltungsbehörde des Schulträgers fehlt. Ich habe es schon erlebt, daß ein im Schulamt tätiger Sachbearbeiter zugleich auch Aufgaben des Schulverwaltungsamtes wahrgenommen hat. Dadurch erhält das Schulverwaltungsamt Kenntnis von Daten, auf die es im Rahmen seiner rechtmäßigen Aufgabenerfüllung keinen berechtigten Zugriff hätte. Dies gilt nicht nur für Daten aus dem Sonderschul-Aufnahmeverfahren, sondern selbstverständlich auch für die gesamte Datenverarbeitung durch das Schulamt, insbesondere die der Personaldaten der Lehrerinnen und Lehrer.

### 5.14.4 Ausleihverfahren einer Stadtbücherei

Eine Bürgerinitiative, die regelmäßig bestimmte von ihren Mitgliedern ausgeliehene Bücher in Presseveröffentlichungen vorstellte und die Tatsache brandmarkte, daß diese Bücher als NS- oder kriegsverherrlichend zur Ausleihe zugelassen seien, bat mich um Überprüfung des Ausleihverfahrens einer Stadtbücherei. Der im Sinne des Presserechts für Veröffentlichungen Verantwortliche hatte festgestellt, daß alle von ihm zurückgegebenen Bücher – darunter auch eines, das in der Presseveröffentlichung überhaupt nicht erwähnt war – in der Rückgabestelle abgesondert wurden. Er habe zwar gewußt, daß immer schon die in Veröffentlichungen kritisierten Bücher dem Leiter der Bücherei bzw. seinen Lektoren vorgelegt worden seien. Auf Grund der Beobachtung müsse er jedoch befürchten, daß jetzt alle von den Mitgliedern der Bürgerinitiative ausgeliehenen Bücher generell kontrolliert würden und damit das **Leseverhalten** der Betroffenen überwacht würde.

Der Leiter der Stadtbücherei teilte mit, daß die Bücher nach der Presseveröffentlichung lediglich vorgemerkt worden seien, um dem Vorwurf, es handele sich um neofaschistische Bücher, nachgehen zu können. Da der gesamte Ausleihvorgang dem Inhalt nach zusammengehörig erschien, sei auch ein in der Veröffentlichung nicht erwähntes Buch erfaßt worden. Die Vormerkungen für das Lektorat seien lediglich im Rahmen der Selbstkontrolle der Bücherei im Sinne einer Prüfung der vorhandenen Medieneinheiten durchgeführt worden, nicht aber, um das Leseverhalten einer oder bestimmter Personen zu erfassen bzw. zu kontrollieren. Die Daten der Buchausleihe würden nur zu Zwecken der Fristüberwachung und des bei Fristüberschreitung notwendigen Mahnverfahrens gespeichert und nach Rückgabe gelöscht.

Meine Prüfung ergab, daß grundsätzlich eine Vormerkung ausgeliehener Bücher nur über die Identnummer des Buches erfolgt, ohne daß der Name des Entleihers mit der Vorbestellung in Verbindung gebracht werden muß. Im vorliegenden Fall wurde aber der Name des Entleihers abgefragt, um alle von ihm ausgeliehenen Bücher bei der Rückgabe durchsehen zu können. Das bedeutet, daß die unter dem Namen des Betroffenen gespeicherten Buchtitel

nicht nur zu Zwecken einer weiteren Ausleih-Vormerkung genutzt wurden. Eine derartige Nutzung der personenbezogenen Daten der Betroffenen war unzulässig.

Die gespeicherten Ausleihdaten hätten nur genutzt werden dürfen, wenn die Kenntnis der personenbezogenen Daten neben der Überwachung von Ausleihe und Rückgabe auch für eine Kontrolle des Buchbestandes notwendig gewesen wäre. Nach meiner Auffassung reichte es aber aus, daß lediglich die in der Presseveröffentlichung genannten Buchtitel für eine interne Überprüfung vorgemerkt wurden. Auf diese Buchtitel mußte sich die Überprüfung durch das Lektorat beschränken. Die Feststellung weiterer, bisher nicht genannter Buchtitel mit NS- bzw. kriegsverherrlichenden Texten im öffentlich zugänglichen Buchbestand der Bücherei durfte nur durch eigene Kontrollen erfolgen. Eine besondere Abfrage in der Ausleihdatei, welche Bücher von einem bestimmten Benutzer ausgeliehen wurden, war deshalb unzulässig.

Der geschilderte Fall macht deutlich, daß Zugriffe auf automatisiert gespeicherte Ausleihdaten auch die Gefahr in sich tragen können, daß Leserprofile von bestimmten Benutzern einer öffentlichen Bücherei – etwa Mitgliedern politischer Parteien oder Bürgerinitiativen – erstellt werden. Zumindest können sie entsprechende Befürchtungen auslösen. Eine öffentliche Bücherei muß alles daransetzen, auch nur den Anschein einer Nutzung derartiger technischer Möglichkeiten auszuschließen. In diesem Zusammenhang ist zudem der Kommissionsvorschlag für eine EG-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr bedeutsam, der die Verarbeitung von Daten, aus denen die politische Meinung hervorgeht, untersagt (Kapitel II Abschnitt III Artikel 8 Nr. 1 der Richtlinie).

## 5.15 Finanzwesen

### 5.15.1 Ermittlung in unbekannten Steuerfällen

Zwei Vorgänge in der Steuerverwaltung, die nach meiner Einschätzung typisch für eine Reihe ähnlicher Fälle sind, veranschaulichen, wie schwer es den Landesfinanzbehörden fällt, sich von einer lang geübten Verwaltungspraxis und der daraus resultierenden rechtlichen Argumentation zu lösen und entsprechend den Anforderungen des Datenschutzes zu verfahren. Bedauerlich ist, daß trotz Novellierung der Abgabenordnung, mit der erfreulicherweise auch datenschutzrechtlich relevante und bedeutsame Regelungen geschaffen worden sind, dennoch Regelungslücken bestehen bleiben.

In beiden Fällen muß in erster Linie die mangelnde Moral der Steuerunehrlichen dafür herhalten, daß die Finanzverwaltung mit dem Argument einer gerechten Besteuerung die Voraussetzungen für eine zulässige Datenverarbeitung vernachlässigt. Bei meinen nachfolgenden Anmerkungen kann davon ausgegangen werden, daß es mir nicht um einen verstärkten Schutz der Steuerunehrlichen geht, die sich zu Lasten der Allgemeinheit ihren steuerlichen Verpflichtungen entziehen. Vielmehr reklamiere ich für alle Bürgerinnen und Bürger, daß ein Eingriff in ihre Grundrechte auf informationelle

Selbstbestimmung nur zulässig ist, wenn normenklare bereichspezifische Regelungen die Ermächtigungsgrundlage für solche Eingriffe schaffen.

In einem Fall wurden Städte eines Finanzamtsbezirks, die im Rahmen der Denkmalförderung Zuschüsse gewährten, aufgefordert, für den Zeitraum 1980 bis 1988 alle Personen mit Angaben über die Höhe der gewährten Zuschüsse und über die geförderten Objekte aufzulisten. In dem anderen Fall wurde eine kirchliche Einrichtung aufgefordert, eine Liste derjenigen Personen vorzulegen, denen Spendenbescheinigungen erteilt worden waren. Es sollten in dieser Liste aber nur solche Personen erfaßt werden, die durch Vereinbarung mit einem Bankinstitut – ebenfalls in kirchlicher Trägerschaft, aber nicht identisch mit der kirchlichen Einrichtung – ihr Zinsguthaben als Spende der kirchlichen Einrichtung zukommen ließen. Beide Vorgehensweisen erfolgten nicht etwa durch Finanzämter für Steuerstrafsachen und Steuerfahndung, sondern durch die jeweiligen Festsetzungsfinanzämter in Besteuerungsverfahren bzw. Betriebsprüfungsverfahren. Gestützt wird die Rechtmäßigkeit der Ermittlungen in unbekannten Steuerfällen auf das Legalitätsprinzip des § 85 der Abgabenordnung (AO), das die Finanzverwaltung verpflichte, im Rahmen ihrer Möglichkeiten auch unbekannten Steuerfällen nachzugehen, um eine gleichmäßige Besteuerung sicherzustellen. Diese Möglichkeit sei durch § 93 AO gegeben, da auch andere Personen als die im Besteuerungsverfahren Beteiligten zur Auskunft verpflichtet seien. Die Auslegung dieser Bestimmung könne heute als gefestigt und durch die höchstrichterliche Rechtsprechung abgesichert angesehen werden.

Demgegenüber habe ich die Auffassung vertreten, daß § 85 AO als allgemeine Aufgabennorm keine ausreichende Ermächtigungsgrundlage für mit der Datenverarbeitung verbundene Eingriffe, auch soweit sie der Zielsetzung des § 85 Satz 2 AO dienen, darstellen kann. Selbst die Kommentierung zu dieser Vorschrift erkennt an, daß zur Ausfüllung der allgemeinen Aufgabennorm normenklare gesetzliche Einzelbefugnisse geregelt sein müssen und meint, daß die Normenklarheit verbesserungsbedürftig sei (vgl. Tipke-Kruse, Abgabenordnung, Kommentar, 14. Aufl., § 85 Tz. 14).

Datenschutzrechtlich bedenklich ist auch die Anwendung des § 93 Abs. 1 Satz 1 AO auf Fälle, in denen Steuerermittlungen nicht auf ein oder mehrere bestimmte Besteuerungsverfahren beschränkt, sondern losgelöst von einem konkreten Steuerverfahren Ermittlungen in unbekannten Steuerfällen betrieben werden. In den beiden oben dargestellten Fällen erhoben die Festsetzungsfinanzämter Daten von Steuerpflichtigen ohne eine normenklare gesetzliche Einzelbefugnis. § 93 AO berechtigt das Festsetzungsfinanzamt nur, die zur Feststellung eines für die Besteuerung erheblichen Sachverhalts erforderlichen Daten zu erheben und hierzu die Beteiligten und andere Personen bzw. Stellen zu befragen. Die Vorschrift trifft eine nähere Regelung des Beweismittels „Auskunftseinholung jeder Art von Beteiligten und anderen Personen" (§ 92 Nr. 1 AO) innerhalb eines oder mehrerer bestimmter Steuerverfahren. Eine Ausdehnung der Auskunftseinholung auch auf unbestimmte Besteuerungsverfahren oder unbekannte Steuerfälle ist dieser Vorschrift im

Gegensatz zu § 208 Abs. 1 Satz 1 Nr. 3 AO nicht zu entnehmen. Die Datenerhebung kann in beiden Fällen nicht auf § 93 AO gestützt werden, weil davon auszugehen ist, daß die Festsetzungsfinanzämter nicht im Rahmen der Steuerfahndung nach § 208 AO tätig geworden sind.

Auch wenn mir das Finanzministerium in seiner Stellungnahme zugesteht, daß eine Klarstellung in § 93 AO anzustreben sei, wird dennoch das auf diese Vorschrift gestützte „Sammelauskunftsersuchen" der Finanzämter für zulässig gehalten. Dazu beruft es sich nicht nur auf die Rechtsprechung des Bundesfinanzhofes, sondern auch auf das Bundesverfassungsgericht, das in seinem Beschluß vom 06.04.1989 (NJW 1990 S. 701) eine uneingeschränkte Auskunftspflicht der Presseangehörigen für den nicht-redaktionellen Teil, insbesondere den Anzeigenteil festgestellt hat. Die dortigen Ausführungen, die Vorschriften der § 93 Abs. 1 Satz 1, 208 Abs. 1 Nr. 3 AO genügten den verfassungsrechtlichen Anforderungen, weil sie eine ausreichende gesetzliche Ermächtigung zu Eingriffen in das Recht auf informationelle Selbstbestimmung enthielten, kann die Auffassung des Finanzministeriums in keiner Weise stützen. Das Bundesverfassungsgericht hatte nämlich ausdrücklich über verfassungsrechtliche Anforderungen an Auskunftsersuchende im Rahmen der Steuerfahndung zu entscheiden. Es geht hier aber gerade nicht um die Ermittlungstätigkeit der Steuerfahndung, sondern um die der Festsetzungsfinanzämter.

### 5.15.2 Freistellungsauftrag zur Zinsbesteuerung

Nach Inkrafttreten des Gesetzes zur Neuregelung der Zinsbesteuerung (Zinsabschlaggesetz), mit dem Zinseinnahmen direkt besteuert werden, kann eine Zinsbesteuerung bis zu den festgesetzten Höchstbeträgen durch einen Freistellungsauftrag gegenüber Kreditinstituten, Bausparkassen und Lebensversicherungsunternehmen vermieden werden. In den von diesen Instituten herausgegebenen Vordrucken wird auch – unter dem abgekürzten Hinweis „ggf." – nach dem Namen, dem abweichenden Geburtsnamen, Vornamen und Geburtsdatum des Ehegatten gefragt. Außerdem wird die Unterschrift des Ehegatten verlangt.

Betroffene haben sich an mich gewandt und Bedenken dagegen erhoben, daß Kreditinstitute die Annahme ihres Freistellungsauftrages mit der Begründung verweigert hätten, daß die **Angaben über den Ehegatten** fehlten und der Freistellungsauftrag nicht vom Ehegatten unterschrieben sei. Dies sei geschehen, obwohl der Freistellungsauftrag erkennbar nur das eigene Konto betroffen habe, der Ehegatte kein Konto bei diesem Kreditinstitut führe und der Freistellungsauftrag deutlich unter der Höchstgrenze von 6 100 DM geblieben sei.

In § 44 a Abs. 2 Satz 1 Nr. 1 Zinsabschlaggesetz ist lediglich geregelt, daß dem zum Steuerabzug verpflichteten Kreditinstitut ein Freistellungsauftrag nach amtlich vorgeschriebenem Vordruck vorliegen muß. Erst in den Hinweisen des Bundesministeriums der Finanzen zu Einzelfragen der Zinsbesteuerung (Bundessteuerblatt 1992, Teil 1 S. 693) wird vorgeschrieben, daß Ehe-

gatten, die unbeschränkt einkommensteuerpflichtig sind und nicht dauernd getrennt leben, nur gemeinsame Freistellungsaufträge erteilen können.

Diese nicht im Zinsabschlaggesetz enthaltene Regelung führt dazu, daß die Steuerpflichtigen auch gegenüber dem Kreditinstitut Daten bekanntgeben müssen, obwohl deren Kenntnis für das Kreditinstitut in allen Fällen, in denen antragstellende Steuerpflichtige allein ein Konto bei diesem Institut haben, nicht erforderlich ist. Eine derartige Bekanntgabe von Daten gegenüber dem Kreditinstitut ist nur erforderlich und verhältnismäßig, wenn Freistellungsaufträge für ein Gemeinschaftskonto gestellt werden. Eine etwa mit der Datenerhebung bezweckte Erleichterung der Kontrolle durch die Finanzbehörden rechtfertigt nicht die Bekanntgabe der Angaben über den Ehegatten gegenüber dem Kreditinstitut, das mit den Angaben in den meisten Fällen nichts anfangen kann. Außerdem werden die Antragsteller veranlaßt, dem Ehegatten zu offenbaren, bei welchem Kreditinstitut sie bis zu welcher Höhe einen Freistellungsauftrag gestellt haben. Eine Kenntnisnahme von Bankdaten in diesem Umfang ist nicht einmal in der gemeinsamen Steuererklärung möglich. Im übrigen würde ein Verzicht auf die Angaben über den Ehegatten im Freistellungsauftrag keine schlechtere Kontrolle zur Sicherstellung einer gerechten Besteuerung bewirken, da den Finanzbehörden im einzelnen Besteuerungsverfahren alle Kontrollrechte nach der Abgabenordnung bis hin zur Auskunft bei den Kreditinstituten, Bausparkassen und Lebensversicherungen nach § 93 Abs. 1 AO zur Verfügung stehen. Das Bundesministerium der Finanzen ist um Klärung dieser Fragen gebeten worden.

### 5.15.3 Dateien in Finanzämtern für Steuerstrafsachen und Steuerfahndung

Im Zusammenhang mit der Durchführung der Steuerfahndung nach § 208 AO habe ich anläßlich der Novellierung der Abgabenordnung auf eine weitere gesetzlich nicht geregelte und daher unzulässige Datenverarbeitung hingewiesen. Bei mehreren Finanzämtern für Steuerstrafsachen und Steuerfahndung habe ich festgestellt, daß in sehr unterschiedlichem Umfang und in unterschiedlicher Form zu jedem eingeleiteten Verfahren Daten u. a. in einer Steuerfahndungskartei erfaßt und gespeichert werden. Die Karteikarte sieht insbesondere Angaben über Beruf, Familienstand, Name und Geburtsdatum des Ehegatten, Staatsangehörigkeit, Fahndungsmaßnahmen und Fahndungsergebnisse vor. Die Steuerfahndungskartei wird nicht nur als interne Suchdatei genutzt, sondern dient auch für Auskünfte an andere Finanzbehörden in Nordrhein-Westfalen und in den anderen Bundesländern. Die Fahndungskartei wird neben einer Namenskartei StraBu (Steuerstrafsachen und Bußgeldverfahren) geführt.

Darüber hinaus werden Daten aus dieser Datei an die Informationszentrale für den Steuerfahndungsdienst beim Finanzamt Wiesbaden II auf der Grundlage einer Vereinbarung der Bundesländer übermittelt. Nach dem Merkblatt für die Meldungen an die Informationszentrale sind alle Fälle zu melden, in denen ein sog. Fallheft angelegt wird, d. h. also bereits dann, wenn die Ermittlung aufgenommen und eine Karteikarte angelegt wird.

Zwar hat die Steuerfahndung im wesentlichen die Aufgabe, Steuerkriminalität zu bekämpfen. Insoweit stehen ihr für die Ermittlung primär die Strafverfolgungsmaßnahmen der StPO – in der aber ebenfalls eine bereichspezifische normenklare Regelung über die Errichtung von Strafverfolgungsdateien fehlt – zur Verfügung. Daneben sind der Steuerfahndung aber auch Aufgaben übertragen, die nicht dem Strafprozeßordnungs-Bereich zuzuordnen sind. Dies gilt beispielsweise für die Fahndung in unbekannten Steuerfällen. Soweit sie daher in diesem Bereich tätig wird, fehlt in der Abgabenordnung eine bereichspezifische normenklare Regelung über die Zulässigkeit derartiger Dateien.

§ 208 AO – der im wesentlichen Aufgabenzuweisungsnorm ist – enthält insbesondere keine Regelung über die Verarbeitung personenbezogener Daten, die suchfähig in Dateien gespeichert, verändert und genutzt werden können. Außerdem müssen Datenübermittlungen aus diesen Dateien an die Informationszentrale und an Finanzbehörden oder andere Stellen gesetzlich geregelt sein. Längst beschäftigt sich eine Arbeitsgruppe mit der Automatisierung dieser Dateien, ohne daß eine gesetzliche Regelung dies zuläßt und die erforderlichen Vorgaben für eine Automatisierung trifft. Auch anläßlich der Novellierung der Abgabenordnung ist nicht an eine entsprechende Regelung gedacht worden. Mit einer landesweiten Automatisierung dieser Dateien wäre eine Verknüpfung der Daten aller Finanzämter für Steuerstrafsachen und Steuerfahndung und damit auch eine rastermäßiger Fahndung technisch möglich. Daher greift diese Datenverarbeitung in besonderem Maße in das Recht auf informationelle Selbstbestimmung der dort erfaßten Steuerpflichtigen – u. U. sogar von Personen, die nicht steuerpflichtig sind – ein. Sie bedarf daher einer spezielleren Regelung als der in § 88 Abs. 3 und 4 oder der in § 30 Abs. 8 des Änderungsgesetzes der Abgabenordnung (i.V.m. der Steuerdatenabrufverordnung) vorgesehenen. Das Fehlen einer entsprechenden Regelung erstaunt um so mehr, als im Gesetz über das Zollkriminalamt eine spezielle Regelung zur Errichtung entsprechender Dateien vorgesehen ist.

### 5.15.4 Pfändungs- und Überweisungsverfügungen gegen Drittschuldner

Auf Grund mehrerer Eingaben habe ich die Vorgehensweise der Finanzämter bei der Ausbringung von Pfändungs- und Überweisungsverfügungen gegen Drittschuldner datenschutzrechtlich geprüft. Dabei mußte ich feststellen, daß Finanzämter vor Ausbringung derartiger Verfügungen den Sachverhalt nicht hinreichend geklärt haben, so daß sich einige Verfügungen am Rande einer „Pfändung ins Blaue" bewegten.

In einem Fall wurden mehrere Pfändungsverfügungen gegen die Mieter der Ehefrau des Steuerschuldners – bei getrennter Veranlagung – ausgebracht, in der Annahme, der Betroffene sei Bezieher der Einkünfte aus dem Mietverhältnis, obwohl sich aus den Steuerakten – u. a. dem Einheitswertbescheid – ergab, daß die Ehefrau alleinige Eigentümerin des Grundstückes und Empfängerin der Mietzahlungen war. Eine andere Verfügung richtete sich gegen ein Postgiroamt, obwohl der Betroffene dort kein Konto unterhielt. Offenbar

entnahm das Finanzamt die Kontonummer einem Überweisungsträger, der aber die Zahlung eines Kunden des Steuerschuldners über dieses Postgiroamt enthalten hatte. Es wurde auch die Versicherungsleistung bei einer Versicherungsgesellschaft gepfändet, bei der der Steuerschuldner nie einen Versicherungsvertrag abgeschlossen hatte.

Voraussetzung für eine zulässige Pfändung ist, daß hinreichende Anhaltspunkte für das Bestehen der Forderung gegeben sind. Nach Auffassung des Finanzamtes sind **Ermittlungen** darüber, ob tatsächlich Forderungen bestehen, weder gesetzlich vorgeschrieben noch geboten, da ansonsten der Pfändungszweck gefährdet werden könne. Dieser Auffassung kann ich mich nicht anschließen.

Nach § 249 Abs. 2 AO stehen der Finanzbehörde eigene Ermittlungen zu. Eine gesetzliche Ermittlungspflicht besteht zwar nicht; im Rahmen der pflichtgemäßen Ermessensausübung und unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit sind aber Ermittlungen insbesondere auch aus datenschutzrechtlicher Sicht erforderlich. Die Finanzbehörde hat nicht nur die Verpflichtung, Pfändungen nicht willkürlich auszubringen, sie muß vielmehr auch ermitteln, ob hinreichende Anhaltspunkte für das Bestehen einer Forderung vorliegen. In dem einen Beispielsfall hätte das Finanzamt diese Möglichkeit gehabt, ohne den Pfändungszweck zu gefährden, denn bereits an Hand der vorhandenen Steuerakten hätte sich der Sachverhalt aufklären lassen. Ich habe nicht nur empfohlen, künftig vor Ausbringung von Pfändungs- und Überweisungsverfügungen nach § 309 i.V.m. § 249 AO die aus dem Steuerverfahren vorhandenen Unterlagen sorgfältig zu prüfen und ggf. eigene Ermittlungen anzustellen, sondern auch, daß die zu Unrecht erlassenen Pfändungs- und Überweisungsverfügungen von den vermeintlichen Drittschuldnern zurückgefordert und vernichtet werden, soweit nicht der betroffene Steuerpflichtige nach § 19 Abs. 2 Satz 1 b DSG NW die Sperrung verlangt.

### 5.15.5 Lohnsteuerkarten

Als eine vermeidbare Einschränkung ihres Rechtes auf informationelle Selbstbestimmung betrachten betroffene Arbeitnehmerinnen und Arbeitnehmer, daß sie beim **Wechsel des Arbeitgebers** durch Vorlage der alten Lohnsteuerkarte dem neuen Arbeitgeber die bisherigen Einkünfte und die Beschäftigungszeiten offenbaren müssen.

Nach § 39 Abs. 1 Satz 1 des Einkommensteuergesetzes (EStG) haben die Gemeinden den unbeschränkt einkommensteuerpflichtigen Beschäftigten für jedes Kalenderjahr unentgeltlich eine Lohnsteuerkarte nach amtlich vorgeschriebenem Muster auszustellen und zu übermitteln. Nur für den Fall, daß eine Steuerkarte verlorengegangen, unbrauchbar geworden oder zerstört worden ist, hat die Gemeinde eine Ersatzlohnsteuerkarte auszustellen. Die Ausstellung einer zweiten Steuerkarte aus Anlaß des Wechsels des Arbeitgebers ist nicht vorgesehen.

Der Bundesbeauftragte für den Datenschutz hatte das Bundesministerium der Finanzen bereits aus früherem Anlaß gebeten, auf eine Gesetzesänderung hinzuwirken, welche die Ausstellung einer zweiten Lohnsteuerkarte beim Wechsel des Arbeitgebers ermöglicht. Dem Anliegen wurde entgegengehalten, daß zwingende Gründe, die eine solche Gesetzesänderung erforderlich machen würden, nicht ersichtlich seien. In Einzelfällen könne zwar ein schutzwürdiges Interesse vorliegen, dem neuen Arbeitgeber die bisherigen Beschäftigungsdaten nicht zu offenbaren. Neben dem Gesichtspunkt der weiteren Komplizierung des Steuerrechts würden aber auch steuerrechtliche Erwägungen gegen die Ausstellung einer zweiten Lohnsteuerkarte beim Wechsel des Arbeitgebers sprechen. Die Beschäftigten könnten ja nach geltendem Recht die Offenbarung ihrer Beschäftigungsdaten dadurch vermeiden, daß sie den neuen Arbeitgeber die Lohnsteuer nach der Steuerklasse VI ermitteln ließen. Dazu seien die Arbeitgeber verpflichtet, wenn die Lohnsteuerkarte schuldhaft nicht vorgelegt werde (§ 39 c Abs. 1 EStG).

Unabhängig davon, daß diese Verfahrensweise nicht gerade das Vertrauen eines neuen Arbeitgebers stärkt, erscheint diese Lösung insbesondere im Hinblick auf das informationelle Selbstbestimmungsrecht nicht akzeptabel. Beschäftigte müssen – ohne Gefahr zu laufen, finanziell massiv benachteiligt zu werden – selbst entscheiden können, ob sie ihrem neuen Arbeitgeber die bisherigen Einkünfte und Beschäftigungszeiten offenbaren wollen. Bis jetzt konnte insoweit noch keine das Grundrecht auf informationelle Selbstbestimmung achtende Lösung gefunden werden.

Desweiteren ist die Angabe der **Konfession des Ehegatten** auf der Lohnsteuerkarte problematisiert worden. Beschäftigte, die z. B. bei einer kirchlichen Einrichtung tätig sind, müssen befürchten, daß sich aus der Kenntnisnahme der anderen Konfession, vielleicht sogar der Konfessionslosigkeit des Ehegatten berufliche Nachteile ergeben.

Das um Stellungnahme gebetene Finanzministerium hat ausgeführt, daß auf die Angabe der Religionszugehörigkeit des Ehegatten bei konfessionsverschiedenen Ehen im Falle der Zusammenveranlagung nicht verzichtet werden könne, da die Ehegatten für die Kirchenlohnsteuer als Gesamtschuldner hafteten (§ 6 Abs. 1 Satz 2 des Kirchensteuergesetzes Nordrhein-Westfalen) und die Steuer je hälftig beiden Religionsgemeinschaften zustehe. Die Frage, ob auch bei konfessionsgleichen oder glaubensverschiedenen Ehen (nur ein Ehegatte gehört einer steuerberechtigten Kirche an) die Eintragung für den Lohnsteuerabzug erforderlich ist, sei auf Bundesebene erörtert worden. Es sei beschlossen worden, der Bundesregierung zu empfehlen, die Lohnsteuerrichtlinien 1993 so zu formulieren, daß in Zukunft nur auf die Religionsgesellschaft abgestellt wird, die zur Erhebung der Steuer berechtigt ist. Das Finanzministerium geht daher davon aus, daß ab 1994 bei konfessionsgleichen und glaubensverschiedenen Ehen keine Angaben zur Konfession des Ehegatten auf der Lohnsteuerkarte mehr verzeichnet sein werden.

## 5.16 Umweltschutz

### 5.16.1 Zugang zu Informationen über die Umwelt

Die Umweltbehörden werden sich auf eine neue Form der Öffentlichkeitsarbeit einstellen, weil sie ab 1993 den Bürgerinnen und Bürgern in Nordrhein-Westfalen den freien Zugang zu Informationen über die Umwelt gewähren müssen. Da ein Gesetz zur Umsetzung der EG-Umweltinformationsrichtlinie bisher nur im Entwurf vorliegt, gilt mit Ablauf der bis zum 31. Dezember 1992 gesetzten Frist die Richtlinie des Rates vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt unmittelbar. Die zügige Umsetzung der Richtlinie in ein Umweltinformationsgesetz halte ich dennoch für dringend geboten.

Der Anspruch auf freien Zugang zu Informationen über die Umwelt steht naturgemäß in einem Spannungsverhältnis zum Grundrecht auf informationelle Selbstbestimmung. Unabhängig davon, ob der Anspruch der Bürgerinnen und Bürger auf freien Informationszugang auch aus dem allgemeinen Persönlichkeitsrecht hergeleitet werden kann, wird man im Hinblick auf den Schutz der Umwelt und die damit in engem Zusammenhang stehende Lebensqualität jedem das Recht einräumen müssen, sich die einschlägigen Informationen zu beschaffen, die Kenntnisse über den Zustand von Luft, Wasser, Boden und Klima vermitteln. Solange diese Informationen als anonymisierte oder aggregierte Daten den auf der anderen Seite bestehenden Anspruch auf Schutz der personenbezogenen Daten Betroffener nicht berühren, ist die Einräumung eines Anspruches auf freien Zugang zu Informationen über die Umwelt unproblematisch.

Erst wenn mit diesen Informationen auch personenbezogene Daten über eine natürliche Person verbunden sind, kann der Informationsanspruch nur unter Berücksichtigung des Grundrechts auf informationelle Selbstbestimmung bestehen. Auch die Richtlinien des Rates sehen eine Einschränkung des Anspruches auf freien Zugang zu Umweltinformationen vor, wenn die Vertraulichkeit personenbezogener Daten berührt ist. Im Entwurf des Umweltinformationsgesetzes wird dieses Spannungsverhältnis durch eine Abwägung beider Interessen gelöst. Danach soll der Informationsanspruch dann hinter den Anspruch auf Datenschutz zurücktreten, wenn durch ihn schutzwürdige Interessen der Betroffenen beeinträchtigt werden. Diese Entscheidung ist aus datenschutzrechtlicher Sicht grundsätzlich zu begrüßen.

Die Umweltbehörden müssen dementsprechend nach meiner Auffassung bei der Entscheidung über eine Auskunftserteilung von folgenden Grundsätzen ausgehen:

- Vorrangig werden nur anonymisierte und aggregierte Informationen, z. B. Strukturdaten, die Kenntnisse über den Zustand von Luft, Wasser, Boden und Klima vermitteln, mitgeteilt.
- Grundsätzlich werden immer dann, wenn Umweltdaten einen Personenbezug aufweisen, nur mündliche oder schriftliche Auskünfte erteilt oder Informationen auszugsweise zur Verfügung gestellt; eine Einsichtnahme durch Dritte in Akten mit personenbezogenen Daten wird nicht gewährt.

- Sollen Informationen über Umweltdaten, die auch Angaben über persönliche oder sachliche Verhältnisse von Betroffenen beinhalten, mitgeteilt werden, müssen die Betroffenen vorher angehört werden; außerdem muß geprüft werden, ob durch die Bekanntgabe von Umweltdaten keine schutzwürdigen Interessen Betroffener beeinträchtigt werden.

Danach lassen sich künftig Anträge auf Informationen über Umweltdaten besser und gerechter entscheiden, als dies mit der für allgemeine Auskünfte an private Personen oder Stellen geltenden Regelung des § 16 Abs. 1 DSG NW möglich war. Dies wird an einem Beispielfall, der eine Umweltbehörde über lange Zeit beschäftigt hat und wohl auch noch beschäftigt, deutlich.

Nachdem eine Stadt im Ruhrgebiet Grundstücke aus aufgegebener Industrieansiedlung als Wohnsiedlungsgebiete ausgewiesen, erschlossen und zur Bebauung an Siedlungswillige verkauft hatte, stellte sich nach Bebauung der Grundstücke heraus, daß der Boden unter den Häusern durch die vorher dort tätigen Industriebetriebe stark belastet war. Wegen der unterschiedlichen **Altlasten,** die teilweise ein weiteres Bewohnen unmöglich machten, wurden Teile des Siedlungsgebietes von der Stadt zurückgekauft, während andere Grundstücke auf Kosten der Stadt mit entsprechenden Schutzmaßnahmen behandelt wurden. Die Bodenbelastungen waren durch Bodenuntersuchungen und einschlägige Gutachten für das gesamte Siedlungsgebiet und auf jedes einzelne Grundstück bezogen festgestellt worden. Informationen über die Bodenbelastungen wurden von der Stadt, soweit sie das gesamte Siedlungsgebiet und das jeweilige Grundstück betrafen, den einzelnen Grundstückseigentümern mitgeteilt. Darüber hinaus wollten aber einzelne Eigentümer auch über die Bodenbelastung des Nachbargrundstückes informiert werden. Solche Informationen hat die Umweltbehörde unter Berufung auf den Datenschutz insbesondere wegen des Widerspruchs von Nachbarn verweigert.

Nach § 16 Abs. 1 Satz 1 Buchstabe d DSG NW war eine Auskunftserteilung nur dann zulässig, wenn sie im öffentlichen Interesse lag bzw. ein berechtigtes Interesse der Auskunftsbegehrenden geltend gemacht wurde und – in beiden Fällen – die Betroffenen nicht widersprachen. Das bedeutet, daß eine Auskunftserteilung immer dann, wenn der Betroffene widersprochen hatte, datenschutzrechtlich nicht zulässig war.

Nunmehr besteht nach Anwendung der Richtlinie des Rates, wie sie im Gesetzentwurf umgesetzt werden soll, ein Anspruch auf Informationserteilung immer dann, wenn durch eine Offenbarung der das Nachbargrundstück betreffenden Daten über die Bodenbelastung keine schutzwürdigen Interessen der benachbarten Grundstückseigentümer beeinträchtigt werden. Dazu muß die Umweltbehörde durch Anhörung des Betroffenen feststellen, ob schutzwürdige Interessen von Grundstücksnachbarn bestehen. Ein bloßer Widerspruch des Betroffenen genügt nicht mehr. Er muß seine Bedenken gegen die Auskunftserteilung vortragen. Im Einzelfall ist dann zu prüfen, ob das vorgetragene Interesse im Hinblick auf das Informationsinteresse

schutzwürdig ist. Etwaige Verkaufsabsichten von Nachbarn können dann nicht mehr als schutzwürdig angesehen werden, wenn bereits eine allgemeine Bodenbelastung des Siedlungsgebietes öffentlich bekanntgeworden ist.

### 5.16.2 Abfallbeseitigung

Ein Bürger machte mich auf einen kuriosen Fall behördlicher Ermittlungen aufmerksam. In einer Stadt wurde eine **fotografische Dokumentation des Hausmülls** vorgenommen, weil ein kleinerer Abfallbehälter beantragt worden war. Dem Bürger erschien es bedenklich, daß beim Fotografieren der geöffneten Mülltonnen personenbezogene Daten etwa in Form von lesbaren Schriftstücken, die er dem Müll überantwortet hatte, festgehalten wurden. Außerdem könnte eine Fotodokumentation über einen längeren Zeitraum hinweg Rückschlüsse auf seinen Lebensstil und sein Verbraucherverhalten zulassen.

Zur Überprüfung, ob der Antrag auf Bereitstellung eines kleineren Abfallbehälters – und damit verbunden eine geringere Gebühr – gerechtfertigt war, ließ die Stadt durch Bedienstete Fotos der anfallenden Müllmenge am Abfuhrtag anfertigen. Die Stadt hielt diese Kontrolle auch für erforderlich, um eine ordnungsgemäße Abfallentsorgung sicherzustellen. Es sei nämlich festzustellen, daß ein großer Teil der Anträge auf Verringerung der Tonnengröße nicht mit einer tatsächlichen Reduzierung der Müllmenge einhergehe und dadurch ständig zusätzliche Abfallsäcke zur Müllabfuhr gegeben würden. Die fotografische Beweissicherung habe sich außerdem bei gerichtlichen Entscheidungen als unerläßliches Hilfsmittel erwiesen. Zu der Verfahrensweise der Stadt habe ich folgende Auffassung vertreten:

Es gehört zur Aufgabenerfüllung des Amtes für Umweltschutz, zu prüfen, ob die Voraussetzungen für eine Verringerung der Abfallbehältergröße vorliegen. Dazu können auch Feststellungen zur Müllmenge vor Ort erforderlich sein. Derartige Überprüfungen müssen grundsätzlich vom Antragsteller hingenommen werden, vor allem, wenn die beantragte Verringerung nach den Erfahrungen der Stadtreinigung als nicht unproblematisch angesehen werden kann. Art und Umfang dieser Überprüfungen sind aber unter Berücksichtigung des verfassungsrechtlichen Grundsatzes der Verhältnismäßigkeit durchzuführen. Insoweit habe ich erhebliche Zweifel, ob die Feststellungen vor Ort in der vorgenommenen fotografischen Dokumentation von Hausmüll erfolgen mußten. Zur Feststellung der anfallenden Müllmenge sollte eine Augenscheinnahme vor Ort durch Personal der Stadtverwaltung genügen; dies jedenfalls dann, wenn das Ergebnis der Feststellung den Darlegungen des Antragstellers nicht zuwiderläuft. Ein fotodokumentarisches Festhalten der bei der Überprüfung angetroffenen Situation mag im Einzelfall aus Gründen der Beweissicherung gerechtfertigt sein, aber nicht eine Dokumentation, die Einblick in die Mülltonne eröffnet und Einzelheiten des Verbraucherverhaltens festhält. In diesem Fall hat die Stadt den danach gesetzten Rahmen überschritten.

Ich habe deshalb empfohlen, bei künftigen Überprüfungen von einer derart detaillierten fotografischen Dokumentation abzusehen sowie die im Falle des Betroffenen bereits angefertigten Fotos aus der Akte zu entfernen und zu vernichten.

Mehrere Städte planen z. Z. Versuche zur Müllgefäßidentifikation mit **codierten Mülltonnen**. Dabei sollen die Abfalltonnen mit einem Chip und die Müllfahrzeuge mit einer Wiege- und Leseeinrichtung versehen werden. Auf Grund der auf dem Chip gespeicherten Daten wie Tonnennummer, Straße und Hausnummer, Leerungsrythmus, Gewicht und Datum, könnte eine neue Gebührengrundlage auf der Basis der Abfallmenge und der Leerungshäufigkeit erstellt werden. Außerdem sollen damit die beteiligten Haushalte zur Müllvermeidung und Gebührenersparnis veranlaßt werden.

Das in einer Stadt durchgeführte Pilotprojekt zur Identifizierung und Einzelverwiegung von Abfallgefäßen mußte zwar als fehlgeschlagen angesehen werden, da der Unsicherheitsgrad beim Wiegen des Hausmülls noch so hoch war, daß eine Eichung der Geräte nicht in Frage kam. Die Identifizierung der Müllgefäße war jedoch problemlos möglich. Daraus ergab sich die Überlegung, eine verursacherorientierte Abfallgebührenstruktur durch ein modernes Wertmarkensystem einzuführen. Es soll nicht die jeweilige Abfalltonne gewogen, sondern das Volumen des Abfalls veranschlagt werden. Derjenige, der die Restmülltonne gefüllt und dem Entsorgungsunternehmen zur Entleerung übergeben hat, soll über das Identifikationssystem am Müllwagen festgehalten werden. In diesem Falle wurde mir mitgeteilt, daß es bei dem geplanten Verfahren nicht möglich sei, im Müllwagen Namen festzustellen.

Die weitere Entwicklung in diesem Bereich wird von mir insbesondere unter dem Aspekt, welche personenbezogenen Daten erhoben und – auch automatisiert – weiterverarbeitet werden, verfolgt.

## 5.17 Verkehr

### 5.17.1 Örtliches Fahrzeugregister

Zur Information und Beratung habe ich mehrere Kraftfahrzeug-Zulassungsstellen von Städten und Kreisen besucht und mir dort die Verarbeitung von Halterdaten in den örtlichen Fahrzeugregistern angesehen. Dabei habe ich festgestellt, daß zu einzelnen örtlichen Fahrzeugregistern interne **On-line-Verbindungen** der Führerscheinstelle, Bußgeldstelle, Verkehrsüberwachung, Gewerbeüberwachungsstelle bestehen. Andere dagegen haben nur On-line-Zugriffe der örtlich zuständigen Polizeibehörde zugelassen.

Die für einen On-line-Anschluß zum örtlichen Fahrzeugregister maßgebliche Vorschrift des § 36 Abs. 2 Satz 2 des Straßenverkehrsgesetzes (StVG) erlaubt die Übermittlung aus dem örtlichen Fahrzeugregister in einem automatisierten Verfahren nur an die örtliche Polizeidienststelle. Weitere On-line-Zugriffe sind danach nicht vorgesehen.

Der **On-line-Zugriff durch Bußgeldstellen** nimmt allerdings gegenüber den anderen o. g. Zugriffsmöglichkeiten eine Sonderstellung ein. Auch im Kreise

der Datenschutzbeauftragten wurde die spezielle Frage der Erteilung von Halterauskünften an die Bußgeldstellen zur Verfolgung von Verkehrsordnungswidrigkeiten diskutiert. Das StVG läßt bei den Polizeidienststellen, nicht aber bei den kommunalen Verkehrsüberwachungsdiensten, eine Halterfeststellung im automatisierten Verfahren zu. Wegen der sehr großen Zahl derartiger Anfragefälle halte ich es für bedenkenswert, die gesetzliche Regelung zum automatisierten Abrufverfahren in § 36 Abs. 2 StVG auch auf die zur Verfolgung von Verkehrsordnungswidrigkeiten zuständigen Stellen zu erstrecken. Nach meinem Erkenntnisstand wird in der Praxis die fehlende Regelung als Mangel angesehen und ein On-line-Abruf auch für diesen Zweck für erforderlich gehalten. Außerdem hat die Bundesregierung schon bei der letzten Gesetzesänderung zum StVG die Prüfung vorgeschlagen, ob die vom Bundesrat insoweit gewünschte Ausweitung der Befugnisse zum Direktabruf geboten und vertretbar sei, so daß mit einer entsprechenden gesetzlichen Regelung bei der Novellierung des StVG gerechnet werden kann.

Bei meinen Besuchen habe ich weiter festgestellt, daß im automatisierten Abrufverfahren verschiedentlich keine **Aufzeichnungen** über die Abrufe nach § 36 Abs. 6 Satz 1 StVG geführt werden, bzw. der Zulassungsstelle nicht bekannt war, daß Aufzeichnungen durch die zentrale Datenverarbeitungsstelle gefertigt wurden. Die Zulassungsstellen erfuhren erstmals anläßlich meiner Besuche, welchen Sinn und Zweck die Aufzeichnungen haben, und welche Kontrollmöglichkeiten dadurch gegeben sind.

Keine der besuchten Zulassungsstellen hatte eine **Dienstanweisung**, in der die erforderlichen organisatorischen und technischen Maßnahmen zur Datensicherung getroffen sind (vgl. 10. Tätigkeitsbericht, S. 166). In der Dienstanweisung sollten insbesondere die Art und Weise der Datenerhebung bei der Antragstellung, die Art und der Umfang der Übermittlung an andere Behörden, vor allem wer welche Auskünfte erteilen darf sowie wem gegenüber und unter welchen Voraussetzungen auch telefonische Auskünfte erteilt werden dürfen, die besonderen Aufzeichnungen über erteilte Auskünfte außerhalb des On-line-Abrufverfahrens und die Löschungsfristen geregelt sein. Zur Überprüfung der Einhaltung der getroffenen Maßnahmen halte ich es außerdem für erforderlich, festzulegen, durch wen die Kontrolle ausgeübt werden soll.

Im übrigen war den Zulassungsstellen, die alle zu Zulassungszwecken benötigten Antragsunterlagen mikroverfilmen, eine andere datenschutzrechtliche Problematik nicht bewußt. Die dort angewandte Dokumentationstechnik bringt es mit sich, daß die gespeicherten Daten nur unter einem Merkmal, nämlich dem Tag der Bearbeitung, aufgefunden werden können und so gespeichert sind, daß die Löschung einzelner Daten technisch nicht möglich ist.

Das Ministerium für Stadtentwicklung und Verkehr des Landes Nordrhein-Westfalen (MSV), dem ich das Ergebnis meiner Besuche mitgeteilt habe, hat sich zum Erlaß einer Musterdienstanweisung bereit erklärt. Ebenfalls wird es zum Problem der Löschung bei mikroverfilmten Zulassungsunterlagen die Behörden darauf hinweisen, daß die Daten nur so gespeichert werden dürfen, daß eine vorschriftsmäßige Löschung möglich bleibt. Dagegen sieht das MSV

trotz meiner Hinweise auf die in den von mir besuchten Städten und Kreisen festgestellten unzulässigen On-line-Verbindungen zum örtlichen Fahrzeugregister keinen Handlungsbedarf. Damit wird es seiner Verpflichtung nach § 7 DSG NW nicht gerecht. Wenn das MSV nicht auf den datenschutzrechtlich unzulässigen Zustand reagiert, sehe ich mich gezwungen, diese Datenverarbeitung der Zulassungsstellen zu beanstanden.

Um die Massenarbeit der Halteranfragen durch die Bußgeldstelle im Zusammenhang mit den „Knöllchen" in den Griff zu bekommen, hätte ich gegen ein automatisiertes **Datenabgleichverfahren**, bei dem ein Datenträger der Bußgeldstelle mit dem automatisierten Bestand des örtlichen Fahrzeugregisters in der jeweiligen Datenverarbeitungszentrale abgeglichen wird, keine Bedenken. Da ein derart gestaltetes automatisiertes Abgleichverfahren weder in rechtlicher noch in technischer Hinsicht mit einem On-line-Abrufverfahren vergleichbar ist, sehe ich die Voraussetzung des § 35 Abs. 1 Nr. 3 StVG als gegeben an, wonach an Behörden für Zwecke der Verfolgung von Ordnungswidrigkeiten Fahrzeug- und Halterdaten aus dem örtlichen Fahrzeugregister übermittelt werden dürfen. Ebensowenig wird hierdurch das grundsätzlich bestehende Verbot weiterer On-line-Anschlüsse umgangen.

Allerdings muß den durch ein automatisiertes Abgleichverfahren bedingten besonderen Anforderungen an den Datenschutz und die Datensicherheit durch organisatorische und technische Vorkehrungen Rechnung getragen werden. Dazu müßten insbesondere in einer Dienstanweisung gegenüber der Datenverarbeitungszentrale die erforderlichen Weisungen zur Datenverarbeitung im Auftrag erteilt werden, die sicherstellen, daß die Verantwortlichkeit der örtlichen Zulassungsstelle nicht verwischt wird. Hierzu gehört auch die Durchführung der Übermittlungskontrolle.

### 5.17.2 Führung von Fahrzeugakten

Neben dem manuellen oder automatisierten Fahrzeugregister führen Zulassungsstellen über Fahrzeuge eigene Akten, die im allgemeinen nur den Antrag auf Zulassung des Fahrzeugs und die Versicherungsdoppelkarte enthalten. Es ist zweifelsfrei, daß derartige Unterlagen für Zulassungszwecke aufbewahrt werden müssen. Die Zulässigkeit der Aktenführung ergibt sich allerdings nicht aus den Straßenverkehrsvorschriften. Im vorliegenden Fall greift die Vorschrift des § 24 Abs. 1 PolG NW, da die Zulassungsstelle als Teil der Straßenverkehrsbehörde eine Sonderordnungsbehörde ist und § 24 OBG bestimmt, daß die genannte Vorschrift des Polizeigesetzes für diese Behörden entsprechend anzuwenden ist.

In den Fahrzeugakten sind beispielsweise auch Mitteilungen der Polizei darüber enthalten, daß bei einer Verkehrskontrolle das Fehlen des Warndreiecks oder Verbandskastens (**Fahrzeugmängel**) in dem Fahrzeug festgestellt wurde. In derartigen Fällen sieht zwar die Zulassungsstelle von aktuellen Maßnahmen gegen den Fahrzeughalter ab, speichert aber die mitgeteilten Daten in der Akte und verwertet sie auch bei späteren zulassungsrechtlichen Entscheidungen.

Das MSV vertritt die Auffassung, daß derartige Angaben zwar nicht in der Fahrzeugakte, aber in dem örtlichen Fahrzeugregister gespeichert werden müßten. Es bezieht sich dabei auf die Vorschrift des § 3 Abs. 2 Nr. 10 der Fahrzeugregisterverordnung (FRV). Danach dürfen bei Fahrzeugen mit amtlichen Kennzeichen im örtlichen Fahrzeugregister Vermerke über Fahrzeugmängel und Maßnahmen zur Mängelbeseitigung gespeichert werden. Als Fahrzeugmangel gelte auch das Fehlen von Warndreieck und Verbandskasten, da grundsätzlich nicht zwischen Ausrüstungs- und technischen Mängeln unterschieden werde. Das Fehlen derartiger Gegenstände müsse bei einer Überprüfung durch die Polizei als Mangel festgestellt werden. Allerdings sollten diese Fahrzeugmängel nicht Anlaß der Zulassungsstelle für Maßnahmen gegen den Halter sein.

Ich folge der Auffassung des MSV, daß Angaben über das Nichtmitführen von Warndreieck oder Verbandskasten im Fahrzeug in dem örtlichen Fahrzeugregister gespeichert werden dürfen. Die Datenspeicherung halte ich aber nur in den Fällen für erforderlich und mit dem Sinngehalt der Vorschrift des § 3 Abs. 2 Nr. 10 FRV für vereinbar, in denen derartige Fahrzeugmängel Anlaß der Behörde für Maßnahmen gegen den Halter sein sollen. Andernfalls ist eine Datenspeicherung nicht erforderlich und damit unzulässig.

### 5.17.3 Führerscheindatei

Im Gegensatz zu den normenklaren Regelungen zur Datenverarbeitung im örtlichen Fahrzeugregister fehlen immer noch die dringend notwendigen bereichspezifischen gesetzlichen Regelungen zur **Speicherung von Führerscheindaten** (vgl. 9. Tätigkeitsbericht, S. 30). Lediglich in § 10 Abs. 2 der Straßenverkehrs-Zulassungs-Ordnung (StVZO) wird bestimmt, daß die Straßenverkehrsbehörde Listen über vorbereitete Führerscheine und eine Kartei über die ausgehändigten Führerscheine zu führen hat. Die Listen und Karteien sollen eine Übersicht über alle Inhaber gewährleisten.

In den Führerscheindateien werden jedoch auch Vermerke über die Entziehung und vorläufige Entziehung der Fahrerlaubnis gespeichert. In von mir geprüften Fällen lagen die Verwaltungs- und Gerichtsverfahren über 20 Jahre zurück. Die Fahrerlaubnisbehörden sehen sich zur Speicherung dieser Angaben bis zum Tode des Inhabers der Fahrerlaubnis verpflichtet. Ein aus dem Jahr 1974 – also weit vor dem für den Datenschutz grundlegenden Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 – stammender Erlaß des damaligen Ministers für Wirtschaft, Mittelstand und Verkehr des Landes Nordrhein-Westfalen legt für die Aufbewahrung von Führerscheinkarten fest, daß diese erst zwei Jahre nach dem Tode des Inhabers zu vernichten sind. Eine spezielle Löschungsregelung für einzelne Eintragungen ist nicht getroffen.

Die meisten Betroffenen waren davon ausgegangen, daß diese Daten bereits gelöscht sind. Einige der Betroffenen haben von der weiteren Datenspeicherung erfahren, als die Vorfälle gegen sie in einem neuen polizeilichen Ermittlungsverfahren verwendet wurden. Ich habe festgestellt, daß die Daten

über die Altfälle auf Anfrage von der Straßenverkehrsbehörde übermittelt worden waren.

In den Beschwerdefällen bin ich zu dem Ergebnis gelangt, daß eine weitere Speicherung der Angaben über die früheren Verfahren unzulässig ist. Die Vorschrift des § 10 Abs. 2 StVZO kommt für diese Datenspeicherung nicht in Betracht, da hiernach nur Angaben über ausgehändigte und nicht auch über entzogene Führerscheine zu speichern sind. Darüber hinaus kann daher als Auffangnorm nur die Vorschrift des § 24 OBG i.V.m. § 24 Abs. 1 PolG NW entsprechend herangezogen werden. Danach ist das Speichern rechtmäßig erlangter Daten in Akten oder Dateien zulässig, soweit es zur Erfüllung der Aufgaben der Behörde, insbesondere zur zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung, erforderlich ist.

In den von mir beurteilten Fällen konnte die Datenspeicherung nicht mehr als erforderlich angesehen werden, da die Angaben über die früheren Verfahren keine wesentlichen Erkenntnisse zur Kraftfahreignung der Betroffenen erwarten ließen. Von diesem Umstand konnte ausgegangen werden, weil über die Betroffenen eine Führerscheinakte mit den Vorgängen über die Entziehung der Fahrerlaubnis nicht mehr vorhanden war bzw. im Fall der vorläufigen Entziehung der Fahrerlaubnis fast 25 Jahre vergangen waren.

Den Hinweisen auf die Maßnahmen gegen die Betroffenen ist im übrigen nicht zu entnehmen, aus welchen Gründen die Fahrerlaubnis entzogen worden war. Dies kann zur Folge haben, daß über einen Betroffenen ein nicht mehr zutreffendes oder fehlerhaftes Persönlichkeitsbild entsteht. Aus diesem Grund stellt die weitere Datenverarbeitung eine unverhältnismäßige Belastung des Betroffenen dar. Außerdem ist die Speicherung auch zur Gewährleistung der Sicherheit des Straßenverkehrs nicht mehr zwingend geboten.

Dementsprechend habe ich gefordert, daß in den vorliegenden Fällen die Daten entsprechend der Regelung in § 32 PolG NW in der Führerscheindatei gelöscht werden. Diese datenschutzrechtliche Forderung ergibt sich auch aus dem Grundsatz der Verhältnismäßigkeit.

### 5.17.4 Mitteilungen über Fahreignung

Auch das Fehlen bereichspezifischer Regelungen zur Übermittlung von Erkenntnissen und Unterlagen an die Fahrerlaubnisbehörde führt immer wieder zu Unklarheiten und Unsicherheiten über die Zulässigkeit derartiger Mitteilungen. Insbesondere bleibt den Betroffenen dieser Informationsfluß verborgen. Erst wenn die Fahrerlaubnisbehörde unter Hinweis auf die übermittelten Erkenntnisse etwa mit der Aufforderung zur Überprüfung der Fahreignung an die Betroffenen herantritt, erfahren sie von der Datenweitergabe. Auf diese unbefriedigende Situation führe ich den Umstand zurück, daß sich Bürgerinnen und Bürger, aber auch Behörden mit Fragen zur Zulässigkeit derartiger Mitteilungen an mich gewandt haben.

So erlebten **schwerbehinderte Autofahrer** eine böse Überraschung. Nachdem sie sich beim örtlich zuständigen Ordnungsamt um Erteilung eines besonderen Parkausweises für Schwerbehinderte oder um Einrichtung eines

persönlichen Parkplatzes in Wohnungsnähe wegen außergewöhnlicher Gehbehinderung bemüht hatten, erhielten sie wenig später von der Fahrerlaubnisbehörde die Aufforderung, ein ärztliches Gutachten über ihre Fahrtüchtigkeit einzureichen. Den Sachbearbeitern im Ordnungsamt waren auf Grund der Angaben der Betroffenen Bedenken an deren Kraftfahreignung gekommen. Deshalb unterrichteten sie die Fahrerlaubnisbehörde über ihre Erkenntnisse. Die Betroffenen wären nicht aus allen Wolken gefallen, wenn ihnen folgende Umstände klar gewesen wären.

Die Fahrerlaubnisbehörde ist verpflichtet, einem Fahrerlaubnisinhaber die Fahrerlaubnis zu entziehen, wenn er sich als ungeeignet zum Führen von Kraftfahrzeugen erweist (§ 4 Abs. 1 StVG, § 15 b Abs. 1 Satz 1 StVZO). Die Eignung kann u. a. wegen körperlicher oder geistiger Mängel beschränkt oder ausgeschlossen sein (§ 9 StVZO). Die Fahrerlaubnisbehörde ist deshalb auf die Kenntnis von Sachverhalten angewiesen, die Zweifel an der Kraftfahreignung von Fahrerlaubnisinhabern begründen können. Es unterliegt nicht der datenschutzrechtlichen Beurteilung, inwieweit Schwerbehinderungen im Einzelfall Zweifel an der Fahrtauglichkeit rechtfertigen. Jedenfalls kann bei außergewöhnlicher Gehbehinderung nicht ausgeschlossen werden, daß hierdurch der Betreffende ein Fahrzeug nicht mehr sicher im Straßenverkehr führen kann und seine Teilnahme am Straßenverkehr eine konkrete Gefahr für alle Verkehrsteilnehmer darstellt.

Daher durften die für die Erteilung der Parkausweise für Schwerbehinderte und für die Einrichtung von persönlichen Schwerbehindertenparkplätzen zuständigen Stellen ihre Erkenntnisse der Fahrerlaubnisbehörde auf der Grundlage des § 24 OBG i.V.m. § 27 Abs. 1 Satz 1 und 2 PolG NW mitteilen. Danach können zwischen Ordnungsbehörden personenbezogene Daten übermittelt werden, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Es gehört zu den Aufgaben der mit den Anträgen der Schwerbehinderten befaßten Stellen, nach § 14 Abs. 1 OBG die notwendigen Maßnahmen zu treffen, um eine im Einzelfall bestehende Gefahr für die öffentliche Sicherheit und Ordnung abzuwehren. Hierzu kann auch die Übermittlung von Tatsachen, aus denen sich Bedenken gegen die Eignung eines Kraftfahrers ergeben, an die Fahrerlaubnisbehörde gehören.

Wenngleich damit eine ausreichende gesetzliche Grundlage für die Datenübermittlung vorliegt, halte ich es im Hinblick auf das Gebot der Transparenz der Datenverarbeitung für notwendig, den Betroffenen vor der Antragstellung darauf hinzuweisen, daß eine Mitteilung über die Fahreignung an die Fahrerlaubnisbehörde erfolgen kann.

In einem anderen Fall lagen einer Polizeibehörde Erkenntnisse darüber vor, daß ein Fahrerlaubnisinhaber mit **Drogen** handele und sie auch konsumiere und deswegen verschiedene Ermittlungsverfahren der Staatsanwaltschaft wegen Verstoßes gegen das Betäubungsmittelgesetz eingeleitet worden seien. Auf Grund dieser Erkenntnisse waren der Polizei Zweifel an der Kraftfahreignung des Betroffenen gekommen, so daß sie darüber die Fahrerlaubnisbehörde informiert hat.

Die Tatsache, daß jemand als Drogenkonsument in Betracht kommt, kann für die Frage der Kraftfahreignung und damit zur Gewährleistung der Sicherheit der Verkehrsteilnehmer von Bedeutung sein. Darüber wird in dem Gutachten „Krankheit und Kraftverkehr" des Gemeinsamen Beirates für Verkehrsmedizin beim Bundesministerium für Verkehr ausführlich berichtet. Das Gutachten ist den Polizeibehörden und den Fahrerlaubnisbehörden bekannt.

Daher habe ich gegen derartige Mitteilungen der Polizei an die Fahrerlaubnisbehörde grundsätzlich keine datenschutzrechtlichen Bedenken. Mit § 28 Abs. 2 PolG NW ist eine ausreichende Rechtsgrundlage für diese Datenübermittlung vorhanden (vgl. oben S. 48/49). Aber auch hier halte ich es für angezeigt, die Betroffenen über den Übermittlungsvorgang zu unterrichten.

Die Weitergabe eines ärztlichen Attestes durch die Bußgeldstelle an die Fahrerlaubnisbehörde gab Veranlassung für eine weitere Bürgereingabe. Dem Betroffenen war ein **Parkverstoß** vorgehalten worden, wogegen er Einspruch eingelegt hatte. Er legte hierzu ein ärztliches Attest vor, da für die Verkehrsordnungswidrigkeit sein Gesundheitszustand mit ursächlich war. Das Verfahren wurde zwar eingestellt. Aber nach dem vorgelegten ärztlichen Attest erschien der Bußgeldstelle die Fahrtauglichkeit, insbesondere die Reaktionsfähigkeit des Betroffenen erheblich beeinträchtigt. Daher übersandte sie eine Kopie des ärztlichen Attestes an die Fahrerlaubnisbehörde. Diese hat dann den Betroffenen aufgefordert, ein fachärztliches Gutachten beizubringen, um prüfen zu können, ob die in dem Attest aufgeführte Diagnose seine Fahrtüchtigkeit beeinträchtigt.

Auch in diesem Fall war die Datenweitergabe zulässig. Im Unterschied zu den vorstehenden Mitteilungsfällen gilt für die Datenweitergabe durch die Bußgeldstelle das Ordnungswidrigkeitengesetz (OWiG), weil die Bußgeldstelle als Ordnungswidrigkeitenbehörde ausschließlich für die Verfolgung und Ahndung von Ordnungswidrigkeiten zuständig ist, und diese Aufgaben nicht zur Gefahrenabwehr im Sinne des Ordnungsbehördengesetzes gehören.

Dem OWiG – ebenso wie den nach § 46 OWiG anzuwendenden Vorschriften der StPO – ist eine bereichspezifische normenklare Regelung für die Übermittlung von Daten an die für die Gefahrenabwehr zuständigen öffentlichen Stellen – also auch an die Fahrerlaubnisbehörde – nicht zu entnehmen. Nach meinem Kenntnisstand wird allerdings eine derartige Vorschrift im Strafverfahrensänderungsgesetz enthalten sein. Bis zum Erlaß dieses Gesetzes wird die Datenübermittlung hinzunehmen sein, soweit die Bekanntgabe des ärztlichen Attestes an die Führerscheinstelle zur rechtmäßigen Aufgabenerfüllung erforderlich ist. Nach § 4 Abs. 1 StVG, § 15 b StVZO hat die Straßenverkehrsbehörde die Fahrerlaubnis zu entziehen, wenn sich der Inhaber der Fahrerlaubnis zum Führen von Kraftfahrzeugen als ungeeignet erweist.

Obgleich im Einzelfall eine Datenübermittlung zulässig sein kann, muß gewährleistet sein, daß nicht schon in aller Regel in Ordnungswidrigkeitenverfahren bekanntgewordene Tatsachen an die Fahrerlaubnisbehörde übermittelt werden. Auch hier hielte ich es insbesondere wegen der fehlenden bereichspezifischen Regelung für geboten, den Betroffenen darauf hin-

zuweisen, daß das vorgelegte Attest an die Führerscheinstelle weitergegeben werden kann.

## 5.18 Wirtschaft und öffentliche Unternehmen

### 5.18.1 Gewerbemelderegister

Der Entwurf eines Gesetzes zur Änderung der Gewerbeordnung geht davon aus, daß die **Gewerbeanzeigen** in einem Register gespeichert werden, ohne es als solches zu bezeichnen. Das in den meisten Behörden bereits als automatisierte Datei geführte Auskunftsregister erfüllt den Zweck, neben den Gewerbeüberwachungsbehörden auch öffentliche Stellen zu unterrichten, die auf die Kenntnis der anzeigepflichtigen Tatbestände zur eigenen Aufgabenerfüllung angewiesen sind. Aber auch nicht-öffentlichen Stellen sollen – wie bisher schon – Daten aus den Gewerbeanzeigen zugänglich gemacht werden. Im Ergebnis wird mit dem Gesetzentwurf die bisherige Datenübermittlung auf eine normenklare gesetzliche Grundlage gestellt.

Hervorzuheben sind folgende datenschutzrechtlich bedeutsamen Grundsätze.

Im Entwurf werden die öffentlichen Stellen im einzelnen aufgeführt, die regelmäßig Daten aus der Gewerbeanzeige erhalten dürfen. Anderen öffentlichen Stellen dürfen nur die im Gesetz genannten „Grunddaten" übermittelt werden; weitere Daten dürfen nur unter engen Voraussetzungen zur Verfügung gestellt werden.

Auch innerhalb der Verwaltung – etwa von der Gewerbemeldestelle an das Ordnungsamt, Amt für Umweltschutz, Amt für Abfallwirtschaft oder Wirtschaftsförderung – dürfen die Daten unter den im Gesetz aufgeführten Voraussetzungen fließen. Darüber hinaus soll bereits in der künftigen gesetzlichen Regelung unter den verwaltungsinternen Dienststellen ein automatisiertes Abrufverfahren zugelassen werden, soweit es angemessen ist. Schließlich sollen die Angaben über Name, betriebliche Anschrift und ausgeübte Tätigkeit des Gewerbetreibenden zur Übermittlung an nicht-öffentliche Stellen und öffentliche Unternehmen, die am Wettbewerb teilnehmen, bei berechtigtem Interesse zur Verfügung stehen. Für die Übermittlung weiterer Daten muß allerdings ein rechtliches Interesse glaubhaft gemacht werden, und es darf kein überwiegendes schutzwürdiges Interesse des Gewerbetreibenden berührt sein.

Insgesamt handelt es sich um eine Gesetzesnovellierung, die erkennen läßt, daß auch den datenschutzrechtlichen Anforderungen Rechnung getragen werden soll. Neben der datenschutzgerechten Ausgestaltung gewerberechtlicher Vorschriften über die Verarbeitung personenbezogener Daten in gewerberechtlichen Verfahren werden außerdem die Durchführung einer monatlichen bundeseinheitlichen Gewerbeanzeigestatistik angeordnet sowie Voraussetzungen für eine Auskunftserteilung aus dem Gewerbezentralregister für wissenschaftliche Forschungsvorhaben geregelt.

Im Rahmen meiner Kontrolltätigkeit sind im übrigen folgende Fragen zu Auskünften über Gewerbedaten aufgetreten.

Nachdem vielfach Gewerbemelderegister schon automatisiert geführt werden, stellen die Behörden immer mehr die Überlegung an, einen **automatischen Mitteilungsdienst** über die Gewerbeanzeigen an andere öffentliche Stellen einzurichten. Bisher leiten die Behörden je eine Durchschrift der Gewerbeanzeigen auf der Grundlage der Ausführungsanweisung des Ministeriums für Wirtschaft, Mittelstand und Technologie des Landes Nordrhein-Westfalen (MWMT) zu den § 14, 15 und 55 c GewO (SMBl. NW. 71011) folgenden Stellen zu: Landesamt für Datenverarbeitung und Statistik, Finanzamt, Staatliches Gewerbeaufsichtsamt, Industrie- und Handelskammer oder Handwerkskammer, Eichamt, Registergericht, Landesverband Rheinland-Westfalen der gewerblichen Berufsgenossenschaften, Landesarbeitsamt, MWMT, Kreise und kreisfreie Städte als Arznei- und Lebensmittelüberwachungsbehörden sowie als Sonderordnungsbehörden nach dem Abfallrecht, Ausländerbehörde, Behörde oder Stelle, die zur Erteilung einer Erlaubnis oder Zulassung für das angezeigte Gewerbe zuständig ist.

Soweit mit einem automatischen Mitteilungsdienst personenbezogene Gewerbedaten an Stellen außerhalb der Gemeinde übermittelt werden sollen, wäre hierfür nach § 9 Abs. 1 DSG NW eine bereichspezifische Rechtsvorschrift oder nach § 9 Abs. 2 Satz 1 DSG NW eine Rechtsverordnung erforderlich. Das MWMT sieht allerdings von dem Erlaß einer entsprechenden Rechtsverordnung ab, da – wie oben aufgezeigt – eine bereichspezifische gesetzliche Regelung auch für die regelmäßige Übermittlung personenbezogener Daten in gewerberechtlichen Angelegenheiten erarbeitet wird. Unter diesen Umständen würde ich die Einrichtung eines automatischen Mitteilungsdienstes nicht beanstanden, wenn und soweit eine regelmäßige Übermittlung von Daten in dem Umfang erfolgt, wie er in der Ausführungsanweisung zu den § 14, 15 und 55 c GewO bestimmt ist.

Darüber hinaus sind verschiedene Gemeinden bestrebt, daß weitere Stellen innerhalb der Verwaltung an dem automatischen Mitteilungsdienst beteiligt werden, und zwar das Steueramt, Amt für Zivilschutz, Einwohnermeldeamt, Amt für Wirtschaftsförderung, Zulassungsstelle, Liegenschaftsamt, Bauordnungsamt, Tiefbauamt. Soweit automatisierte Datenverarbeitung bei den genannten Ämtern vorhanden ist, soll ein On-line-Zugriff auf das Gewerbemelderegister realisiert werden.

Nach der derzeitigen Rechtslage darf innerhalb einer Gemeindeverwaltung nach § 9 Abs. 4 DSG NW eine regelmäßige Datenübermittlung nur zugelassen bzw. ein automatisiertes Abrufverfahren nur eingerichtet werden, soweit dies unter Berücksichtigung des informationellen Selbstbestimmungsrechts des betroffenen Personenkreises und der Aufgaben der beteiligten Stellen angemessen ist (§ 9 Abs. 2 Satz 2 DSG NW). Bei der Frage der Angemessenheit sind die Grundsätze der Zweckbestimmung der Daten (§ 13 Abs. 1 Satz 2 und 3 DSG NW) und der Erforderlichkeit der Datenübermittlung (§ 14 Abs. 1 Satz 1 DSG NW) zu beachten.

Soweit regelmäßige Mitteilungen aus dem Gewerbemelderegister an das Steueramt erfolgen, halte ich diesen Vorgang für zulässig. Denn mit der Anzeige erfüllt der Gewerbetreibende gleichzeitig seine steuerliche Anzeigepflicht nach § 138 Abs. 1 AO. Danach hat derjenige, der einen Betrieb der Land- und Forstwirtschaft, einen gewerblichen Betrieb oder eine Betriebsstätte eröffnet, dies auf amtlich vorgeschriebenem Vordruck der Gemeinde mitzuteilen. Auf dem Vordruck der Gewerbeanzeige wird darauf hingewiesen, daß mit der Anzeige gleichzeitig der steuerlichen Anzeigepflicht genügt wird. Auch sehe ich die Voraussetzung der Erforderlichkeit der Datenübermittlung als erfüllt an. Nach § 19 Abs. 4 des Gewerbesteuergesetzes kann die Gemeinde für Gewerbebetriebe, die im Laufe des Erhebungszeitraumes neu gegründet werden, Vorauszahlungen der Gewerbesteuer festsetzen. Zur Wahrnehmung dieser Aufgabe ist die Gemeinde auf die Kenntnis von Angaben über Betriebseröffnungen angewiesen.

Dagegen konnte ich eine beabsichtigte Datenübermittlung über einen On-line-Anschluß an das Amt für Zivilschutz, Einwohnermeldeamt, Amt für Wirtschaftsförderung, Liegenschaftsamt, Bauordnungsamt, Tiefbauamt sowie an die Zulassungsstelle nicht als zulässig ansehen, da die Angemessenheit dieser Maßnahmen im Sinne des § 9 Abs. 2 Satz 2 DSG NW nicht überzeugend dargelegt wurde.

Für die Übermittlung bestimmter Daten aus dem Gewerbemelderegister oder sonstigen gewerberechtlichen Unterlagen der Ordnungsbehörden an Berufs- oder Interessenverbände zur Mitgliederwerbung, Markt- oder Meinungsforschungsinstitute, Unternehmen (z. B. Versicherungen, Banken) und andere Gewerbetreibende zur Geschäftsanbahnung weist das MWMT in seinem Runderlaß vom 21. Juni 1990 (SMBl. NW. 7100) darauf hin, daß sich diese Auskunftserteilung nach § 16 DSG NW richtet. Nach § 16 Abs. 1 Satz 1 Buchstabe d DSG NW ist die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs zulässig, wenn u. a. hierfür ein berechtigtes Interesse geltend gemacht wird und der Betroffene in diesen Fällen der Datenübermittlung nicht widersprochen hat.

Hierzu sieht der o.g. Gesetzentwurf allerdings künftig vor, daß für die Zulässigkeit einer Übermittlung von Name, betrieblicher Anschrift und angezeigter Tätigkeit nur noch das berechtigte – also auch ein wirtschaftliches – Interesse an der Kenntnis dieser Daten glaubhaft gemacht werden muß. Dies ist eine gegenüber der bisherigen Regelung offenere Zulässigkeitsvoraussetzung, die der Gewerbemeldestelle die Entscheidung erheblich erleichtert, allerdings dazu führen wird, daß diese Daten vermehrt erfragt und übermittelt werden.

### 5.18.2 Sparkassen

Zwischen Sparkassen, Landesbausparkasse (LBS) und öffentlich-rechtlichen Versicherern (Provinzial) besteht ein **Verbundkonzept**, das sich auf die Vermittlung von Finanzdienstleistungen der jeweils anderen Verbundpartner erstreckt. Eine bekannte Form dieser Zusammenarbeit ist das Sparkassenprodukt der „Finanzierung aus einer Hand". Danach ist die Sparkasse vertrag-

lich ermächtigt, im Namen und für Rechnung der LBS für bestimmte Baumaßnahmen Bausparkredite zu gewähren. Vor jeder Kreditbewilligung informiert sich die Sparkasse bei der LBS über die notwendigen Bauspardaten der Kunden. Soweit die Übermittlung in dem Sofortauskunftssystem erfolgt, das zwischen der Landesbausparkasse und den Sparkassen eingerichtet ist, halte ich nach meinem derzeitigen Erkenntnisstand eine schriftliche Einwilligung der Betroffenen für unerläßlich. Hierauf habe ich in meinem 8. Tätigkeitsbericht (S. 132) hingewiesen. Demgegenüber sehe ich die Übermittlung der aus der Vermittlung des Bausparkredits anfallenden Daten an die LBS von dem Vertragszweck gedeckt, so daß diese Übermittlungsvorgänge auf § 28 Abs. 1 Satz 1 Nr. 1 BDSG gestützt werden können.

Nach meinen Informationen besteht die Absicht, die Zusammenarbeit zwischen den Verbundpartnern Sparkasse, LBS und Provinzial zu intensivieren. Dabei wird auch daran gedacht, die Außendienste von LBS und Provinzial, die von selbständigen Handelsvertretern unterhalten werden, in den Verbund einzubeziehen. Eine Umsetzung dieser Bestrebungen wird von der Zulässigkeit insbesondere des Austauschs von Kundendaten zwischen den Verbundpartnern abhängig sein. Ein derartiger Datenaustausch ist nur mit einer wirksamen Einwilligung der Kunden möglich. Für die Sparkassen und die Landesbausparkasse ergibt sich das Erfordernis einer Einwilligung bereits aus dem Bankgeheimnis.

Die noch zu erarbeitenden Einwilligungserklärungen, die die Datenweitergabe zwischen den Verbundpartnern rechtlich absichern sollen, müssen den Anforderungen an Inhalt und Form einer Einwilligung nach § 4 Abs. 2 BDSG entsprechen. Danach ist der Betroffene auf den Zweck der Speicherung und etwa vorgesehene Übermittlungen sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen (Satz 1). Eine wirksame Einwilligung setzt voraus, daß der Betroffene weiß, welche Daten von welcher Stelle zu welchem Zweck übermittelt werden sollen. Dies gebietet auch der Grundsatz der Transparenz der Datenverarbeitung.

Die Einwilligung bedarf grundsätzlich der Schriftform (§ 4 Abs. 2 Satz 2 BDSG). Soll der Erklärungstext in bestehende Vordrucke aufgenommen werden, so ist dem betroffenen Kunden zwischen der Abgabe und der Nichtabgabe der Erklärung ein Wahlrecht einzuräumen. Darüber hinaus muß der Einwilligungstext im äußeren Erscheinungsbild der Vordrucke hervorgehoben werden (§ 4 Abs. 2 Satz 3 BDSG).

Bei der Ausgestaltung der erforderlichen Einwilligungserklärungen soll das Ergebnis der Erörterungen der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich im „Düsseldorfer Kreis" über die in Versicherungsverträgen verwendeten Klauseln abgewartet werden.

### 5.18.3 Versorgungsunternehmen

Den Gas- und Wasserwerken einer Stadt ist von einem Inkassounternehmen angeboten worden, **uneinbringliche Forderungen** von Stadtwerke-Kunden gegen Erfolgshonorar einzutreiben. Bei den Forderungen handelt es sich um

Fälle, die von den Stadtwerken selbst bis zum Abschluß von Konkursverfahren bzw. Verfahren der eidesstattlichen Versicherung verfolgt worden waren. Die Stadtwerke haben mich um Beratung gebeten, ob dem Inkassounternehmen die entsprechenden Akten über die Forderungsfälle zur Durchführung der Eintreibungsmaßnahmen übergeben werden dürfen.

Sofern die Angaben in den Akten aus Dateien stammen, kann die Datenübermittlung auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG gestützt werden. Es ist davon auszugehen, daß die Stadtwerke zum Zwecke der Beitreibung ausstehender Forderungen ein berechtigtes Interesse an der Datenübermittlung an Inkassounternehmen haben. Eine Datenübermittlung zur Wahrung dieser Interessenlage setzt weiter die Erforderlichkeit dieser Übermittlung voraus. Erforderlich in diesem Fall heißt, die Übermittlung muß zur Wahrung der berechtigten Interessen notwendig sein. Dies kann nur in jedem Einzelfall entschieden werden. So wäre eine Datenweitergabe in den Fällen unzulässig, in denen inzwischen feststeht, daß die ausstehenden Forderungen absolut uneinbringlich sind und auch künftig sein werden. Dieselbe Erwägung gilt allerdings auch für den Umfang der zu übermittelnden Daten. Es muß daher auch geprüft werden, ob die ganze Akte übermittelt werden muß, oder ob nicht ein Auszug aus der Akte ausreicht.

Das Interesse der Stadtwerke ist aber außerdem gegen etwaige schutzwürdige Belange des Betroffenen an dem Ausschluß der Übermittlung abzuwägen. Insoweit muß unter Berücksichtigung der bekannten Umstände geprüft werden, ob Gründe für eine solche Annahme vorliegen. Sofern die beabsichtigte Datenweitergabe erst nach Abschluß von Konkursverfahren bzw. Verfahren der eidesstattlichen Versicherung erfolgt, sind diese Umstände objektiv zu der Feststellung geeignet, daß die Forderungen der Stadtwerke gegenüber dem Schuldner zu Recht bestehen. Daher kann in diesen Fällen die Datenübermittlung in aller Regel gerechtfertigt sein.

Das Inkassounternehmen ist darauf hinzuweisen, daß es die übermittelten Daten nur für den Zweck verarbeiten oder nutzen darf, zu dessen Erfüllung sie ihm übermittelt wurden (§ 28 Abs. 4 BDSG). Eine Verarbeitung oder Nutzung für andere Zwecke muß durch eine entsprechende Vertragsregelung zwischen den Stadtwerken und dem Inkassounternehmen ausgeschlossen werden. Auch der Betroffene sollte im Hinblick auf den verfassungsrechtlichen Grundsatz der Transparenz der Datenverarbeitung im Falle der Übermittlung über diese Tatsache vorher unterrichtet werden.

## 5.19 Telekommunikation

Im Berichtszeitraum sind die in meinem 10. Tätigkeitsbericht (S. 22/23) angekündigten Datenschutzverordnungen auf Grund des § 30 Abs. 2 Postverfassungsgesetz in Kraft getreten. Seit dem 1. Juli 1991 gilt die „Verordnung über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM" (**TELEKOM-Datenschutzverordnung – TDSV**) vom 29. Juni 1991. Sie löste die im Fernmeldeverkehr geltenden Datenschutzbestimmungen der Telekommunikationsordnung (TKO) ab, die mit Ablauf des

30. Juni 1991 außer Kraft trat. Die TDSV regelt den Schutz personenbezogener Daten der am Fernmeldeverkehr Beteiligten für den Bereich der Deutschen Bundespost TELEKOM. Für Telekommunikationsleistungen, die von privaten Unternehmen erbracht werden, gilt die „Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsleistungen erbringen" (**Teledienstunternehmen-Datenschutzverordnung – UDSV**) vom 28. Dezember 1991.

Die Datenschutzbeauftragten des Bundes und der Länder äußerten sich in ihrer Entschließung vom 8. März 1991 (Anlage 7, S. 167 bis 169) zu den wesentlichen Mängeln der damaligen Entwürfe. Die von ihnen erhobenen Forderungen wurden in den verabschiedeten Verordnungen nur unzureichend berücksichtigt.

So enthält die TDSV insbesondere folgende Defizite:

- Entgegen der Forderung der Datenschutzbeauftragten, alle **Verbindungsdaten** nach dem Ende der Verbindung zu löschen und nur die für die Entgeltabrechnung unerläßlichen Daten verkürzt zu speichern, darf die Deutsche Bundespost TELEKOM sämtliche Verbindungsdaten zum Zweck der Berechnung der Entgelte nutzen. Sie müssen erst 80 Tage nach Versendung der Entgeltrechnung gelöscht werden.

- Die Deutsche Bundespost TELEKOM darf ihrem Kunden die gespeicherten Daten derjenigen Verbindungen mitteilen, für die er entgeltpflichtig ist (**Einzelentgeltnachweis**). Der Angerufene muß die Speicherung seiner Rufnummer während dieser Zeit hinnehmen, ohne darauf Einfluß nehmen zu können. Ausnahmen gelten lediglich für „Anrufe bei Personen, Behörden und Organisationen, die selbst oder deren Mitarbeiter besonderen Verschwiegenheitsverpflichtungen unterliegen und die Beratungsaufgaben in sozialen oder kirchlichen Bereichen ganz oder überwiegend über Telefon abwickeln". Diese können beantragen, daß ihre Telefonnummern nicht auf Telefonrechnungen erscheinen. Da eine abschließende Regelung, welchen Einrichtungen das Antragsrecht zusteht, nicht getroffen ist, bleibt offen, wo die Grenze zu ziehen ist: Fallen etwa allgemeine Beratungsstellen, die auch in sozialen oder kirchlichen Bereichen beraten, unter die Regelung? Sind Stellen, bei denen die persönliche Beratung überwiegt, nicht antragsberechtigt?

- Bei entsprechender technischer Ausstattung des Telefonapparates gibt es eine **Rufnummernanzeige.** Dabei erscheint die Telefonnummer des Anrufers auf dem Display des Apparates des Angerufenen. Nach der geltenden Regelung hat der Anrufer lediglich die Wahlmöglichkeit zwischen der Anzeige seiner Rufnummer bei jedem Anruf oder dem dauernden Ausschluß der Anzeige. Aus datenschutzrechtlicher Sicht muß dem Anrufer dagegen das Recht zugebilligt werden, bei jedem einzelnen Telefonat darüber zu entscheiden, ob er sich identifiziert. Die TDSV sieht die Einräumung einer Wahlmöglichkeit für den einzelnen Anruf erst ab 1. Januar 1994 vor.

Da der Inhalt der UDSV sich weitgehend mit dem der TDSV deckt, verweise ich auf meine obige Bewertung. Die UDSV enthält gegenüber der TDSV datenschutzrechtliche Verbesserungen insoweit, als die Verbindungsdaten dort abschließend aufgezählt werden und das Bundesministerium für Post und Telekommunikation nicht die Erhebung und Verarbeitung weiterer Verbindungsdaten zulassen darf. Außerdem wurde die der Deutschen Bundespost TELEKOM für die technische Realisierung der Rufnummernunterdrükkung bei Beratungsstellen eingeräumte Übergangsfrist bis 1. Juli 1992 den privaten Anbietern von Telekommunikationsleistungen nicht zugebilligt. Der Bundesrat hat die Bundesregierung in seinem Beschluß vom 27. September 1991 (Bundesratsdrucksache 416/91) aufgefordert, die TDSV den für die UDSV vorgeschlagenen Änderungen anzupassen.

In dem vorgenannten Beschluß hat der Bundesrat außerdem gefordert, § 12 des Fernmeldeanlagengesetzes (FAG) im Hinblick auf die durch die Einführung von ISDN eingetretene neue Situation zu ändern. Nach dieser Vorschrift kann in strafgerichtlichen Untersuchungen der Richter, bei Gefahr im Verzug auch die Staatsanwaltschaft **Auskunft über den Fernmeldeverkehr** verlangen. Da im ISDN-Netz die Verbindungsdaten aller über das Telefon laufenden Kontakte gespeichert werden, könnte § 12 FAG eine ursprünglich nicht vorgesehene neue Qualität erhalten. Nach dem Willen des Bundesrates soll der Gesetzgeber deshalb eine Neuregelung vornehmen, mit der die Eingriffsmöglichkeiten – abgestimmt mit den Vorschriften der Strafprozeßordnung – unter engen Voraussetzungen und abschließend festgelegt werden.

Der im Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG), Bundestagsdrucksache 12/989, vorgesehene § 12 a FAG sah vor, daß die Überwachung und Aufzeichnung des Fernmeldeverkehrs angeordnet werden darf, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leben, Leib oder Freiheit einer Person erforderlich ist. Die zwischenzeitlich in Kraft getretene Fassung des OrgKG vom 15. Juli 1992 enthält dagegen keine Bestimmung zur Änderung des Fernmeldeanlagengesetzes.

Am 25. März 1992 entschied das Bundesverfassungsgericht (NJW 1992, S. 1875), daß die Deutsche Bundespost TELEKOM ohne gesetzliche Grundlage handelt, wenn sie im Auftrag eines Kunden anonyme Telefonanrufer über Fangschaltungen und Zählervergleichseinrichtungen identifiziert. Zwar sehe die TDSV derartige Eingriffe in das Grundrecht des Fernmeldegeheimnisses vor. Es fehle jedoch an der dafür erforderlichen gesetzlichen Ermächtigung. Das Bundesverfassungsgericht hat den Gesetzgeber aufgefordert, alsbald einen verfassungsmäßigen Zustand herzustellen. In der Übergangszeit ist die TDSV nur eingeschränkt anwendbar.

Nach mir vorliegenden Informationen wird die vom Bundesverfassungsgericht geforderte Ermächtigungsgrundlage derzeit vom Bundesministerium für Post und Telekommunikation erarbeitet.

Die Rechtsprechung des Bundesverfassungsgerichts sollte Anlaß sein, die Regelungen der Verarbeitung von Verbindungsdaten in der TDSV und der

UDSV neu zu überdenken. Aus datenschutzrechtlicher Sicht sollte die gesetzliche Grundlage selbst grundlegende inhaltliche Feststellungen dazu enthalten, in welchem Umfang die Netzbetreiber und Diensteanbieter personenbezogene Daten ihrer Kunden verarbeiten dürfen. Dabei sollte von dem Grundsatz ausgegangen werden, daß die Verbindungsdaten nach dem Ende der Verbindung zu löschen sind.

Außerdem müßte die gesetzliche Regelung der Datenverarbeitung in der Telekommunikation auch einheitliche Verarbeitungsregeln für die Sprachkommunikation und sonstige Dienste (z. B. Telefax, Telebox u. a.) enthalten. Die Unterscheidung zwischen der Sprachkommunikation und sonstigen Diensten in TDSV und UDSV kann vor dem Hintergrund der technischen Entwicklung nicht mehr aufrechterhalten werden.

Letztlich dürfte die Entscheidung des Bundesverfassungsgerichts deutlich gemacht haben, daß § 12 FAG im Zuge der Digitalisierung der öffentlichen Telekommunikationsnetze wegen seiner dadurch gewonnenen Reichweite kaum mehr als verfassungsmäßig angesehen werden kann. Er sollte deshalb den neuen technischen Möglichkeiten angepaßt werden.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich im Berichtszeitraum außerdem mit dem Thema „Datenschutz bei internen Telekommunikationsanlagen" befaßt. Der zunehmende Einsatz digitaler Telekommunikationsanlagen in den Verwaltungen birgt die Gefahr von Eingriffen in das Fernmeldegeheimnis sowie den Schutzbereich des nichtöffentlich gesprochenen Wortes von Arbeitnehmern und Dritten, die anrufen oder angerufen werden. Die Datenschutzbeauftragten fordern deshalb, daß umgehend datenschutzrechtliche Regelungen für den Einsatz und die Nutzung interner Telekommunikationsanlagen mit einer bereichspezifischen Rechtsgrundlage für die Verarbeitung von Arbeitnehmerdaten geschaffen werden. Den Wortlaut der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 enthält die Anlage 8, S. 169/170.

# 6. Organisatorische und technische Maßnahmen

## 6.1 Einsatz von persönlichen Computern (PCs)

### 6.1.1 Programmviren

Über Programmviren und mögliche Maßnahmen dagegen informierte ich erstmals im Jahr 1986 in meinem 7. Tätigkeitsbericht. Da in den Jahren 1990/1991 eine deutliche Zunahme der Zahl der Berichte über Programmviren festzustellen war, hielt ich es für erforderlich, durch eigene Erhebungen Kenntnisse darüber zu gewinnen, in welchem Umfang im Landesbereich Nordrhein-Westfalen damit zu rechnen ist, daß PCs von Programmviren befallen sind.

Eine Ende 1991 durchgeführte Prüfung bei zwölf unterschiedlichen öffentlichen Stellen führte zu einem beunruhigenden Ergebnis. Der Anteil der im Rahmen der Überprüfung als infiziert festgestellten PCs an den insgesamt überprüften PCs war nicht unerheblich. Einzelheiten der Prüfung und vor allem auch ergänzende Beobachtungen werden im folgenden dargestellt.

Nach diesen Feststellungen war es angemessen, systematisch und koordiniert gegen die Virengefahr anzugehen. Im Hinblick auf seine Zuständigkeit für die Koordinierung der automatisierten Datenverarbeitung (§ 4 Abs. 1 Satz 1 ADV-Organisationsgesetz NW) unterrichtete ich daher das Innenministerium über die durchgeführten Untersuchungen, über meine Beobachtungen und die daraus resultierenden Empfehlungen und regte koordinierte Maßnahmen zur Bekämpfung von Programmviren unter Berücksichtigung dieser Empfehlungen an. Ich regte darüber hinaus an, in diese Maßnahmen im Rahmen der bestehenden Möglichkeiten auch die Gemeinden und Gemeindeverbände sowie die sonstigen Behörden und Körperschaften, die der Aufsicht des Landes unterstehen, einzubeziehen. Eine abschließende Stellungnahme zu meinen Anregungen liegt mir bisher nicht vor.

#### 6.1.1.1 Überprüfung zahlreicher PCs

Im August 1991 wurde in der Fachpresse über Untersuchungen berichtet, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) bei Bundesbehörden durchgeführt hatte. Es wurde berichtet, das BSI habe in etwa zwei Prozent der untersuchten PCs Programmviren festgestellt. Diese Aussage war alarmierend. Bei einer Befallsrate der PCs von zwei Prozent ist die Datensicherheit bei der Arbeit mit PCs als erheblich beeinträchtigt anzusehen.

Daher sollten durch eigene Erhebungen Kenntnisse darüber gewonnen werden, inwieweit auch im Landesbereich Nordrhein-Westfalen damit zu rechnen ist, daß PCs von Programmviren befallen sind. Für diese Erhebungen stellte das BSI auf meine Bitte kostenlos eine aktuelle Version seines Virensuchprogramms zur Verfügung. Das **Virensuchprogramm** gestattet die Untersuchung von PCs, die unter DOS arbeiten.

Es war mein Ziel, mit diesem Virensuchprogramm Prüfungen bei einer Reihe möglichst unterschiedlicher öffentlicher Stellen des Landesbereichs und innerhalb dieser Stellen bei möglichst unterschiedlichen Organisationseinheiten durchzuführen. Die Prüfungen sollten ausschließlich mit Zustimmung der Leitung der jeweiligen Stellen durchgeführt werden.

Bei meinen Anfragen fand ich in jedem Fall starke Resonanz bei den angesprochenen Behörden und Körperschaften. Es bestanden großes Interesse und große Bereitschaft, mich bei meinem Anliegen zu unterstützen, eine für den Landesbereich Nordrhein-Westfalen nutzbare Aussage über die Bedeutung der Gefahr der Programmviren zu gewinnen. Interesse bestand im allgemeinen aber auch daran, ein Bild der Situation im eigenen Hause zu erhalten.

Prüfungen wurden bei zwölf sehr unterschiedlichen öffentlichen Stellen durchgeführt. Bei jeder dieser Stellen wurden innerhalb der für die Prüfung zur Verfügung stehenden Zeit – in den meisten Fällen innerhalb eines Tages – möglichst viele PCs bei möglichst unterschiedlichen Organisationseinheiten geprüft. Insgesamt wurden 256 PCs im Rahmen dieser Aktion geprüft.

Die Prüfung führte zu einem beunruhigenden Ergebnis:

Der Anteil der im Rahmen der Überprüfung als infiziert festgestellten PCs war erheblich; er lag deutlich höher als fünf Prozent der insgesamt überprüften PCs. Die Angabe eines genauen Prozentsatzes ist allerdings ohne Aussagewert, da die Prüfung schon wegen ihres notwendigerweise begrenzten Umfangs keinesfalls in dem Sinne repräsentativ war, daß daraus eine aussagefähige Prozentzahl für den Landesbereich abgeleitet werden könnte.

#### 6.1.1.2 Allgemeine Feststellungen

Das Bild der Situation, die bei den Prüfungen vorgefunden wurde, wird aus einer Reihe ergänzender Feststellungen deutlich.

- Bei der Virenproblematik handelte es sich nicht um ein Phantom, sondern um eine reale Gefährdung der Datensicherheit.

  Sehr häufig konnten Bedienstete der überprüften Stellen von eigenen Erfahrungen mit Viren berichten. Immer wieder wurde auch berichtet, man habe in der Vergangenheit bereits Veranlassung gesehen, Virentests durchzuführen und gefundene Viren zu beseitigen.

  Das Bild, das sich bei der Prüfung ergab, war daher eine Momentaufnahme in einer sich ständig ändernden Situation. Gefunden wurden fast nur Viren, die z. Z. inaktiv waren. Aktive Viren waren, sobald sie erkannt wurden, jeweils kurzfristig beseitigt worden.

- Die Wahrscheinlichkeit, im Rahmen der Prüfung bei einem PC ein Virus zu finden, hing offensichtlich von der Intensität der Eigenvorsorge der öffentlichen Stelle oder auch von der Initiative der Bediensteten von Organisationseinheiten innerhalb der öffentlichen Stelle ab.

Einige öffentliche Stellen betrieben die Aktionen gegen Programmviren bereits mit großer Systematik und Konsequenz. Auffallend war auch, wie häufig einzelne Organisationseinheiten innerhalb einer öffentlichen Stelle angetroffen wurden, in denen die Leitung oder besonders interessierte Bedienstete aus eigener Initiative ein Prüfprogramm zum Virentest einsetzten. Wenngleich auch in diesen Fällen keine absolute Sicherheit gewährleistet werden konnte, ergab sich doch, daß bei konsequenter Anwendung geeigneter Maßnahmen die Wahrscheinlichkeit des Virenbefalls besonders gering war.

- Sehr häufig wurde von der öffentlichen Stelle oder von deren Bediensteten der Wunsch nach Unterstützung bei eigenen Aktionen gegen die Virengefahr geäußert.

  Vor allem wurde nach einer Empfehlung gefragt, welches Virensuchprogramm man einsetzen solle. Gefragt wurde aber auch nach weiteren sinnvollen Maßnahmen zur Vorbeugung und nach den erforderlichen Maßnahmen, falls ein Programmvirus nachgewiesen wird. Unsicherheit bestand schließlich auch bezüglich des angemessenen Umfanges der Aktivitäten gegen Programmviren.

- Eine besondere Rolle spielte, daß die Hersteller von Programmen teilweise in den Speicherbereichen für Datum und Uhrzeit eigene Angaben ablegen.

  Es gibt Programmviren, die Datum oder Uhrzeit der letzten Dateiänderung mit einem ungültigen Wert versehen, um daraus erkennen zu können, ob ein Programm bereits durch sie infiziert wurde. Das eingesetzte Virensuchprogramm überprüfte daher zusätzlich Datum und Uhrzeit auf gültige Werte, um auch derartige Hinweise auswerten zu können.

  In einer größeren Zahl von Fällen wurde ein ungültiges Datum oder eine ungültige Uhrzeit der letzten Dateiänderung vorgefunden. Ein wirklicher Hinweis auf ein Virus ergab sich aber in keinem dieser Fälle, da sich jeweils herausstellte, daß der ungültige Wert im Rahmen der normalen Bearbeitung – im allgemeinen vom Hersteller des Programms – absichtlich gespeichert worden war, um dadurch ein auswertbares Kennzeichen zu setzen.

#### 6.1.1.3 Empfehlungen

Aus meinen Beobachtungen leitete ich eine Reihe von Empfehlungen ab:

a) Es sollte eine Überprüfung der auf dem Markt erhältlichen Virensuchprogramme erfolgen mit dem Ziel, eines oder einige dieser Programme zum Einsatz bei den öffentlichen Stellen des Landesbereichs zu empfehlen.

b) Den öffentlichen Stellen des Landesbereichs sollten konkrete Maßnahmen zur Vorbeugung gegen einen Befall von PCs durch Programmviren empfohlen werden. Beispiele dafür sind etwa:

   - Regelmäßige Überprüfung aller PCs mit einem Virensuchprogramm,
   - Überprüfung fremder Disketten – insbesondere Programmdisketten – vor deren Nutzung,

- Verbot der Nutzung privater Disketten,
- Verbot der Nutzung dienstlicher Disketten auf privaten PCs,
- Nutzung von Programmdisketten nur mit Schreibschutz,
- Maßnahmen der Zugangs- und Zugriffskontrolle bei PCs,
- Verbot der Verwendung von Software einer nicht vertrauenswürdigen Stelle.

c) Es sollten Maßnahmen genannt werden, die zu treffen sind, falls auf einem PC ein Virus festgestellt wird.

d) Es ist davon auszugehen, daß zahlreiche – vor allem kleinere – öffentliche Stellen die Technik ihrer PCs und des Betriebssystems nur insoweit beherrschen, als dies für deren Anwendung im normalen Betrieb erforderlich ist. Daher könnte es zweckmäßig sein, zentrale Ansprechpartner für die Beratung bei der Beseitigung von Programmviren zu benennen.

e) Es sollte vorgeschrieben werden, daß Programme nur von einem solchen Hersteller bezogen werden dürfen, der gewissen Anforderungen genügt. Derartige Anforderungen könnten etwa sein:

- Prüfung aller gelieferten Programme durch ein Virensuchprogramm beim Hersteller,
- Versiegeln von Programmen durch Zuordnung einer Prüfzahl und Mitlieferung der Prüfsoftware,
- Verzicht auf Speicherung unzulässiger Angaben in Datum oder Uhrzeit.

f) Es könnte überlegt werden, entsprechende Vorsichtsmaßnahmen bei jedem Programmaustausch vorzusehen.

### 6.1.2 Private PCs

Mit dem Einsatz von PCs, die sich nicht im Eigentum der öffentlichen Stelle befinden (private PCs), für dienstliche Zwecke sind spezifische Gefährdungen der Datensicherheit verbunden. Unter Hinweis auf diesen Sachverhalt hatte ich bereits im Juli 1990 das Innenministerium im Hinblick auf seine Zuständigkeit für die Koordinierung der automatisierten Datenverarbeitung (§ 4 Abs. 1 Satz 1 ADV-Organisationsgesetz NW) gebeten, sich für eine innerhalb der Landesverwaltung einheitliche Lösung der angesprochenen Problematik einzusetzen. Ich hatte empfohlen zu prüfen, ob der Einsatz privater PCs ausnahmslos untersagt werden könne. Für den Fall, daß es als unumgänglich angesehen werden sollte, Ausnahmen von einem derartigen Verbot zuzulassen, hatte ich weitere Empfehlungen ausgesprochen. Eine Antwort erhielt ich im Rahmen der Stellungnahme der Landesregierung zu meinem 10. Tätigkeitsbericht, jedoch wurden dabei nur Einzelfragen angesprochen.

Weitere Eingaben und Beratungsersuchen veranlaßten mich in der Zwischenzeit, meine Empfehlungen zu konkretisieren und mit einigen öffentlichen Stellen zu erörtern. Dabei erwies sich, daß die Empfehlungen praxisgerecht sind und in den jeweiligen Dienstanweisungen berücksichtigt werden sollten.

Bestätigt wurde auch meine Ansicht, daß der Einsatz privater PCs nach Möglichkeit untersagt und nur in Ausnahmefällen zugelassen werden sollte, wenn dies dienstlich erforderlich ist. So erklärte sich das Finanzministerium inzwischen bereit, nach Abschluß der Ausstattung der Betriebsprüfer mit tragbaren Personalcomputern den Einsatz privateigener DV-Geräte grundsätzlich zu untersagen und nur noch die Textverarbeitung zuzulassen.

#### 6.1.2.1 Spezifische Gefährdungen

Der Einsatz eines privaten PCs für dienstliche Zwecke kann nicht einfach der Benutzung eines privaten Bleistifts oder eines privaten Taschenrechners für dienstliche Zwecke gleichgesetzt werden. Es gibt vielmehr spezifische Gefährdungen der Datensicherheit, die mit der Nutzung eines privaten PCs für dienstliche Zwecke verbunden sind. Im Hinblick auf diese Gefährdungen der Datensicherheit bedarf der Einsatz privater PCs zur Verarbeitung dienstlicher personenbezogener Daten der ausdrücklichen Regelung.

Derartige **Gefährdungen** sind insbesondere:

- Fehlen einer jederzeitigen Verfügungsmöglichkeit der öffentlichen Stelle über die gespeicherten Daten, da das Speichermedium nicht Eigentum der öffentlichen Stelle ist,
- Fehlen von Hilfsmitteln oder Kenntnissen bei den Bediensteten zum Löschen der Daten und daher Übernahme des PCs in den privaten Bereich ohne vorheriges Löschen oder nach unvollständigem Löschen (vgl. unten S. 149; 10. Tätigkeitsbericht, S. 147),
- Möglichkeit der alternierenden Nutzung des PCs für dienstliche Zwecke und im privaten Bereich, obgleich in dem PC dienstliche personenbezogene Daten gespeichert sind,
- unrealistische Vorstellungen über die Wirksamkeit von Sicherungstechniken bezüglich der dadurch erreichten Sicherheit gespeicherter personenbezogener Daten,
- Möglichkeit der Beschädigung des Datenbestandes,
- überraschend auftretende Notwendigkeit einer Reparatur des PCs wegen eines Defekts von Platte oder Elektronik, wobei durch den Defekt das Löschen gespeicherter Daten verhindert wird und
- fehlendes Wissen über die mit der Nutzung eines privaten PCs verbundenen Gefährdungen der Datensicherheit bei der genehmigenden Person.

#### 6.1.2.2 Allgemeine Voraussetzungen für die Zulässigkeit der Nutzung privater PCs

In meinem 10. Tätigkeitsbericht (S. 144 bis 148) wurde eingehend begründet, daß es sich beim Einsatz eines privaten PCs durch Bedienstete der öffentlichen Stelle zur Verarbeitung dienstlicher personenbezogener Daten im allgemeinen um eine Datenverarbeitung der öffentlichen Stelle handeln muß, da Übermittlung (§ 3 Abs. 2 Nr. 4 DSG NW) an Bedienstete als Privatpersonen unzulässig sein und Datenverarbeitung im Auftrag (§ 11 DSG NW) praktisch

nicht vorkommen wird. Als Voraussetzung der Zulässigkeit der Verarbeitung dienstlicher personenbezogener Daten auf einem privaten PC muß daher feststehen, daß es sich bei dieser Arbeit um eine Arbeit der öffentlichen Stelle handelt. Das bedeutet jedenfalls:

- Die öffentliche Stelle muß wissen, daß auf dem privaten PC dienstliche personenbezogene Daten verarbeitet werden.
- Die Daten müssen jederzeit der Weisungsbefugnis der öffentlichen Stelle unterliegen. Insbesondere muß es möglich sein, die Herausgabe und Löschung durchzusetzen.

#### 6.1.2.3 Dienstliche Nutzung im privaten Bereich

Falls eine Verarbeitung dienstlicher personenbezogener Daten im privaten Bereich nur deshalb erfolgt, weil Bedienstete im privaten Bereich über einen PC verfügen, während ihnen dienstlich kein PC zur Verfügung gestellt wird, könnte die damit verbundene Gefährdung der Datensicherheit durch Anschaffung eines dienstlichen PCs beseitigt werden. Eine solche Anschaffung wäre in diesem Fall grundsätzlich eine angemessene Maßnahme zur Verbesserung der Datensicherheit. Daraus folgt, daß es im allgemeinen unzulässig ist, nur deshalb dienstliche personenbezogene Daten im privaten Bereich zu verarbeiten, weil dort ein PC zur Verfügung steht. Die Nutzung eines privaten PCs zur Verarbeitung dienstlicher personenbezogener Daten im privaten Bereich darf daher allenfalls in dem Umfang zugelassen werden, in dem dies aus anderen Gründen erforderlich ist.

Es gibt Arbeitsgebiete, auf denen generell erwartet wird, daß dienstliche Arbeiten im privaten Bereich durchgeführt werden. So sind z. B. Lehrkräfte im allgemeinen darauf angewiesen, dienstliche Arbeiten im privaten Bereich zu erledigen. In derartigen Fällen sollten nur dann private PCs verwendet werden dürfen, wenn die im folgenden genannten Minimalanforderungen insgesamt erfüllt werden.

Wie oben (S. 129) dargelegt wurde, ist – auch bei einer Arbeitsdurchführung im privaten Bereich – davon auszugehen, daß es sich um eine Datenverarbeitung der öffentlichen Stelle handelt. Die öffentliche Stelle ist daher für die Datensicherheit bei dieser Verarbeitung verantwortlich. Die Nutzung von privaten PCs durch Bedienstete zur Verarbeitung dienstlicher personenbezogener Daten im privaten Bereich bedarf daher der (schriftlichen) Genehmigung. Eine Kopie der Genehmigung muß bei der Dienststelle abgelegt werden, damit es jederzeit möglich ist nachzuweisen, in welchen Fällen eine derartige Genehmigung erteilt wurde.

Die Genehmigung sollte nur unter folgenden Voraussetzungen erteilt werden dürfen:

- Es muß gewährleistet sein, daß die öffentliche Stelle jederzeit über die gespeicherten personenbezogenen Daten verfügen kann. Möglichkeiten dafür sind etwa:

Die Daten dürfen nur auf Disketten gespeichert werden, und es wird nur die Verwendung von Disketten zugelassen, die sich im Eigentum der öffentlichen Stelle befinden.

Bei einer Speicherung auf der Festplatte (oder Wechselfestplatte) des PCs müßte ein Vertrag geschlossen werden, der die Rechte der öffentlichen Stelle sichert.

- Die gespeicherten Daten müssen gegen unbefugten Zugriff gesichert werden. Möglichkeiten dazu sind etwa:

  Bei ausschließlicher Speicherung auf Diskette oder Wechselfestplatte ist es möglich, dieses Speichermedium bei Abwesenheit unter Verschluß zu halten.

  Beim Speichern auf der Festplatte des PCs müssen die Bediensteten sich verbindlich äußern, wie sie den unbefugten Zugriff verhindern.

- Gespeicherte dienstliche personenbezogene Daten müssen gelöscht sein, bevor das Speichermedium wieder in den privaten Bereich übernommen oder sonstigen Dritten verfügbar gemacht wird.

- Die Bediensteten müssen in der Lage sein, die gespeicherten personenbezogenen Daten zu löschen. Sie sollten der öffentlichen Stelle gegenüber schriftlich das Verfahren nennen, wie sie die gespeicherten personenbezogenen Daten löschen werden.

- Es muß festgelegt werden, welche dienstlichen personenbezogenen Daten auf dem privaten PC durch Bedienstete im privaten Bereich verarbeitet werden dürfen.

- Die Beschreibungen der Dateien der gespeicherten personenbezogenen Daten müssen dem Landesbeauftragten für den Datenschutz vorgelegt werden. Die öffentliche Stelle ist speichernde Stelle.

- Die Möglichkeit der Auskunfterteilung an Betroffene muß gewährleistet sein.

- Die gespeicherten personenbezogenen Daten sind zum frühest möglichen Zeitpunkt zu löschen.

- Verarbeitungen mit verbindlicher Verarbeitungslogik, d. h. Verarbeitungen, deren Verarbeitungslogik für die öffentliche Stelle vorgeschrieben ist oder von der öffentlichen Stelle verbindlich zugesagt wurde, sollten im privaten Bereich nicht zugelassen werden, da die öffentliche Stelle gewährleisten muß, daß diese Verarbeitungslogik eingehalten wird.

#### 6.1.2.4 Dienstliche Nutzung im dienstlichen Bereich

Im dienstlichen Bereich sollten im Regelfall ausschließlich PCs der öffentlichen Stelle zur Verarbeitung dienstlicher personenbezogener Daten genutzt werden dürfen. Die Nutzung privater PCs sollte im dienstlichen Bereich nur in besonders begründeten Ausnahmefällen zugelassen sein.

Für den im dienstlichen Bereich eingesetzten privaten PC sollten nicht nur die Regelungen sinngemäß gelten, die bei der dienstlichen Nutzung eines privaten PCs im privaten Bereich einzuhalten sind. Zusätzlich sollten darüber hinaus vielmehr Regelungen folgenden Inhalts schriftlich mit den Bediensteten vereinbart werden:

- Die öffentliche Stelle sollte die uneingeschränkte Verfügungsgewalt über den PC und alle in ihm gespeicherten Daten und Programme haben.
- Die Dienstanweisung, die sonstigen organisatorischen und technischen Maßnahmen zum Gewährleisten der Datensicherheit und die Kontrollbefugnis der öffentlichen Stelle und des Landesbeauftragten für den Datenschutz sollten uneingeschränkt für den privaten PC gelten.

## 6.2 Netze

### 6.2.1 Sicherheit bei Verwendung von Netzknoten

Es ist üblich, daß Datenzentralen mit den an sie angeschlossenen Anwendern über ein Datennetz aus fest geschalteten Fernsprechleitungen verbunden sind. Falls die Anwender räumlich über eine große Fläche verteilt sind – etwa bei einer kommunalen Datenzentrale, an die die Gemeinden eines Kreises angeschlossen sind – ist dazu ein Datennetz großer Ausdehnung erforderlich. Um Leitungs- und Anlagekosten zu sparen, wird im allgemeinen darauf verzichtet, jedes einzelne Datenendgerät durch eine eigene Leitung direkt an die Datenverarbeitungsanlage der Datenzentrale anzuschließen. Es wird vielmehr von der Datenzentrale eine geringere Anzahl von Leitungen zu entfernten Netzknoten geführt. Von jedem Netzknoten gehen dann Leitungen zu den Anwendern oder auch zu weiter entfernten Netzknoten.

Sehr häufig werden als Netzknoten **Schnittstellenvervielfacher** eingesetzt. Bei deren Verwendung – etwa bei Verwendung des Schnittstellenvervielfachers SK 12 der Deutschen Bundespost TELEKOM (SK 12) – ist die Datensicherheit aber beeinträchtigt. Der SK 12 überträgt Daten, die von einer Datenverarbeitungsanlage an eine hinter dem SK 12 angeschlossene Datenendeinrichtung gesendet werden, in alle hinter dem SK 12 angeschlossenen Leitungen. Dadurch kann ein Endgerät nicht nur die für dieses Gerät bestimmten Daten empfangen, sondern nach Manipulation an dem Endgerät oder durch Aufschalten eines Leitungsmonitors können auch alle Daten empfangen werden, die für irgendwelche anderen Endgeräte bestimmt sind, die hinter dem SK 12 angeschlossen sind. Diese Gefährdung der Datensicherheit ist für die Benutzer nicht ohne weiteres ersichtlich.

Eine grundsätzliche Wertung dieser Problematik enthält bereits mein 7. Tätigkeitsbericht (S. 159 bis 162). Meine darin geäußerten Bedenken gegen den Einsatz des Schnittstellenvervielfachers SK 12 der Deutschen Bundespost TELEKOM werden von der Landesregierung geteilt (vgl. ihre Stellungnahme zu meinem 7. Tätigkeitsbericht – Drucksache 10/1644, S. 34/35 ).

Bei dem Kontrollbesuch bei einer kommunalen Datenzentrale stellte ich jetzt fest, daß deren Datennetz noch immer eine größere Zahl von Schnittstel-

lenvervielfachern enthält. Eingesetzt werden sowohl Schnittstellenvervielfacher des Typs SK 12 der Deutschen Bundespost TELEKOM als auch solche eines anderen Unternehmens. Die Datenzentrale berichtete, die Schnittstellenvervielfacher des anderen Unternehmens arbeiteten nach demselben Prinzip wie der SK 12. Die o. a. Bedenken gegen die Arbeit des SK 12 gelten daher ebenfalls für diesen anderen Schnittstellenvervielfacher.

Die Datenzentrale konnte sich darauf berufen, daß auf dem Markt keine Technik verfügbar war, die einen sicheren Netzbetrieb ermöglicht hätte, ohne gleichzeitig die Netzkosten erheblich zu steigern. Wegen der großen Bedeutung dieses Problems habe ich daher gemeinsam mit der Datenzentrale nach einer Lösung gesucht. Überprüft wurden unterschiedliche technische Wege unter den Gesichtspunkten Sicherheit, Kosten und Praktikabilität.

Die gemeinsame Arbeit hat schließlich zu einem Erfolg geführt. Die Deutsche Bundespost TELEKOM erklärte sich bereit, bei der Datenzentrale als Pilotversuch einen neu entwickelten Netzknoten zu erproben, der nach dem Prinzip der **Paketvermittlung** (X.25 – Schnittstelle) arbeitet. Bei Einsatz dieses Netzknotens bestehen die bisherigen Sicherheitsbedenken nicht mehr.

Nach Abschluß der Tests konnte die Datenzentrale mir inzwischen mitteilen, daß der neue Netzknoten als Ersatz für den bisher installierten SK 12 einsetzbar ist. Die Antwortzeiten haben sich nicht verändert. Man erwartet sogar, in weiteren Tests einen Performance-Gewinn erreichen zu können. Die Datenzentrale berichtete, das gesamte Datennetz werde z. Z. überarbeitet, und die neue Netzplanung sehe den Einsatz des SK 12 nicht mehr vor.

Nachdem dieses Ziel erreicht ist, sehe ich keinen Grund mehr, ein Datennetz hinzunehmen, in dem die Datensicherheit durch Verwendung eines Schnittstellenvervielfachers beeinträchtigt ist. Öffentliche Stellen, die noch ein Datennetz mit Schnittstellenvervielfachern betreiben, sollten dieses umgehend daraufhin überprüfen, ob die Datensicherheit beeinträchtigt ist. Kriterien dafür können meinem 7. Tätigkeitsbericht (S. 159 bis 162) entnommen werden. Falls die Sicherheit beeinträchtigt ist, sollten möglichst kurzfristig Netzknoten, die einen sicheren Betrieb gewährleisten, installiert werden.

### 6.2.2 Breitbandnetze

Die Medizinischen Einrichtungen einer Universität baten mich um Beratung bezüglich der datenschutzkonformen Gestaltung ihres Krankenhausnetzes. Geplant war ein Backbone-Netz mit angeschlossenen lokalen Netzen (**LANs**). Übertragen werden sollten Daten der Kliniken, wissenschaftliche Daten und Verwaltungsdaten.

Bereits in meinem 10. Tätigkeitsbericht (S. 148 bis 150) wies ich auf die Beeinträchtigung der Datensicherheit bei Einsatz eines LAN hin. Die Situation bei Einsatz eines LAN kann mit derjenigen bei Einsatz eines Schnittstellenvervielfachers (oben S. 132) verglichen werden. Auch das LAN bietet alle übertragenen Informationen zahlreichen Endgeräten an, und es wird erst in dem Endgerät geprüft, ob eine Information an dieses Gerät adressiert ist und daher übernommen werden soll. Das mißbräuchliche Lesen von Nach-

richten, die an andere Endgeräte gerichtet sind, ist damit grundsätzlich nicht ausgeschlossen.

Nach dem derzeitigen Stand der Technik wurden im vorliegenden Fall insbesondere folgende Maßnahmen zur Verbesserung der Datensicherheit angeregt:

- Die einzelnen LANs werden so ausgelegt, daß möglichst nur gleichartige Benutzer an ein LAN angeschlossen sind. Anzustreben ist, daß alle an ein LAN angeschlossenen Endbenutzer jeweils gleiche Zugriffsbefugnisse haben.
- Jedenfalls sollen für die Bereiche Klinik, Wissenschaft und Verwaltung ausschließlich getrennte LANs eingesetzt werden.
- Eine recht hohe Sicherheit kann durch Einsatz von Verschlüsselungstechniken erreicht werden. Für die bei den Medizinischen Einrichtungen vorgesehene LAN-Technik war auch eine fertige Lösung am Markt verfügbar. Kosten und organisatorischer Aufwand wären allerdings erheblich gewesen.

Zur Veranschaulichung der Situation könnte man sagen, daß die Datensicherheit des LAN deshalb im Vergleich zum Fernsprechnetz beeinträchtigt ist, weil es bei dem LAN keine Telefonzentrale gibt, von der Leitungen zu den einzelnen Teilnehmern abgehen und in der der einzelne Datenstrom jeweils zu dem Teilnehmer gelenkt wird, für den er vorgesehen ist. Weil das LAN nicht über eine derartige Telefonzentrale verfügt, ist es nicht möglich, jeden Datenstrom ausschließlich auf den jeweiligen Adressaten zu lenken, sondern jeder Datenstrom wird einer Vielzahl von Teilnehmern angeboten.

Allerdings hoffe ich, daß diese durch die Technik bedingte Beeinträchtigung der Datensicherheit in einigen Jahren nicht mehr bestehen wird. Ich habe aus der Fachliteratur und durch Kontakte zur Industrie den Eindruck gewonnen, daß möglicherweise in wenigen Jahren eine erheblich bessere Lösung zur Verfügung stehen wird. Der Stand der Entwicklungsarbeiten auf dem Gebiet der Vermittlungstechnik für Breitbandleitungen läßt erwarten, daß in absehbarer Zeit die breitbandige Vermittlung in ähnlicher Weise möglich sein wird wie heute die Vermittlung in einer Telefonzentrale.

Es mag zwar sein, daß in Zukunft die Vermittlungsknoten für die Breitbandvermittlung nicht an einem Ort – vergleichbar der heutigen Telefonzentrale – räumlich zusammengefaßt werden. Vielleicht wird es technisch günstiger sein, die Vermittlungsknoten für Breitbandvermittlungen räumlich verteilt anzuordnen. Möglicherweise entsteht dadurch eine Installation, die man organisatorisch als eine über ein Gebäude oder gar ein Gelände ausgedehnte Vermittlungsstelle bezeichnen könnte. Wesentlich unter dem Gesichtspunkt der Datensicherheit wird aber sein, daß alle Vermittlungsknoten in einem Bereich liegen, der ausschließlich einer zentralen Stelle zugeordnet ist und zu dem nur diese Zugang hat. Den Endgeräten werden dann ausschließlich die an die jeweiligen Teilnehmer adressierten Daten angeboten.

Eine solche Entwicklung wäre aus Gründen der Datensicherheit sehr zu begrüßen. Daher rege ich an, daß öffentliche Stellen, die ein LAN installieren oder erweitern wollen, gegenüber den Herstellern ihr Interesse an dieser Art der breitbandigen Vermittlungstechnik äußern, um die Hersteller anzuregen, baldmöglichst die entsprechende Technik auf den Markt zu bringen.

## 6.3 Datensicherheit bei zentraler Verfahrensentwicklung

Ein Beratungsersuchen gab mir Veranlassung, mich zu grundsätzlichen Fragen der Datensicherheit für den Fall zu äußern, daß zentral entwickelte Programme bei einer größeren Zahl von öffentlichen Stellen eingesetzt werden sollen.

- Gewährleisten der erforderlichen Datensicherheit bei allen Einsatzfällen

  Nach dem Inhalt des Beratungsersuchens mußte ich davon ausgehen, daß die zu entwickelnden Programme auf Datenverarbeitungsanlagen sehr unterschiedlicher Größe und Ausstattung eingesetzt werden sollen. Das gab mir Veranlassung, ausdrücklich darauf hinzuweisen, daß der Grad der Datensicherheit nicht von der Art der zum Einsatz kommenden Datenverarbeitungsanlagen abhängen darf.

- Programmfreigabe

  Eine öffentliche Stelle, die ein Programm einsetzt, ist im allgemeinen für dessen Inhalt verantwortlich. Diese Verantwortung kommt in der in jedem Einzelfall erforderlichen Programmfreigabe zum Ausdruck.

  Es ist davon auszugehen, daß die zentral entwickelten Programme auch durch eine zentrale Stelle freigegeben werden sollen. Dann sollten die Programme so geartet sein, daß sie von allen anderen Stellen ohne erneute Programmfreigabe übernommen werden können. Dazu ist es erforderlich, daß der Einsatz im Einzelfall ohne jede auf diesen Einzelfall bezogene Änderung des logischen Programminhalts erfolgt.

- Unveränderter Programmeinsatz

  Falls ein zentral entwickeltes Programm in einer größeren Zahl von Organisationseinheiten eingesetzt werden soll, ist es von besonderer Bedeutung, Voraussetzungen dafür zu schaffen, daß dessen unveränderter Einsatz gewährleistet werden kann. Bei Einsatz kleinerer Datenverarbeitungsanlagen bereitet diese Anforderung im allgemeinen erhebliche Schwierigkeiten. Unter dem Stichwort „Programmeinsatz – unveränderte Fassung" können dem Sammelband Datensicherheit (unten S. 158) weitere Hinweise entnommen werden.

  Insbesondere durch den Einsatz geeigneter Sicherheitssoftware mag es heute in vielen Fällen möglich sein, auch bei Einsatz kleinerer Datenverarbeitungsanlagen einen unveränderten Programmeinsatz zu gewährleisten. Auch wird es in vielen Fällen möglich sein, durch Sicherheitssoftware für alle wesentlichen Maßnahmen die Einhaltung des Vier-Augen-Prinzips zu sichern.

Besondere Bedeutung kann dabei die Möglichkeit erlangen, Programme durch Versiegeln gegen jede unzulässige Änderung zu sichern. Ich verweise hierzu auch auf meinen 7. Tätigkeitsbericht (S. 175/176).

- Revisionsfähigkeit

  Bereits bei der Konzeption der Programme sollte sichergestellt werden, daß deren Revisionsfähigkeit gewährleistet ist. Wichtig ist dabei allerdings die konkrete Ausgestaltung der Revisionsfähigkeit, wichtig ist eine Eigenschaft, die ich in meinem 10. Tätigkeitsbericht (S. 139 und 142) als Revisionsoberfläche bezeichnet habe. Die Revisionsoberfläche sollte unmanipulierbar sein, und sie sollte – vor allem bei kleineren Datenverarbeitungsanlagen – so geartet sein, daß sie von einem Revisor genutzt werden kann, der nur über begrenzte Kenntnisse in der automatisierten Datenverarbeitung verfügt.

  Von erheblicher Bedeutung für die Revisionsfähigkeit sind unmanipulierbare Aufzeichnungen über alle Systemaktivitäten. Im allgemeinen ist es sinnvoll, die Systemnachrichten maschinenlesbar aufzuzeichnen. Dann sollten allerdings auch entsprechende Programme zu deren Auswertung bereitgestellt werden. Soweit Systemnachrichten personenbezogen aufgezeichnet werden, sind sie besonders zu sichern. Hinweise dazu enthält mein 9. Tätigkeitsbericht (S. 117/118).

- Zugriffsbeschränkung, Zugriffssicherung

  Es ist notwendig, in dem System Zugriffsbeschränkungen zu realisieren. Diese Zugriffsbeschränkungen betreffen sowohl die Frage, auf welche personenbezogenen Daten dem einzelnen Benutzer der Zugriff gestattet wird als auch die Frage, wer in welchem Umfang zu Zugriffen auf die Systemdaten und das System befugt ist.

  Die Zugriffsbeschränkungen müssen durch geeignete Maßnahmen der Zugriffssicherung technisch so integriert sein, daß ihre Einhaltung dadurch sichergestellt ist. Dem System müssen dazu die Zugriffsbefugnisse aller zugriffsberechtigten Bediensteten bekannt sein. Diese in dem System gespeicherten Zugriffsbefugnisse müssen selbstverständlich auch durch eine zuverlässige Zugriffssicherung vor Eingriffen Unbefugter geschützt sein.

- Abfragesprache

  Sofern in dem System vorgesehen ist, eine Abfragesprache zur Eingabe frei formulierter Abfragen einzusetzen, ist folgendes zu beachten: Dem einzelnen Benutzer darf es auch bei Verwendung einer solchen Abfragesprache nicht möglich sein, die für ihn festgelegten Zugriffsbeschränkungen zu durchbrechen. Bei Verwendung einer Abfragesprache dürfen dem Benutzer nur Zugriffe im Rahmen seiner Zugriffsberechtigung möglich sein. Auch darf es nicht möglich sein, durch Verwendung einer Abfragesprache eine erforderliche und durch geeignete Zugriffsbeschränkungen verwirklichte Anonymisierung zu umgehen.

- Datenbank

  Nach den mir vorgelegten Unterlagen sollten die zu entwickelnden Programme auf der Grundlage einer Datenbank arbeiten. Hierzu wies ich darauf hin, daß es notwendig ist, die Einhaltung der aus rechtlichen Gründen erforderlichen Zugriffsbeschränkungen durch angemessene organisatorische und technische Maßnahmen abzusichern. Ein Datenbankprogramm, dessen Einsatz vorgesehen ist, muß daher überprüft werden, ob es dieser Anforderung genügt. Fehlende Eigenschaften eines ausgewählten Datenbankprogramms gestatten nicht, die erforderliche Datensicherheit insoweit einzuschränken.

- Eingabekontrolle/Übermittlungskontrolle

  Bei Kontrollbesuchen mußte ich mehrfach feststellen, daß den Anforderungen der Eingabekontrolle auf kleineren Datenverarbeitungsanlagen nur unzureichend entsprochen wurde. Die Ursache lag im allgemeinen weniger in der beschränkten Leistungsfähigkeit oder Speicherkapazität der kleineren Anlage. Ursächlich war vielmehr die Einstellung, bei einer Entwicklung für eine kleinere Anlage keinen so hohen Entwicklungsaufwand treiben zu müssen.

  Die Frage, in welchem Umfang ein bestimmtes Datensicherungsziel zu verwirklichen ist, darf aber nicht von der Entscheidung des Anwenders über die von ihm eingesetzte Technik der Datenverarbeitung abhängen. Der Weg, wie das Datensicherungsziel erreicht wird, hängt zwar im Einzelfall durchaus von der eingesetzten Technik ab. Die Anforderungen an den Grad der zu erreichenden Datensicherheit bestimmen sich aber unabhängig von dieser Technik. Einsatz einer anderen Technik kann keinen Grund für einen Verzicht auf Datensicherheit darstellen. Den Anforderungen der Eingabekontrolle und Übermittlungskontrolle muß daher unabhängig von der eingesetzten Technik entsprochen werden.

  Bezüglich des Umfangs der im Rahmen der Eingabekontrolle aufzuzeichnenden Daten habe ich darauf hingewiesen, daß auch Eingaben, die eine Änderung gespeicherter Zugriffsbefugnisse bewirken, der Eingabekontrolle unterliegen.

## 6.4 Einzelfragen der automatisierten Datenverarbeitung

### 6.4.1 Dienstanweisungen

Jede öffentliche Stelle sollte die zum Gewährleisten der Datensicherheit erforderlichen Maßnahmen in einer Dienstanweisung verbindlich vorschreiben. Als Hilfen bei dem Entwickeln der Dienstanweisung können die von mir herausgegebenen **Organisationshilfen zur Datensicherung** (unten S. 157) genutzt werden. Den Organisationshilfen können Anregungen entnommen werden, welche Sachverhalte durch Dienstanweisung zu regeln sind und welcher Art diese Regelungen zu sein haben. In einer Reihe von Fällen habe ich zu Dienstanweisungen Stellung genommen.

Eine mir vorgelegte Dienstanweisung enthielt keine Regelungen zum Verfahren des **Programmtests**, zur Programmfreigabe durch den Anwender und zur vorläufigen Programmfreigabe. Auch auf die Anforderungen, die im Hinblick auf die Datensicherheit bei individueller Datenverarbeitung (IDV) zu stellen sind, wurde in der Dienstanweisung nicht eingegangen. Damit wird in dieser Dienstanweisung auf wesentliche Regelungen verzichtet, die bei Einsatz von Fremdprogrammen mit verbindlicher Verarbeitungslogik und bei eigener – zentraler oder dezentraler – Entwicklung von Programmen mit verbindlicher Verarbeitungslogik erforderlich wären. Bei der öffentlichen Stelle wurde unterstellt, daß ein solcher Programmeinsatz und solche Programmentwicklungen nicht erfolgen und auch nicht erfolgen dürfen. Um zu gewährleisten, daß derartige Entwicklungen nicht durchgeführt werden, regte ich an, ein entsprechendes ausdrückliches Verbot in die Dienstanweisung aufzunehmen.

Ergänzend wies ich auf folgendes hin: Falls dieses Verbot in der Dienstanweisung nicht praktikabel sein sollte oder falls mit der Zeit erkennbar wird, daß ein solches Verbot die Arbeit in untragbarer Weise hemmt, ist es notwendig, die Dienstanweisung zu erweitern. Zu regeln sind dann voraussichtlich die Gebiete Programmtest, Freigabe von Anwendungsprogrammen und vorläufige Programmfreigabe. Voraussichtlich wird dann darüber hinaus auch das Gebiet der individuellen Datenverarbeitung einer Regelung in der Dienstanweisung bedürfen. Hinweise bezüglich Art und Umfang der in diesem Fall erforderlichen Regelungen können den von mir herausgegebenen Unterlagen Organisationshilfe-Allgemeiner Teil und Organisationshilfe-IDV (unten S. 158) entnommen werden.

In einer anderen Dienstanweisung war das Verfahren der **Wartung** der aufgestellten DV-Geräte nicht ausdrücklich geregelt. Erfahrungsgemäß ist es aber notwendig, Regelungen zur Wartung und insbesondere auch zur Sicherung personenbezogener Daten im Zusammenhang mit der Wartung in einer Dienstanweisung zu treffen. Hinweise für den Inhalt derartiger Regelungen können unter den Stichworten „Wartung" und „Fernwartung" dem Sammelband Datensicherheit (unten S. 158) entnommen werden.

In einem an mich gerichteten Schreiben vertrat eine städtische Schule die Ansicht, eine formelle Dienstanweisung für Lehrkräfte im Hinblick auf den Datenschutz sei nicht Angelegenheit der **Schulleitung**, sondern des Kultusministeriums oder des Regierungspräsidenten. Dazu wies ich die Schule auf folgendes hin:

Nach § 2 Abs. 2 Satz 3 DSG NW gelten Schulen der Gemeinden und Gemeindeverbände, soweit sie in inneren Schulangelegenheiten personenbezogene Daten verarbeiten, als öffentliche Stellen im Sinne dieses Gesetzes. Die Regelungen des Datenschutzgesetzes Nordrhein-Westfalen gelten daher für eine städtische Schule unmittelbar. Es ist Aufgabe der Schule, die Einhaltung dieser Regelungen zu gewährleisten. Soweit bestehende Dienstanweisungen der Aufsichtsbehörden der Ergänzung bedürfen, damit die Einhaltung der Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen gewährleistet

werden kann, ist es Aufgabe der Leitung der Schule, die erforderlichen zusätzlichen Regelungen zu treffen.

Ein **Hauptpersonalrat** bat mich um Stellungnahme zu der Dienstanweisung des Kultusministeriums für die automatisierte Verarbeitung von personenbezogenen Daten in der Schule. Er wies u. a. darauf hin, daß in dieser Dienstanweisung Regelungen über die Systemverwaltung und deren Aufgaben und Funktionen fehlen, und er erhob Bedenken gegen die Ausführungen zum Einsatz selbstentwickelter Programme.

In meiner Antwort führte ich aus, daß Verantwortung und Zuständigkeit der Systemverwaltung festgelegt werden müssen. Zu regeln sind insbesondere Fragen nach den Aufgaben der Systemverwaltung im Zusammenhang mit der Entwicklung oder Beschaffung von Programmen, nach deren Zuständigkeit bezüglich der zu treffenden Maßnahmen zur Verbesserung der Datensicherheit und nach ihrer Verantwortung im Zusammenhang mit der Bedienung der Datenverarbeitungsanlage.

Mir ist nicht bekannt, ob es möglich ist, Regelungen zu diesen Fragen in einer für viele Schulen geltenden Dienstanweisung umfassend zu treffen. Da die Dienstanweisung des Kultusministeriums keine entsprechenden Regelungen enthält, sollten diese in den einzelnen Schulen durch schriftliche Anweisung getroffen werden. Einen Hinweis in der Dienstanweisung des Kultusministeriums auf die Notwendigkeit derartiger Anweisungen in den einzelnen Schulen würde ich begrüßen.

Hinweise zur Frage des Einsatzes selbstentwickelter Programme können dem Sammelband Datensicherheit (unten S. 158) unter dem Stichwort „individuelle Datenverarbeitung" entnommen werden. Falls individuelle Datenverarbeitung in einer Schule nicht zugelassen ist, sollte sie schriftlich verboten werden. Falls sie zugelassen ist, sollten die Bedingungen, unter denen sie zugelassen ist, schriftlich festgelegt sein.

Eine Regelung in der Dienstanweisung des Kultusministeriums würde ich begrüßen. Falls eine zentrale Entscheidung des Kultusministeriums zu diesem Sachverhalt nicht sachgerecht sein sollte, wäre es vorteilhaft, wenn jede Schule verpflichtet würde, eine verbindliche Regelung zu treffen.

### 6.4.2 Kontrolle der Einhaltung von Anweisungen

Dienstanweisungen enthalten u. a. die zum Gewährleisten der Datensicherheit getroffenen Regelungen (oben S. 137). Wie die allgemeine Lebenserfahrung zeigt, ist es aber zum Gewährleisten von Datensicherheit nicht ausreichend, lediglich die Dienstanweisung zu erlassen. Es muß vielmehr auch kontrolliert werden, ob diese Dienstanweisung eingehalten wird. Auf die Notwendigkeit, dazu eine **interne Kontrolle** zu institutionalisieren, habe ich in fast jedem der bisherigen Tätigkeitsberichte hinweisen müssen. Heute kann ich feststellen, daß diese Notwendigkeit nur noch selten in Frage gestellt wird. In den Vordergrund rücken daher jetzt Fragen der Ausgestaltung dieser Funktion.

In einer mir vorgelegten Dienstanweisung wurde zwar eine „Kontrollierende Stelle" institutionalisiert. Die untergeordnete **Einordnung** in der Hierarchie und der Verzicht auf ergänzende Regelungen, in denen die Pflichten der kontrollierten Stelle festgelegt werden, beeinträchtigten aber die Wirkungsmöglichkeit der kontrollierenden Stelle. Daher habe ich darauf hingewiesen, daß die Stellung der kontrollierenden Stelle und damit auch deren Einwirkungsmöglichkeit durch einige ergänzende Regelungen erheblich verstärkt werden könnten. In diesem Zusammenhang könnten insbesondere folgende Regelungen getroffen werden:

- Direkte Unterstellung unter die Leitung des Hauses im Rahmen dieser Aufgabe,
- Auskunftspflicht der kontrollierten Stellen,
- Verpflichtung der kontrollierten Stellen, zu den Ergebnissen einer Prüfung Stellung zu nehmen sowie
- Bericht an die Leitung des Hauses.

Dem **Städtetag** Nordrhein-Westfalen gab ich eine Anregung zu dem Entwurf einer Empfehlung für eine **Dienstanweisung** über die Organisation des Informations- und Datenschutzes. Bezüglich der internen Kontrolle der Einhaltung von Vorschriften zum Gewährleisten der Datensicherheit wies ich darauf hin, daß eine für die interne Kontrolle zuständige Person oder Stelle fachlich kompetent sein muß – d. h., sie muß u. a. mit der automatisierten Datenverarbeitung vertraut sein –, und sie muß die erforderliche Unabhängigkeit besitzen. Sie sollte direkt der Behördenleitung berichten.

Nach meinen Feststellungen ist es im kommunalen Bereich häufig mit Schwierigkeiten verbunden, die Aufgabe der internen Kontrolle organisatorisch so zuzuordnen, daß diesen Anforderungen entsprochen wird. Günstig wäre eine Zuordnung zum Datenschutzbeauftragten, falls sowohl die zeitliche Belastung als auch die fachliche Kompetenz – insbesondere auf dem Gebiet der automatisierten Datenverarbeitung – eine solche Zuordnung möglich macht. Naheliegend wäre auch eine Zuordnung zum Rechnungsprüfungsamt. Dazu könnte die Aufgabe dem Rechnungsprüfungsamt nach § 102 Abs. 2 der Gemeindeordnung für das Land Nordrhein-Westfalen durch den Rat übertragen werden. Eine enge Zusammenarbeit zwischen Rechnungsprüfungsamt und Datenschutzbeauftragtem sollte in diesem Fall festgelegt werden.

Im Hinblick auf die bestehende besondere Problematik regte ich an zu prüfen, ob der Entwurf der Empfehlung um Aussagen folgender Art ergänzt werden sollte:

- Die interne Kontrolle der Einhaltung der Vorschriften für die Datensicherheit bedarf der ausdrücklichen Regelung. (Eine Konkretisierung der Aufgabe könnte im Rahmen einer Anlage zu der Empfehlung erfolgen.)
- Es muß festgelegt werden, wer oder welche Stelle für die interne Kontrolle der Einhaltung der Vorschriften zur Datensicherheit zuständig ist. Die

Empfehlung sollte auch Hinweise zur sachgerechten Aufgabenzuordnung enthalten.

- Die Zusammenarbeit dieser Stelle mit dem Datenschutzbeauftragten ist zu regeln, falls keine Personalunion besteht.

Meine Anregungen wurden leider in der vom Städtetag inzwischen verteilten Dienstanweisung nicht berücksichtigt.

Eine Datenzentrale berichtete bei einem Kontrollbesuch, sie habe einen innerbetrieblichen Datenschutzbeauftragten bestellt, dessen Aufgaben in einer Dienstanweisung festgelegt sind. Nach dieser Dienstanweisung hat er u. a. die Aufgabe, die Einhaltung der von der Datenzentrale zu beachtenden Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen und der einschlägigen internen Dienstanweisung zu überwachen.

Dem innerbetrieblichen Datenschutzbeauftragten waren darüber hinaus allerdings weitere Aufgaben übertragen worden, durch die seine **Unbefangenheit** bei der Wahrnehmung der Überwachung beeinträchtigt werden kann:

a) Nach der Dienstanweisung für den Datenschutzbeauftragten hat dieser alle Datenschutz- und Datensicherungsmaßnahmen der Datenzentrale zu koordinieren.

b) Eine Dienstanweisung über den Datenschutz und die Datensicherheit bei Einsatz von Personalcomputern enthält folgende Regelungen:

   - „Der Datenschutzbeauftragte legt nach vorheriger Entscheidung durch den Geschäftsführer fest, welche Softwareprodukte von welchem Mitarbeiter genutzt werden können."
   - „Auf dem PC des Testsystems ist ein Anti-Virus Testprogramm einzusetzen. Dieses Programm ist immer auf dem neuesten Stand zu halten. Bei auftretenden Programmhinweisen, die auf das Vorhandensein von Viren schließen lassen, ist die Verteilung von Dateien aus dem Testsystem unverzüglich zu unterlassen. Die Ursache des Virenbefalls ist sofort zu untersuchen. Zuständig ist der Datenschutzbeauftragte."
   - „Für die Installation auf PC, die von den Verbandsmitgliedern über die Datenzentrale erworben wurden, ist ausschließlich Originalsoftware zu verwenden. Dabei ist immer die neueste Version der Programmprodukte, die von dem Datenschutzbeauftragten als offiziell einsetzbar erklärt wurden, zu verwenden."
   - „Als Standardsoftwareprodukte dürfen nur solche Programme zum Einsatz gebracht werden, die offiziell durch den Datenschutzbeauftragten zur Nutzung zur Verfügung gestellt wurden."

Während des Kontrollbesuchs wurden Möglichkeiten erörtert, die Aufgabe der internen Kontrolle durch eine andere Person oder Organisationseinheit wahrnehmen zu lassen. Naheliegend wäre eine Zuordnung dieser Aufgabe zur Rechnungsprüfung. Es wurde erörtert, daß beide Aufgaben sich gegenseitig in günstiger Weise ergänzen würden.

Die Datenzentrale hat mich inzwischen unterrichtet, daß die interne Kontrolle der Einhaltung der Vorschriften zur Datensicherung dem Rechnungsprüfungsamt übertragen wird.

Bei der Bearbeitung einer Bürgereingabe stellte ich fest, daß einer Stadt bei der automatisierten Verarbeitung von Einwohnerdaten ein Fehler unterlaufen war. Ursache war ein unentdeckter Programmfehler. Der Stellungnahme der Stadt entnahm ich, daß in drei Fällen gegen geltende organisatorische Regelungen verstoßen worden war und daß vermutlich dadurch der Fehler des Programmierers unentdeckt blieb.

- Der Programmierer hatte Test und Freigabe des Fachamtes nicht angefordert.
- Die Unterschrift des Abschnittsleiters war nicht eingeholt worden.
- Das Programm war zum Ablauf gekommen, obgleich in dem Übergabe-Protokoll die Angabe zur Freigabe und die Unterschrift des Abschnittsleiters fehlten.

Ich ging davon aus, daß der entstandene Fehler wegen der **Nichteinhaltung von Organisationsverfügungen** unentdeckt geblieben ist. Um in Zukunft derartige Fehler zu verhindern, empfahl ich daher, daß eine geeignete Organisationseinheit den Auftrag erhalten solle, den ordnungsgemäßen und vollständigen Ablauf – insbesondere bei dem Freigabeverfahren von Programmen – zu überwachen.

Bei datenverarbeitenden Stellen ist es häufig eine Organisationseinheit mit der Bezeichnung „Arbeitsvorbereitung" (seltener „Produktionssteuerung"), die besonders geeignet ist, in der hier angesprochenen Weise eine Verbindungsaufgabe zwischen Entwicklung und Durchführung wahrzunehmen. Ich regte an zu prüfen, ob auch bei der Stadt eine entsprechende Aufgabenzuordnung erfolgen sollte. Zusätzliche Vorteile für die Datensicherheit würden sich darüber hinaus ergeben, wenn die Arbeitsvorbereitung weitere Funktionen wie etwa die Verwaltung von Bibliotheken freigegebener Programme und die Verwaltung der Arbeitsaufträge übernimmt.

Möglicherweise ist der jetzt bekannt gewordene Fehler als Zeichen dafür anzusehen, daß es bereits zum üblichen Ablauf gehört, gewisse Organisationsverfügungen nicht einzuhalten. Ich wies daher die Stadt darauf hin, daß in diesem Zusammenhang Erkenntnisse aus systematischen Prüfungen einer institutionalisierten internen Kontrolle von Bedeutung sind, die derartige Gewohnheiten aufdecken müßten.

### 6.4.3 Programmfreigabe

Im Rahmen des Kontrollbesuchs bei einer Stadt wurde u. a. die Programmfreigabe erörtert. Für ihre automatisierte Datenverarbeitung ist die Stadt an eine **kommunale Datenzentrale** angeschlossen, die als Zweckverband organisiert ist. Aus den bei dem Kontrollbesuch vorgelegten Unterlagen ging hervor, daß die Stadt die bei der Datenzentrale für sie eingesetzten Programme nicht selbst freigab. Die Freigabe erfolgte vielmehr durch die Datenzentra-

le. Zur Begründung berief sich die Stadt auf die Verbandssatzung der Datenzentrale, die bestimmte: „Der Zweckverband gibt Verfahren und Programme frei, sofern gesetzliche Bestimmungen nicht entgegenstehen."

Ohne Programmfreigabe durch den fachlich zuständigen Auftraggeber ist dessen Verantwortlichkeit aber nicht mehr gewährleistet. Er kann sich zwar noch auf den Inhalt seines Programmauftrages berufen. Ohne eigenen Programmtest und ohne Programmfreigabe ist der Auftraggeber aber nicht in der Lage, aus eigenem Wissen zu bestätigen, daß das entwickelte Programm entsprechend seinem Programmauftrag arbeitet.

Erst mit der abschließenden Programmfreigabe durch die fachlich verantwortliche Stelle wird von dieser endgültig die Verantwortung für die inhaltliche Wahrnehmung der Gesamtaufgabe übernommen. Als Voraussetzung für die Programmfreigabe muß der Anwender ein Anwendungsprogramm vor dem ersten Einsatz und nach jeder fachlichen Änderung eingehend testen. Dieser Anwendertest muß unabhängig von den vorher durchgeführten Programmierertests erfolgen. Auf der Grundlage des Anwendertests entscheidet der Anwender über die Freigabe des Programms und übernimmt damit die Verantwortung für dessen fachlichen Inhalt.

In einer Besprechung mit der Datenzentrale schilderte diese den Ablauf von Entwicklung und Freigabe. Ein bei der Datenzentrale entwickeltes Verfahren wird im Rahmen einer Pilotinstallation bei einem oder mehreren Anwendern getestet. Falls dieser Test erfolgreich abgeschlossen wird, enthält der zu fertigende Testbericht eine entsprechende Erklärung. Verfahrens- und Programmfreigabe erfolgen dann unter Einbeziehung eines Koordinierungskreises, in dem die dem Verwaltungsrat der Datenzentrale angehörenden Hauptverwaltungsbeamten vertreten sind, durch den Geschäftsführer der Datenzentrale.

Während der Besprechung wurde erörtert, daß die Zuständigkeit der Datenzentrale für die Freigabe nicht den Anforderungen des Datenschutzes entspricht. Die Datenzentrale erklärte hierzu allerdings erläuternd, unter Verfahrens- und Programmfreigabe im Sinne der Verbandssatzung sei nicht die Freigabe in dem o. a. Sinn zu verstehen. Die Verfahrens- und Programmfreigabe im Sinne der Verbandssatzung habe vielmehr lediglich die Bedeutung des praktischen Produktionsauftrages. Die eigentliche Freigabe erfolge durch den Koordinierungskreis. Grundlage hierfür sei die fachliche Aussage der Anwender der Pilotinstallation in dem erstellten Testbericht.

Um diese Interpretation verbindlich und unmißverständlich festzulegen, sollte ein entsprechender Beschluß der Verbandsversammlung getroffen werden. Die Datenzentrale ist meiner entsprechenden Anregung gefolgt, und die Verbandsversammlung hat folgende Beschlüsse gefaßt:

- Die Freigabe von Verfahren als Übernahme der fachlichen Verantwortung für den Verfahrensinhalt erfolgt durch den Koordinierungskreis.

- Die Freigabe von Verfahren durch den Koordinierungskreis ist erforderlich vor dem erstmaligen produktionsmäßigen Einsatz eines Verfahrens sowie nach wesentlichen Verfahrensänderungen.
- Der Verbandsvorsteher wird zur vorläufigen Freigabe in Fällen besonderer Dringlichkeit ermächtigt.

Ergänzend stellte die Verbandsversammlung fest, daß unter Verfahrens- und Programmfreigabe nach der derzeitigen Fassung der Verbandssatzung der Produktionsauftrag zu verstehen sei. Sie erklärte darüber hinaus ihre Absicht, den Text der Verbandssatzung im Zusammenhang mit deren nächster Änderung so abzuändern, daß ein Mißverständnis dieser Regelung ausgeschlossen ist.

Abschließend habe ich der kontrollierten Stadt empfohlen, sich diese Freigabe in jedem Einzelfall schriftlich bestätigen lassen. Bei unverändertem Einsatz der so freigegebenen Programme bestehen keine durchgreifenden Bedenken, wenn die Stadt auf einen eigenen Anwendertest als Voraussetzung ihrer Freigabe verzichtet.

### 6.4.4 Elektronische Unterschrift

In meinem 8. Tätigkeitsbericht (S. 161 bis 163) nahm ich zu Fragen der maschinellen Authentifizierung im Zahlungsverkehr Stellung. Ich wies darauf hin, welche Bedeutung das Gebiet der maschinellen Authentifizierung in Zukunft für den Datenschutz erlangen wird und forderte, die damit verbundenen Fragen und Probleme möglichst frühzeitig zu untersuchen. Dabei sprach ich bereits konkrete Empfehlungen zur Verbesserung des Datenschutzes bei Verfahren mit maschineller Authentifizierung aus.

Eine Anfrage der EG-Kommission gab mir jetzt Veranlassung, meine damaligen Überlegungen aufzugreifen. Thema dieser Anfrage war die „elektronische Unterschrift". Unter elektronischer Unterschrift versteht man ein Verfahren, bei dem einem in maschinell verwertbarer Form vorliegenden Schriftstück – etwa der codierten Aufzeichnung eines Briefs, einer Bestellung oder eines Schecks auf einem Datenträger – eine Zusatzinformation zugefügt wird. Die Zusatzinformation wird durch einige Eigenschaften zur elektronischen Unterschrift:

a) Nur eine einzige Person, die unterzeichnende Person, ist in der Lage, gerade diese Zusatzinformation zuzufügen. (In der Praxis hat man davon auszugehen, daß die spezielle Zusatzinformation nur unter Verwendung einer Chipkarte, die sich im Besitz der unterzeichnenden Person befindet, erzeugt werden kann. Durch Verwendung einer persönlichen Identifikationsnummer (PIN) kann zusätzlich abgesichert werden, daß die Chipkarte nicht von Unbefugten benutzt werden kann.)

b) Es ist Dritten auch ohne Mitwirkung der unterzeichnenden Person und ohne Rückgriff auf deren Chipkarte möglich nachzuweisen, daß die Zusatzinformation nur bei Benutzung dieser Chipkarte erzeugt werden konnte.

c) Jede Änderung an dem „unterzeichneten" Schriftstück bewirkt, daß sich der Nachweis b) nicht mehr führen läßt.

Es ist damit zu rechnen, daß Verfahren, die sich der elektronischen Unterschrift bedienen, in Zukunft erhebliche Bedeutung gewinnen werden. Daher halte ich es für erforderlich, wesentliche schon heute erkennbare Gefahren, die damit verbunden sind, aufzuzeigen und Vorschläge zu machen, wie diesen **Gefahren** zu begegnen ist.

- Beweismittel für Betroffene

  Jedes Verfahren, bei dem elektronische Unterschriften verwandt werden, setzt insoweit den Glauben an die Zuverlässigkeit dieses automatisierten Verfahrens voraus. Ein entsprechender Nachweis liegt im allgemeinen nicht vor und kann auch meist nicht gefordert werden. Das führt dazu, daß sich beispielsweise Betroffene, die eine Falschbuchung in einem solchen System reklamieren, dem schwerwiegenden Verdacht aussetzen können, selbst eine kriminelle Handlung begangen zu haben oder begehen zu wollen. Dieser Vorwurf ist von den Betroffenen selbst nicht widerlegbar, wenn der reklamierten Transaktion kein von ihnen selbst unterschriebener materieller Beleg zugrunde liegt. Die besondere Gefahr für die Betroffenen besteht daher immer dann, wenn Transaktionen ausschließlich auf der Basis einer elektronischen Unterschrift erfolgen. In einem solchen Fall wird kein materieller Beleg archiviert, der zur Prüfung der Echtheit des Belegs einschließlich der Unterschrift einer neutralen Stelle übergeben werden könnte.

  Bei einer Bezahlung mit einem elektronisch unterschriebenen Scheck kann die Bank oder Sparkasse zwar den nichtmateriellen elektronischen Scheck archivieren und ist damit zu einem Nachweis gegenüber ihrem Kunden und gegenüber Dritten in der Lage. Implizite Grundlage eines eventuellen Nachweises über die erfolgte Unterschrift ist aber die Behauptung, das automatisierte System sei absolut sicher. Es sei z. B. bei dem elektronisch unterschriebenen Scheck der geheime Schlüssel in der zur Unterschrift benutzten Chipkarte wirklich geheim und auch nicht aus allgemein bekannten Daten berechenbar.

  Ein eventueller Fehler oder Mißbrauch eines automatisierten Systems wird im allgemeinen aus der archivierten Nachricht nicht erkennbar sein. Es ist keinesfalls sicher, daß ein Fehler oder Mißbrauch überhaupt nachweisbare Spuren hinterlassen würde.

  Betroffene haben daher im Ernstfall keine Möglichkeit, ihre Aussagen durch Unterlagen zu stützen, und der Nachweis der Gegenseite beruht wesentlich auf der Aussage, ihr eigenes automatisiertes System sei sicher. Diese Aussage werden Außenstehende nur sehr selten widerlegen können. Gegen die Betroffenen werden damit Aussagen als Beweismittel genutzt, deren Wahrheitsgehalt allenfalls nur die Gegenseite beurteilen kann.

Daher habe ich vorgeschlagen, Verfahren mit elektronischer Unterschrift so zu gestalten, daß die Betroffenen als **Beweismittel** über Zusammenstellungen aller von ihnen veranlaßten Transaktionen verfügen. Bei einem Einspruch wären sie damit in der Lage nachzuweisen, daß bestimmte Transaktionen nicht oder nicht so von ihnen veranlaßt wurden.

Bei einer zur elektronischen Unterschrift verwandten Chipkarte könnte man etwa an eine nachträglich nicht beeinflußbare vollständige Archivierung von Nachweisen der unterschriebenen Dokumente – etwa der elektronischen Unterschriften – in der Chipkarte denken.

- Gefahr für die Anonymität von Transaktionen

  In einem automatisierten Zahlungssystem wird die elektronische Unterschrift häufig mit einer Zusatzinformation verbunden. Ein elektronischer Scheck wird etwa in einem bestimmten Geschäft unter Verwendung einer Chipkarte unterschrieben. Der unterschriebene Scheck enthält zwar keinerlei Aussage darüber, bei welcher Gelegenheit er unterschrieben wurde. Es ist aber damit zu rechnen, daß dem Scheck eine Information über seine Herkunft zugefügt wird, mit der er bei seiner weiteren automatisierten Bearbeitung verbunden bleibt. Zur Begründung wird gesagt werden, ohne eine solche Information könnten spätere Zweifelsfragen nicht hinreichend geklärt werden. Durch das Archivieren des elektronischen Schecks mit Herkunftsangabe entsteht aber bei der Bank oder Sparkasse eine Art **Verhaltensprofil** des einzelnen Kunden.

  Um das Erstellen von Verhaltensprofilen unmöglich zu machen, sollte das Gesamtverfahren so gestaltet werden, daß vom archivierten elektronischen Scheck nicht auf den Erstempfänger des Schecks geschlossen werden kann. Möglicherweise könnte auch die maschinenlesbare Archivierung elektronischer Schecks bei der Bank oder Sparkasse untersagt werden.

### 6.4.5 Zugriffssicherung

In fast jedem meiner Tätigkeitsberichte bestand Veranlassung, auf Schwächen des Paßwortschutzes einzugehen, die bei Kontrollbesuchen festgestellt wurden. Zur Rechtfertigung wird von den kontrollierten Stellen im allgemeinen angeführt, der sichere Paßwortschutz sei zu aufwendig, er belaste die Bediensteten zu sehr und hemme den Arbeitsablauf in untragbarer Weise. Nach allen bisherigen Erfahrungen gehe ich davon aus, daß ein Paßwortschutz nur selten die erforderliche Authentifizierung mit hinreichender Sicherheit gewährleistet.

Eine die Bediensteten weniger belastende Möglichkeit, die Benutzer von Datenverarbeitungsanlagen mit hinreichender Sicherheit zu authentifizieren, sehe ich in absehbarer Zeit vor allem über die Verwendung maschinenlesbarer Ausweise.

Bisher waren allerdings die auf dem Markt angebotenen Datenendgeräte noch nicht entsprechend ausgerüstet. Daher habe ich in der Vergangenheit immer

wieder die öffentlichen Stellen aufgefordert, die Hersteller durch Anfragen zu entsprechenden Entwicklungsarbeiten anzuregen und habe selbst auch einzelne Hersteller unmittelbar in diesem Sinne angesprochen. Das von den Anwendern und von mir geäußerte Interesse hat inzwischen zum Erfolg geführt. Datenendgeräte mit Zugriffssicherung über **Chipkarte** sind heute auf dem Markt erhältlich, und ich wiederhole daher meine schon mehrfach geäußerte Anregung, jedenfalls im Rahmen einer mittelfristigen Planung zu prüfen, ob zur Zugriffssicherung Chipkarten an Stelle des Paßwortschutzes eingesetzt werden können.

Im Rahmen eines Beratungsersuchens schilderte das Rechnungsprüfungsamt eines Kreises folgenden Sachverhalt: Der Leiter einer kommunalen Datenzentrale hat durch Dienstanweisung die Bediensteten angewiesen, bei einer die Dauer von neun Tagen überschreitenden Abwesenheit ihr Kennwort, das den Zugriff zu dem in der zentralen Datenverarbeitungsanlage geführten persönlichen **elektronischen Briefkasten** ermöglicht, an den jeweiligen Vertreter weiterzugeben. Die Beanstandung dieser Regelung durch das Rechnungsprüfungsamt hat der Leiter der Datenzentrale nicht anerkannt. Dem Schreiben des Rechnungsprüfungsamtes an mich und der beigefügten Korrespondenz war zu entnehmen, daß mit einem solchen Kennwort nicht nur der Zugriff zu den elektronischen Briefkästen der Bediensteten ermöglicht wird, sondern darüber hinaus der Zugriff zu Dateien mit personenbezogenen Daten, für die eine Eingabekontrolle erforderlich ist und daß im Rahmen dieses Zugriffs auch Änderungen möglich sind.

In meiner Stellungnahme wies ich darauf hin, daß es sehr bedenklich ist, wenn auf diese Weise die Vertreter unter den Namen der abwesenden Bediensteten Zugriff zu personenbezogenen Daten erhalten und sogar Änderungen durchführen können. Von den in § 10 Abs. 2 DSG NW genannten Anforderungen werden durch eine solche Regelung die Speicherkontrolle (Nr. 3), Benutzerkontrolle (Nr. 4), Zugriffskontrolle (Nr. 5) und Eingabekontrolle (Nr. 7) beeinträchtigt. Die Aussagekraft der personenbezogenen maschinellen Protokollierungen – wie etwa Aufzeichnungen zur Eingabekontrolle – wird dadurch erheblich beeinträchtigt. Auch der Hinweis in einem Schreiben des Leiters der Datenzentrale auf die Möglichkeit des Rückgriffs auf schriftliche Aufzeichnungen über die Abwesenheit der Bediensteten kann diese Bedenken nicht ausräumen.

So sollten jedenfalls Aufzeichnungen der Eingabekontrolle solange verfügbar sein, wie Daten, auf die sich diese Aufzeichnungen beziehen, unverändert in der Datei vorhanden sind. Bei einzelnen Dateien kann es daher erforderlich sein, Aufzeichnungen der Eingabekontrolle über eine lange Zeit aufzubewahren. Es muß jederzeit möglich sein, mit Hilfe dieser Aufzeichnungen zu rekonstruieren, wann und von wem die Daten eines Datenfeldes in die Datenverarbeitungsanlage eingegeben wurden. Mit der durch den Leiter der Datenzentrale getroffenen Regelung dürfte es kaum möglich sein, dieser Anforderung zuverlässig zu genügen.

Allerdings gehe ich davon aus, daß in dem vorliegenden Fall einfache Maßnahmen getroffen werden könnten, um den Anforderungen der Datenzentrale zu entsprechen und gleichzeitig die Datensicherheit in angemessenem Umfang zu gewährleisten. In diesem Zusammenhang habe ich auf folgendes hingewiesen:

- In seinem Schreiben betonte der Leiter der Datenzentrale: „Gerade externe Anwender dürften wenig Verständnis dafür aufbringen, wenn per Bürokommunikation übermittelte Post nicht beantwortet wird." Falls dieser Satz so zu verstehen ist, daß Briefe an die Datenzentrale direkt in die elektronischen Briefkästen der Bediensteten gelangen und dadurch dem regulären Geschäftsgang entzogen sind, wäre damit eine Regelung getroffen, die unter organisatorischen Gesichtspunkten bedenklich ist. Für diesen Fall regte ich an, einen speziellen – zentralen – elektronischen Briefkasten für eingehende Post einzurichten und für diesen eine Kennwort-Regelung vorzusehen, wie sie für eine Poststelle angemessen ist.
- Der Dienstanweisung war zu entnehmen, daß die Weitergabe des Kennworts deshalb erforderlich ist, weil anstehende Post, sofern kein Abruf erfolgt, nach neun Tagen gelöscht wird. Die Vorgabe des Zeitraums von neun Tagen war durch die Datenzentrale erfolgt. Eine wesentliche Verlängerung dieses Zeitraums könnte die bestehenden Schwierigkeiten beseitigen, ohne daß eine Weitergabe von Kennworten notwendig wird.
- Es wäre zu klären, ob und in welchem Umfang Sicherungskopien der gespeicherten Briefe angefertigt werden, die eine Rekonstruktion nach dem Löschen im Briefkasten ermöglichen.
- Darüber hinaus könnte der Leiter der Datenzentrale in Einzelfällen die Systemverwaltung beauftragen, die Inhalte der elektronischen Briefkästen in die Dokumentablagen der abwesenden Bediensteten zu stellen. Für derartige Fälle könnten zum Gewährleisten der Datensicherheit ergänzende Regelungen getroffen werden.

### 6.4.6 Eingabekontrolle, Übermittlungskontrolle

Aufzeichnungen der **Eingabekontrolle** (§ 10 Abs. 2 Nr. 7 DSG NW) sollten jedenfalls so lange aufbewahrt werden, wie die Daten, auf die sich diese Aufzeichnungen beziehen, unverändert in der Datei vorhanden sind. Es muß jederzeit möglich sein, mit Hilfe dieser Aufzeichnungen zu rekonstruieren, wann und von wem die Daten eines Datenfeldes in die Datenverarbeitungsanlage eingegeben wurden.

Bei einer kontrollierten Datenzentrale werden in verschiedenen Datenbeständen Daten gespeichert, die für Zwecke der Eingabekontrolle verwendbar sind. Während des Kontrollbesuchs wurde erörtert, daß es möglich sein muß, Fragen der Eingabekontrolle durch Auswerten dieser Datenbestände zu beantworten und daß dazu auch die für die Eingabekontrolle erforderlichen Daten während eines hinreichend langen Zeitraums archiviert werden müssen. Während des Kontrollbesuchs blieb offen, ob die Datenzentrale in jedem Fall in der Lage ist, den Anforderungen der Eingabekontrolle zu entsprechen.

Ich habe daher empfohlen zu überprüfen, ob für die Eingabekontrolle zusätzliche Maßnahmen erforderlich sind, und evtl. erforderliche zusätzliche Maßnahmen zu verwirklichen.

Die Anforderungen zur **Übermittlungskontrolle** nach dem Datenschutzgesetz Nordrhein-Westfalen vom 15. März 1988 unterscheiden sich von den Anforderungen zur Übermittlungskontrolle nach der bis zu diesem Zeitpunkt geltenden alten Fassung dieses Gesetzes. Nach der neuen Fassung des Datenschutzgesetzes muß es möglich sein zu überprüfen, welche Daten übermittelt worden sind, während es in der alten Fassung um die Möglichkeit ging zu überprüfen, welche Daten übermittelt werden können.

Die Datenzentrale berichtete, sie sei bisher noch nicht in jedem Fall in der Lage, den Anforderungen der Übermittlungskontrolle gemäß der neuen Fassung des Datenschutzgesetzes Nordrhein-Westfalen zu entsprechen. Es wurde besprochen, daß die Datenzentrale ihre Verfahren überprüfen und feststellen wird, ob und bei welchen Verfahren ergänzende Maßnahmen erforderlich sind, um den Anforderungen der Übermittlungskontrolle zu entsprechen. Evtl. erforderliche ergänzende Maßnahmen müssen getroffen werden.

### 6.4.7 „Löschen" oder „Aufgeben"

Selbst die irreführende Benutzung von Begriffen kann sich auf die Datensicherheit auswirken. Ein besonders bedenkliches Beispiel dafür liefert das Wort „Löschen". Löschen ist nach dem Datenschutzgesetz das Unkenntlichmachen gespeicherter Daten (§ 3 Abs. 2 Nr. 6 DSG NW). Unter Unkenntlichmachen ist ein Vorgang zu verstehen, der die gespeicherten Daten so verändert, daß deren Rekonstruktion unmöglich wird.

Beispiele für das Löschen sind etwa das Zerkleinern oder Verbrennen von Papier, wodurch die darauf aufgezeichneten Daten gelöscht werden oder bei Magnetbändern das Ändern von deren Magnetisierung in einem Löschgerät. In jedem dieser Fälle werden die aufgezeichneten Daten beim Löschen so verändert, daß es praktisch unmöglich gemacht wird, diese Daten zu rekonstruieren. Anforderungen an den Vorgang des Löschens sind auch in DIN-Normen festgelegt. So schreibt die Norm DIN 32 757 Anforderungen an das Vernichten von Informationsträgern vor.

Sehr bedauerlich und irreführend ist es, daß es üblich geworden ist, – entgegen dieser unstrittigen Bedeutung des Wortes „Löschen" – auch im Zusammenhang mit einer Gruppe von Maßnahmen anderer Art von „Löschen" zu sprechen. In der automatisierten Datenverarbeitung wird häufig vereinfachend gesagt, Daten seien gelöscht, wenn lediglich die bisherige Zugriffsmöglichkeit unterbunden wurde, während die Daten selbst unverändert gespeichert sind. Die angeblich gelöschten Daten sind in einem solchen Fall aber nicht gelöscht, da sie mit geeignetem Zusatzwissen rekonstruierbar sind.

Wenn in der Beschreibung des Betriebssystems eines PCs gesagt wird, eine Anweisung lösche die gespeicherten Daten, so ist leider keineswegs sicher,

daß die Daten nach diesem „Löschen" nicht mehr rekonstruierbar sind. Vielleicht wurde nur der Zugriff auf dem normalen Weg unmöglich gemacht, während eine Rekonstruktion mit geeigneten – und allgemein verbreiteten – Programmwerkzeugen keine Schwierigkeit bereiten würde. Es kann vorkommen, daß solche scheinbar gelöschten Daten noch nach Jahren unverändert auf der Festplatte eines PCs stehen und von dort auch gelesen werden können.

Von den PCs wurde diese unzulässige Verwendung des Wortes „Löschen" zur Textverarbeitung übernommen. Schon in meinem 10. Tätigkeitsbericht (S. 151 bis 153) wies ich auf die dadurch verursachte Irreführung der Benutzer hin. Falsche Verwendung des Wortes „Löschen" in den Bedienungshandbüchern führt dazu, daß vielen Benutzern nicht bekannt ist, daß scheinbar gelöschte Dokumente weiterhin unverändert auf den Festplatten ihrer Textverarbeitungssysteme stehen und von dort grundsätzlich auch wieder abgerufen werden können. Eine evtl. Unterscheidung zwischen logischem und physikalischem Löschen bringt zwar den Fachleuten der automatisierten Datenverarbeitung eine gewisse Klarheit, ist für die Benutzer von Textverarbeitungssystemen im allgemeinen aber nur verwirrend.

Damit führt aber die irreführende Benutzung des Wortes „Löschen" zu einer erheblichen Beeinträchtigung der Datensicherheit. Schützen wird man nur Daten, von deren Existenz man weiß. Gelöschte Daten wird niemand schützen, der – begrifflich zutreffend – davon ausgeht, daß deren Rekonstruktion als ausgeschlossen gelten kann.

Um die aus Gründen der Datensicherheit erforderliche begriffliche Klarheit zu erreichen, rege ich an, den bisher häufig als Löschen bezeichneten Vorgang, bei dem die Daten selbst erhalten bleiben und nur die normale Möglichkeit des Zugriffs genommen wird, als „Aufgeben" und nicht als „Löschen" zu bezeichnen. Damit würde der Begriff „Aufgeben" in der Bedeutung übernommen, die ihm in der Norm DIN 44 300 zugewiesen wird:

„aufgeben — Daten unzugänglich machen, indem nur die Verweise oder Zeiger auf diese Daten gelöscht werden, wobei die Daten selbst erhalten bleiben können."

Der Begriff „Löschen" bliebe dann – entsprechend den Begriffsbestimmungen im Datenschutzgesetz und auch in der Norm DIN 44 300 – solchen Vorgängen vorbehalten, die gewährleisten, daß die Rekonstruktion der Daten unmöglich ist.

Durch Verwendung des Begriffs „Aufgeben" für Vorgänge, bei denen Daten rekonstruierbar bleiben, wird die bisherige Irreführung vermieden, da dem Benutzer nicht suggeriert wird, diese Daten seien bereits unkenntlich gemacht. Aufgegebene Daten sind solange zu sichern, bis sie gelöscht sind. Die öffentlichen Stellen sollten selbst die Begriffe „Aufgeben" und „Löschen" in der hier dargelegten Bedeutung benutzen; sie sollten aber auch von den Lieferanten ihrer Software fordern, daß eine irreführende Verwendung des Wortes „Löschen" ausnahmslos zu unterbleiben hat.

### 6.4.8 Telefax

Bereits in meinem 10. Tätigkeitsbericht (S. 153 bis 155) habe ich auf die besondere Gefährdung der Datensicherheit bei der Übertragung von Schriftstücken durch Telefax hingewiesen und Maßnahmen genannt, um dennoch eine angemessene Datensicherheit zu gewährleisten. Die von mir aufgezeigten Gefahren sind inzwischen auch durch die Rechtsprechung bestätigt worden (vgl. Urteil OLG Nürnberg vom 26.11.1991, NJW-RR 1992, 703).

In einem Beratungsersuchen wurde jetzt an mich die Frage gerichtet, ob es zulässig sei, ein Telefaxgerät im Wartezimmer einer Hochschulklinik aufzustellen.

Bei der Übertragung medizinischer Daten als Fernkopie ist der Beeinträchtigung der Datensicherheit mit besonderen Maßnahmen zu begegnen. Hierbei ist zu berücksichtigen, daß es sich bei einer Fernkopie immer um eine offene Unterlage, vergleichbar etwa einer Postkarte, handelt. Jedenfalls muß daher gewährleistet sein, daß bei Absendung und Annahme das Schriftstück in einer Umgebung ist, in der medizinische Unterlagen offen vorliegen dürfen.

Bei der Absendung einer Fernkopie ist insbesondere zu beachten, daß

- sichergestellt ist, daß der Partner, zu dem beim Anwählen die Verbindung hergestellt wurde, auch der vorgesehene Empfänger ist,
- sichergestellt ist, daß eine Fernkopie mit medizinischen Daten ausschließlich in eine Umgebung kommt, in der medizinische Daten offen vorliegen dürfen. In diesem Zusammenhang habe ich besonders darauf hingewiesen, daß allein die Tatsache, daß der Empfänger zum Versand medizinischer Daten selbst ein Telefaxgerät benutzt, nicht gewährleistet, daß dort immer eine ausreichende Datensicherheit gegeben ist.

Bei der Annahme einer Fernkopie mit medizinischen Daten ist insbesondere zu beachten, daß

- die Fernkopie nur in einer Umgebung ankommen darf, in der medizinische Daten offen vorliegen dürfen. Insbesondere muß das Gerät des Empfängers in einer sicheren Umgebung stehen, und es muß gewährleistet sein, daß Unbefugte keinen Zugriff erhalten.

Ein Wartezimmer ist daher als Aufstellungsort für ein Telefaxgerät ungeeignet.

## 6.5 Konventionelle Datenverarbeitung

### 6.5.1 Vernichten von Unterlagen

Im Berichtszeitraum gab es wieder eine Reihe von spektakulären Aktenfundfällen. Amtliche Unterlagen, ja ganze Aktensammlungen mit teilweise sensiblen personenbezogenen Daten wurden im Abfall oder an anderen öffentlich zugänglichen Stellen entdeckt. Derartige gravierende Datenschutzverstöße, die zu Recht oft auch öffentliches Aufsehen erregen, lassen sich nur bei hoher

Sorgfalt in der Aufbewahrung und beim Vernichten solcher Unterlagen vermeiden.

Werden Datenträger 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). 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.

Eine öffentliche Stelle ist solange für die Sicherung von Unterlagen mit personenbezogenen Daten verantwortlich, wie diese nicht als vernichtet angesehen werden können. 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.

Die Vernichtung von Schriftgut einer öffentlichen Stelle durch ein Privatunternehmen ist Auftragsdatenverarbeitung, bei der der Auftraggeber für die Einhaltung der Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen und anderer Vorschriften über den Datenschutz verantwortlich bleibt (§ 11 Abs. 1 Satz 1 DSG NW). Auch ist dieser nach § 11 Abs. 3 Satz 1 DSG NW verpflichtet sicherzustellen, daß der Auftragnehmer die Bestimmungen des Datenschutzgesetzes Nordrhein-Westfalen befolgt und sich, sofern die Datenverarbeitung im Geltungsbereich dieses Gesetzes durchgeführt wird, der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft.

Eingaben und Beratungsersuchen gaben mir wiederholt Veranlassung, mich zu unterschiedlichen Anliegen beim Vernichten von Unterlagen zu äußern. Immer wieder mußte ich feststellen, daß eine erhebliche Unsicherheit bezüglich des Umfangs der Verantwortung und bezüglich der Technik und Organisation bestand. Zur Unterstützung bei diesen Fragen habe ich daher eine Organisationshilfe zur Datensicherung beim Vernichten von Unterlagen (Organisationshilfe-Unterlagenvernichtung; unten S. 158) erarbeitet und an die öffentlichen Stellen verteilt.

Die an mich gerichteten Fragen zur Vernichtung von Unterlagen waren von sehr unterschiedlicher Art. So wurde ich etwa gefragt, ob es zur Vernichtung von **Personalunterlagen** ausreiche, diese zu zerreißen. In meiner Antwort führte ich aus, daß es mit erheblichen Schwierigkeiten verbunden sein dürfte, den Anforderungen an ein ordnungsgemäßes Löschen gerecht zu werden, ohne sich dabei eines technischen Hilfsmittels – etwa eines Aktenvernichters – zu bedienen. Ein geeignetes Gerät für die Aktenvernichtung sollte daher verfügbar sein. Durch ergänzende organisatorische Maßnahmen sollte die öffentliche Stelle gewährleisten, daß in jedem Einzelfall eine ordnungsgemäße Durchführung der Vernichtung der Unterlagen erfolgt.

Bei der **Prüfung eines Vertrages**, der das Vernichten von Unterlagen einer öffentlichen Stelle zum Gegenstand hatte, stellte ich verschiedene Regelungen fest, die der Änderung bedürfen:

- Eigentum an den zu vernichtenden Unterlagen

  Die öffentliche Stelle ist für die Datensicherheit von Unterlagen, die vernichtet werden sollen, verantwortlich, bis deren Vernichtung abgeschlossen ist, d. h., bis die in den Unterlagen enthaltenen personenbezogenen Daten als gelöscht (§ 3 Abs. 2 Nr. 6 DSG NW) gelten können. Die öffentliche Stelle muß daher über alle Unterlagen mit personenbezogenen Daten bis zu deren Vernichtung uneingeschränkt verfügen können. Insbesondere dürfen bei derartigen Verträgen die zu vernichtenden Unterlagen mit personenbezogenen Daten vor Abschluß der Vernichtung nicht in das Eigentum Dritter übergehen.

- Vermischen mit den Unterlagen anderer Auftraggeber

  Vor der Vernichtung werden die Unterlagen der öffentlichen Stelle bei einer Zwischenlagerung mit den Unterlagen anderer Auftraggeber vermischt. Gegen dieses Vermischen der zu vernichtenden Unterlagen mit Unterlagen anderer Auftraggeber bestehen Bedenken, weil dadurch die Möglichkeiten der öffentlichen Stelle, Eigentumsrechte wahrzunehmen und das Vernichten zu kontrollieren, erschwert werden. Auch erscheint es sehr fraglich, ob die erforderliche Datensicherheit noch gewährleistet werden kann, falls andere Auftraggeber ebenfalls bezüglich ihrer zu vernichtenden Unterlagen, die mit denen der öffentlichen Stelle vermischt sind, Eigentums- und Kontrollrechte haben und von diesen Rechten Gebrauch machen. Im Hinblick auf diese Bedenken sollte mit dem Auftragnehmer ein anderer Ablauf der Vernichtung vereinbart werden.

- Löschen der personenbezogenen Daten

  Bedenklich ist auch, wenn der Vertrag keine Festlegung zu dem Zustand enthält, in dem sich das zu entsorgende Material befinden muß, um als vernichtet zu gelten.

- Unterauftragsverhältnisse

  In einem erläuternden Schreiben teilte mir die öffentliche Stelle mit, daß die Unterlagen ausschließlich in dem Datenträgervernichtungsbetrieb des Auftragnehmers vernichtet werden. Nach den mir vorliegenden Unterlagen mußte ich allerdings davon ausgehen, daß Unterauftragsverhältnisse nicht vertraglich ausgeschlossen waren. Der Vertrag sollte aber ein entsprechendes Verbot enthalten. Jede Weitergabe der Unterlagen an Dritte vor Abschluß der Vernichtung der Unterlagen sollte vertraglich ausgeschlossen sein.

- Zeitpunkt der Vernichtung

  Nach Aussage der öffentlichen Stelle war vereinbart, daß die Vernichtung innerhalb von längstens 24 Stunden vorgenommen wird. Dem Vertrag konnte ich allerdings eine entsprechende Verpflichtung des Auftragnehmers nicht entnehmen. Der Zeitpunkt der Vernichtung sollte in jedem Fall schriftlich vereinbart sein.

Auch im Rahmen von Kontrollbesuchen wurden von mir die Regelungen für das Vernichten von Unterlagen geprüft. Bei einer der kontrollierten Stellen erfolgt das Vernichten der Unterlagen durch eine Entsorgungsfirma. Innerhalb der öffentlichen Stelle wird ein Teil der Unterlagen durch Arbeitskräfte einer **Reinigungsfirma** eingesammelt.

In den Arbeitsräumen der öffentlichen Stelle 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 entsorgenden Unterlagen mit personenbezogenen Daten vorgesehen. Über das zweite Behältnis sollen sonstige Abfälle entsorgt werden.

Es ist Aufgabe der Reinigungskräfte, die Behältnisse zu leeren. Dabei wird der Inhalt der Papierkörbe in Plastiksäcken gesammelt und anschließend in einem abgeschlossenen Raum im Keller der öffentlichen Stelle abgelegt. Diese Arbeit wird von der Reinigungsfirma im Rahmen des mit dieser abgeschlossenen Gebäudereinigungsvertrages durchgeführt.

Sieht man von einer allgemeinen Verschwiegenheitsverpflichtung im Gebäudereinigungsvertrag ab, so enthält der mit der Reinigungsfirma abgeschlossene Vertrag keinerlei Regelungen zur zuverlässigen Entsorgung des Inhalts der Papierkörbe. Der Vertrag verpflichtet die Reinigungsfirma insbesondere nicht zu gewährleisten, daß der Inhalt der Papierkörbe durch die Reinigungskräfte sicher gehandhabt wird. Auch bei den Regelungen über die Aufsicht durch Aufsichtskräfte der Reinigungsfirma wird lediglich die gründliche und fachgerechte Reinigung und nicht die Datensicherheit beim Sammeln der in den Papierkörben abgelegten Unterlagen angesprochen.

Soweit das Reinigungsunternehmen Unterlagen aus den Papierkörben sammelt, in Plastiksäcken zusammenfaßt und in dem verschlossenen Keller ablegt, führt dieses 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 kommt in dem mit dem Reinigungsunternehmen abgeschlossenen Gebäudereinigungsvertrag bisher nicht zum Ausdruck. Die öffentliche Stelle berichtete allerdings, daß z. Z. ein neuer Gebäudereinigungsvertrag vorbereitet wird.

Ich habe empfohlen, in den neuen Gebäudereinigungsvertrag Regelungen aufzunehmen, die der Tatsache Rechnung tragen, daß es sich bei der Arbeit des Reinigungsunternehmens um Datenverarbeitung im Auftrag handelt, soweit das Reinigungsunternehmen im Rahmen des Löschens von Unterlagen tätig wird.

Von einem Verfahren, das mir praktikabel und sicher erschien, berichtete eine Stadt anläßlich eines Besuchs. Dort war geplant, für das Vernichten von Unterlagen, die im Rahmen der laufenden Arbeit an den Arbeitsplätzen ausgesondert werden, **Aktenvernichter** anzuschaffen. Man erwartete, für je 25 Bedienstete einen Aktenvernichter anschaffen zu müssen, damit nicht

durch zu lange Wege die Akzeptanz des Verfahrens gefährdet werde. Für das Vernichten von Unterlagen im Rahmen größerer Aussonderungsaktionen sollte ein Vertrag mit einer Entsorgungsfirma abgeschlossen werden.

Einem mir jetzt vorliegenden Bericht der Stadt ist zu entnehmen, daß das seinerzeit vorgestellte Büroabfallkonzept inzwischen umgesetzt wurde.

### 6.5.2 Aufbewahrung von Akten

Einer stärkeren Aufmerksamkeit bedarf nach meinem Eindruck die Datensicherheit bei der Aufbewahrung von Akten. Mehrfach mußte ich feststellen, daß selbst Akten mit sehr sensiblen Daten nur unzureichend gesichert werden. Als wichtig erscheint es mir in diesem Zusammenhang, darauf hinzuweisen, daß es nicht ausreichend ist, lediglich die technischen Voraussetzungen für eine sichere Aufbewahrung der Akten zu schaffen. Das Benutzen dieser technischen Voraussetzungen muß auch durch Dienstanweisung vorgeschrieben werden, und in angemessenem Umfang muß durch Kontrollen deren Einhaltung gewährleistet sein.

Die Presse hatte berichtet, in einem Gesundheitsamt seien **Unterlagen entwendet** worden. Meine Prüfung ergab, daß die Entwendung der Unterlagen dadurch erleichtert oder sogar erst ermöglicht worden war, daß gegen geltende Anweisungen verstoßen wurde. Der Schreibtisch, in dem sich die Unterlagen befunden hatten, war nicht verschlossen gewesen. Auch der Arbeitsraum war möglicherweise unverschlossen geblieben. Zwischenzeitlich veranlaßte bauliche Sicherheitsmaßnahmen sollten jetzt verhindern, daß Besucher unbemerkt die Flure betreten können.

Ich habe empfohlen, dem Gesundheitsamt vorzuschreiben, eine der Leitung des Amtes unmittelbar verantwortliche interne Kontrolle zu institutionalisieren, durch die die Einhaltung von Maßnahmen zur Datensicherheit kontrolliert wird. Darüber hinaus regte ich an zu prüfen, ob es angemessen ist vorzuschreiben, daß sich Besucher nur in Begleitung eines Berechtigten in dem durch die baulichen Sicherheitsmaßnahmen abgeschlossenen Bereich bewegen dürfen.

Nach einer Mitteilung des Direktors der Klinik einer Hochschule werden seit mehr als drei Jahren die **Patientenakten**, die sämtliche Krankengeschichten und alle erhobenen Befunde umfassen, in dieser Klinik in Aktenschränken aufbewahrt, die sich in den Fluren der der Allgemeinheit zugänglichen Poliklinik befinden. Die Aktenschränke beinhalten nach dieser Mitteilung mehr als 14 000 Patientenakten, die dem Arztgeheimnis unterliegen. Der Direktor der Klinik wies darauf hin, es sei nicht auszuschließen, daß Unbefugte sich mit verhältnismäßig geringen Mitteln der Akten bedienen können. Die Datensicherheit sei somit in seinen Augen nicht gewährleistet.

Auf meine Anfrage teilte mir die Hochschule mit, der vom Direktor der Klinik geschilderte Zustand werde im Rahmen einer kleinen Baumaßnahme in den nächsten Monaten behoben werden können. Es sei nämlich beabsichtigt, die derzeit noch auf den Fluren aufgestellten Aktenschränke in abschließbaren Räumen unterzubringen. Darüber hinaus werde ein Teil der Patientenakten in Kürze der Mikroverfilmung zugeführt werden.

Eine Ortsbesichtigung und Besprechung in der Klinik sowie ein vorhergehender und daran anschließender Schriftwechsel haben ergeben, daß es möglich ist, mit einem dem Schutzzweck angemessenen Aufwand Akten und Karteikarten der Klinik durch Verlagerung so unterzubringen, daß deren Sicherheit gewährleistet ist. Daß der dazu zu erbringende Aufwand im Verhältnis zu der erheblichen Gefährdung der Datensicherheit als angemessen anzusehen ist, kommt u. a. darin zum Ausdruck, daß die Hochschule zunächst mitteilte, den Zustand im Rahmen einer kleinen Baumaßnahme in den nächsten Monaten beheben zu können.

Von einer angemessenen Maßnahme kann dagegen nicht die Rede sein, wenn eine erhebliche Beeinträchtigung der Datensicherheit noch über Jahre bestehen bleibt, obgleich die Beseitigung innerhalb von Monaten möglich wäre. Da die Hochschule nach Ortsbesichtigung, Unterredung und längerem Schriftwechsel nicht bereit war, angemessene Maßnahmen zu treffen, um den Zugriff Unbefugter bei der Aufbewahrung der Akten und Karteikarten der Klinik zu verhindern, habe ich das Verhalten der Hochschule förmlich beanstandet.

### 6.5.3 Datenschutz im Bürgeramt

Als Eingabe erhielt ich eine Beschwerde über unzureichenden Datenschutz im Bürgeramt einer Stadt. Bei der Ortsbesichtigung wurde dann folgendes festgestellt: Das Bürgeramt war erst vor kurzer Zeit renoviert worden. Die räumlichen Gegebenheiten hatten dabei allerdings nur geringe Möglichkeiten geboten, eine hinreichende Trennung zwischen den Wartenden und den Arbeitsplätzen der Sachbearbeitung zu gewährleisten. Die Warteschlange begann daher jeweils direkt hinter den Arbeitsplätzen. Markierungen und eine schriftliche Bitte, Abstand zu halten, waren zwar vorhanden. Die räumliche Enge bewirkte aber, daß diese Hinweise – jedenfalls bei stärkerem Besucherandrang – nicht beachtet wurden. Die Gespräche konnten dann von Dritten mitgehört und vorgelegte Unterlagen eingesehen werden.

Die Stadt wurde darauf hingewiesen, daß das Grundrecht auf Datenschutz bei der Führung von Gesprächen mit vertraulichem Inhalt im Bürgeramt in angemessener Weise zu gewährleisten ist. Unterschiedliche Möglichkeiten wurden während der Ortsbesichtigung erörtert. Auf meine Empfehlung hat die Stadt inzwischen verschiedene Maßnahmen getroffen, um den Anforderungen des Datenschutzes trotz der schwierigen räumlichen Voraussetzungen zu entsprechen.

- Zur Optimierung der Geräuschkulisse wurde ein Akustiker gutachtlich eingeschaltet. Seiner Empfehlung folgend wird die Decke oberhalb der Wartezone mit Dämmplatten versehen. Der Gutachter geht davon aus, daß hierdurch der Geräuschpegel auf ein den Anforderungen entsprechendes Maß gesenkt werden kann.
- Es werden verschiedene Möglichkeiten getestet, um durch geeignete Einrichtungselemente – Stellwände, Ständer mit Unterlagen, Pflanzen – die Bedienung/Besucherplätze von der Wartezone weiter abzuschirmen.

Ich gehe davon aus, daß durch die Maßnahmen der Stadt in Zukunft die Vertraulichkeit der Gespräche im Bürgeramt gewährleistet wird.

### 6.5.4 Privatpost

Eine Eingabe gab mir Veranlassung, zu Regelungen bezüglich der Behandlung von Privatpost Stellung zu nehmen.

Die bei einer öffentlichen Stelle eingehende Post ist zunächst grundsätzlich als Dienstpost zu betrachten. Es ist jedoch eine Angelegenheit der Dienststelle sicherzustellen, daß persönliche Schreiben für die Beschäftigten ungeöffnet die Adressaten erreichen. Zu diesem Zweck sollte eine entsprechende Dienstanweisung erstellt werden, die allen Beschäftigten bekanntgegeben wird. Sie sollte klar festlegen, welche Eingänge ungeöffnet weitergeleitet werden sollen. Ist aus der Formulierung der Anschrift der private Charakter des Schreibens nicht zweifelsfrei ersichtlich, kann der Brief geöffnet werden. Wird dabei festgestellt, daß es sich um persönliche Post handelt, ist diese unmittelbar in einem verschlossenen Umschlag an den Empfänger weiterzuleiten und nicht auf den Dienstweg zu geben.

Bei persönlicher Post sollte der persönliche Charakter des Schreibens unmißverständlich aus der Anschrift hervorgehen. Um sicherzustellen, daß persönliche Post nicht durch die Poststelle geöffnet wird, sollten derartige Schreiben daher mit dem Zusatz „persönlich" versehen oder an „Herrn/Frau ... bei ..." gerichtet werden.

Ich halte es für zulässig, daß Postsendungen, die mit dem Zusatz „zu Händen von" versehen sind, von der Poststelle geöffnet werden. Eine entsprechende Regelung enthält auch Nr. 1.4 in Anlage 1 der Gemeinsamen Geschäftsordnung für die Ministerien des Landes Nordrhein-Westfalen (GGO) vom 16. Mai 1991 (SMBl. NW. 20020 S. 840): „Sendungen an das Ministerium mit dem Zusatz „eigenhändig" oder „zu Händen von ..." sowie Sendungen, die durch Boten übergeben werden, sind von der Poststelle wie die übrige Post auf dem normalen Weg in den Geschäftsgang zu geben, soweit es sich nicht erkennbar um Verschlußsachen im Sinne der Verschlußsachenanweisung handelt."

## 6.6 Unterrichtung über Anforderungen an die Datensicherheit

### 6.6.1 Organisationshilfen zur Datensicherung

Als Hilfsmittel zum Gestalten einer sicheren Datenverarbeitung werden von mir bereits seit einer Reihe von Jahren Organisationshilfen zur Datensicherung herausgegeben und an öffentliche Stellen in Nordrhein-Westfalen verteilt. Die Organisationshilfen enthalten Fragen zur Datensicherheit und einzelne Hinweise auf wesentliche Maßnahmen. Sie sollen helfen zu erkennen, unter welchen Gesichtspunkten die Datensicherheit zu überprüfen ist und welche Sicherungsziele im Einzelfall durch geeignete Maßnahmen in angemessenem Umfang erreicht werden müssen. Bei der Entscheidung über die zu treffenden

Maßnahmen müssen insbesondere die Empfindlichkeit der Daten und der Grad der Verbindlichkeit der Verarbeitungslogik berücksichtigt werden.

Durch Aufbau und Inhalt sind die Organisationshilfen aber nicht nur für Untersuchungen, die die Datensicherheit betreffen, geeignet. Sie können vielmehr in gleicher Weise als Hilfen bei der Entwicklung von Dienstanweisungen genutzt werden. Den Organisationshilfen können in diesem Fall Anregungen entnommen werden, welche Sachverhalte durch Dienstanweisung zu regeln sind und welcher Art die Regelungen zu sein haben, die im Einzelfall zu treffen sind.

Bisher wurden von mir vier Organisationshilfen herausgegeben und zwar die

- Organisationshilfe-Allgemeiner Teil (in einer Reihe von Auflagen),
- Organisationshilfe-PC,
- Organisationshilfe-Netze,
- Organisationshilfe-IDV.

Die Organisationshilfe-Allgemeiner Teil wurde im Berichtszeitraum überarbeitet und liegt nunmehr in einer neu erstellten Fassung vor.

Einen Schwerpunkt bei Beratungsersuchen der letzten Zeit bildete die Frage, auf welche Weise die Datensicherheit beim Vernichten von Unterlagen zu gewährleisten ist (oben S. 151). Gefragt wurde nach den Anforderungen an die einzusetzende Technik und nach einer dem Sicherungsziel angemessenen Organisationsform. Gefragt wurde auch nach den Grenzen der eigenen Verantwortung, die insbesondere dann von erheblicher Bedeutung sind, wenn das Vernichten der Unterlagen Dritten übertragen werden soll. Hinweise und Anregungen zu diesen Fragen können einer neu erstellten

- Organisationshilfe-Unterlagenvernichtung

entnommen werden. Auch diese Organisationshilfe wurde in Nordrhein-Westfalen an die öffentlichen Stellen verteilt.

Die Organisationshilfen kommen offensichtlich einem bestehenden Bedarf sehr entgegen. Laufend erreichen mich Anfragen und Bitten um Übersendung aus den unterschiedlichsten Bereichen. Für meine Arbeit bedeuten die Organisationshilfen eine wesentliche Stütze, die es mir ermöglicht, auf dem Gebiet der Datensicherheit insoweit meiner Beratungsaufgabe nach § 22 Abs. 2 Satz 1 DSG NW mit besonders geringem Personalaufwand möglichst weitgehend nachzukommen.

### 6.6.2 Sammelband Datensicherheit

Als Arbeitshilfe habe ich einen „Sammelband Datensicherheit" herausgegeben. Es handelt sich dabei um eine Zusammenstellung der Kapitel meiner zehn bisherigen Tätigkeitsberichte, die sich mit den technischen und organisatorischen Maßnahmen zum Datenschutz befassen. Bereits im Jahre 1988 hatte ich eine entsprechende Zusammenstellung aus den bis dahin erschienenen acht Tätigkeitsberichten herausgegeben, die allseits auf lebhaftes Interesse stieß.

Der Sammelband Datensicherheit bietet einen Überblick über meine Aussagen zu Fragen der Datensicherheit, und er liefert konkrete und auf die Praxis ausgerichtete Antworten auf zahlreiche Fragen aus diesem Gebiet. Ein ausführliches Stichwortverzeichnis macht es möglich, die Aussagen und Empfehlungen des Sammelbandes gezielt anzusprechen. Zusätzlich wurden dem Sammelband als Anhang Abdrucke der bis zur Herausgabe des Sammelbandes von mir erstellten Organisationshilfen zur Datensicherung (oben S. 157) angefügt.

Verteilt wurde der Sammelband Datensicherheit an die öffentlichen Stellen in Nordrhein-Westfalen. Weitere Anforderungen erreichen mich laufend.

Düsseldorf, den 17. Februar 1993

Maier-Bode

# Anlagen

**Anlage 1** (zu 3.)

**Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. April 1992**

**zum Grundrecht auf Datenschutz**

1. Seit dem Volkszählungsurteil des Bundesverfassungsgerichts im Jahre 1983 ist allgemein anerkannt, daß die Grundrechte auch die Befugnis des einzelnen umfassen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu entscheiden. Die Datenschutzbeauftragten treten dafür ein, dieses Recht ausdrücklich im Grundgesetz zu verankern. Damit würde

   - für die Bürger deutlicher erkennbar, daß unsere Verfassung ihr Recht auf Datenschutz in gleicher Weise garantiert wie die traditionellen Grundrechte,
   - der wachsenden Bedeutung des Datenschutzes für das Funktionieren der freiheitlichen Demokratie Rechnung getragen und auf die negativen Erfahrungen der DDR-Geschichte reagiert,
   - der Grundrechtskatalog dem technologischen Wandel angepaßt und
   - die Konsequenz aus den positiven Erfahrungen gezogen, die in mehreren Ländern des Bundes und im Ausland mit ähnlichen Verfassungsbestimmungen gemacht wurden.

   Die Konferenz begrüßt deshalb die Vorstellungen, die in der Verfassungskommission des Bundesrates entwickelt worden sind.

   Die Datenschutzbeauftragten empfehlen der Gemeinsamen Verfassungskommission des Bundestages und Bundesrates im Zusammenhang mit Art. 1 und Art. 2 GG den nachfolgenden Text zur Beratung:

   „Jeder hat das Recht, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen. Dazu gehört das Recht auf Auskunft und Einsicht in amtliche Unterlagen. Dieses Recht darf nur durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden, soweit überwiegende Interessen der Allgemeinheit es erfordern."

2. Darüber hinaus empfiehlt die Konferenz, die unabhängige Datenschutzkontrolle, die für die Verwirklichung des Grundrechts auf Datenschutz im Alltag von entscheidender Bedeutung ist, in der Verfassung zu verankern.

3. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es zusätzlich für erforderlich, in die Verfassungsdiskussion folgende Punkte miteinzubeziehen, die sich aus der Entwicklung der Informationstechnik ergeben:

   - Stärkung der Grundrechte aus Art. 10 und 13 im Hinblick auf neue Überwachungstechniken

- Recht auf Zugang zu den Daten der Verwaltung (Aktenöffentlichkeit, Informationsfreiheit)
- Instrumente zur Technikfolgenabschätzung.

**Anlage 2** (zu 5.3.3)

**Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. April 1992**

**zur Neuregelung des Asylverfahrens (BT-Drs. 12/2062)**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält Änderungen des Gesetzentwurfs zur Neuregelung des Asylverfahrens für erforderlich, insbesondere der geplanten Regelungen

1. über die erkennungsdienstliche Behandlung von Asylbewerbern zur Sicherung der Identität (§ 16 Abs. 1) und
2. über die Nutzung der dabei gewonnenen erkennungsdienstlichen Unterlagen zur Strafverfolgung und zur Gefahrenabwehr (§ 16 Abs. 5).

**Zu 1.:**

Nach dem geltenden Recht sind Lichtbilder und Fingerabdrucke bei Asylbewerbern nur dann zu fertigen, wenn deren Identität nicht eindeutig bekannt ist. Demgegenüber sieht der Gesetzentwurf zur Neuregelung des Asylverfahrens vor, daß von sämtlichen Asylbewerbern – bis auf wenige Ausnahmen – Lichtbilder und Fingerabdrucke zu fertigen sind. Dies ist mit dem Verfassungsgrundsatz der Verhältnismäßigkeit nicht vereinbar:

Der Staat hat selbstverständlich das Recht zu wissen, mit wem er es zu tun hat. Jeder – gleichgültig ob Deutscher oder Ausländer – muß sich deshalb durch Dokumente ausweisen können; nur wenn Zweifel an der Identität bestehen, kommen erkennungsdienstliche Maßnahmen in Betracht. Dieser Grundsatz unserer Rechtsordnung muß auch im Rahmen der Neuregelung des Asylverfahrens beachtet werden. Nur wenn feststeht, daß die Identität eines hohen Anteils der Asylbewerber – also nicht bloß diejenige einzelner oder bestimmter Gruppen – zweifelhaft ist, wäre eine erkennungsdienstliche Behandlung aller Asylbewerber gerechtfertigt. Gerade dies aber ist bisher nicht hinreichend belegt: In der amtlichen Begründung des Gesetzentwurfs ist allein davon die Rede, daß nach Feststellung niederländischer Behörden 20 % der Asylbewerber unter falschem Namen einen weiteren Asylantrag stellen. Aussagekräftige Angaben, in welchem Umfang in der Bundesrepublik Deutschland Asylbewerber unter Täuschung über ihre Identität gleich bei der ersten Antragstellung oder nach dessen Ablehnung erneut versuchen, Asyl zu erhalten, fehlen bislang.

**Zu 2.:**

Bei der zentralen Auswertung der Fingerabdrucke von Asylbewerbern durch das Bundeskriminalamt muß – ungeachtet dessen, ob das Bundeskriminalamt dabei in eigener Zuständigkeit oder für das Bundesamt für die Anerkennung ausländischer Flüchtlinge tätig wird – unbedingt folgendes sichergestellt sein:

- Fingerabdrucke von Asylbewerbern, die unter Beachtung des zu Nr. 1 Gesagten gefertigt wurden, dürfen nur gespeichert werden, soweit dies zur Sicherung der Identität unbedingt erforderlich ist. Dazu reicht die bisher vom Bundeskriminalamt angewandte Methode der sog. Kurzsatzverformelung der Fingerabdrucke aus. Gerade aber dabei soll es nicht bleiben:

  Mit der bevorstehenden Einführung von AFIS – einem neuen automatisierten Fingerabdruckverfahren – sollen künftig auch die Fingerabdrucke von Asylbewerbern, die allein zur Feststellung deren Identität gefertigt wurden, genauso erfaßt und ausgewertet werden wie die Fingerabdrucke mutmaßlicher oder tatsächlicher Straftäter. Asylbewerber würden damit von vornherein wie Straftäter behandelt. Eine solche Verfahrensweise wird dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot nicht gerecht. Zudem unterläuft sie die in § 16 Abs. 4 des Gesetzentwurfs vorgesehene Trennung der erkennungsdienstlichen Unterlagen von Asylbewerbern und Straftätern. Um die gebotene Differenzierung sicherzustellen, sollte – über das Trennungsgebot des § 16 Abs. 4 hinaus – die Verformelung auf den Abdruck eines Fingers des Asylbewerbers beschränkt werden, da dies zur eindeutigen Feststellung seiner Identität genügt.

- Die Datenschutzbeauftragten verkennen nicht, daß es unter Umständen im überwiegenden Allgemeininteresse notwendig sein kann, im Rahmen asylrechtlicher Identitätsfeststellung gefertigte Fingerabdrucke für Zwekke der Strafverfolgung zu nutzen. Weil eine solche Verwendung einen neuen und zudem erheblichen Eingriff in das Grundrecht auf Datenschutz darstellt, darf sie nicht – wie es der Gesetzentwurf aber vorsieht – praktisch voraussetzungslos erfolgen. Notwendig ist vielmehr, die Voraussetzungen in einem abschließenden Straftatenkatalog aufzuführen; darin könnten auch die in der amtlichen Begründung des Gesetzentwurfs erwähnten Fälle des Sozialhilfebetrugs enthalten sein.

- Ein entsprechender Maßstab ist an die Regelung anzulegen, wann zur Identitätssicherung gefertigte Fingerabdrucke von Asylbewerbern zur polizeilichen Gefahrenabwehr genutzt werden dürfen. Eine solche Nutzung sollte nur zugelassen werden, soweit dies zur Abwehr einer gegenwärtigen erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist.

**Anlage 3** (zu 5.6.2)

**Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992**

**zum „Lauschangriff"**

Die Datenschutzbeauftragten des Bundes und der Länder erklären (bei Gegenstimme des LfD Bayern);

Nachdem erst vor kurzem mit dem Gesetz zur Bekämpfung der organisierten Kriminalität die Befugnisse der Strafverfolgungsbehörden erheblich erweitert

worden sind und obwohl über den Erfolg dieser Maßnahmen noch keine Erfahrungen gesammelt werden konnten, wird gegenwärtig parteiübergreifend vielfach die Forderung erhoben, der Polizei in bestimmten Fällen das heimliche Abhören und Herstellen von Bild- und Tonaufzeichnungen in und aus Wohnungen (sog. „Lauschangriff") zu ermöglichen.

1. Das Grundgesetz gewährt jedem einen unantastbaren Bereich privater Lebensgestaltung, der der Einwirkung der öffentlichen Gewalt entzogen ist. Dem einzelnen muß um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein „Innenraum „ verbleiben, in dem er „sich selbst besitzt" und „in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt" (BVerfGE 27,1 ff.). Jedem muß ein privates Refugium, ein persönlicher Bereich bleiben, der obrigkeitlicher Ausforschung – insbesondere heimlicher – entzogen ist. Dies gilt gegenüber Maßnahmen der Strafverfolgung vor allem deshalb, weil davon auch unverdächtige oder unschuldige Bürger betroffen sind. Auch strafprozessuale Maßnahmen dürfen nicht den Wesensgehalt eines Grundrechts, insbesondere nicht das Menschenbild des Grundgesetzes verletzen.

2. Die Datenschutzbeauftragten nehmen die Gefahren, die das organisierte Verbrechen für die Opfer und auch für die Demokratie und den Rechtsstaat heraufbeschwört, sehr ernst. Sie sind allerdings der Meinung, daß eine angemessene Abwägung zwischen der Verfolgung der organisierten Kriminalität und dem Schutz der Persönlichkeitsrechte der Bürger geboten und möglich ist und es eine Wahrheitserforschung um jeden Preis auch künftig im Strafprozeßrecht nicht geben darf. Daraus folgt, daß der Lauschangriff auf Privatwohnungen für Zwecke der Strafverfolgung auch in Zukunft nicht erlaubt werden darf.

3. Eine andere Frage ist, ob und unter welchen Voraussetzungen der Gesetzgeber für Räume, die allgemein zugänglich sind oder beruflichen oder geschäftlichen Tätigkeiten dienen (z. B. Hinterzimmer von Gaststätten, Spielcasinos, Saunaclubs, Bordelle), einen Lauschangriff zulassen kann. Hierfür sind Mindestvoraussetzungen ein eng begrenzter abschließender Straftatenkatalog, die Verwendung der gewonnenen Erkenntnisse ausschließlich zur Verfolgung dieser Straftaten, ein strikter Richtervorbehalt sowie die Wahrung besonderer Amts- und Berufsgeheimnisse.

**Anlage 4** (zu 5.9.2)

**Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992**

**zum Entwurf eines Gesetzes zur Sicherung und Strukturverbesserung der gesetzlichen Krankenversicherung**

**Gesundheits-Strukturgesetz 1993**

Die Bundesregierung will mit dem Gesundheits-Strukturgesetz dem Kostenanstieg in der gesetzlichen Krankenversicherung entgegenwirken. Dieses

begrüßenswerte Ziel soll nach dem vorgelegten Gesetzentwurf u. a. auch durch eine verstärkte automatisierte Datenverarbeitung erreicht werden. Die damit verbundenen Eingriffe in die Persönlichkeitsrechte der Versicherten und in die sie schützende ärztliche Schweigepflicht müssen auf das unbedingt Notwendige beschränkt werden. Die Datenschutzkonferenz hält vor allem folgende Verbesserungen des Gesetzentwurfs für notwendig:

- Der Gesetzentwurf sieht vor, daß die Krankenhäuser den Krankenkassen mehr Versichertendaten zur Verfügung stellen müssen als bisher. Es sollte deshalb eingehend geprüft werden, ob die Krankenkassen tatsächlich alle geforderten Angaben benötigen; die Aufgabenteilung zwischen Krankenkassen und Medizinischem Dienst muß aufrechterhalten bleiben.
- Für das Modellvorhaben zur Überprüfung des Krankenhausaufenthalts müssen die Erhebung, Verwendung und Löschung von Versichertendaten durch den Medizinischen Dienst präziser als bisher vorgesehen geregelt werden.
- Beim Einzug der Vergütung der Krankenhausärzte für Wahlleistungen durch Krankenhäuser sollte die Einschaltung privater Abrechnungsstellen ohne Einwilligung der Patienten nicht zugelassen werden, da dabei Abrechnungsdaten an Dritte offenbart werden. Die Daten sind gegen unbefugte Offenbarung und Beschlagnahme rechtlich besser geschützt, wenn sie – auch zur Abrechnung – im Krankenhaus verbleiben. Die Krankenhäuser sind zudem selbst in der Lage, die Vergütung einzuziehen.
- Für die neu vorgesehenen Patienten-Erhebungsbogen zur Ermittlung des Bedarfs an Pflegepersonal im Krankenhaus sollte eine strikte Zweckbindung sowie eine frühestmögliche Löschungs- oder Anonymisierungspflicht festgelegt werden. Eine Überlassung der Patienten-Erhebungsbogen in der im Gesetzentwurf vorgesehenen Fassung an die Krankenkassen ist abzulehnen.

**Anlage 5** (zu 5.9.7)

**Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992**

**zur Chip-Karte als elektronische Krankenversicherungskarte**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt wegen der wachsenden Automatisierung bei allen Institutionen des Gesundheitswesens und der Erweiterung des Anteils maschinenlesbarer Datenträger fest, daß eine Speicherung auf einer Chip-Karte als elektronische Krankenversicherungskarte auf die gesetzlich festgelegten Grunddaten beschränkt bleiben muß und nicht auf Gesundheitsdaten ausgedehnt werden darf. Eine technische Sicherung dieser Beschränkung ist zu gewährleisten.

**Anlage 6** (zu 5.11.1)

**Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. März 1992**

**zum Arbeitnehmerdatenschutz**

I.

Im Rahmen des Arbeitsverhältnisses werden personenbezogene Daten aus ganz unterschiedlichen Lebensbereichen des Arbeitnehmers erhoben und gespeichert. Diese Daten verwendet der Arbeitgeber nicht nur für eigene Zwecke. Aus dem Arbeitsverhältnis ergeben sich auch Auskunfts-, Bescheinigungs- und Meldepflichten, die der Arbeitgeber gegenüber öffentlichen Stellen zu erfüllen hat. Durch die Möglichkeit, im Arbeitsverhältnis anfallende personenbezogene Daten miteinander zu verknüpfen und sie – losgelöst vom Erhebungszweck – für andere Verwendungen zu nutzen, entstehen Gefahren für das Persönlichkeitsrecht des Arbeitnehmers. Mit der Intensität der Datenverarbeitung, insbesondere durch Personalinformationssysteme und digitale Telekommunikationsanlagen, nehmen die Kontroll- und Überwachungsmöglichkeiten des Arbeitgebers zu.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb bereits seit 1984 bereichspezifische und präzise gesetzliche Bestimmungen zum Arbeitnehmerdatenschutz. Bundestag, Bundesrat und Bundesregierung haben ebenfalls eine Regelungsnotwendigkeit bejaht; gleichwohl stehen bundesgesetzliche Regelungen über den allgemeinen Arbeitnehmerdatenschutz immer noch aus.

Die Notwendigkeit zur gesetzlichen Regelung besteht unabhängig davon, ob Arbeitnehmerdaten in automatisierten Dateien, in Akten oder in sonstigen Unterlagen verarbeitet werden. Der erhöhten Gefährdung durch die automatisierte Datenverarbeitung ist durch spezifische Schutzvorschriften Rechnung zu tragen.

Angesichts der besonderen Abhängigkeit des Arbeitnehmers im Arbeitsverhältnis und während der Phase einer Bewerbung um einen Arbeitsplatz ist durch Gesetz zu untersagen, daß Rechte, die dem Arbeitnehmer nach einschlägigen Datenschutzvorschriften zustehen, durch Rechtsgeschäft, Tarifvertrag und Dienst- oder Betriebsvereinbarung ausgeschlossen werden. Außerdem ist durch Gesetz festzulegen, daß eine Einwilligung des Arbeitnehmers oder Bewerbers nur dann als Grundlage einer Datenerhebung, -verarbeitung oder -nutzung in Frage kommt, wenn die Freiwilligkeit der Einwilligung sichergestellt ist, also die Einwilligung ohne Furcht vor Nachteilen verweigert werden kann. Deshalb dürfen allein aufgrund einer Einwilligung z. B. keine Gesundheitszeugnisse, Ergebnisse von Genomanalysen u. ä. angefordert werden, wenn sie den Rahmen des Fragerechts des Arbeitgebers überschreiten.

II.

Die gesetzliche Ausgestaltung des Arbeitnehmerdatenschutzes muß insbesondere folgende Grundsätze beachten:

1. Die Datenerhebung muß grundsätzlich beim Arbeitnehmer erfolgen.
2. Der Arbeitgeber darf Daten des Arbeitnehmers – auch durch Befragen des Arbeitnehmers oder Bewerbers – nur erheben, verarbeiten oder nutzen, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Arbeitsverhältnisses erforderlich oder sonst gesetzlich vorgesehen ist. Dabei ist der Grundsatz der Zweckbindung zu beachten. Auch ist zwischen der Bewerbungs- und Einstellungsphase zu unterscheiden.
3. Der Arbeitgeber darf Daten, die er aufgrund gesetzlicher Vorgaben für andere Stellen (z. B. Sozialversicherungsträger) erheben muß, nur für diesen Zweck verwenden.
4. Eine Datenauswertung und -verknüpfung, die zur Herstellung eines umfassenden Persönlichkeitsprofils des Arbeitnehmers führen kann, ist unzulässig.
5. Beurteilungen und Personalauswahlentscheidungen dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen werden.
6. Notwendige Datenübermittlungen zwischen Arzt und Arbeitgeber sind eindeutig zu regeln. Dem Arbeitgeber darf grundsätzlich nur das Ergebnis der ärztlichen Untersuchung zugänglich gemacht werden. Darüber hinaus dürfen ihm – soweit erforderlich – nur tätigkeitsbezogene Risikofaktoren mitgeteilt werden. Medizinische und psychologische Befunde sind getrennt von den übrigen Personalunterlagen aufzubewahren. Die Ergebnisse medizinischer oder psychologischer Untersuchungen und Tests des Beschäftigten dürfen automatisiert nur verarbeitet werden, wenn dies dem Schutz des Beschäftigten dient.
7. Dem Arbeitnehmer sind umfassende Auskunfts- und Einsichtsrechte in die Unterlagen einzuräumen, die sein Arbeitsverhältnis betreffen. Diese Rechte müssen sich auch auf Herkunft, Verarbeitungszwecke und Empfänger der Daten sowie die Art und Weise ihrer Auswertung erstrecken.
8. Dem Personal-/Betriebsrat muß ein Mitbestimmungsrecht bei der Einführung, Anwendung und der wesentlichen Änderung von automatisierten Dateien mit personenbezogenen Daten der Arbeitnehmer für Zwecke der Personalverwaltung zustehen. Das gilt auch bei sonstigen technischen Einrichtungen, mit denen das Verhalten und die Leistung der Beschäftigten überwacht werden kann.
9. Gesetzlich festzulegen ist, welche Daten der Arbeitnehmervertretung für ihre Aufgabenerfüllung zugänglich sein müssen und wie der Datenschutz bei der Verarbeitung von Arbeitnehmerdaten im Bereich der Arbeitnehmervertretung gewährleistet wird. Regelungsbedürftig ist auch das

Verhältnis zwischen dem Personal-/Betriebsrat und dem behördlichen/betrieblichen Datenschutzbeauftragten.

10. Die Befugnis des Personal-/Betriebsrats, sich unmittelbar an die Datenschutzkontrollinstanzen zu wenden, ist gesetzlich klarzustellen.

11. Arbeitnehmerdaten dürfen nur dann ins Ausland übermittelt werden, wenn dort ein dem deutschen Recht vergleichbarer Datenschutzstandard gewährleistet ist oder wenn der Betroffene nach den oben genannten Grundsätzen (vgl. Abschn. I Abs. 4) eingewilligt hat.

**Anlage 7** (zu 5.19)

**Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 8. März 1991**

**Telekommunikation und Datenschutz**

I.

Die Telekommunikation hat außerordentlich stark an Bedeutung gewonnen und ersetzt häufig den Brief oder auch das persönliche Gespräch: Über die dreißig Millionen deutschen Telefone werden monatlich rund drei Milliarden Gespräche geführt. Für die Privatsphäre des Bürgers in einer freiheitlichen Gesellschaft ist es unverzichtbar, daß Telefongespräche unkontrolliert und unbeobachtet geführt werden können. Von existentieller Bedeutung wird dies, wenn der Bürger in Notlagen gerät, aus denen er sich nur mit vertraulicher Beratung und Hilfe befreien kann. Daher unterstützen sowohl die Kirchen als auch Hilfs- und Beratungsorganisationen die Forderung, das „Grundrecht auf unbeobachtete Kommunikation" zu sichern.

Dieser Forderung muß die technische Ausgestaltung der Telekommunikationsnetze und -dienste folgen, und die rechtlichen Regelungen müssen diesen sich aus der Verfassung ergebenden Auftrag erfüllen. Der Gesetzgeber hat in dem am 01.07.1989 in Kraft getretenen Poststrukturgesetz die Bundesregierung aufgefordert, „Rechtsverordnungen zum Schutz personenbezogener Daten der am Fernmeldeverkehr Beteiligten" zu erlassen. Der Ausschuß für Post und Telekommunikation und der Innenausschuß des Deutschen Bundestages haben mehrfach den Schutz des Fernmeldegeheimnisses angemahnt.

Die vom Bundesminister für Post und Telekommunikation vorgelegten Entwürfe von Verordnungen über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM (TDSV) und über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (UDSV), widersprechen in wesentlichen Punkten dem Grundrecht auf unbeobachtete Kommunikation. Dabei ist besonders unverständlich, daß der Bundesminister von bereits früher gemachten Zusagen an den Deutschen Bundestag wieder abgerückt ist.

Die Entwürfe bleiben in wichtigen Punkten unter dem Datenschutzniveau, das von der EG-Kommission in ihrem Richtlinienentwurf zum Schutz perso-

nenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen für den europäischen Binnenmarkt angestrebt wird.

II.

Ein wesentlicher Mangel besteht in der beabsichtigten Vollerfassung aller Verbindungsdaten von Telefongesprächen: Für jedes Telefonat soll bis zur Versendung der Entgeltrechnung bei der Deutschen Bundespost TELEKOM festgehalten werden dürfen, wer wann wie lange und mit wem telefoniert hat, nach Wahl des Kunden achtzig Tage darüber hinaus. Eine monatliche Auflistung dieser dem Fernmeldegeheimnis unterliegenden Informationen (Einzelentgeltnachweis) sollen Kunden – auch Arbeitgeber – auf Wunsch erhalten können. Außerdem können nach § 12 Fernmeldeanlagengesetz (FAG) auch Gerichte und Staatsanwaltschaften bei strafrechtlichen Ermittlungen jeder Art, also auch bei Bagatelldelikten, ohne besondere Voraussetzungen auf diese Daten zugreifen.

Abzulehnen ist auch die vorgesehene Beschränkung des Kunden auf die Alternative, daß von einem Anschluß die Telefonnummer des Anrufers immer oder nie beim Angerufenen angezeigt wird. Dem Recht auf informationelle Selbstbestimmung entspricht es, daß der Anrufer in jedem Einzelfall entscheiden kann, ob seine Rufnummer beim Angerufenen angezeigt wird. Umgekehrt hat jeder Angerufene selbstverständlich das Recht, nur Gespräche entgegenzunehmen, bei denen die Nummer des Anrufers angezeigt wird.

III.

Die Datenschutzbeauftragten fordern:

1. Alle – durch die computergesteuerte Vermittlungstechnik entstehenden – Verbindungsdaten sind nach dem Ende der Verbindung mit folgender Maßgabe unverzüglich zu löschen:

   In die Entgeltdatenverarbeitung dürfen nur diejenigen Daten eingehen, die zur Berechnung der Entgelte in Summenform unerläßlich sind. Auf Antrag des Kunden darf zur Prüfung der Richtigkeit des in Rechnung gestellten Entgelts oder zur Erstellung des Einzelentgeltnachweises die Rufnummer des Angerufenen nur in einer zumindest um die letzten vier Ziffern verkürzten Form gespeichert werden. Die Daten sind spätestens achtzig Tage nach dem Absenden der Entgeltrechnung zu löschen.

   Die Entscheidung des Kunden über die Form der Abrechnung muß auch bei der Abrechnung zwischen verschiedenen Netzbetreibern respektiert werden.

2. Die Erstellung von „Kommunikationsprofilen", die Aussagen über das persönliche Telefonierverhalten des Bürgers und die Nutzung anderer Telekommunikationsdienste enthalten, muß ausgeschlossen sein.

3. Bei der Anzeige der Rufnummer des Anrufers beim Angerufenen müssen beide die Wahlmöglichkeit haben, diese Anzeige entweder auf Dauer oder im Einzelfall „auf Knopfdruck" zu unterdrücken.

4. Ausnahmen von diesen Grundsätzen – zum Beispiel zur Aufklärung telefonischer Bedrohungen oder in Notfällen – müssen begründet, ausdrücklich geregelt und für den Betroffenen transparent sein.

5. Die Konferenz bekräftigt ihre Forderung (Beschluß vom 4./5.10.1990), Eingriffe in das grundgesetzlich geschützte Fernmeldegeheimnis (Art. 10 GG) auf das unerläßliche Maß zu beschränken und insbesondere nicht schon im Bereich der Bagatellkriminalität zuzulassen. Die Regelung des § 12 FAG hat im Zuge der technischen Entwicklung eine verfassungsrechtlich bedenklich neue Qualität erhalten, da sie nunmehr auch die bei Einsatz neuer Kommunikationstechniken anfallenden Abrechnungs-, Verbindungs-, Nutzungs- und Inhaltsdaten umfaßt. Statt im FAG sollten die Eingriffsmöglichkeiten in das Fernmeldegeheimnis im Rahmen der Strafverfolgung – schon aus Gründen der Normenklarheit – in der Strafprozeßordnung unter engen Voraussetzungen und Beschränkungen abschließend geregelt werden.

**Anlage 8** (zu 5.19)

**Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992**

**zum Datenschutz bei internen Telekommunikationsanlagen**

Der zunehmende Einsatz von digitalen Telekommunikationsanlagen (TK-Anlagen) in Wirtschaft und Verwaltung birgt Datenschutzrisiken in sich, denen durch eine datenschutzfreundliche Ausgestaltung der Technik und durch geeignete bereichspezifische Regelungen entgegengewirkt werden muß. Telefongespräche stehen – auch wenn sie von einem Dienstapparat aus geführt werden – unter dem Schutz des Grundgesetzes. Dies hat das Bundesverfassungsgericht in seiner neueren Rechtsprechung hervorgehoben.

Der Schutz des Fernmeldegeheimnisses und des nichtöffentlich gesprochenen Wortes ist gerade bei Arbeitnehmern bedeutsam, da diese sich in einem besonderen Abhängigkeitsverhältnis befinden; aber auch das informationelle Selbstbestimmungsrecht Dritter, die anrufen oder angerufen werden, muß gewahrt werden.

Entsprechende bundesrechtliche Regelungen für interne TK-Anlagen sind überfällig, da in diesen Anlagen – insbesondere wenn sie digital an das öffentliche ISDN angeschlossen sind – umfangreiche Sammlungen sensibler personenbezogener Daten entstehen können, die sich auch zur Verhaltens- und Leistungskontrolle eignen und zudem Hinweise auf das Kommunikationsverhalten aller Gesprächsteilnehmer geben.

Die Regelungen sollten verbindliche Vorgaben für die technische Ausgestaltung von TK-Anlagen geben und den Umfang der zulässigen Datenverarbeitung festlegen:

- Es müssen die technischen Voraussetzungen gewährleistet sein, daß Anrufer und Angerufene die Rufnummernanzeige fallweise abschalten können.

- Die automatische Speicherung der Rufnummern von externen Anrufern nach Beendigung des Telefongesprächs ist auszuschließen, es sei denn, eine sachliche Notwendigkeit besteht hierfür (z. B. bei Feuerwehr und Rettungsdiensten).
- Die Weiterleitung eines Anrufs an einen anderen als den gewählten Anschluß sollte dem Anrufer so rechtzeitig signalisiert werden, daß dieser den Verbindungsaufbau abbrechen kann.
- Das Mithören und Mitsprechen weiterer Personen bei bestehenden Verbindungen sollte nur nach eindeutiger und rechtzeitiger Ankündigung möglich sein.
- Verbindungsdaten einschließlich der angerufenen Telefonnummern sollten nach Beendigung der Gespräche nur insoweit gespeichert werden, als dies für Abrechnungszwecke und zulässige Kontrollzwecke erforderlich ist. Die Nummern der Gesprächspartner von Arbeitnehmervertretungen, internen Beratungseinrichtungen und sonstigen auf Vertraulichkeit angewiesenen Stellen dürfen nicht registriert werden.
- Die TK-Anlagen müssen durch geeignete technische Maßnahmen gegen unberechtigte Veränderungen der Systemkonfiguration und unberechtigte Zugriffe auf Verbindungs- und Inhaltsdaten geschützt werden.

Da TK-Anlagen geeignet sind, das Verhalten und die Leistung der Arbeitnehmer zu kontrollieren, und sie überdies häufig die Arbeitsplatzgestaltung beeinflussen, löst ihre Einführung in Betrieben und Behörden Mitbestimmungsrechte der Betriebsräte und überwiegend auch der Personalräte aus. Sie dürfen daher nur betrieben werden, wenn unter Beteiligung der Arbeitnehmervertretungen verbindlich festgelegt wurde, welche Leistungsmerkmale aktiviert und unter welchen Bedingungen sie genutzt werden, welche Daten gespeichert, wie und von wem sie ausgewertet werden. Die Nutzer der TK-Anlage sind über den Umfang der Datenverarbeitung umfassend zu unterrichten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, daß umgehend datenschutzrechtliche Regelungen für den Einsatz und die Nutzung von internen TK-Anlagen mit einer bereichsspezifischen Rechtsgrundlage für die Verarbeitung von Arbeitnehmerdaten geschaffen werden.

# Stichwortverzeichnis

Die fettgedruckten Zahlen weisen auf den jeweiligen Tätigkeitsbericht, die übrigen Zahlen auf die Seiten hin.

**S**