Der Landesbeauftragte für den Datenschutz Nordrhein-Westfalen

10. Tätigkeitsbericht

Zehnter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Nordrhein-Westfalen

für die Zeit vom 1. Januar 1989
bis zum 31. Dezember 1990

Herausgeber: Der Landesbeauftragte
für den Datenschutz Nordrhein-Westfalen
Reichsstraße 43, 4000 Düsseldorf 1
ISSN 0179-2431
Druck: Moeker Merkur · Köln

Gliederung

1. Einleitung

1.1 Vorbemerkung

Die Entwicklung des Datenschutzes in den Jahren 1989 und 1990 ist gekennzeichnet durch wichtige Fortschritte in der Gesetzgebung, durch die zunehmende Bedeutung des grenzüberschreitenden Austauschs personenbezogener Daten, durch das Zusammenwachsen der beiden deutschen Staaten und durch die sich weiter beschleunigende Einführung neuer Informations- und Kommunikationstechniken in allen Bereichen der öffentlichen Verwaltung.

Wichtigster Meilenstein in der Gesetzgebung auf Bundesebene ist die erst kurz vor Ende des Berichtszeitraums verabschiedete Neufassung des Bundesdatenschutzgesetzes mit grundlegenden neuen Vorschriften. Erwähnt seien an dieser Stelle jedoch auch bedeutsame Neuregelungen zum Ausländerrecht, zum Betreuungsrecht und zur Sozialgesetzgebung, schließlich auch die sog. Sicherheitsgesetze, die den Verfassungsschutz, den Bundesnachrichtendienst und den Militärischen Abschirmdienst betreffen. Auf Landesebene ragt das Gesetz zur Fortentwicklung des Datenschutzes im Bereich der Polizei und der Ordnungsbehörden heraus, das am 1. Mai 1990 in Kraft getreten ist. Nordrhein-Westfalen hat mit diesem Gesetz nach Hessen und Bremen als eines der ersten Bundesländer für diesen wichtigen Bereich Konsequenzen aus dem Volkszählungsurteil des Bundesverfassungsgerichts vom Jahre 1983 gezogen. Auch auf anderen Gebieten wurden datenschutzbezogene landesrechtliche Neuregelungen getroffen, z.B. im Archivwesen und im Melderecht.

Wenn mit den genannten neuen Gesetzesvorschriften auch nicht alle Wünsche nach einer möglichst ausgewogenen und normenklaren Gewährleistung des Rechtes auf informationelle Selbstbestimmung erfüllt worden sind und weitere Bereiche dringend noch der Regelung bedürfen, ist der wesentliche Fortschritt der Datenschutzgesetzgebung in Bund und Land während der letzten beiden Jahre doch unübersehbar.

In einer Zeit, in der unüberwindbar scheinende Mauern gefallen sind und Grenzen durchlässiger werden, erlebt der grenzüberschreitende Austausch von Informationen aller Art einen starken Aufschwung. Besonders gilt dies für den werdenden europäischen Binnenmarkt. Es liegt auf der Hand, daß in diesem Zuge auch der Transfer personenbezogener Daten erheblich zunimmt. International wächst die Erkenntnis, daß diese Entwicklung neuartiger Regelungen bedarf. Im Rahmen der Europäischen Gemeinschaften gibt es hierzu richtungweisende und erfolgversprechende Initiativen.

Probleme des grenzüberschreitenden Datenverkehrs mußten zunächst auch beim Zusammenwachsen der beiden deutschen Staaten beachtet werden. So wurden im Bereich der Polizei und der Justiz vorläufige Vereinbarungen getroffen, die dann allerdings vom Einigungsvertrag abgelöst wurden. Danach gilt in den neuen Bundesländern das Bundesdatenschutzgesetz. Es gilt auch – vorerst und mit bestimmten Fristen – im landesrechtlichen Bereich, bis dort entsprechende Landesgesetze beschlossen sind und in Kraft

treten. Die Datensammlungen des ehemaligen Ministeriums für Staatssicherheit und dessen nachgeordneten Bereichs wurden der Verwaltung durch einen Sonderbeauftragten unterstellt; eine gesetzliche Regelung dieser Materie ist vorgesehen.

Die Entwicklung moderner Informations- und Kommunikationstechniken befindet sich in einem stürmischen Verlauf. Sie dringt immer mehr in unser alltägliches Leben ein. Der Weg in die Informationsgesellschaft ist längst beschritten und unumkehrbar. Automatisierte Datenverarbeitung findet allenthalben statt, oft ohne daß es uns bewußt wird oder zur Kenntnis gelangt. Die Behörden und öffentlichen Einrichtungen bedienen sich in immer stärkerem Ausmaß solcher Techniken oder planen deren Anschaffung in unterschiedlicher Ausgestaltung. Dabei stellen sich auch neue Fragen zum Datenschutz und zur Sicherheit der Datenverarbeitung. Neben angemessenen technischen und organisatorischen Maßnahmen ist hierbei auf die richtige Personalschulung Wert zu legen. Außer dem technischen Fachwissen müssen die eingesetzten Beschäftigten mit dem erforderlichen Wissen und Verantwortungsbewußtsein zur Gewährleistung des Datenschutzes ausgerüstet sein. Zu fordern ist auch die Beachtung der Datenschutzbelange schon bei der Planung der Einführung neuer Techniken in der öffentlichen Verwaltung.

Insgesamt läßt sich die Situation des Datenschutzes in unserem Land mit einem großen Haus vergleichen, das schon bewohnt wird, gleichzeitig aber noch Baustelle ist. Die Bewohner genießen schon einen gewissen Schutz, währenddessen wird aber renoviert, umgebaut und erweitert zu den Nachbargrundstücken. Die Innenausstattung wird derweil fortlaufend modernisiert.

Es bedarf keiner näheren Ausführung, daß der Landesbeauftragte für den Datenschutz mit seinen Mitarbeiterinnen und Mitarbeitern unter diesen Umständen an allen Ecken und Enden gefragt ist, aber nicht überall zugleich tätig werden kann. Vielmehr sind Schwerpunkte zu bilden, über die im folgenden berichtet wird. Im Hinblick auf den Umfang und die Bedeutung der Gesetzgebung, die maßgeblichen Einfluß auf die Entwicklung des Datenschutzes hat, habe ich der Darstellung von Einzelproblemen einen besonderen Abschnitt über das novellierte Bundesdatenschutzgesetz sowie zu Aktivitäten und Handlungsbedarf im Rahmen der bereichspezifischen Gesetzgebung vorangestellt. Außerdem ist ein eigener Abschnitt den immer wichtiger werdenden Fragen des grenzüberschreitenden Datenverkehrs gewidmet.

1.2 Schwerpunkte der Tätigkeit

Vorrang bei der Aufgabenerfüllung haben für mich nach wie vor die zahlreichen **Eingaben** von Bürgerinnen und Bürgern. Es geht dabei nicht immer um Beschwerden über Datenschutzverstöße. Vielfach werde ich um nähere Aufklärung oder um praktische Auskünfte gebeten. Auch erhalte ich manche Anregung zur Verstärkung des Datenschutzes. Ich bin für alle diese Hinweise dankbar, die mich schriftlich und oft auch fernmündlich erreichen. Denn gerade aus der Einzelfallpraxis lassen sich wichtige Erkenntnisse zur Durchsetzung des Datenschutzes und zu konkreten Verbesserungsvorschlägen gewinnen.

Auch die Berichterstattung in den Medien gibt mir gelegentlich wertvolle Anhaltspunkte, Einzelfragen nachzugehen.

Positiv zu bewerten ist darüber hinaus der Gedankenaustausch mit einer Reihe von Verbänden, die im öffentlichen Bereich Einfluß ausüben. Sowohl durch eingehenden Schriftwechsel als auch in Gesprächsrunden habe ich insbesondere mit den kommunalen Spitzenverbänden, Gewerkschaften, Berufsverbänden, der Landeselternschaft, dem Landesfeuerwehrverband und Verbänden aus dem Bereich des Gesundheits- und Sozialwesens Datenschutzfragen erörtert. Solche Kontakte fördern das gegenseitige Verständnis und dienen der Verbreitung des Datenschutzgedankens.

Großen Raum nahmen in den beiden vergangenen Jahren die **Stellungnahmen** ein, die ich zu zahlreichen Gesetz- und Verordnungsentwürfen sowie zu Verwaltungsvorschriften abgegeben habe. Dabei handelte es sich sowohl um bundesrechtliche Vorschriften als auch um Landesregelungen. Ich bin bemüht, solche Stellungnahmen schon im Stadium der Vorbereitung auf Referentenebene abzugeben, um frühzeitig Datenschutzgesichtspunkte einbringen zu können. Vielfach war es aber auch erforderlich, später noch während der parlamentarischen Beratungen Stellung zu beziehen. Ich habe mehrfach entsprechende Landtagsvorlagen erarbeitet und hatte auch Gelegenheit, meine Bedenken und Anregungen mündlich vor den zuständigen Ausschüssen vorzutragen. So habe ich in einer öffentlichen Anhörung vor dem Innenausschuß des Deutschen Bundestages zur Novellierung des Bundesdatenschutzgesetzes Stellung genommen. Vor den federführend zuständigen Ausschüssen des Landtags Nordrhein-Westfalen habe ich in öffentlichen Anhörungsterminen zu den Beratungen des neuen Polizeigesetzes und des Archivgesetzes meine Auffassungen erläutert.

Immer wieder wenden sich öffentliche Stellen an mich mit der Bitte um **Beratung**. Ich komme solchen Wünschen im Rahmen meiner Möglichkeiten gern nach, wobei für ihre Erfüllung um so höhere Chancen bestehen, je konkreter und besser aufbereitet die Anfrage ist. Bei generellen oder weitgespannten Fragestellungen vermag ich nur mit allgemein gehaltenen Auskünften zu antworten.

Weiterer Schwerpunkt meiner Tätigkeit waren umfangreiche **Kontrollbesuche** und thematisch begrenzte Informationsbesuche bei öffentlichen Stellen, sowohl bei kleineren Verwaltungen als auch bei Behörden oder Einrichtungen mit großen Rechenzentren. Auch im Rahmen der Kontrollbesuche steht die Beratung im Vordergrund. Bei festgestellten Mängeln und Defiziten habe ich in aller Regel Bereitschaft zur Abhilfe angetroffen, Verbesserungsvorschläge wurden im allgemeinen aufgeschlossen entgegengenommen.

Für die Durchführung dieser wichtigen Beratungstätigkeit stehen mir leider nur eingeschränkte Möglichkeiten zur Verfügung, namentlich im personellen Bereich. Das gilt in erster Linie für die Personalausstattung im technisch-organisatorischen Aufgabengebiet meiner Dienststelle. Bedauerlicherweise sah sich die Landesregierung bisher nicht in der Lage, meine Vorschläge zu einer personellen Verstärkung ausreichend zu unterstützen.

Um so mehr danke ich allen Mitarbeiterinnen und Mitarbeitern meiner Dienststelle für ihren engagierten und sachkundigen Einsatz auch bei sehr angespannter Arbeitsbelastung.

1.3 Durchsetzungsmöglichkeiten

Bei aller wachsenden Bereitschaft zur Beachtung des Datenschutzes und trotz einer Reihe von neuen – auch unter dem Gesichtspunkt der Normenklarheit geschaffenen – Vorschriften ist es bei den meiner Kontrolle unterliegenden Stellen wieder zu einer erheblichen Anzahl von Verstößen gegen datenschutzrechtliche Vorschriften gekommen. Von einer rückläufigen Tendenz kann noch keine Rede sein. Ursachen hierfür finden sich vorwiegend in mangelnder Kenntnis über die Gesetzeslage und in organisatorischen Unzulänglichkeiten. Daneben spielt sicherlich eine nicht unwesentliche Rolle, daß in manchen für die rechtliche Beurteilung maßgeblichen Regelungen allgemeine Aussagen enthalten sind, die auf den ersten Blick unterschiedlichen Auslegungen zugänglich zu sein scheinen. Es hat sich im Berichtszeitraum erneut erwiesen, daß öffentliche Stellen zum Teil immer noch dazu neigen, den Bürgern gegenüber aber auch in an mich abgegebenen Stellungnahmen solche Auslegungen für ihre Entscheidungen vorzuziehen, die vorrangig einem reibungslosen Verwaltungsablauf und weniger den Belangen des Datenschutzes Rechnung tragen. Diese Erfahrungen unterstreichen, wie notwendig eine nachgehende Kontrolle durch den Landesbeauftragten im Interesse der Durchsetzung des Datenschutzes für den Bürger, aber auch im Interesse der kontrollierten Stelle ist, die auf diesem Wege zur Einhaltung ihrer gesetzlichen Verpflichtungen angehalten werden kann. Das allein kann aber nicht ausreichen. Vielmehr ist es auch eine wesentliche Aufgabe der Dienst- und Fachaufsicht, den Belangen des Datenschutzes im jeweils nachgeordneten Bereich Geltung zu verschaffen.

Als besonders bedenkliches Zeichen mußte ich werten, daß sich anläßlich von eingeleiteten Kontrollmaßnahmen zwei Stellen schon geweigert haben, dem Landesbeauftragten für den Datenschutz Auskünfte zur Aufklärung der Sach- und Rechtslage entsprechend der Regelung in § 26 Abs. 1 Nr. 1 DSG NW zu erteilen. Um eine sachliche Überprüfung nicht von vornherein unmöglich zu machen oder nachhaltig zu erschweren, mußte ich deshalb in diesen beiden Fällen allein die Nichtbeachtung der gesetzlich festgelegten Verpflichtung zur Erteilung von Auskünften förmlich beanstanden (§ 24 DSG NW).

Von den mir zur Durchsetzung des Datenschutzes zur Verfügung stehenden Mitteln sehe ich in der förmlichen Beanstandung eine besonders gewichtige Möglichkeit, von der ich je nach Lage des Falles Gebrauch mache. Insoweit hängt die Notwendigkeit nicht vorrangig von der Schwere der Verstöße ab, so daß förmlich unbeanstandet bleibende Fälle der Sache nach bedeutsamer sein können. Meist kann von einer förmlichen Beanstandung dann abgesehen werden, wenn die Behebung der Mängel entsprechend meinen Empfehlungen sichergestellt scheint. Nähere Rückschlüsse aus Zahl oder Anlaß der förmlichen Beanstandungen auf den Stand der Beachtung des Datenschutzes durch öffentliche Stellen insgesamt lassen sich daher nicht

ziehen. Der Übersicht halber nenne ich aber neben den oben genannten noch die weiteren 13 Fälle, in denen ich wegen letztlich gegenteiliger Bewertung und der Gefahr weiterer Verstöße gegen Vorschriften über den Datenschutz eine förmliche Beanstandung ausgesprochen habe. Zugrunde lagen:

- Übermittlung von Daten aller Wahlberechtigten einer Stadt an eine politische Partei,
- übermäßige Datenerhebung durch Fragebögen im Wohnungsbauförderungsverfahren,
- Verweigerung der Akteneinsicht im gemeindlichen Bereich,
- Erfragung detaillierter Angaben über die Einkommensverhältnisse Betroffener und ihrer Ehegatten durch die Polizei in Verkehrsvergehenssachen,
- Unterrichtung der Vermieterin durch die Polizei über ein Ermittlungsverfahren gegen den Mieter,
- Offenbarung von Sozialdaten bei der Gewährung von Sach- statt Barleistungen,
- Unterrichtung des Versicherten über die Durchführung eines Beratungsverfahrens gegen seinen Arzt im Vorfeld einer Wirtschaftlichkeitsprüfung in der kassenärztlichen Versorgung,
- Offenbarung von Sozialdaten eines Asylbewerbers gegenüber der Presse,
- Offenbarung des Sozialleistungsverhältnisses durch Verwendung der Amtsgliederungsnummer des Leistungsträgers auf einer Überweisung,
- übermäßiges Erheben von Angaben im Rahmen der Wahrnehmung von Amtspflegschaften,
- Aufdeckung von Adoptionen durch Erhebung des Familiennamens in Personalbögen,
- Verstoß gegen die gebotene Vertraulichkeit bei der Behandlung von Personalangelegenheiten in der Schule und
- Versendung von Bescheiden über Grundbesitzabgaben als „Briefdrucksache".

Einzelfragen, die von allgemeiner Bedeutung sind oder eine besonders gewichtige Datenschutzproblematik zum Gegenstand haben, sind in einem gesonderten Überblick (unten S. 10) zusammengefaßt.

1.4 Öffentlichkeitsarbeit

Die an Fragen zum Datenschutz dienstlich, beruflich oder persönlich Interessierten in angemessener Weise zu informieren, hat sich auch im Berichtszeitraum als eine wichtige Daueraufgabe erwiesen. Wie die Zahl und die Vielfalt bei mir eingegangener allgemeiner Anfragen zum Thema Datenschutz zeigen, steht der Datenschutz nach wie vor im Blickpunkt einer interessierten Öffentlichkeit.

In zahlreichen Fällen habe ich auf Anfragen **Informationshilfen** zum Datenschutz durch Versendung zu diesem Zweck bei mir vorgehaltener Broschüren sowie meiner Tätigkeitsberichte geben können. Insgesamt habe ich im Berichtszeitraum nahezu 15 000 Exemplare dieser Art versandt. Für besonders erfreulich bewerte ich die stark angestiegene Nachfrage aus dem schulischen Bereich, die deutlich macht, daß das Thema Datenschutz sowohl in der Lehrerfortbildung als auch im Unterricht vermehrt behandelt wird. Verschiedentlich konnte auch öffentlichen und privaten Institutionen der Erwachsenenbildung Informationsmaterial an die Hand gegeben werden.

Im Hinblick auf die gestiegene Bedeutung von technischen und organisatorischen Maßnahmen zur Datensicherung habe ich die vier hierzu von mir erstellten Organisationshilfen in Sonderaktionen den öffentlichen Stellen des Landesbereichs sowie sonstigen Interessenten zur Verfügung gestellt (unten S. 166). Die Organisationshilfen geben den speichernden Stellen Hinweise auf Fragen zur Datensicherung und deren Lösungen. Sie sollen insbesondere zu erkennen helfen, wie die Datensicherheit geprüft werden kann, und durch welche Maßnahmen die Sicherungsziele im Einzelfall realisiert werden können.

Verständlicherweise ist der Informationsbedarf zum Datenschutz in den **neuen Bundesländern** besonders groß. Dem steht bei den öffentlichen Stellen – sicher noch eine geraume Zeit – ein erheblicher Mangel an für Grundlagenkenntnisse wichtigem Schrifttum gegenüber. Mir zugegangene Anfragen weisen aber darauf hin, daß der Datenschutz in den neuen Bundesländern als ein wichtiger Bestandteil behördlicher Tätigkeit verstanden wird. Gern bin ich entsprechenden Bitten um Informationshilfe u.a. durch Vortragstätigkeit nachgekommen und werde dies im Rahmen des mir möglichen auch in Zukunft tun.

Ein sich fortlaufend entwickelnder Datenschutz stellt hohe Anforderungen an die Beschäftigten. Dem kann in erster Linie durch entsprechende Angebote zur **Aus- und Fortbildung** Rechnung getragen werden. Zur Sicherstellung der Erfüllung dieser wichtigen Aufgabe sind vor allem die öffentlichen Stellen selbst bzw. deren Aufsichtsbehörden aufgerufen. Soweit dies in Anbetracht der Belastung möglich war, hat sich aber auch meine Dienststelle im Berichtszeitraum an der Durchführung von Fortbildungsmaßnahmen intensiv beteiligt.

Aus aktuellem Anlaß haben sich Angehörige meiner Dienststelle und ich wiederholt zu Problembereichen des Datenschutzes gegenüber den **Medien** geäußert. Auch wurde die Gelegenheit wahrgenommen, Überlegungen zur Fortentwicklung des Datenschutzes in Fachzeitschriften darzustellen.

1.5 Dateienregister

Mit Wirkung vom 17. Mai 1989 ist die nach Maßgabe des § 23 Abs. 3 DSG NW notwendig gewordene **Dateienregisterverordnung** – DRegVO NW – (GV. NW. S. 226) in Kraft getreten. An den vorbereitenden Arbeiten zu dieser Verordnung, die als Nachfolgeregelung die Verordnung vom 16. Dezember 1980 (GV. NW. S. 1096) abgelöst hat, habe ich beratend teilgenommen.

Die neue Dateienregisterverordnung wird eine Umgestaltung des bei mir geführten Registers zur Folge haben. Die speichernden Stellen sind inzwischen nur noch zur Vorlage von Beschreibungen zu automatisiert geführten Dateien verpflichtet. Darüber hinaus sind die Vorgaben für die in einer Dateibeschreibung zu dokumentierenden Angaben zum Teil neu formuliert, zum Teil aber auch erweitert worden. Insoweit messe ich der Notwendigkeit, nunmehr auch Angaben zu Maßnahmen der Datensicherung zu machen, eine besondere Bedeutung bei. Damit lassen sich in einem wichtigen Bereich meiner Kontrolltätigkeit schon aus den vorgelegten Dateibeschreibungen erste Hinweise auf die von den speichernden Stellen getroffenen technischen und organisatorischen Maßnahmen zur Datensicherung entnehmen. Durch die Verpflichtung zur Vorlage von Dateibeschreibungen wird zudem der speichernden Stelle die notwendige Selbstkontrolle in Bezug auf die Datenverarbeitung aus gegebenem Anlaß ermöglicht.

Nach § 1 Abs. 1 DRegVO NW ist die Beschreibung automatisiert geführter Dateien meiner Dienststelle unverzüglich vorzulegen. Für bereits zum Register gemeldete Dateien finden die Vorschriften der Verordnung erstmals in Fällen eintretender Veränderungen Anwendung (§ 35 Abs. 3 DSG NW, § 2 Abs. 2 DRegVO NW). Bis jetzt sind mir lediglich 1 719 Dateibeschreibungen vorgelegt worden.

Erstmals seit dem Inkrafttreten der gesetzlichen Neuregelungen zum Dateienregister in § 23 DSG NW sind mir nunmehr auch Beschreibungen der von den Behörden des Verfassungsschutzes geführten automatisierten Dateien vorzulegen. Von der in § 23 Abs. 2 Satz 1 DSG NW vorgesehenen Möglichkeit einer Einsichtnahme in das Register bzw. Auskunft aus dem Register sind die von den Verfassungsschutzbehörden vorgelegten Beschreibungen ausgenommen. Dies gilt auch für die Dateibeschreibungen der Staatsanwaltschaft, der Polizei, der Eigenbetriebe sowie für bestimmte Dateien der Landesfinanzbehörden und öffentlich-rechtlichen Unternehmen.

Im Berichtszeitraum haben einige in der Vergangenheit umstrittene Fragen zur Anwendung des DSG NW ihre Erledigung gefunden. Dies betrifft die von **Notaren** vertretene Auffassung, nicht zur Vorlage einer Dateibeschreibung verpflichtet zu sein, weil neben den Gerichten auch die Notare als Organe der Rechtspflege generell von den landesrechtlichen Vorschriften über den Datenschutz ausgenommen seien. In ihrer Stellungnahme zum 7. Tätigkeitsbericht (Drucksache 10/1644, S. 13) teilt die Landesregierung demgegenüber die von mir in meinen Tätigkeitsberichten dargelegte Auffassung, daß die Notare als Träger eines öffentlichen Amtes öffentliche Stellen sind und deshalb in vollem Umfang den Bestimmungen des Datenschutzgesetzes unterliegen. An dieser Auffassung ist auch auf der Grundlage des neuen Datenschutzgesetzes vom 15.03.1988 festzuhalten. Meine Auffassung wird inzwischen durch einen zu diesen Fragen vom Bundesgerichtshof am 30. Juli 1990 ergangenen Beschluß (NotZ 19/89) vollinhaltlich bestätigt. Das Justizministerium hat auf dem Erlaßwege die zur entsprechenden Umsetzung erforderlichen Maßnahmen getroffen.

Es ist auch zu unterschiedlichen Auffassungen über die Frage gekommen, nach welchen Regelungen **Sozialleistungsträger** zur Vorlage einer Dateibeschreibung verpflichtet sind. Während nach meiner Auffassung die Vorlage einer Dateibeschreibung entsprechend den Regelungen der DRegVO NW zu erfolgen hat, haben mir Sozialleistungsträger auf § 19 BDSG gestützte Dateibeschreibungen vorgelegt, in denen Angaben insbesondere zu den von den speichernden Stellen getroffenen Datensicherungsmaßnahmen fehlten. Zwar verweist das für Sozialleistungsträger maßgebliche Sozialgesetzbuch hinsichtlich einer dateimäßigen Datenverarbeitung auf Regelungen des Bundesdatenschutzgesetzes, dies betrifft jedoch nicht Art und Umfang der Meldepflicht (unten S. 77). Nachdem sich auch das Innenministerium meiner Auffassung angeschlossen hat, wird inzwischen von den Sozialleistungsträgern nach Maßgabe der Regelungen der neuen Dateienregisterverordnung NW verfahren.

Auf das Beratungsersuchen einer Gemeinde habe ich zu der grundsätzlichen Frage Stellung genommen, wer zur Vorlage einer Dateibeschreibung verpflichtet ist, wenn meldepflichtige Dateien vom Bürgermeister oder einer Ratsfraktion zur Erfüllung einer nach der Gemeindeordnung zugewiesenen Aufgabe dort vorgehalten werden. Nach dem Datenschutzgesetz NW trifft die Meldepflicht zum Dateienregister die Gemeinden. Für deren Verpflichtung ist es unerheblich, wenn einzelne Aufgabenträger von Stellen der Gemeindeverwaltung – organisatorisch selbständig – unterscheidbare Aufgaben wahrnehmen. Daß die Gemeinde als speichernde Stelle der sich aus § 23 Abs. 1 Satz 1 DSG NW ergebenden Meldepflicht nachzukommen hat, ergibt sich aus § 2 Abs. 1 Satz 1 DSG NW. Danach gilt das Datenschutzgesetz (u. a.) für die Gemeinden. Die einzelne Gemeinde ist insoweit als Einheit anzusehen. Hieraus folgt jedenfalls in den Fällen, in denen Rechte Betroffener nach Maßgabe des Datenschutzgesetzes geltend gemacht werden oder das Datenschutzgesetz der Gemeinde Verpflichtungen auferlegt, daß Normadressat die Gemeinde und nicht etwa die einzelne Stelle ist, die innerhalb der Gemeindeverwaltung eine abgrenzbare Aufgabe erfüllt.

1.6 Zusammenarbeit im Datenschutz

Die **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** hat im Berichtszeitraum sechsmal getagt. Hierbei wurden zu verschiedenen Gesetzgebungsaktivitäten sowie weiteren wesentlichen aktuellen Datenschutzfragen u. a. nachstehende Entschließungen und Beschlüsse gefaßt:

- zur Neuregelung des Bundesdatenschutzgesetzes,
- zum Entwurf eines Rentenreformgesetzes 1992,
- zum Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts,
- zu den Änderungen des Gesetzes zu Artikel 10 des Grundgesetzes und der Strafprozeßordnung im Rahmen der Poststrukturreform,

- zu den Entwürfen eines Bundesverfassungsschutzgesetzes (BVerfSchG), eines MAD-Gesetzes (MADG) und eines BND-Gesetzes (BNDG),
- über Genomanalyse und informationelle Selbstbestimmung,
- zum Entwurf einer EG-Statistikverordnung,
- zum Entwurf eines Schengener Zusatzübereinkommens über den schrittweisen Abbau der Grenzkontrollen,
- über den Datenschutz in der Europäischen Gemeinschaft,
- zum Datenschutz im deutsch-deutschen Verhältnis,
- zum Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität,
- zur Stärkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nichtöffentlich gesprochenen Wortes,
- zur Neuregelung des Melderechtsrahmengesetzes,
- zur Erarbeitung von Krebsregistergesetzen in Bund oder Ländern.

In den Arbeitskreisen Steuerverwaltung und Statistik habe ich weiterhin den Vorsitz geführt. Der Arbeitskreis Steuerverwaltung hat sich im wesentlichen mit Problemen befaßt, die durch die Einführung dialogorientierter Verfahren bei der automatisierten Datenverarbeitung im Bereich der Steuerfestsetzung verursacht werden. Im Arbeitskreis Statistik wurde eine Reihe von Einzelgesetzen zur Durchführung statistischer Erhebungen auf ihre datenschutzrechtliche Zulässigkeit überprüft und Vorschläge hierzu erarbeitet. Die Konferenz hat im Berichtszeitraum den Arbeitskreis EG eingerichtet, der sich schwerpunktmäßig mit Fragen des Datenschutzes in der Europäischen Gemeinschaft befaßt.

Auch auf internationaler Ebene haben Zusammenkünfte der Datenschutzbeauftragten stattgefunden. So hat die **Internationale Konferenz** im August 1989 in Berlin und im September 1990 in Paris getagt. Schwerpunkte waren u. a. Probleme des Datenschutzes bei der Telekommunikation und beim Schutz medizinischer Daten. Von besonderem Interesse waren auch Fragen, die vor dem Hintergrund eines wachsenden grenzüberschreitenden Datenaustauschs erörtert wurden.

2. Überblick

In den Abschnitten 3. bis 6. wird die immer noch zunehmende Vielschichtigkeit der Fragen und Probleme des Datenschutzes deutlich. Der Bericht enthält eine Reihe von Aussagen und Feststellungen genereller Art, die aus meiner Sicht für die künftige Entwicklung des Datenschutzes bedeutsam sind. Solche können insbesondere den Abschnitten zur Gesetzgebung (3.) und zum grenzüberschreitenden Datenverkehr (4.) entnommen werden. Die nachfolgende Auswahl von Aussagen veranschaulicht im übrigen stichwortartig das Bild:

Telekommunikationsdienste

Bei der Inanspruchnahme von Telekommunikationsdiensten durch öffentliche Stellen des Landesbereichs dürfen keine landesrechtlichen Regelungen zum Datenschutz umgangen werden. Eine solche Gefahr wird mit Blick auf das sich im Zuge der Einführung der ISDN-Technik vergrößernde Angebot von Telekommunikationsdiensten eher noch zunehmen (3.2.8).

Ed. Behandlung von Asylbewerbern

Eine erkennungsdienstliche Behandlung von Asylbewerbern ist nur nach Lage des jeweiligen Einzelfalles und nicht generell zulässig. Das Innenministerium beabsichtigt entsprechende Klarstellungen auf dem Erlaßwege (5.4.2).

Wohnanschriften an Straftäter

Mit der Aufnahme der Anschriften von Zeugen und damit auch Tatopfern in die Anklageschrift oder den Strafbefehl werden auch diese Daten dem Angeschuldigten bekanntgegeben. Hiergegen bestehen erhebliche datenschutzrechtliche Bedenken. Gleiches gilt für die Angabe der Anschrift des Anzeigenerstatters im Bußgeldbescheid (5.7.1).

Abhören des Polizeifunks

Die Möglichkeit, den Polizeifunk abzuhören, muß beseitigt werden (5.8.7).

Durchführung des Gesundheitsreformgesetzes

Hierbei ergeben sich für die Krankenkassen erhebliche Umsetzungsprobleme, weil das Gesetz – entgegen der bisherigen Praxis – die Angabe der Diagnose auf Krankenscheinen, die Übersendung von Krankenhaus-Entlassungsberichten sowie die Übersendung von Röntgenaufnahmen zwecks Überprüfung zur Qualitätssicherung ohne Einwilligung des Patienten nicht zuläßt (5.10.2).

Einschulungsuntersuchung

Zweck der Einschulungsuntersuchung ist die Beurteilung der Schulfähigkeit aus medizinischer Sicht. Beurteilungsgrundlage ist der körperliche Ist-Zu-

stand. Deshalb sprengt die Erhebung von Angaben zu Schwangerschaft und Geburtsverlauf sowie zur Familienanamnese der Großeltern, Eltern und Geschwister hinsichtlich bestimmter Krankheiten den vorgegebenen Rahmen (5.11.5).

Genomanalyse

Die Genomanalyse kann das Persönlichkeitsrecht des einzelnen in besonderer Weise beeinträchtigen. Hieraus ergibt sich die Notwendigkeit, Grundsätze für die Zulässigkeit sowie Art und Umfang von Genomanalysen wie auch für die Durchführung genomanalytischer Untersuchungen und die Verarbeitung der genetischen Daten gesetzlich normenklar festzulegen (5.11.6 und Anlage 4).

Polizeiarzt

Die unterschiedlichen Aufgaben, die der Polizeiarzt in seinen Funktionen als behandelnder Arzt, als Betriebsarzt und als Amtsarzt wahrnimmt, werfen besondere datenschutzrechtliche Probleme auf. Diese können letztlich nur durch die Schaffung normenklarer gesetzlicher Grundlagen gelöst werden (5.12.1).

Personalnebenakten

Die Führung von Datensammlungen über Mitarbeiter durch Vorgesetzte ist in der Praxis offenbar verbreitet. Dies birgt die Gefahr der Entstehung unzulässiger Personalnebenakten in sich. Geheime Personalakten darf es aber nicht geben (5.12.5).

Überwachung am Arbeitsplatz

Eine arbeitsplatzbezogene Überwachung durch versteckte Videokameras ohne Kenntnis der Beschäftigten verletzt deren Persönlichkeitsrecht. Aber auch gegen eine permanente Kontrolle durch offen montierte Kameras bestehen erhebliche Bedenken (5.12.10).

Preisgabe von Einwenderdaten

In Planfeststellungs- und Genehmigungsverfahren dürfen Name und Anschrift von Einwendern den Antragstellern zur Vorbereitung des Erörterungstermins oder einer Stellungnahme nur bekanntgegeben werden, wenn die Bekanntgabe dieser Daten unbedingt notwendig ist. Generelle Übermittlungen von Namen und Anschriften aller Einwender sind deshalb nicht zulässig (5.17.2).

Schuldnerlisten im Wald

Von einem Spaziergänger im Wald aufgefundene Schuldnerlisten haben erneut auf eine problematische Verfahrensweise der Industrie- und Handelskammern aufmerksam gemacht. Sie überlassen ihren Mitgliedern im Abon-

nement eine vollständige Liste mit den Daten aller Schuldner, so wie sie in den Schuldnerverzeichnissen der jeweiligen Amtsgerichte geführt wird. Der Umgang mit diesen Listen ist letztlich nicht kontrollierbar (5.19.2).

Datensicherheit

In dem Einsatz von **privaten persönlichen Computern (PCs)** oder privaten maschinenlesbaren Datenträgern zur Verarbeitung dienstlicher personenbezogener Daten muß eine erhebliche Beeinträchtigung des Datenschutzes gesehen werden (6.2.2).

Technische Eigenarten eines **lokalen Netzwerks (LAN)** bewirken, daß dessen Datensicherheit beeinträchtigt ist. Öffentliche Stellen, die ein lokales Netzwerk installieren, sollten die durch die Technik des Netzes bedingte Unsicherheit bei der Entscheidung über die zu treffenden Maßnahmen berücksichtigen (6.2.3).

Immer häufiger ist die Organisationsform der **individuellen Datenverarbeitung (IDV)** anzutreffen. Zum Gewährleisten der Datensicherheit sollten Einzelheiten zur IDV rechtzeitig durch Dienstanweisung geregelt werden (6.2.4).

Bei der **Textverarbeitung** bewirkt die Anweisung zum Löschen eines gespeicherten Dokuments möglicherweise nur dessen Freigabe zum Löschen und nicht das Löschen selbst. In derartigen Fällen sind zusätzliche Maßnahmen zu treffen, um eine angemessene Datensicherheit zu gewährleisten. Dieser Sachverhalt ist den Anwendern im allgemeinen nicht bekannt (6.2.5).

3. Bundesdatenschutzgesetz und bereichspezifische Gesetzgebung

3.1 Aktivitäten des Bundesgesetzgebers

3.1.1 Bundesdatenschutzgesetz

Nach langwierigen Beratungen ist das in der vorigen Legislaturperiode wieder aufgegriffene und – fast sieben Jahre nach dem Volkszählungsurteil – dringlich gewordene Gesetzesvorhaben zur Novellierung des Bundesdatenschutzgesetzes (Bundesratsdrucksache 618/88) 1990 abgeschlossen worden. Damit hat der Bundesgesetzgeber in einem für den Datenschutz wichtigen Bereich die aus seiner Sicht notwendigen Folgerungen aus der Entscheidung des Bundesverfassungsgerichts zur Volkszählung 1983 gezogen. Bis zuletzt sind im Gesetzgebungsverfahren zahlreiche Regelungsvorschläge umstritten gewesen. Schließlich ist über das Gesetzgebungsvorhaben erst nach Anrufung des Vermittlungsausschusses durch den Bundesrat auf der Grundlage der Empfehlungen dieses Ausschusses beschlossen worden. Das neue Bundesdatenschutzgesetz ist als Artikel 1 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20. Dezember 1990 im Bundesgesetzblatt 1990, S. 2954 verkündet worden. Es tritt – mit Ausnahme einer Vorschrift zum automatisierten Abrufverfahren – am 1. Juni 1991 in Kraft.

Mehrfach habe ich im Berichtszeitraum die Gelegenheit wahrgenommen, mich zu einzelnen der vorgesehenen Regelungen oder zur Novelle insgesamt zu äußern. Anläßlich einer vom Innenausschuß des Deutschen Bundestages durchgeführten öffentlichen Anhörung habe ich insbesondere herausgestellt, daß

- auch ein novelliertes Bundesdatenschutzgesetz die Schaffung (ergänzender) bereichspezifischer Datenschutzregelungen nicht in Frage stellen dürfe,
- die Anwendung der Regelungen des Gesetzes nicht – jedenfalls nicht prinzipiell – von der Art der Datenverarbeitung (akten- oder dateimäßig) abhängen dürfe,
- die Weiterverarbeitung personenbezogener Daten sich an den vom Bundesverfassungsgericht im Volkszählungsurteil ausdrücklich hervorgehobenen Grundsatz der Zweckbindung auszurichten habe und eine Weiterverarbeitung abweichend hiervon nur auf der Grundlage normenklarer (Ausnahme-) Regelungen zugelassen werden dürfe. Keineswegs dürfe insoweit dem Interesse an einem reibungslosen Verwaltungsablauf Vorrang vor Belangen des Datenschutzes eingeräumt werden,
- die Einrichtung automatisierter Abrufverfahren im öffentlichen Bereich wegen der von solchen Verfahren ausgehenden Gefährdungen für das informationelle Selbstbestimmungsrecht nur auf Grund spezieller Rechtsvorschriften zugelassen werden dürfe,

- Auskunftsrechte und Benachrichtigungspflichten im Hinblick auf die damit erreichbare Transparenz der Datenverarbeitung für den Bürger sicher noch verbessert werden könnten und
- sich Regelungen zur Ausgestaltung der Datenschutzkontrolle an den Aussagen im Volkszählungsurteil zu messen haben, denenzufolge eine unabhängige Datenschutzkontrolle ein kraft der Verfassung notwendiges Element des Grundrechtsschutzes darstellt.

Den aus der Entscheidung des Bundesverfassungsgerichts abzuleitenden Zielvorgaben war im Regierungsentwurf in vielen Punkten nicht in dem möglichen Umfang Rechnung getragen worden. Die bis zuletzt intensiven Bemühungen des Bundesbeauftragten für den Datenschutz und der Datenschutzbeauftragten der Länder dürften mit dazu beigetragen haben, daß noch einige Verbesserungen des Entwurfs erreicht werden konnten. Insbesondere begrüße ich es, daß im öffentlichen Bereich die Datenverarbeitung in oder aus Akten in den Anwendungsbereich des Gesetzes aufgenommen wurde. Dies gilt auch für die Erhebung personenbezogener Daten, die nunmehr als eigene Phase der Datenverarbeitung in diesem Bereich geschützt wird.

Demgegenüber ist einigen wesentlichen Forderungen leider nicht bzw. nicht in dem gebotenen Umfang Rechnung getragen worden. Insoweit bleibt u. a. zu nennen, daß

- ein gesonderter Gesetzesvorbehalt für die Einrichtung von Direktzugriffsverfahren zumindest in besonders sensiblen Bereichen nicht geschaffen worden ist,
- der Katalog erlaubter Zweckänderungen sehr großzügig ausgestaltet wurde,
- nur unzureichende Auskunftsmöglichkeiten der Bürger im Sicherheitsbereich gewährt werden und
- Vorschriften für den nicht-öffentlichen Bereich deutlich hinter Regelungen für den öffentlichen Bereich zurückbleiben.

Zwangsläufig werden sich Schwächen und Defizite des Bundesdatenschutzgesetzes auch auf den Datenschutz der Bürger in Nordrhein-Westfalen auswirken, weil das Gesetz mit wesentlichen Teilen auch auf meiner Kontrolle unterliegende öffentliche Stellen Anwendung findet (9. Tätigkeitsbericht, S. 21). Dies bedarf künftig auch insoweit der besonderen Beobachtung, als der Bundesgesetzgeber in bestimmten für die Bürger wichtigen Bereichen Regelungen des Bundesdatenschutzgesetzes mit der Begründung für anwendbar erklären könnte, den Datenschutz möglichst bundeseinheitlich regeln zu wollen. Für den Bereich der Steuerverwaltung ist dies bereits in einem Entwurf zur Änderung der Abgabenordnung zum Ausdruck gekommen (unten S. 20).

Im Hinblick darauf, daß auf diesem Wege bürgerfreundlichere Regelungen im nordrhein-westfälischen Datenschutzgesetz zunehmend von Regelungen des Bundesdatenschutzgesetzes verdrängt werden könnten, ist die Landesregierung aufgefordert, solchen Tendenzen frühzeitig entgegenzuwirken.

Für insbesondere auch verfassungsrechtlich bedenklich halte ich die Regelung in § 24 Abs. 2 BDSG mit der – trotz der hiergegen von den Datenschutzbeauftragten des Bundes und der Länder wiederholt geäußerten Kritik – erstmals auf legislativem Weg der Umfang der **Kontrollbefugnis** eingeschränkt und eine auch von den Datenschutzbeauftragten der Länder zu beachtende Widerspruchsmöglichkeit geschaffen wird (§ 24 Abs. 6). Das nordrhein-westfälische Datenschutzgesetz ist demgegenüber auf eine umfassendere Kontrollbefugnis ausgerichtet und sieht generell keine die Kontrolle einschränkenden Widerspruchsmöglichkeiten vor.

Die Umsetzung der Widerspruchsregelung in die Praxis wird nach meiner Einschätzung zudem eine Reihe von Auslegungsfragen aufwerfen, die bei den meiner Kontrolle unterliegenden öffentlichen Stellen zu einer erheblichen Rechtsunsicherheit führen kann. So ist beispielsweise nicht ersichtlich, ob die Widerspruchsmöglichkeit auch bei einer Kontrolle im Bereich der Personalaktenbearbeitung Platz greifen soll, wenn sich die Datenverarbeitung sowohl auf landesrechtliche Regelungen wie auch auf bundesrechtliche Regelungen stützen ließe. Auch ist unklar, wie verfahren werden soll, wenn im Rahmen systematischer Kontrollen in diesen Bereichen von der Feststellung ausgegangen werden muß, daß es die kontrollierte Stelle unterlassen hat, die Betroffenen über eine bestehende Widerspruchsmöglichkeit rechtzeitig zu unterrichten.

Mit der vom Bundesverfassungsgericht im Volkszählungsurteil hervorgehobenen Bedeutung der Beteiligung unabhängiger Datenschutzbeauftragter für einen effektiven Schutz des informationellen Selbstbestimmungsrechts wäre es jedoch unvereinbar, wenn sich Auseinandersetzungen über die Auslegung der Widerspruchsregelung zu Lasten der Wirksamkeit von Kontrollmaßnahmen auswirken würden.

3.1.2 Sicherheitsgesetze

In meinem 9. Tätigkeitsbericht (S. 22 bis 24) habe ich auf die Notwendigkeit bereichspezifischer gesetzlicher Grundlagen für die Verarbeitung personenbezogener Daten im Bereich der Sicherheitsbehörden hingewiesen. Inzwischen sind die entsprechenden gesetzlichen Regelungen getroffen worden: Das Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz; Artikel 2 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20. Dezember 1990, BGBl. I S. 2970), das Gesetz über den Militärischen Abschirmdienst (MAD-Gesetz; Artikel 3 des o. a. Gesetzes vom 20. Dezember 1990, BGBl. I S. 2977), das Gesetz über den Bundesnachrichtendienst (BND-Gesetz; Artikel 4 des o. a. Gesetzes vom 20. Dezember 1990, BGBl. I S. 2979).

Weiterhin gilt, worauf die Datenschutzbeauftragen des Bundes und der Länder schon in dem Beschluß zum Bundesdatenschutzgesetz und zum Bundesverfassungsschutzgesetz vom 22./23. März 1990 hingewiesen haben, daß die im Bundesverfassungsschutzgesetz enthaltenen Regelungen zur Sicherheitsüberprüfung nicht eine bereichspezifische, präzise Rechtsgrundlage in einem Geheimschutzgesetz für das Überprüfungsverfahren ersetzen können.

Festzuhalten bleibt weiter, daß nicht allen Bedenken, die die Datenschutzbeauftragten des Bundes und der Länder gegenüber den vorausgegangenen Entwürfen geäußert haben, Rechnung getragen worden ist. So ist etwa das eingeschränkte Auskunftsrecht des Bürgers mit der Darlegungspflicht eines besonderen Interesses an der Auskunft ein deutlicher Rückschritt hinter die in Nordrhein-Westfalen bestehende Rechtslage und die Auskunftspraxis der Verfassungsschutzbehörde.

3.1.3 Ausländerrecht

In der nunmehr abgelaufenen Legislaturperiode des Bundestages wurde das neue Ausländergesetz verabschiedet. Neben dem Bundesbeauftragten haben auch die Landesbeauftragten für den Datenschutz zu dem Entwurf ausführlich Stellung genommen. Aus meiner Sicht ist zwar zu begrüßen, daß das Gesetz gegenüber den im Entwurf vorgesehenen, nahezu schrankenlosen Mitteilungspflichten die Offenbarungstatbestände nunmehr enumerativ und präzise regelt. Gleichwohl ist zu bedauern, daß damit wieder einmal das Sozialgeheimnis zu Lasten der Ausländer durchbrochen und damit empfindlich in das informationelle Selbstbestimmungsrecht dieser Bevölkerungsgruppe eingegriffen wird (vgl. schon 4. Tätigkeitsbericht, S. 48). Weiter gibt es zahlreiche nicht normenklare Vorschriften, und auch dem Zweckbindungsgebot wird nicht in angemessener Weise Rechnung getragen. Das Recht auf informationelle Selbstbestimmung der betroffenen Ausländer erfordert daher für die Handhabung der gesetzlichen Bestimmungen in der Praxis zumindest eine strenge Anwendung des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes.

3.1.4 Betreuungsgesetz

Die Schaffung normenklarer gesetzlicher Regelungen im Entmündigungs-, Vormundschafts- und Pflegschaftsbereich war wegen der besonderen Sensibilität der Daten vordringlich. Der Bundesgesetzgeber hat nunmehr mit dem Gesetz zur Reform des Rechts der Vormundschaft und Pflegschaft für Volljährige (Betreuungsgesetz – BtG) den Versuch unternommen, den Anforderungen des Bundesverfassungsgerichts insoweit Rechnung zu tragen. Das Gesetz tritt am 1. Januar 1992 in Kraft.

Die Grundkonzeption des Gesetzes habe ich in einer Stellungnahme gegenüber der Landesregierung befürwortet. Dies gilt insbesondere für die stärkere Betonung des Erforderlichkeitsgrundsatzes für die Verarbeitung personenbezogener Daten im materiellen Betreuungsrecht, aber auch für den Wegfall entsprechender Mitteilungen an das Bundeszentralregister. Allerdings enthält das Gesetz auch zahlreiche wenig präzise Formulierungen, die der Konkretisierung bedurft hätten.

Im Hinblick auf die grundlegenden Neuerungen, die das Betreuungsgesetz mit sich bringt, wird es längere Zeit bedürfen, um seine Praktikabilität auch in datenschutzrechtlicher Hinsicht zu erweisen.

3.1.5 Rentenreformgesetz 1992 (SGB VI)

Durch Artikel 1 des Rentenreformgesetzes 1992 ist das Recht der Rentenversicherung als Sechstes Buch in das Sozialgesetzbuch eingeordnet worden. Im Gesetzgebungsverfahren haben die Datenschutzbeauftragten des Bundes und der Länder auf die Schaffung normenklarer Regelungen über Befugnisse zur Erhebung, Speicherung, Löschung, Auswertung und Weitergabe personenbezogener Daten hingewirkt. Das Rentenreformgesetz 1992 berücksichtigt zwar einige dieser Forderungen, wie z. B. die Festlegung der Aufgaben der Rentenversicherungsträger im Gesetz, die Beschränkung der Verarbeitung personenbezogener Versichertendaten auf die Erfüllung dieser Aufgaben, die Regelung der Voraussetzungen und des Inhalts von Auskünften, die die Deutsche Bundespost den Sozialleistungsträgern über die ihr bekanntgewordenen Versichertendaten erteilen darf sowie eine Klarstellung der Rechtsaufsicht und der Datenschutzkontrolle über die Datenstelle der Rentenversicherungsträger. Jedoch ist in der Schlußphase des Gesetzgebungsverfahrens durch Einfügung einer neuen Vorschrift ein schwerwiegendes Datenschutzproblem entstanden. Danach erlaubt das Gesetz den automatisierten Direktabruf aller Rentendaten nicht nur durch die Rentenversicherungsträger, sondern auch durch sämtliche Krankenkassen, Berufsgenossenschaften und Arbeitsämter. Darüber hinaus wird der Direktabruf auch den entsprechenden ausländischen Stellen ermöglicht.

Eine so umfassende Erlaubnis zum Direktabruf geht weit über die Bedürfnisse hinaus. Sie beschwört nicht überschaubare Risiken für die Versicherten herauf, weil die Datenflüsse in diesem Abrufverfahren weder begrenzbar noch kontrollierbar sind. Dies gilt im besonderen Maße für den Direktabruf aus dem Ausland. Im Gesetz hätte deshalb der Kreis der Abrufberechtigten eingeschränkt sowie Art und Umfang der abrufbaren Daten festgelegt werden müssen. Direktabrufe durch ausländische Stellen sollten grundsätzlich nicht zugelassen werden.

3.1.6 Kinder- und Jugendhilfegesetz (SGB VIII)

Das am 1. Januar 1991 in Kraft getretene Gesetz zur Neuordnung des Kinder- und Jugendhilferechts (Kinder- und Jugendhilfegesetz – KJHG –) löst als Achtes Buch des Sozialgesetzbuchs das Jugendwohlfahrtsgesetz aus dem Jahre 1922 ab. Es enthält ein eigenes Kapitel über den Schutz personenbezogener Daten mit Vorschriften über die Erhebung, Speicherung, Zweckbindung, Einschränkung der Offenbarungsbefugnis sowie Löschung der Daten. Damit sind die Belange des Datenschutzes im wesentlichen berücksichtigt.

3.2 Handlungsbedarf im Bundesbereich

3.2.1 Strafprozeßordnung

Auch in meinem 9. Tätigkeitsbericht (S. 26) hatte ich auf das Fehlen von Vorschriften über den Umgang mit personenbezogenen Daten in wesentlichen Bereichen des Strafprozeßrechts hingewiesen, die den Anforderungen der Rechtsprechung des Bundesverfassungsgerichts genügen. Mit der Vorlage

eines Regierungsentwurfs eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts – **Strafverfahrensänderungsgesetz 1989** (StVÄG 1989) – ist der wiederholte Versuch unternommen worden, die Strafprozeßordnung auch unter dem Gesichtspunkt des Datenschutzes zu novellieren. Gegenüber dem in meinem 9. Tätigkeitsbericht erwähnten Strafverfahrensänderungsgesetzentwurf 1988 war insgesamt eine Verschlechterung festzustellen. Gegen die Regelungen des Entwurfs bestanden aber auch im einzelnen eine Reihe von datenschutzrechtlichen Bedenken, so etwa wenn den Strafverfolgungsbehörden, den Gerichten und den Vollstreckungsbehörden die Befugnis eröffnet wird, einschränkungslos gemeinsame Dateien zu bilden, oder wenn Kinderdaten in einem zentralen staatsanwaltschaftlichen Verfahrensregister über einen Zeitraum von zumindest zwei Jahren vorgehalten werden dürfen. Das Strafverfahrensänderungsgesetz ist in der zurückliegenden Legislaturperiode des Bundestages nicht weiter behandelt worden.

Demgegenüber hat der Bundesrat im Jahr 1990 den Versuch unternommen, mit dem Entwurf eines **Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität** erstmals in die Strafprozeßordnung Regelungen zur Rasterfahndung, zum Einsatz verdeckter Ermittler sowie von Wanzen und Richtmikrofonen und heimlichen Film- und Fotoaufnahmen einzufügen. Auch wenn nicht zu verkennen ist, daß bestimmte Erscheinungsformen von Kriminalität im Interesse des Schutzes der Bürger besondere Ermittlungsmethoden erforderlich machen können, bin ich der Auffassung, daß der Entwurf das Ziel, hierüber verfassungskonforme, datenschutzgerechte Regeln zu treffen, verfehlt hat.

In meiner Stellungnahme gegenüber dem Justizministerium des Landes Nordrhein-Westfalen habe ich zudem zum Ausdruck gebracht, daß der Entwurf bedauerlicherweise weit hinter dem Datenschutzstandard zurückbleibt, der mit dem im Land Nordrhein-Westfalen verabschiedeten Gesetz zur Fortentwicklung des Datenschutzes im Bereich der Polizei und der Ordnungsbehörden (GFD Pol) vom 7. Februar 1990 erreicht wurde. So bestimmt das Polizeigesetz NW in § 8 Abs. 3 den unklaren Begriff „Straftaten von erheblicher Bedeutung" durch einen wenigstens nahezu abschließenden Straftatenkatalog, auch ist der Einsatz besonderer technischer Mittel oder der Einsatz eines verdeckten Ermittlers klarer und erheblich einschränkender geregelt.

Darüber hinaus hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 27. Juni 1990 festgestellt, daß dieser Entwurf selbst hinter den datenschutzrechtlichen Ansätzen, wie sie etwa noch im Strafverfahrensänderungsgesetz 1989 enthalten waren, zurückbleibt. Sie hat den Deutschen Bundestag aufgefordert, die Vorschläge des Gesetzentwurfs abzulehnen und die unterbrochenen Arbeiten an der umfassenden datenschutzrechtlichen Novellierung der Strafprozeßordnung, die dringend geboten ist, wieder aufzunehmen (vgl. Anlage 1, S. 168/169). Die Datenschutzbeauftragten haben hierzu wiederholt konkrete Vorschläge vorgelegt.

Eine Verabschiedung des Gesetzentwurfs ist nicht erfolgt.

3.2.2 Justizmitteilungsgesetz

Noch immer ist es nicht gelungen, den Entwurf eines Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (Justizmitteilungsgesetz) im parlamentarischen Raum auf den Weg zu bringen. Zur datenschutzrechtlichen Gesamtproblematik derartiger Mitteilungen habe ich ausführlich in meinem 8. Tätigkeitsbericht (S. 36 /37) Stellung genommen.

Im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts zum sog. Übergangsbonus ist darauf hinzuweisen, daß die bisherige Praxis auf der Grundlage der Anordnung über Mitteilungen in Strafsachen (MiStra) und der Anordnung über Mitteilungen in Zivilsachen (MiZi) nur noch in stark eingeschränktem Umfang hingenommen werden kann. Mitteilungen der Justiz sind insoweit allenfalls zulässig, soweit sie für die Aufgabenerfüllung der jeweiligen Empfängerbehörde unerläßlich sind.

3.2.3 Arbeitnehmerdatenschutz

Der Arbeitnehmer muß wegen seiner Abhängigkeit von Arbeitsplatz und Einkommen weitgehend unter faktischem Zwang personenbezogene Daten zur Durchführung des Beschäftigungsverhältnisses preisgeben und deren – auch automatisierte – Verarbeitung durch den Arbeitgeber hinnehmen. Der damit verbundene Eingriff in seine Persönlichkeitsrechte bedarf nach der Rechtsprechung insbesondere des Bundesverfassungsgerichts einer gesetzlichen Grundlage. Dies gilt auch für den öffentlichen Dienst. Informationelle Eingriffe gegenüber den Mitarbeitern des öffentlichen Dienstes dürfen sich nicht länger nur auf Richtlinien und Erlasse oder tarifvertragliche Regelungen stützen. Aus den hergebrachten Grundsätzen des Berufsbeamtentums, insbesondere der Treuepflicht oder aus § 8 des Bundesangestelltentarifvertrages bzw. § 9 des Manteltarifvertrages der Länder läßt sich aus datenschutzrechtlicher Sicht eine allgemeine Ermächtigung für solche Eingriffe gegenüber Beamten, Angestellten und Arbeitern nicht herleiten. Die gesetzliche Grundlage muß um so präziser sein, je tiefer in das allgemeine Persönlichkeitsrecht, einschließlich des informationellen Selbstbestimmungsrechts, eingegriffen wird. Mit der beabsichtigten Neuregelung des Personalaktenrechts im Beamtenrechtsrahmengesetz wird also erst der Anfang gemacht.

3.2.4 Beamtenrechtsrahmengesetz

Das Neunte Gesetz zur Änderung dienstrechtlicher Vorschriften ist in der Legislaturperiode des 11. Deutschen Bundestages nicht mehr verabschiedet worden. Ich gehe davon aus, daß der Gesetzgeber das Vorhaben auf der Grundlage des bisherigen Gesetzentwurfs wieder aufgreift. Der Entwurf enthält erstmals eine Reihe von datenschutzrechtlichen Bestimmungen zur Personalaktenführung, zur Behandlung von Beihilfeunterlagen, zur Weitergabe der Personalakte bzw. Übermittlung von Personaldaten an andere Behörden und an Dritte, zur Löschung sowie eine Regelung über automatisierte Abrufverfahren. An der vorgesehenen Regelung ist vor allem begrüßenswert die Abkehr von dem in Rechtsprechung und Verwaltung immer noch beharrlich

verfochtenen, aber datenschutzrechtlich bedenklichen Grundsatz der Vollständigkeit und Lückenlosigkeit der Personalakte (unten S. 100).

Einigen wesentlichen Forderungen der Datenschutzbeauftragten des Bundes und der Länder wird in dem Entwurf aber nicht Rechnung getragen. So fehlt z. B. die Präzisierung des Inhalts der Personalakte, die Trennung der Beihilfeakte und der Besoldungsakte von der Personalakte, die Definition des Begriffes „Personalaktendaten" und die Festlegung des Umfanges zulässiger automatisierter Speicherung dieser Daten sowie eine umfassendere Regelung über automatisierte Abrufverfahren.

3.2.5 Statistik

Obwohl im Berichtszeitraum eine Reihe von wichtigen Gesetzen zur Durchführung von Statistiken, wie z. B. die Gesetze über die Agrarstatistik, den Mikrozensus, die Hochschulstatistik und die Straßenverkehrsunfallstatistik verabschiedet wurden, besteht weiterer Regelungsbedarf, insbesondere für folgende statistische Erhebungen: Strafverfolgungs- und Bewährungshilfestatistik, Umweltstatistik, Ausländerstatistik und Schwangerschaftsabbruchstatistik. Darüber hinaus bedürfen eine Reihe von einzelstatistischen Gesetzen dringend einer Überarbeitung; dies gilt insbesondere für das Bevölkerungsstatistikgesetz, das Beherbergungsstatistikgesetz, das Handelsstatistikgesetz und das Gesetz über die Statistik im Produzierenden Gewerbe.

Nach meiner Auffassung ist die weitere Durchführung von Statistiken ohne ausreichende Rechtsgrundlage nicht länger hinnehmbar, da sie mit den Anforderungen des Volkszählungsurteils des Bundesverfassungsgerichts von 1983 nicht zu vereinbaren ist.

3.2.6 Abgabenordnung

In meinem 9. Tätigkeitsbericht (S. 31) habe ich auf einen aus datenschutzrechtlicher Sicht unzureichenden Gesetzentwurf zur Änderung der Abgabenordnung (AO) hingewiesen und mich insbesondere gegen eine Anwendung der Regelungen des Bundesdatenschutzgesetzes auf die Landesfinanzbehörden gewandt. Im neuen Bundesdatenschutzgesetz ist zwar das Steuergeheimnis in der Aufzählung der Bereiche, für die eine Kontrolle durch den Datenschutzbeauftragten nur zulässig sein soll, wenn der Betroffene nicht widersprochen hat (§ 24 Abs. 2 Satz 4 BDSG), nicht mehr genannt. Aber die in der Entwurfsfassung weiterhin enthaltene Verweisung auf das Bundesdatenschutzgesetz birgt die Gefahr in sich, daß der Landesbeauftragte bei seiner Kontrolltätigkeit im Bereich der Finanzverwaltung auf eine Einzelfallprüfung verwiesen werden könnte. Ich werde demgegenüber erforderlichenfalls auch weiterhin systematische Kontrollen durchführen. Die Landesregierung hat in ihrer Stellungnahme meine Auffassung geteilt, daß Kontrollrechte unabhängiger Datenschutzbeauftragter für alle Phasen und Formen der Datenverarbeitung auch im Bereich der Finanzverwaltung anerkannt und gesetzlich abgesichert werden sollten.

Meine Bedenken gegen den überarbeiteten Gesetzentwurf bleiben darüber hinaus weiter bestehen, weil er zahlreiche datenschutzrechtliche Defizite enthält. Soweit eine Offenbarung von dem Steuergeheimnis unterliegenden Daten nach § 30 Abs. 4 Nr. 1 und 4 AO (neu) dann zulässig sein soll, wenn sie den dort genannten Verwendungszwecken dient, verstößt diese Regelung gegen den Grundsatz der Erforderlichkeit und Verhältnismäßigkeit. Danach reicht es nicht aus, wenn die Kenntnis der Daten einer Aufgabenerfüllung lediglich dient oder nützlich ist. Die Vorschrift läßt außerdem nicht klar erkennen, daß sie Ausnahmen vom Grundsatz der Zweckbindung zulassen will. In der Aufzählung fehlt auch die Mitteilung von Steuerschulden zur Durchführung von Gewerbeuntersagungsverfahren.

Die in § 31 Abs. 3 AO (neu) vorgesehene Verwendung von Namen und Anschriften der Grundstückseigentümer über die Nutzung für grundstücksbezogene Zwecke hinaus für alle nur denkbaren Verwaltungszwecke geht zu weit. In dieser allgemeinen Fassung verstößt sie ebenfalls gegen das verfassungsrechtliche Gebot der Verhältnismäßigkeit. Gleiches gilt für die in § 88 Abs. 3 und 4 AO (neu) zugelassenen Verwendungsmöglichkeiten. Durch derart allgemein gefaßte Zulässigkeitsvoraussetzungen wird das Steuergeheimnis ausgehöhlt.

Der Gesetzentwurf geht schließlich in keiner Weise auf die wiederholt vorgetragene Forderung ein, in die bisherigen Regelungen über Auskunfts-, Vorlage- und Mitteilungspflichten (§§ 105 und 116 AO) als weitere Einschränkungen auch die Wahrung der ärztlichen Schweigepflicht und des Sozialgeheimnisses einzubeziehen. Dies gilt ebenso für die zu § 184 Abs. 3 AO erhobene Forderung, die Mitteilung des vollständigen Inhalts von Steuermeßbescheiden in den Ländern, in denen die Gemeinden nicht den gesamten Inhalt zur Steuerfestsetzung benötigen, zu unterlassen und nur den festgesetzten Steuermeßbetrag mitzuteilen.

3.2.7 Gewerbeordnung

Die Gewerbeordnung und die gewerberechtlichen Nebengesetze wie z. B. das Gaststättengesetz enthalten Ermächtigungen, die eine Verarbeitung von personenbezogenen Daten für gewerberechtliche Entscheidungen bedingen, ohne daß hierzu normenklare datenschutzrechtliche Regelungen getroffen sind. Dies ist insbesondere der Fall bei der Gewerbeanzeige, der Erteilung, der Rücknahme und dem Widerruf von Erlaubnissen, bei der Gewerbeuntersagung sowie den Aufzeichnungspflichten von Kundendaten im Rahmen der gewerblichen Überwachungen.

Inzwischen liegt ein Arbeitsentwurf des Bund-Länder-Ausschusses „Gewerberecht" vor. Allerdings begegnet der Entwurf in der vorliegenden Fassung noch datenschutzrechtlichen Bedenken. Insbesondere läßt § 11 der neuen Regelung für den Betroffenen nicht normenklar erkennen, welche Daten zu welchem Zweck erhoben und übermittelt werden dürfen. Auch soweit es der Behörde gestattet sein soll, über den Betroffenen Steuerdaten bei Finanzämtern und Sozialdaten bei Sozialversicherungsträgern zu erheben, bestehen wegen des Steuergeheimnisses bzw. Sozialgeheimnisses erhebliche daten

schutzrechtliche Bedenken. Darüber hinaus müssen auch in den gewerberechtlichen Nebengesetzen datenschutzrechtliche Defizite behoben werden.

3.2.8 Poststrukturreform/ISDN

Mit dem am 01.07.1989 in Kraft getretenen **Poststrukturgesetz** hat der Bundesgesetzgeber die Voraussetzungen für die Umgestaltung des Post- und Fernmeldewesens geschaffen. Das Kernstück der Regelungen betrifft die neugestaltete Struktur der Deutschen Bundespost, die sich nunmehr in drei Teilbereiche untergliedert und als öffentliche Unternehmen mit den Bezeichnungen Deutsche Bundespost POSTDIENST, Deutsche Bundespost POSTBANK sowie Deutsche Bundespost TELEKOM geführt wird. Darüber hinaus haben die Regelungen im Fernmeldeanlagengesetz (FAG) die sektorale Zulassung (§ 2 FAG) bzw. Erfassung (§ 1 a FAG) privater Anbieter von Telekommunikationsdiensten zum Ziel. Insoweit kommt der Gewährleistung des Datenschutzes bei der Datenverarbeitung im Rahmen bereits nutzbarer sowie im Rahmen neu hinzukommender Telekommunikationsdienste eine besondere Bedeutung zu. Auch der Landtag hat sich in der letzten Wahlperiode mit der Problematik „Verbesserter Datenschutz bei ISDN" (Drucksache 10/5180) befaßt und in einem Beschluß vom 15.02.1990 (Plenarprotokoll 10/133) einen entsprechenden Forderungskatalog aufgestellt. Hinsichtlich des Beschlusses, den die Internationale Konferenz der Datenschutzbeauftragten am 30.08.1989 zu ISDN gefaßt hat, verweise ich auf Anlage 2, S. 169 bis 171.

Ich habe das Ministerium für Wirtschaft, Mittelstand und Technologie gebeten, sich anläßlich der Beteiligung des Infrastrukturrates bei den für die Unternehmen der Deutschen Bundespost zu schaffenden Datenschutzverordnungen (§ 30 Abs. 2 Postverfassungsgesetz) dafür einzusetzen, daß den Anforderungen zum Schutz personenbezogener Daten der am Post- und Fernmeldeverkehr Beteiligten in dem notwendigen Umfang entsprochen wird. Darüber hinaus sind derartige durch Rechtsverordnung zu regelnde Festlegungen für den Datenschutz nunmehr auch für private Anbieter (§ 14 a Abs. 2 FAG) von Telekommunikationsdiensten dringlich geworden, weil das Angebot solcher Dienste zunimmt und – wie die Konferenz der Datenschutzbeauftragten schon in ihren Entschließungen vom 10. Oktober 1988 festgestellt hat – die für den privaten Bereich einschlägigen Regelungen des Bundesdatenschutzgesetzes der speziellen Datenschutzproblematik insoweit nicht gerecht werden können. An dieser Einschätzung ist aus meiner Sicht auch nach dem Inkrafttreten des neuen Bundesdatenschutzgesetzes mit seinen nur geringfügigen Verbesserungen für den Datenschutz im privaten Bereich festzuhalten.

Soweit meiner Kontrolle unterliegende öffentliche Stellen des Landesbereichs von der Deutschen Bundespost TELEKOM oder von privaten Betreibern angebotene Telekommunikationsdienste in Anspruch nehmen, und sie hierbei personenbezogene Daten verarbeiten, ist darauf zu achten, daß durch eine solche Inanspruchnahme keine landesrechtlichen Regelungen zum Datenschutz umgangen werden. Eine solche Gefahr wird mit Blick auf das sich im Zuge der Einführung der ISDN-Technik vergrößernde Angebot von Telekommunikationsdiensten eher noch zunehmen. Ihr kann gegebenenfalls

durch ergänzende landesrechtliche Regelungen zum Datenschutz Rechnung getragen werden (zur Zuständigkeit vgl. 9. Tätigkeitsbericht, S. 41).

Im Berichtszeitraum bestand bereits Veranlassung, das Finanzministerium auf eine etwaige Änderung oder Ergänzung der **Dienstanschlußvorschriften**, die Art, Umfang und Aufbewahrung der in Nebenstellenanlagen öffentlicher Stellen gespeicherten Telefondaten regeln, hinzuweisen. Die Einführung der ISDN-Technik im Netz der Deutschen Bundespost TELEKOM (Digitalisierung der Verbindungsstellen) ermöglicht es, auf der Grundlage der noch geltenden Telekommunikationsordnung (TKO) neben privaten Anschlußnehmern auch öffentlichen Stellen zur Gebührenabrechnung einen Einzelgebührennachweis anzubieten, der u. a. die ungekürzte Telefonnummer aller Gesprächsteilnehmer ausweist. Eine ungekürzte Speicherung dieser Telefonnummern, etwa der von Bediensteten geführten Privatgespräche oder der in sensiblen Bereichen geführten Beratungsgespräche, ist im Rahmen der Telefondatenerfassung durch öffentliche Stellen mit dem Datenschutz nicht vereinbar. Im Hinblick darauf, daß durch die Anforderung eines Einzelgebührennachweises die bestehenden Dienstanschlußvorschriften umgangen werden könnten, kann eine Klarstellung dahingehend notwendig werden, daß öffentliche Stellen keinen Einzelgebührennachweis anfordern dürfen. Das Finanzministerium hat zugesagt, die Notwendigkeit einer solchen Klarstellung bei der nächsten Änderung der Dienstanschlußvorschriften zu prüfen.

3.3 Aktivitäten des Landesgesetzgebers

3.3.1 Polizeigesetz

Am 7. Februar 1990 wurde das neue Gesetz zur Fortentwicklung des Datenschutzes im Bereich der Polizei und der Ordnungsbehörden (GFD Pol) für das Land Nordrhein-Westfalen verabschiedet (GV. NW. S. 46). Nordrhein-Westfalen hat damit als eines der ersten Bundesländer auf diesem wichtigen bereichspezifischen Gebiet Konsequenzen aus dem Volkszählungsurteil von 1983 gezogen. Eine Reihe von Anregungen und Bedenken, die ich bei der Vorbereitung des Gesetzes vorgetragen hatte (vgl. u. a. 9. Tätigkeitsbericht, S. 35 bis 37), sind dabei berücksichtigt worden, andere Forderungen wurden jedoch nicht erfüllt.

Als offen gebliebene Kritikpunkte möchte ich insbesondere herausgreifen:

- Nach wie vor enthält das Gesetz zu viele Generalklauseln (z. B. Personen im räumlichen Umfeld, Kontakt- und Begleitpersonen).
- Es fehlt eine Dokumentationspflicht bei der Datenübermittlung an andere als öffentliche Stellen oder ins Ausland.
- Die Aufzählung der Straftaten von erheblicher Bedeutung wird in der Vorschrift selbst wieder aufgeweicht („insbesondere"). Hier wird durch Auslegung klarzustellen sein, daß Straftaten, die über den Straftatenkatalog hinaus erfaßt werden sollen, an der Schwere der aufgezählten Straftaten zu messen sind.

Die vielen weitgehenden Ermächtigungsnormen, die das Gesetz enthält, erfordern in der Praxis eine besonders strenge Beachtung des Verhältnismäßigkeitsgrundsatzes (vgl. auch § 2 PolG NW), wenn sich das Gesetz in der Praxis bewähren soll.

3.3.2 Landesenteignungsgesetz

In meinem 9. Tätigkeitsbericht (S. 34/35) habe ich zum damaligen Entwurf eines Gesetzes über Enteignung und Entschädigung für das Land Nordrhein-Westfalen Stellung genommen. Darüber hinaus habe ich auf Wunsch der Mehrheitsfraktion des Landtags Formulierungsvorschläge entsprechend meinen Empfehlungen und Anregungen erarbeitet, die aber zu meinem Bedauern keinen Eingang in das inzwischen verabschiedete Gesetz gefunden haben.

3.3.3 Vermessungs- und Katastergesetz

Ebenfalls in meinem 9. Tätigkeitsbericht habe ich zum damaligen Referentenentwurf des Gesetzes zur Änderung des Vermessungs- und Katastergesetzes – VermKatG NW – Bedenken und Anregungen aufgezeigt (S. 37/38). Inzwischen ist das Gesetz verabschiedet worden. Nicht alle Vorschläge wurden dabei berücksichtigt.

So fehlt nach wie vor eine klare Festlegung, welche Angaben das Liegenschaftskataster enthält. Eine Festschreibung der Datenarten (z. B. Größe, Fläche) im Sinne einer abschließenden Aufzählung wäre anders als eine Festschreibung der Datenfelder (z. B. ha, qm) aus Gründen der Transparenz notwendig und auch unter dem Gesichtspunkt der Praktikabilität möglich gewesen. Die Neufassung des entsprechenden Gesetzes im Bundesland Bremen enthält eine solche Bestimmung. Auch fehlt eine Klarstellung, daß die Angabe des Berufs des Eigentümers oder Erbbauberechtigten nicht in das Liegenschaftskataster mit aufgenommen wird.

Da nähere Einzelheiten noch in einer Rechtsverordnung bzw. in der Berufsordnung geregelt werden sollen, wird zu gegebener Zeit zu prüfen sein, ob diese in Aussicht gestellten Regelungen den datenschutzrechtlichen Anforderungen genügen.

3.3.4 Meldegesetz

Zahlreiche Bürger hatten sich in Eingaben, die auch an mich gerichtet waren, gegen die Bestimmung des § 35 Abs. 1 des Meldegesetzes für das Land Nordrhein-Westfalen gewandt, nach der die Meldebehörde im Zusammenhang mit Parlaments- und Kommunalwahl in den sechs der Wahl vorangehenden Monaten Auskunft aus dem Melderegister über Namen, akademische Grade und Anschriften der Wahlberechtigten erteilen darf, für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist. Mit dem Gesetz zur Änderung des Meldegesetzes vom 28. November 1989 ist den Betroffenen nunmehr auch ein Widerspruchsrecht gegen die Datenübermittlung an Parteien eingeräumt worden. Diese Gesetzesänderung habe ich aus datenschutzrechtlicher Sicht befürwortet.

3.3.5 Archivgesetz

Durch das neue Archivgesetz Nordrhein-Westfalen (ArchivG NW) ist endlich eine Rechtsgrundlage für die Arbeit der Archive auch in datenschutzrechtlicher Hinsicht geschaffen worden. Es hat aber leider einige wesentliche Vorschläge, die ich zur Verbesserung des Persönlichkeitsschutzes gemacht hatte, unberücksichtigt gelassen. So hatte ich darauf hingewiesen, daß das Zusammenwirken von Bundesrecht und Landesrecht lückenhaft und unklar bleibt, so daß bei der Ausführung dieses Gesetzes mit erheblichen Schwierigkeiten insbesondere auf kommunaler Ebene zu rechnen ist. Ich sehe die Gefahr, daß Verstöße gegen den Datenschutz vorprogrammiert sind.

So ist nicht verständlich, daß nur bei Archivgut, das bundesrechtlichen Geheimhaltungsvorschriften unterliegt, die schutzwürdigen Belange Betroffener zu berücksichtigen und die Vorschriften über die Verarbeitung und Sicherung dieser Unterlagen zu beachten sind, die für die abgebende Stelle gelten (§ 12 ArchivG NW). Ebenso ist unbefriedigend, daß der Auskunftsanspruch des Betroffenen nur in Bezug auf öffentliches Archivgut besteht (§ 6 Abs. 1 Satz 1 ArchivG NW). Bedauerlicherweise bleiben auch die Nutzungsregelungen in § 7 Abs. 2 Satz 3 und Abs. 4 Satz 1 Buchstabe b ArchivG NW hinter dem datenschutzrechtlichen Standard des Bundesarchivgesetzes (BArchG) zurück. Während die landesrechtlich viel kürzer geregelte Sondersperrfrist voraussetzt, daß das Archivgut sich nach seiner Zweckbestimmung oder nach seinem wesentlichen Inhalt auf eine natürliche Person bezieht, reicht für die wesentlich längere Sperrfrist des Bundesarchivgesetzes aus, daß sich das Archivgut auf natürliche Personen bezieht. Deshalb ist zu befürchten, daß die in sog. Sachakten enthaltenen personenbezogenen Daten einen geringeren Schutz erfahren, obwohl die Daten für den Betroffenen sehr bedeutsam sein können.

Weiter ist die Nutzungsmöglichkeit des Archivgutes zu wissenschaftlichen Zwecken (§ 7 Abs. 4 Satz 1 Buchstabe b ArchivG NW) sehr weit gefaßt; hier wäre eine dem Bundesarchivgesetz entsprechende Regelung der Nutzung nur für ein wissenschaftliches Forschungsvorhaben, das im öffentlichen Interesse liegt, dem Schutz der Betroffenen nach meiner Auffassung angemessen gewesen. Im übrigen bleibt diese Regelung hinter dem Standard der Forschungsklausel in § 28 Abs. 2 Satz 1 letzter Halbsatz DSG NW zurück. Ich bedauere auch, daß in diesem Zusammenhang nicht die klarere Forderung nach Anonymisierung vor Einsichtsgewährung entsprechend § 5 Abs. 5 Satz 3 BArchG gestellt worden ist. Unsicherheit besteht nach meiner Erfahrung in der Praxis bei der Abgrenzung der „wissenschaftlichen Untersuchungen" interessierter Bürger von der Nutzung zu wissenschaftlichen Zwecken. Hier kann nur eine strenge Auslegung und Handhabung dem Persönlichkeitsschutz ausreichend Rechnung tragen.

Die inzwischen nach § 8 Abs. 1 ArchivG NW erlassene **Archivbenutzungsordnung** Nordrhein-Westfalen – ArchivBO NW – vom 27. September 1990 (GV. NW. S. 587) enthält leider eine Reihe von Vorschriften, die die Gefahr mit sich bringen, daß sich eine über das Archivgesetz hinausgehende Nutzung von Archivgut entwickelt. Meine weiter oben aufgezeigte Befürchtung

hinsichtlich einer extensiven Nutzung des Archivgutes zu wissenschaftlichen Zwecken wird durch die Einbeziehung auch heimat- und familienkundlicher Benutzung in die Zwecke der Wissenschaft und Forschung (§ 3 Buchstabe b ArchivBO NW) voll und ganz bestätigt. Offenbar rechnen auch Studierende einer Hochschule zu den für wissenschaftliche Zwecke Forschenden, für die sogar die Sperrfristen verkürzt werden können (vgl. § 7 Abs. 5 Satz 3 i.V.m. Abs. 3 Satz 3 Nr. 3 ArchivBO NW). Zudem sieht die Verordnung die Nutzung von Archivgut für Bildungs- und Unterrichtszwecke vor.

Eine weitere Gefahr unzulässiger Nutzung ergibt sich aus der Fassung des § 9 ArchivBO NW. Danach können Behörden Archivgut, das von ihnen nachgeordneten Stellen stammt, grundsätzlich nutzen, ohne daß in jedem Fall ein berechtigtes Interesse glaubhaft gemacht werden muß; Gerichten und Staatsanwaltschaften wird insoweit Zugriff auf jegliches Archivgut ermöglicht. Die Zulässigkeitsvoraussetzungen des § 7 Abs. 1 ArchivG NW (Ablauf der Sperrfrist und Glaubhaftmachung des berechtigten Interesses) kommen damit nur eingeschränkt zur Geltung. Zumindest eine Klarstellung halte ich hier für geboten.

Weiterhin wird durch die Benutzungsordnung die Einsicht in Findbehelfe vor Ablauf der Sperrfristen ermöglicht. Es ist davon auszugehen, daß sich darin auch personenbezogene Daten befinden können. Erforderlich ist indes lediglich die Genehmigung der Archivleitung (§ 7 Abs. 8 ArchivBO NW). Dies erscheint mir unzureichend.

Die sich aus der Benutzungsordnung ergebenden datenschutzrechtlichen Probleme werde ich mit dem Kultusministerium erörtern.

3.4 Handlungsbedarf im Landesbereich

3.4.1 Verfassungsschutzgesetz

Nach der Verabschiedung des neuen Bundesverfassungsschutzgesetzes durch den Bundesgesetzgeber ist zu erwarten, daß nunmehr auch auf Landesebene das Verfassungsschutzgesetz den Anforderungen angepaßt wird, die das Bundesverfassungsgericht an die Normenklarheit gesetzlicher Regelungen für die Verarbeitung personenbezogener Daten gestellt hat. Ich werde die Entwicklung im Land Nordrhein-Westfalen verfolgen und darum bemüht sein, daß die Anregungen und Bedenken, die bereits im Zusammenhang mit der Neufassung des Bundesverfassungsschutzgesetzes von den Datenschutzbeauftragten des Bundes und der Länder geäußert wurden, Berücksichtigung finden.

3.4.2 Geheimschutzgesetz

In meinem 9. Tätigkeitsbericht (S. 37) habe ich darauf hingewiesen, daß es für die Durchführung von Sicherheitsüberprüfungen in der öffentlichen Verwaltung und in der Privatwirtschaft keine ausreichende gesetzliche Grundlage gibt und die bisherige Praxis im Rahmen des sog. Übergangsbonus in eingeschränktem Umfang daher nur noch bis zum Ende der Legislaturpe-

riode des Bundes- bzw. Landtages hingenommen werden kann. Das Innenministerium des Landes Nordrhein-Westfalen hatte zum Ausdruck gebracht, insoweit auf den Bundesgesetzgeber warten zu wollen.

Nachdem die Sicherheitsgesetze im Bund verabschiedet worden sind, ist zu erwarten, daß die Problematik der Sicherheitsüberprüfungen nunmehr ebenfalls gesetzlich geregelt wird, ggf. nur auf Landesebene.

In diesem Zusammenhang ist zu erwähnen, daß in Nordrhein-Westfalen zur Zeit ein mit mir abgestimmtes Verfahren praktiziert wird, das ausschließlich von der Einwilligung des Betroffenen abhängt. Dieses Verfahren kann im wesentlichen als beispielhaft für eine künftige gesetzliche Regelung angesehen werden.

3.4.3 Gemeindeordnung

Schon in früheren Tätigkeitsberichten (vgl. 1. Tätigkeitsbericht, S. 34/35; 3. Tätigkeitsbericht, S. 24/25; 7. Tätigkeitsbericht, S. 21/22) habe ich mich zur Problematik der Befangenheit von Ratsmitgliedern und der Notwendigkeit einer klaren gesetzlichen Regelung für die Offenlegung personenbezogener Daten in diesem Zusammenhang geäußert und dabei zum Ausdruck gebracht, daß derartige Grundrechtseingriffe nicht allein auf untergesetzliche Regelungen, z. B. die Ehrenordnung des Rates, gestützt werden können.

Anläßlich der Änderung des § 23 der Gemeindeordnung für das Land Nordrhein-Westfalen (GO NW), mit der eine Konkretisierung des Begriffs „unmittelbarer Vor- oder Nachteil" erreicht und eine weitere Ausnahme vom Mitwirkungsverbot bei Wahlen und Abberufungen des Gemeindedirektors und der Beigeordneten eingeführt wurde, habe ich in diesem Sinne gegenüber dem Ausschuß für Innere Verwaltung des Landtags Stellung genommen.

Darüber hinaus besteht Bedarf, die Gemeindeordnung unter Berücksichtigung des Rechtes auf informationelle Selbstbestimmung der Bürger insgesamt zu novellieren. Dies gilt etwa für Fragen nach Zulässigkeit und Umfang der Datenübermittlung an den Rat und seine Ausschüsse, für die Behandlung von Bürgerbeschwerden im Rat, die Öffentlichkeit von Ratssitzungen, den Inhalt der Tagesordnungen und die Informationsrechte der Fraktionen. Das Innenministerium hat eine Novellierung der Gemeindeordnung für diese Legislaturperiode in Aussicht gestellt.

3.4.4 Gesetz über den Datenschutz im Gesundheitswesen

Das vom Ministerium für Arbeit, Gesundheit und Soziales seinerzeit angekündigte Vorhaben eines Gesetzes über den Datenschutz im Gesundheitswesen (vgl. 9. Tätigkeitsbericht, S. 38) hat sich in der abgelaufenen Legislaturperiode nicht mehr verwirklichen lassen. Das Ministerium hat jedoch seinen Plan zur Schaffung eines derartigen Gesetzes inzwischen wieder aufgegriffen und wird in Kürze einen ersten Entwurf zur Abstimmung in den Ressorts vorlegen. Gleichzeitig ist auch meine Beteiligung vorgesehen. Es bleibt abzuwarten, inwieweit die Feststellungen und Forderungen der Daten-

schutzbeauftragten des Bundes und der Länder in dem Entwurf Berücksichtigung finden werden (vgl. auch 7. Tätigkeitsbericht, S. 68 bis 70).

3.4.5 Landesbeamtengesetz

Durch die beabsichtigte Novellierung des Beamtenrechtsrahmengesetzes wird es für den Landesgesetzgeber unumgänglich werden, die Bestimmungen des Landesbeamtengesetzes zum Personalaktenrecht zu überarbeiten. Dabei wird insbesondere zu prüfen sein, ob weitere Vorschriften des Landesbeamtengesetzes datenschutzrechtliche Defizite aufweisen. Nach meiner Auffassung besteht entsprechender Regelungsbedarf beim Auswahlverfahren (§ 7), bei der Durchführung von amtsärztlichen Untersuchungen (§ 45), beim Beurteilungsverfahren (§ 104) sowie im Bereich der Sondervorschriften für die Polizeibeamten zur freien Heilfürsorge (§ 189) und hinsichtlich der Befugnisse des Polizeiarztes zur Verarbeitung von Gesundheitsdaten der Polizeivollzugsbeamten (§ 194).

3.4.6 Landespersonalvertretungsgesetz

Im Hinblick auf zahlreiche Fragen aus der Praxis der Personalvertretungen sowie divergierende Gerichtsentscheidungen zu den datenschutzrechtlichen Aspekten halte ich es für geboten, daß der Gesetzgeber im Landespersonalvertretungsgesetz die Datenverarbeitung durch Personalvertretungen normenklar regelt und die notwendigen Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung der Beschäftigten im öffentlichen Dienst trifft. Dabei muß insbesondere festgelegt werden, in welchem Umfang und für welche Dauer die Personalvertretung ihr übermittelte Daten der Beschäftigten speichern darf. So ist beispielsweise die Vernichtung der in Mitbestimmungsfällen vorgelegten Unterlagen sowie Art und Dauer der Aufbewahrung von Tagesordnung und Protokoll im Gesetz vorzusehen.

3.4.7 Beihilfenverordnung

Trotz meiner Empfehlung sind in die Beihilfenverordnung (BVO) datenschutzrechtliche Regelungen bisher nicht aufgenommen worden. Insoweit ist das Verfahren zur Beihilfegewährung nach § 13 BVO immer noch unzureichend geregelt. Es fehlen insbesondere Bestimmungen

- zur datenschutzrechtlich befriedigenden Einbindung der Angehörigen in das Antragsverfahren ohne Zwang zur Offenbarung von Diagnose und ärztlichen Leistungen gegenüber dem Beihilfeberechtigten,
- über Umfang und Behandlung von amtsärztlichen oder Fachgutachten bei der Prüfung der Beihilfefähigkeit bestimmter Heilverfahren,
- zum Einsichtsrecht des Antragstellers bzw. seiner beihilfeberechtigten Angehörigen in die sie betreffenden Vorgänge der Beihilfeakte und
- über die Voraussetzungen einer zulässigen automatisierten Datenverarbeitung im Beihilfeverfahren.

Außerdem halte ich das Verlangen nach Angabe der Diagnose in Beihilfeanträgen, das nach meiner Auffassung nicht generell, sondern nur in begründeten Einzelfällen gerechtfertigt erscheint, nur dann für zulässig, wenn dafür eine entsprechende Regelung zumindest in der Beihilfenverordnung vorhanden ist.

3.4.8 Schulrecht

Obwohl die Landesregierung in ihrer Stellungnahme vom Dezember 1989 auf meine Forderung nach einer gesetzlichen Regelung der Erhebung und Verarbeitung von Schüler- und Elterndaten in den Schulen und im Schulgesundheitswesen (vgl. 9. Tätigkeitsbericht, S. 39) hin mitgeteilt hat, daß ein entsprechender Gesetzentwurf erarbeitet worden ist, liegt mir bis heute ein solcher Entwurf nicht vor. Stattdessen arbeitet das Kultusministerium neue Änderungen der Verwaltungsvorschrift zu § 5 Abs. 4 der Allgemeinen Schulordnung aus. In meiner Stellungnahme zu den Verwaltungsvorschriften habe ich noch einmal auf die Notwendigkeit einer gesetzlichen Regelung hingewiesen.

4. Grenzüberschreitender Datenverkehr

4.1 Ausgangslage

Bei einer Verarbeitung personenbezogener Daten durch öffentliche Stellen des Landesbereichs wird künftig zunehmend die Frage einzubeziehen sein, ob gespeicherte Daten aus einem für die Bürger überschaubaren und durch Rechtsvorschriften geregelten Bereich an öffentliche aber auch an nicht-öffentliche Stellen im Ausland übermittelt werden dürfen. In diesen Fällen können sich für die Betroffenen neue Gefährdungen ihres Persönlichkeitsrechts ergeben, denen nach meiner Einschätzung eine gesteigerte Beachtung geschenkt werden muß.

Die Übermittlung personenbezogener Daten durch öffentliche Stellen des Landesbereichs an Stellen außerhalb des Geltungsbereichs des Grundgesetzes ist als Eingriff in das informationelle Selbstbestimmungsrecht des Einzelnen nur auf gesetzlicher Grundlage zulässig. Für die Beurteilung der Zulässigkeit solcher Übermittlungen werden vermehrt internationale Vereinbarungen zugrunde zu legen sein (§ 17 Satz 1 DSG NW). Solchen für weite Verwaltungsbereiche einschlägigen Vereinbarungen kommt deshalb eine besondere Bedeutung zu (unten S. 33/34).

Demgegenüber dürften sich in nur seltenen Fällen Übermittlungen an Stellen außerhalb des Geltungsbereichs des Grundgesetzes unmittelbar auf die Regelungen des Datenschutzgesetzes NW (§ 17 Satz 2) stützen lassen, weil zu den Übermittlungserfordernissen des DSG NW (§ 14 Abs. 1 Satz 1 oder § 16 Abs. 1) die von den speichernden Stellen zu treffende Feststellung treten muß, daß im Empfängerland **gleichwertige Datenschutzregelungen** gelten (hierzu auch 9. Tätigkeitsbericht, S. 122 bis 124). Wegen des in Nordrhein-Westfalen vergleichsweise hohen Datenschutzstandards wird eine solche Feststellung nur selten getroffen werden können. Auch sind aus meiner Sicht an eine entsprechende Prüfung strenge Maßstäbe anzulegen, um zusätzliche Risiken für das informationelle Selbstbestimmungsrecht des Einzelnen möglichst zu vermeiden. Andernfalls bestünde die Gefahr, daß ein nach dem nordrhein-westfälischen Datenschutzrecht gewährleisteter Datenschutz bei Übermittlungen ins Ausland leerlaufen könnte.

Risiken für das informationelle Selbstbestimmungsrecht des Einzelnen können sich aber auch dann ergeben, wenn in Vereinbarungen über die wechselseitige Zulassung von Datenübermittlungen dem Datenschutz nicht Rechnung getragen wird und im Empfängerland keine oder nur unzureichende Datenschutzregelungen bestehen. In diesen Fällen besteht Grund zu der Annahme, daß durch die Übermittlung personenbezogener Daten gegen den Zweck des Datenschutzgesetzes NW oder gegen den Zweck eines anderen Gesetzes im Geltungsbereich des Grundgesetzes verstoßen wird, so daß nach meiner Auffassung das aus § 17 Satz 3 DSG NW herzuleitende Übermittlungsverbot auch in einer solchen Fallkonstellation zu beachten ist. Zur Wahrung des informationellen Selbstbestimmungsrechts darf es nicht hingenommen werden, daß personenbezogene Daten von öffentlichen Stellen des Landesbereichs an „Datenschutzoasen" im Ausland übermittelt werden.

Diese und weitere damit zusammenhängende Probleme werden erheblich an Gewicht verlieren, falls gleichwertige gesetzliche Sicherungen in übermittelnden und empfangenden Ländern geschaffen werden.

4.2 Aktivitäten zur Harmonisierung des Datenschutzes in Europa

4.2.1 Stand

Sollen Datenübermittlungen ins Ausland im Hinblick auf eine für notwendig erachtete Zusammenarbeit öffentlicher Stellen nicht schon deshalb unzulässig sein, weil im Empfängerland keine dem nordrhein-westfälischen Datenschutzrecht vergleichbaren Regelungen bestehen, kann dies nur erreicht werden, wenn der Datenschutz in den beteiligten Staaten weitgehend harmonisiert wird (vgl. oben).

Auf europäischer Ebene sind die Bestrebungen zur Vereinheitlichung des Datenschutzes in den Mitgliedstaaten des Europarats bisher nicht sehr erfolgreich gewesen. Die mit einer solchen Zielsetzung auf den Weg gebrachte **Datenschutzkonvention** vom 28. Januar 1981 ist bisher erst von acht Mitgliedstaaten – darunter auch von der Bundesrepublik Deutschland – ratifiziert worden. Darüber hinaus zeichnet sich ab, daß eine Vereinheitlichung des Datenschutzes nach Maßgabe der Konvention den spezifischen Anforderungen in einzelnen Bereichen nicht gerecht werden kann.

Im Bereich der EG werden derzeit mit hohem Aufwand Infrastrukturmaßnahmen für neue Telekommunikationsdienste durchgeführt (hierzu: Grünbuch über die Entwicklung des gemeinsamen Marktes für Telekommunikationsdienstleistungen und Telekommunikationsgeräte – Bundesratsdrucksache 11/930). Die Schaffung solcher Dienste tangiert die Persönlichkeitsrechte nahezu aller EG-Bürger. Schon die bisherige Entwicklung auf diesem Gebiet hat gezeigt, daß die spezifischen Belange des Datenschutzes – möglichst frühzeitig – EG-weit in die Planung und Realisierung einbezogen werden müssen.

Die EG-Kommission hat mit Blick auf eine für notwendig erachtete Rechtsvereinheitlichung zur Vollendung des EG-Binnenmarktes (Stichtag: 31. Dezember 1992) einen Katalog – Bundesratsdrucksache 690/90 – vorgelegt, der auf folgende Maßnahmen zielt:

- Eine allgemeine Richtlinie des Rates zur Angleichung bestimmter Rechts- und Verwaltungsvorschriften für den Schutz von Personen bei der Verarbeitung personenbezogener Daten (unten S. 32),
- eine Entschließung des Rates mit dem Ziel, auch für den öffentlichen Bereich, für den die EG keine Kompetenzen besitzt (z.B. Verteidigung und Verbrechensbekämpfung), die in der Rahmenrichtlinie enthaltenen Grundsätze anwendbar werden zu lassen,
- eine Selbstverpflichtung der Kommission, die Prinzipien der Rahmenrichtlinie für die Datenverarbeitung der eigenen Dienststellen anzuwenden (unten S. 33),

- eine spezielle Richtlinie des Rates zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen, insbesondere im ISDN und in Mobilfunknetzen,
- einen Beschluß des Rates, Verhandlungen über den Beitritt der EG zur Datenschutzkonvention des Europarats aufzunehmen und
- einen Beschluß des Rates auf dem Gebiet der Informationssicherheit.

4.2.2 Allgemeine Richtlinie des Rates

Mit der allgemeinen Richtlinie soll erreicht werden, daß in den Mitgliedstaaten der EG ein gleichmäßiges und hohes Schutzniveau bei der Verarbeitung personenbezogener Daten geschaffen wird, wobei dem nationalen Gesetzgeber in vielen Fragen allerdings ein Regelungsspielraum überlassen bliebe. Aus meiner Sicht enthält der Entwurf eine Reihe sowohl positiv als auch negativ zu beurteilender Regelungen. Im Grundsatz zu begrüßen ist, daß die Richtlinie auch Vorgaben für die Verarbeitung personenbezogener Daten durch öffentliche Verwaltungen in den Mitgliedstaaten enthalten soll. Positiv zu bewerten ist auch das Gebot der Unabhängigkeit der Datenschutzkontrollbehörden. Kritisch ist demgegenüber insbesondere zu sehen, daß der Entwurf lediglich auf eine dateimäßige Datenverarbeitung abstellt. Auch ist der im Entwurf vorgesehene Katalog von Fällen, in denen die Mitgliedstaaten Ausnahmen von einem Auskunftsrecht des Bürgers hinsichtlich sie betreffender personenbezogener Daten vorsehen können, zu weitgehend.

Auf eine spezielle Problematik ist schon jetzt hinzuweisen. Der Richtlinienvorschlag sieht in Artikel 1 Abs. 2 vor, daß die Mitgliedstaaten untereinander nicht den freien Verkehr personenbezogener Daten aus Gründen des gemäß Abs. 1 gewährleisteten Schutzes beschränken oder untersagen dürfen. Ausweislich der Erörterung zu Artikel 1 (Bundesratsdrucksache 690/90, S. 18) bedeutet dies, daß der freie Verkehr von Daten in den von der Richtlinie abgedeckten Bereichen nicht aus Gründen des Schutzes der betroffenen Person eingeschränkt werden darf. Andererseits ist zu folgern (argumentum e contrario), daß in dem nicht von dem Richtlinienvorschlag erfaßten Bereich einer aktenmäßigen Datenverarbeitung auf gleichwertige Datenschutzregelungen im Empfängerland abstellende Vorbehalte (oben S. 30) weiterhin beachtet werden müssen. Eine auch in diesem Bereich auf den Abbau solcher Vorbehalte gerichtete Interpretation der Richtlinie wäre im Geltungsbereich des Grundgesetzes überdies mit der Rechtsprechung des Bundesverfassungsgerichts zum umfassenden Schutz des informationellen Selbstbestimmungsrechts nicht zu vereinbaren (vgl. hierzu 9. Tätigkeitsbericht, S. 44).

Am 14. Dezember 1990 hat der Bundesrat auf der Grundlage der Empfehlungen seiner Ausschüsse (Bundesratsdrucksache 690/1/90) zu dem Richtlinienentwurf Stellung genommen. Die Datenschutzbeauftragten des Bundes und der Länder haben ihre Auffassung zu dem Entwurf in einem Beschluß (Anlage 3, S. 171 bis 173) zum Ausdruck gebracht, der im Rahmen einer Sonderkonferenz am 29. Januar 1991 gefaßt wurde.

4.2.3 Datenschutz bei Institutionen der EG

Die sich aus § 17 DSG NW ergebenden Voraussetzungen für Datenübermittlungen ins Ausland sind auch bei Übermittlungen an über- oder zwischenstaatliche Stellen zugrunde zu legen. Die Vorschrift gilt insofern auch für Übermittlungen an EG-Behörden. Es ist deshalb von Bedeutung, ob die Organe und Einrichtungen der Europäischen Gemeinschaft Datenschutzregelungen unterliegen und welche Bestimmungen ggf. zur Anwendung kommen. Hierzu hat die Kommission eine Erklärung betreffend die Anwendung der Grundsätze der Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten abgegeben. Die Kommission bringt darin den Wunsch zum Ausdruck, daß die Grundsätze der Richtlinie für die Organe und Einrichtungen der Gemeinschaft gelten sollen. Insoweit ist vorgesehen, daß die Kommission die erforderlichen Maßnahmen trifft und vorschlägt (Bundesratsdrucksache 690/90, S. 79). Es bleibt zu hoffen, daß die in der Erklärung zum Ausdruck gekommene Absicht alsbald verwirklicht wird.

4.3 Grenzüberschreitender Datenverkehr in einzelnen Bereichen

4.3.1 Schengener Informationssystem

Am 19. Juni 1990 wurde von den Regierungsvertretern der „Schengen-Staaten" das „Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 14. Juni 1985 zwischen den Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen" unterzeichnet. In diesem Abkommen werden eine Reihe von Maßnahmen geregelt, die befürchtete Sicherheitsdefizite durch den Wegfall der Grenzkontrollen ausgleichen sollen. Problematisch ist dabei insbesondere der grenzüberschreitende Datenaustausch, vor allem im Hinblick darauf, daß der Datenschutzstandard nicht in allen betroffenen Staaten gleich weit entwickelt ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher in ihrer Entschließung vom 26./27. Oktober 1989 Mindestanforderungen für den grenzüberschreitenden Datenaustausch aufgestellt. Das nunmehr unterzeichnete Abkommen enthält gegenüber den ursprünglichen Fassungen deutliche Verbesserungen. Die Zukunft muß zeigen, ob das Abkommen in dieser Form auch in der Praxis anwendbar ist, ohne daß sich gravierende Verschlechterungen für den Datenschutz ergeben.

4.3.2 Übermittlung von Sozialdaten ins Ausland

In die EWG-Verordnung Nr. 1408/71 des Rates (Amtsblatt EG, L 149 vom 05.07.1971) zur Anwendung der Systeme der sozialen Sicherheit auf Arbeitnehmer und deren Familien, die innerhalb der Gemeinschaft zu- und abwandern, ist durch Verordnung Nr. 2332/89 (Amtsblatt EG, L 224 vom 02.08.1989) eine Vorschrift eingefügt worden, die erheblichen datenschutzrechtlichen Bedenken begegnet. Danach gilt zwar für die Übermittlung an

einen anderen Mitgliedstaat das Datenschutzrecht des übermittelnden Staates. Für den Empfängerstaat wird jedoch die Möglichkeit einer Weiterverarbeitung der Daten nach eigenem Datenschutzrecht eröffnet. Dies führt praktisch zur Aufhebung des in der Bundesrepublik Deutschland geltenden Sozialdatenschutzes. Nach meiner Auffassung müßte eine dem § 78 SGB X vergleichbare Regelung über die Zweckbindung geschaffen werden. Auch die in der Verordnung vorgesehene Verwendung von Sozialdaten zu anderen Zwecken mit dem Einverständnis der betroffenen Personen erscheint bedenklich, weil sich die Betroffenen insoweit unter Druck gesetzt fühlen könnten, die Einwilligung mithin nicht freiwillig erteilt wäre.

4.3.3 Statistikverordnung

In der Verordnung des Rates der Europäischen Gemeinschaft vom 11. Juni 1990 (Amtsblatt der EG Nr. L 151/1) wurde den in der Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 26./27.10.1989 erhobenen Forderungen nach Zulassung der Übermittlung nur auf Grund eines eigenen Rechtsaktes der EG für bestimmte statistische Zwecke sowie nach frühzeitiger Anonymisierung und nach Regelung der notwendigen organisatorisch-technischen Maßnahmen der Datensicherung weitgehend entsprochen. Auch die Forderung nach ausreichender Sanktion für die Verletzung des Statistikgeheimnisses wurde berücksichtigt. Jedoch besteht auf der Ebene der Europäischen Gemeinschaft keine unabhängige Datenschutzkontrolle, die die Einhaltung der statistischen Geheimhaltung überwacht. Der Ausschuß für die statistische Geheimhaltung nach Artikel 7 der Verordnung wird lediglich bei der Festlegung der Modalitäten für die Datenübermittlung und die Gewährung der Zugangsberechtigung beteiligt. Auch das Prüfrecht nach Artikel 8 entspricht nicht den Anforderungen an eine wirksame Datenschutzkontrolle.

5. Datenschutz in den Bereichen der Verwaltung

5.1 Einwohnerwesen

5.1.1 Melderegisterauskünfte

Die im Melderegister gespeicherten personenbezogenen Daten eines Polizeibeamten waren gemäß § 34 Abs. 5 des Meldegesetzes NW (MG NW) mit einer Auskunftssperre versehen. Trotz dieser Auskunftssperre wurde seine Anschrift und sein Geburtsdatum auf eine **telefonische** Anfrage weitergegeben. Der Anrufer täuschte die Meldebehörde, indem er sich als Bediensteter einer öffentlichen Stelle ausgab.

Gegen die Erteilung einer fernmündlichen einfachen Melderegisterauskunft nach § 34 Abs. 1 MG NW, die an keine Voraussetzungen gebunden ist, bestehen keine datenschutzrechtlichen Bedenken. Soweit jedoch eine erweiterte Melderegisterauskunft erteilt werden soll, ist die Identität des Anrufers zu überprüfen. Ist eine Auskunftssperre bei den Meldedaten eingetragen, ist sowohl die fernmündliche als auch die mündliche oder schriftliche Auskunfterteilung gegenüber Privatpersonen unzulässig.

Auskunftssperren haben keine Wirkung gegenüber öffentlichen Stellen. Ist eine Auskunftssperre eingetragen und beantragt eine öffentliche Stelle eine fernmündliche Melderegisterauskunft, so ist die Identität des Anrufers durch Überprüfung der Telefonnummer auf Grund amtlicher Unterlagen durch Rückruf bei der anfragenden Stelle festzustellen. Durch Erlaß von Dienstanweisungen und Kontrolle der Einhaltung solcher Dienstanweisungen sollte das Verfahren der Identitätsüberprüfung bei telefonischen Melderegisterauskünften sichergestellt werden.

Zu der **„Identifizierung des Gesuchten"** bei der Erteilung von Melderegisterauskünften habe ich in meinem 3. Tätigkeitsbericht (S. 18/19) Stellung genommen. Obwohl in den meisten Fällen das von mir empfohlene Verfahren bei der Erteilung von Melderegisterauskünften praktiziert wird, kommt es nach wie vor häufig zu Personenverwechslungen, wodurch den Betroffenen meist große Unannehmlichkeiten, wie Gerichtsvollzieherbesuche, Pfändungen, Vorladungen durch die Polizei und auch Hausdurchsuchungen entstanden sind.

Ursache für die Personenverwechslungen ist in der Regel menschliches Versagen. Dies sollte zwar nicht vorkommen, wird sich aber wohl nie völlig ausschließen lassen. Es kann nur immer wieder darauf hingewiesen werden, bei der Identitätsprüfung größte Sorgfalt walten zu lassen. Es empfiehlt sich auch die Aufnahme eines Vermerks im Datensatz der Betroffenen, die bereits verwechselt worden sind, der auf diese Verwechslungsgefahr hinweist. Ein solcher Hinweis darf jedoch nicht die Form und die Auswirkung einer Auskunftssperre nach § 34 Abs. 5 MG NW haben.

Nach § 34 Abs. 5 MG NW ist jede Melderegisterauskunft unzulässig, wenn der Betroffene der Meldebehörde das Vorliegen von Tatsachen glaubhaft gemacht hat, die die Annahme rechtfertigen, daß ihm oder einer anderen Person hieraus eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange erwachsen kann.

Diese Voraussetzungen für die Eintragung einer Auskunftssperre nach § 34 Abs. 5 MG NW sind in den Fällen der Verwechslungsgefahr nicht erfüllt. Um den Datenschutzbelangen der Betroffenen einerseits und den Belangen der Auskunftsuchenden andererseits Rechnung zu tragen, reicht die Aufnahme eines Vermerks in den Datensatz der Betroffenen aus, der auf die Verwechslungsgefahr hinweist und bei Melderegisteranfragen eine über das übliche Maß hinausgehende Identitätsprüfung sicherstellt. Eine Auskunftssperre bringt nicht nur Schutz für den Betroffenen, sondern kann auch zu Unannehmlichkeiten führen, nämlich dann, wenn der Auskunftsuchende zu rätseln beginnt, weshalb eine Auskunftssperre besteht.

5.1.2 Einsatz veralteter DV-Programme

Im Rahmen eines Kontrollbesuches bei einer Stadt ist bei der stichprobenweisen Überprüfung der im Melderegister gespeicherten personenbezogenen Daten aufgefallen, daß auf den Bildschirmmasken des Melderegisters als gesetzliche Grundlage für die Datenspeicherung nicht die Vorschriften des Meldegesetzes für das Land Nordrhein-Westfalen sondern die Vorschriften des Melderechtsrahmengesetzes erscheinen. Die Speicherung der Vorschriften des Meldegesetzes für das Land Nordrhein-Westfalen sei programmtechnisch nicht möglich, wurde von der Stadt dieser Mangel erläutert.

Bei der Überprüfung wurde weiter festgestellt, daß sich im aktuellen Bestand des Melderegisters auch noch Daten von Personen befanden, die seit Jahren verstorben oder weggezogen waren. Nach Ablauf von fünf Jahren nach Ende des Kalenderjahres, in dem ein Einwohner weggezogen oder verstorben ist, sind die bis dahin gespeicherten Daten für die Dauer von 45 Jahren gesondert aufzubewahren und durch technische und organisatorische Maßnahmen besonders zu sichern. Während dieser Zeit dürfen sie mit Ausnahme der Anschrift sowie des Sterbetages und -ortes nicht mehr verarbeitet oder sonst genutzt werden, es sei denn, daß dies u. a. zu wissenschaftlichen Zwecken oder zur Behebung einer bestehenden Beweisnot unerläßlich ist oder der Betroffene schriftlich eingewilligt hat (§ 11 Abs. 3 MG NW). Auf diesen Mangel sei nach Auskunft der Stadt der Programmhersteller zwar bereits hingewiesen worden, eine Umsetzung des § 11 MG NW sei aber aus programmtechnischen Gründen nicht möglich.

Ich habe empfohlen, einmal beim Programmhersteller sowohl darauf hinzuwirken, daß die Vorschriften des Meldegesetzes für das Land Nordrhein-Westfalen gespeichert werden können, als auch, daß die Vorschrift des § 11 MG NW umgesetzt werden kann, sowie zum anderen die Fälle des § 11 Abs. 2 MG NW zu überprüfen und in eine gesonderte Datei zu übernehmen und die erforderlichen technischen und organisatorischen Maßnahmen zum

Schutz der Daten vor unbefugtem Zugriff zu treffen. Die Änderung des veralteten Programms soll nunmehr in Kürze erfolgen.

Besondere Nachdenklichkeit löst in diesem Zusammenhang die Tatsache aus, daß auf die Notwendigkeit der Programmänderung von den Bediensteten der Stadt seit Jahren hingewiesen worden war, eine Änderung des veralteten Programms jedoch erst nach meinem Kontrollbesuch in Angriff genommen wurde. Erfreulich ist allerdings, daß der Programmhersteller mir fernmündlich versichert hat, er werde auch die anderen Gemeinden in Nordrhein-Westfalen, die dieses Programm verwenden, unter Berücksichtigung meiner Bedenken mit einer neuen Programmversion ausstatten.

5.1.3 Meldedatenübermittlungsverordnung

Innerhalb des Berichtszeitraums wurde vom Innenministerium eine Verordnung zur Änderung der Verordnung über die Zulassung der regelmäßigen Datenübermittlung von Meldebehörden an andere Behörden oder sonstige öffentliche Stellen (MeldDÜV NW – GV. NW. 1991 S. 7 –) erlassen. Gegen den Entwurf der Verordnung habe ich sowohl in einer schriftlichen Stellungnahme als auch in einer mündlichen Erörterung, an der u. a. die Vertreter der kommunalen Spitzenverbände teilnahmen, meine datenschutzrechtlichen Bedenken geäußert. Aus datenschutzrechtlicher Sicht war aus Gründen der Transparenz gegenüber den betroffenen Bürgern zu fordern, die Anzahl der Möglichkeiten **regelmäßiger Datenübermittlungen** durch die Meldebehörde (on-line-Anschlüsse) möglichst gering zu halten. Dieser Forderung wird die Verordnung nicht gerecht. So wird die Möglichkeit regelmäßiger Datenübermittlungen auch gegeben für Bereiche, in denen nur im Einzelfall eine Datenübermittlung erforderlich sein kann. Praktikabilitätsgründe allein können für einen on-line-Anschluß nicht ausreichen.

Wie sich aus zahlreichen Anfragen und Eingaben ergibt, wird vom betroffenen Bürger insbesondere die regelmäßige Datenübermittlung an den Westdeutschen Rundfunk Köln (WDR) als problematisch angesehen. Nach § 9 a Meld DÜV NW dürfen die Meldebehörden zur Erfüllung der Aufgaben des Einzugs der Rundfunkgebühren dem WDR oder der von ihm beauftragten Stelle (**GEZ**) Vor- und Familiennamen, Tag der Geburt, bisherige und neue Anschrift (Haupt- und Nebenwohnung), Tag des Einzugs, Familienstand sowie Sterbetag über alle An- und Abmeldungen volljähriger Einwohner übermitteln.

Meine Bedenken gegen diese Regelung trotz formeller rechtlicher Grundlage hatte ich in der Vergangenheit bereits mehrfach geäußert. Der Unmut der Bürger über diese Vorschrift wird immer wieder an mich herangetragen. Sie empfinden eine derartige „Raster"-Fahndung nach Schwarzhörern und -sehern als unnötigen Eingriff in das Recht auf informationelle Selbstbestimmung der überwiegenden Mehrheit derjenigen, die ordnungsgemäß ihre Rundfunk- und Fernsehgeräte angemeldet haben. Hier stellt sich die Frage, ob sich nach Einführung dieser Regelung (1986) die Zahl der Schwarzhörer und -seher nachhaltig vermindert hat. Bemerkenswert in diesem Zusammenhang ist auch, daß man in anderen Bundesländern auf eine entsprechende Vorschrift verzichtet hat.

Meine datenschutzrechtlichen Empfehlungen, Anregungen und Hinweise hat das Innenministerium nicht berücksichtigt. Meine Bedenken gegen die Verordnung bleiben bestehen.

5.2 Paß- und Personalausweiswesen

5.2.1 Einsichtnahme der Polizei in das Personalausweisregister

In mehreren Eingaben bin ich gefragt worden, inwieweit es zulässig ist, daß die Polizei etwa bei der Verfolgung von Verkehrsordnungswidrigkeiten die Personalausweisbehörde um Weitergabe personenbezogener Daten, zu denen auch Lichtbilder gehören, ersucht. Zu diesem Fragenkomplex habe ich schon in meinem 6. Tätigkeitsbericht Stellung genommen (S. 26/27).

Nach Inkrafttreten des Gesetzes über Personalausweise (PAG) ist die Zulässigkeit der Datenübermittlung nach § 2 b PAG zu beurteilen. Danach dürfen die Personalausweisbehörden anderen Behörden auf deren Ersuchen Daten aus dem Personalausweisregister übermitteln. Voraussetzung ist einmal, daß die ersuchende Behörde auf Grund von Gesetzen oder Rechtsverordnungen berechtigt ist, solche Daten zu erhalten (Abs. 2 Nr. 1). Voraussetzung ist weiter, daß die ersuchende Behörde ohne Kenntnis der Daten nicht in der Lage wäre, eine ihr obliegende Aufgabe zu erfüllen (Abs. 2 Nr. 2) und die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können, oder daß nach der Art der Aufgabe, zu deren Erfüllung die Daten erforderlich sind, von einer solchen Datenerhebung abgesehen werden muß (Abs. 2 Nr. 3).

Im übrigen bleibt auch der Grundsatz der Verhältnismäßigkeit zu beachten. So reicht es insbesondere nicht aus, wenn zur Aufgabenerfüllung etwa die Kenntnis eines Lichtbildes nur dienlich, aber nicht unbedingt notwendig ist. Nach dem Verhältnismäßigkeitsgrundsatz muß die mit dem Eingriff verbundene Belastung des Betroffenen in einem angemessenen Verhältnis zu dem zu erreichenden Zweck stehen.

Auch wenn nach § 2 b Abs. 3 Satz 1 PAG die ersuchende Behörde die Verantwortung dafür trägt, daß die Voraussetzungen des Absatzes 2 vorliegen, ist durch die Personalausweisbehörde zumindest eine Plausibilitätsprüfung durchzuführen. Die hierzu erforderlichen Angaben sind von der Polizei zu machen.

In der Regel ist davon auszugehen, daß auch bei der Durchführung von Ordnungswidrigkeitenverfahren § 2 b Abs. 2 Nr. 1 PAG erfüllt ist. Bedenken bestehen allerdings hinsichtlich des Vorliegens der Voraussetzungen von § 2 b Abs. 2 Nr. 2 und 3 PAG, wenn nicht die Polizei zuvor (vergeblich) versucht hat, den Betroffenen aufzusuchen und zu identifizieren. Dies hat die Polizei schlüssig vorzutragen, insbesondere, daß die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können.

Das Oberlandesgericht Hamm hat in einem Beschluß vom 7. November 1989–3 Ss OWi 695/89 – ausgeführt, daß die Voraussetzungen, die § 2 b

Abs. 2 Nr. 3 PAG an eine Datenweitergabe stellt, nicht vorliegen, wenn der Betroffene im Ort wohnt und zum Zwecke der Identifizierung deshalb ohne weiteres durch einen Polizeibeamten hätte aufgesucht werden können.

Wie die Eingaben gezeigt haben, läßt sich ohne Protokollierung im nachhinein nicht mehr feststellen, ob die Einsichtgewährung in das Personalausweisregister gegen § 2 b Abs. 2 PAG verstieß oder die Voraussetzungen hierfür vorlagen. Auch verpflichtet Artikel 19 Abs. 4 des Grundgesetzes die Behörde, zur Gewährleistung eines effektiven Rechtsschutzes die Übermittlung personenbezogener Daten zu protokollieren, so daß der Bürger von der Weitergabe der Daten Kenntnis erlangen und dagegen den Rechtsweg beschreiten kann (BVerfGE, 65, 1, 70). Nach § 18 Abs. 1 DSG NW ist dem Betroffenen von der speichernden Stelle auf Antrag Auskunft u. a. über die zu seiner Person gespeicherten Daten und die Empfänger von Übermittlungen zu erteilen. Wenn eine Protokollierung im Rahmen einer derartigen Datenübermittlung ausgeschlossen wäre, wäre eine Behörde nicht in der Lage, ihrer gesetzlichen Verpflichtung nach § 18 Abs. 1 Nr. 3 (2. Alternative) DSG NW nachzukommen. Eine Protokollierung erscheint insoweit zwingend erforderlich (vgl. Weyer, Kommentar zum Datenschutzgesetz Nordrhein-Westfalen § 18 Rdnr. 4, S. 143; Stähler, Kommentar zum Datenschutzgesetz Nordrhein-Westfalen § 18 Rdnr. 2, S. 154).

Ich habe den Gemeinden hierzu empfohlen, künftig die Erforderlichkeit der Einsichtnahme in Lichtbildkarteien durch die Polizei unter Beachtung der dargelegten Grundsätze zu prüfen, die Einsichtgewährung zu protokollieren, diese Unterlagen getrennt nur für Kontrollzwecke aufzubewahren und nach sechs Monaten zu vernichten.

5.2.2 Vernichtung fehlerhafter Personalausweise

Im Rahmen eines Kontroll- und Beratungsbesuchs des Bundesbeauftragten für den Datenschutz bei der Bundesdruckerei ist er darüber informiert worden, daß die Paßbehörden in zunehmendem Maß Ziffer 6.7.3 der Allgemeinen Verwaltungsvorschriften zur Durchführung des Paßgesetzes vom 2. Januar 1988 nicht beachten und den entwerteten Ausweis nicht an die Bundesdruckerei zurückgeben.

Nach Ziffer 6.7.3 der Allgemeinen Verwaltungsvorschriften zur Durchführung des Paßgesetzes vom 2. Januar 1988 hat die Paßbehörde bei fehlerhaften Reisepässen den Antrag unter Vergabe einer neuen Serien-Nummer erneut an die Bundesdruckerei zu senden. Die bisherige Serien-Nummer ist durchzustreichen. Dem Antrag ist der fehlerhafte Reisepaß beizufügen. Die Paßbehörde hat den fehlerhaften Reisepaß zuvor durch Abschneiden der linken unteren Ecke ungültig zu machen. Stellt die Bundesdruckerei fest, daß dies nicht geschehen ist, macht sie den Reisepaß unverzüglich nach Eingang ungültig. Die fehlerhaften und ungültigen Reisepässe werden von der Bundesdruckerei vernichtet. Über die Vernichtung ist eine Niederschrift anzufertigen. Dieses gilt nach Ziffer 7.12 der Verwaltungsvorschrift zur Durchführung des Personalausweisgesetzes für das Land Nordrhein-Westfalen auch für fehlerhafte Personalausweise.

Die Bundesdruckerei hat, um Nachteile für den Bürger zu vermeiden zwar neue Ausweispapiere hergestellt und der Paßbehörde ausgeliefert, intern aber die fehlende Rückgabe dokumentiert. Vor einiger Zeit waren ca. 1300 solcher Fälle festgehalten. Die Bundesdruckerei hat den Bundesbeauftragten für den Datenschutz darüber unterrichtet, daß die Zahl der Reklamationsfälle, in denen das Ausweisdokument nicht ordnungsgemäß zurückgeleitet wird, weiter steigt.

Das Innenministerium, dem ich den Sachverhalt vor einiger Zeit zur Kenntnis gegeben hatte, teilte mir mit, daß es nicht feststellen konnte, ob auch Paß- bzw. Personalausweisbehörden in Nordrhein-Westfalen in dieser Form verfahren. Der Bundesbeauftragte für den Datenschutz hat mir daraufhin eine Liste übersandt, die die Behörden des Landes Nordrhein-Westfalen ausweist, die im Reklamationsfall das jeweilige Ausweisdokument nicht an die Bundesdruckerei zurückgeleitet haben.

Bei meinen Nachforschungen habe ich festgestellt, daß in den meisten Fällen, in denen fehlerhafte Ausweispapiere reklamiert worden waren, die Antragsteller diese Papiere dringend benötigten. Da in der Anfangsphase die Herstellung der Ausweispapiere längere Zeit in Anspruch nahm, händigten die Gemeinden die fehlerhaften Ausweispapiere an die Antragsteller aus und reklamierten die Fehlerhaftigkeit gleichzeitig bei der Bundesdruckerei. Ein Mitübersenden der Papiere bei der Reklamation war somit nicht möglich. Nach Fertigstellung der fehlerfreien Papiere und Aushändigung an die Antragsteller wurden die fehlerhaften bei den Gemeinden selbst vernichtet.

In einigen Fällen wurden die fehlerhaften und reklamierten Papiere auch aus Unkenntnis der gesetzlichen Bestimmungen bei den Gemeinden von vornherein vernichtet. Es ist jedoch auch vorgekommen, daß nach den Unterlagen der Gemeinden die reklamierten Papiere ordnungsgemäß an die Bundesdruckerei übersandt worden sind. In diesen Fällen müßte ein Irrtum bei der Bundesdruckerei vorliegen. Ich habe den Bundesbeauftragten für den Datenschutz insoweit unterrichtet und um weitere Nachforschungen gebeten.

5.3 Wahlen

5.3.1 Datenübermittlung an Parteien

Die Übermittlung von Namen, akademischen Graden und Anschriften der Wahlberechtigten nach § 35 Abs. 1 des Meldegesetzes NW (MG NW) an Parteien innerhalb der sechs einer Wahl vorangehenden Monate gab Anlaß zu vielen Bürgereingaben.

Bei den Auskünften nach § 35 Abs. 1 MG NW darf der Empfänger die Daten nur für den Zweck verwenden, zu dessen Erfüllung sie ihm übermittelt worden sind (§ 35 Abs. 1 Satz 3 i.V.m. § 34 Abs. 4 MG NW). Dies bedeutet, daß die Daten nur von der Partei selbst für Zwecke der Wahlwerbung verwendet werden dürfen. Eine Weitergabe an Parteimitglieder zum Zwecke der Wahlwerbung unter ihrem eigenen Namen ist nach meiner Auffassung nicht zu-

lässig. Der Datenempfänger ist bei der Übermittlung der Daten durch die Meldebehörde auf diese Zweckbindung hinzuweisen.

Grund zu einer Beanstandung gab die Übermittlung personenbezogener Daten aller Wahlberechtigten einer Stadt an eine Partei. Für die Zusammensetzung der nach § 35 Abs. 1 MG NW zu übermittelnden Daten ist das Lebensalter der Wahlberechtigten bestimmend.

Das Merkmal „Lebensalter der Betroffenen" ist in § 35 Abs. 1 MG NW eingefügt, um eine Beschränkung auf bestimmte Wählergruppen vorzugeben. § 35 Abs. 1 MG NW stellt eine Ausnahmevorschrift zu § 34 Abs. 3 MG NW dar. Eine Melderegisterauskunft nach § 34 Abs. 3 MG NW (Gruppenauskunft) über eine Vielzahl nicht namentlich bezeichneter Einwohner ist nur unter der einschränkenden Voraussetzung des Vorliegens eines öffentlichen Interesses an der Datenübermittlung zulässig. Die Zahl der nach dieser Vorschrift zugelassenen Datenübermittlungen an nicht-öffentliche Stellen insbesondere zur Verfolgung eigener Interessen ist deshalb äußerst gering. Grund dieser restriktiven Auslegung ist auch die Sorge, daß anderenfalls eine nicht mehr steuerbare Weiterverwendung von Adressen und anderen Angaben zu befürchten wäre.

Vor dem Hintergrund dieser Bestimmung ist auch § 35 Abs. 1 MG NW auszulegen. Die Vorschrift privilegiert die Träger von Wahlvorschlägen in einem bestimmten Zeitraum vor der Wahl, indem sie zu ihren Gunsten Datenübermittlungen ohne die Zustimmung der Betroffenen und ohne weitere Voraussetzungen zuläßt. Wenn der Gesetzgeber in § 35 Abs. 1 MG NW ausdrücklich ein Tatbestandsmerkmal aufgenommen hat, das eine Begrenzung der Datenweitergabe nach dem Lebensalter der Betroffenen vorsieht, so ist dieses Merkmal zwingend zu beachten.

Der Gesetzeswortlaut läßt allerdings nicht nur Auskünfte über alle am Wahltag z. B. 18- bis 22jährigen Wähler (Jung- oder Erstwähler) zu, sondern erlaubt auch die Übermittlung der Daten von Wahlberechtigten etwa im Rentenalter. Für beide Wählergruppen ist ein besonderes Interesse an einer intensiveren Information der Betroffenen erkennbar.

Die Übermittlung von Wählerdaten angefangen von den Jung- oder Erstwählern über alle übrigen Altersbereiche bis hin zu den Senioren, zwar noch aufgeteilt nach Altersgruppen, wäre bereits als Umgehung des restriktiven Tatbestandsmerkmals in § 35 Abs. 1 MG NW anzusehen.

Das Innenministerium hingegen hält die Übermittlung der Daten aller Wahlberechtigten für zulässig. Es stützt seine Auffassung insbesondere auf die Begründung zu § 35 Abs. 1 MG NW, worin es heißt „Die Auskünfte können auch auf Wahlberechtigte eines bestimmten Lebensalters beschränkt werden". Diese Aussage soll jedoch nur Zweifel ausräumen, ob es zulässig ist, die Gruppenauskunft auch auf nur einen Jahrgang zu beschränken. Dies wird aus dem daran anschließenden Satz der Begründung „Damit sind die bisher üblichen Auskünfte über sogenannte Jungwähler ... auch weiterhin möglich" besonders deutlich.

Die Konsequenz der vom Innenministerium vertretenen Auffassung wäre die Zulässigkeit der Schaffung landesweiter zentraler (Zweit-) Wählerregister in der Hand von politischen Parteien. Eine solche Folge kann der Bürger dem Wortlaut der Regelung des § 35 Abs. 1 MG NW nicht entnehmen. Auf die Diskussion im Zusammenhang mit einer derart umfassenden Datenanforderung einer Partei in der Vergangenheit und der Empörung der Bürger darüber, eine derartige Datensammlung in der Hand dieser Partei zuzulassen, habe ich ausdrücklich hingewiesen.

Auch die Datenübermittlung von Wahlberechtigten aufgeteilt nach Stimmbezirken ist nicht zulässig und war daher zu beanstanden. Nach den Vorschriften der Wahlordnungen legt der Gemeindedirektor vor jeder Wahl für jeden allgemeinen Stimmbezirk ein Verzeichnis der Wahlberechtigten nach Familiennamen, Vornamen, Geburtsdatum und Wohnung an. Das Wählerverzeichnis wird unter fortlaufender Nummer in der Buchstabenfolge der Familiennamen, bei gleichen Famliennamen der Vornamen, angelegt. Es kann auch nach Ortsteilen, Straßen und Hausnummern gegliedert werden. Innerhalb der Auslegungsfrist ist das Anfertigen von Auszügen aus dem Wählerverzeichnis durch Wahlberechtigte zulässig, soweit dies im Zusammenhang mit der Prüfung des Wahlrechts einzelner bestimmter Personen steht. Die Auszüge dürfen nur für diesen Zweck verwendet und unbeteiligten Dritten nicht zugänglich gemacht werden.

Aus diesen Regelungen wird deutlich, daß die Übermittlung der Daten von Wahlberechtigten aus dem Wählerverzeichnis, insbesondere auch gegliedert nach Stimmbezirken, bereichspezifisch abschließend geregelt ist. Dies wird besonders deutlich durch Vergleich mit alten Fassungen der Wahlordnungen, die ausdrücklich die Erteilung von Auszügen oder Abschriften des Wählerverzeichnisses zuließen, wobei die Kenntlichmachung bestimmter Altersgruppen möglich war. Der Wegfall dieser Regelungen läßt erkennen, daß der Verordnungsgeber derartige Auskünfte nicht mehr zulassen wollte.

Die in einem Fall als „Service-Leistung" seitens der Meldebehörde durchgeführte Datenübermittlung aufgeteilt nach Stimmbezirken war deshalb schon als Umgehung der normenklaren bereichspezifischen Regelung in der Kommunalwahlordnung unzulässig. Voraussetzung für diese „Service-Leistung" ist, daß die Meldebehörde die Daten der Wahlberechtigten nach Stimmbezirken aufgliedert. Damit erstellt die Meldebehörde ein (zweites) Wählerverzeichnis. Eine Rechtsgrundlage ist hierfür im Meldegesetz Nordrhein-Westfalen nicht vorhanden.

Zur Erfüllung ihrer Aufgaben speichern die Meldebehörden die in § 3 MG NW genannten Daten einschließlich der zum Nachweis ihrer Richtigkeit erforderlichen Hinweise im Melderegister. Die Angabe „Stimmbezirk" ist in § 3 MG NW nicht geregelt.

Die Daten, die an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen im Zusammenhang mit Parlaments- und Kommunalwahlen übermittelt werden dürfen, sind in § 35 Abs. 1 Satz 1 und 2 MG NW abschließend festgelegt. Die Angabe „gegliedert nach Stimmbezirken" fehlt.

Für diesen Teil meiner Beanstandung hat das Innenministerium meine rechtlichen Einwendungen akzeptiert. Nach seiner Auffassung muß es dann der jeweiligen Partei überlassen bleiben, falls sie es aus wahlwerbetaktischen Gründen für angezeigt hält, die ihr übermittelten Daten selbst nach den in den Stimmbezirken wohnhaften Einwohnern aufzugliedern.

5.3.2 Gewinnung von Wahlvorständen

In den Runderlassen des Innenministeriums zur Vorbereitung und Durchführung von Wahlen ist ausgeführt worden, daß die Gewinnung einer ausreichenden Zahl geeigneter Bürger für die Besetzung der **Wahlvorstände** vor allem in größeren Städten zunehmend auf Schwierigkeiten stoße. Die Gemeindebehörden seien deshalb vielfach dazu übergegangen, von anderen am Ort ansässigen Behörden Listen der Mitarbeiter anzufordern, um auch aus dem Kreis dieser Personen die erforderlichen Wahlvorstände zu bestimmen.

Diese Handhabung ist unter Gesichtspunkten des Datenschutzes problematisch. Das Innenministerium geht daher davon aus, daß auf diese Weise Mitglieder für Wahlvorstände nur gewonnen werden können, wenn die Mitarbeiter mit der Aufnahme in die Listen einverstanden sind.

Anläßlich des Kontrollbesuchs bei einer Stadt und auf Grund von Bürgereingaben ist mir aufgefallen, daß mehrere Gemeinden die Ausführungen in diesen Erlassen des Innenministeriums so auslegen, daß nur für die Gewinnung von Mitarbeitern anderer Behörden oder anderer sonstiger Stellen das Einverständnis dieser Personen zur Aufnahme in die Listen erforderlich ist, um sie als Wahlhelfer oder Wahlvorstandsmitglieder vorschlagen zu können. Die Mitarbeiter der eigenen Behörde könnten dagegen ohne deren Einverständnis benannt werden, weil es sich hier um einen Personaleinsatz im Sinne des § 29 Abs. 1 DSG NW handelt.

Ich habe gegenüber dem Innenministerium zu bedenken gegeben, daß die Berufung in einen Wahlvorstand, also zu einer ehrenamtlichen Tätigkeit, mit der Übertragung einer Tätigkeit im Dienstverhältnis nicht gleichsteht. Aus der Sicht des Datenschutzes erscheint daher die Einwilligung auch dieser Betroffenen zur Aufnahme in die Listen erforderlich, solange nicht eine bereichspezifische gesetzliche Regelung etwas anderes bestimmt.

Das Innenministerium teilt meine Bedenken. Angesichts der für die Gemeinden bestehenden Schwierigkeiten, Wahlhelfer in ausreichender Zahl zu gewinnen, habe es bislang jedoch davon abgesehen, in den Wahlerlassen auf die aufgezeigte Problematik zwischen Dienst- bzw. Vertragsverhältnis und Berufung als Wahlvorstandsmitglied einzugehen. Es habe aber in einem Einzelfall klargestellt, daß die Gemeindedirektoren bei der Gewinnung von Wahlhelfern nicht in ihrer Eigenschaft als Dienstherr, sondern als Wahlbehörde tätig werden und deshalb davon abgesehen werden soll, diese beiden Funktionen zu vermischen.

In den Wahlerlassen für die Landtags- und Bundestagswahl 1990 hat das Innenministerium herausgestellt, daß datenschutzrechtliche Bedenken bestehen, wenn ohne Einverständnis der Betroffenen die von der Personal-

stelle verwalteten Daten dem Wahlamt zur Verfügung gestellt werden. Eine Verpflichtung öffentlicher und auch privater Stellen, beispielsweise Personallisten den Wahlbehörden zwecks Gewinnung von Wahlvorstandsmitgliedern zur Verfügung zu stellen, könnte nur durch eine Gesetzesregelung erreicht werden, die derzeit nicht besteht.

Da nach Einschätzung des Innenministeriums auch künftig bei der Gewinnung von Wahlhelfern in erheblichem Umfang auf Angehörige des öffentlichen Dienstes zurückgegriffen werden muß, ist zu prüfen, welche Rechtsnormen geschaffen werden sollen, damit bei einer Nutzung von Personaldateien für diesen Zweck eine rechtlich einwandfreie Lösung gewährleistet ist.

5.4 Ausländerwesen

5.4.1 Erteilung eines Sichtvermerks

Bei der Erteilung von Aufenthaltserlaubnissen in Form von Sichtvermerken, sei es an ausländische Studenten aus sichtvermerkspflichtigen Staaten für Touristen- und Besuchsreisen während der Ferienmonate oder an Besucher und Touristen aus den osteuropäischen Staaten, ist in der Regel eine Verpflichtung des Einladenden erforderlich, daß er für alle durch den Besuch entstehenden Kosten aufkommt. Um zu prüfen, ob der Einladende zur Übernahme einer solchen Verpflichtung in der Lage ist, erhebt die bewilligende Behörde die Höhe seines Einkommens.

Soweit die Angabe der Höhe des Einkommens erforderlich ist, bedeutet dies nicht, daß grundsätzlich die Höhe des Einkommens in den Vordruck für die Verpflichtungserklärung aufzunehmen ist, der dem Eingeladenen ausgehändigt werden muß. Um den Datenschutzbelangen der Betroffenen besser Rechnung zu tragen, sollte in eine derartige Verpflichtungserklärung nur allgemein aufgenommen werden, daß sich der Einladende zur Übernahme aller durch den Besuch entstehenden Kosten verpflichtet, dazu finanziell in der Lage ist und der Behörde ein entsprechendes Einkommen nachgewiesen hat. Das Innenministerium, an das ich mich auf Grund einer Bürgereingabe gewandt habe, teilt meine Auffassung in diesem Fall.

Ist ein Einkommensnachweis zu erbringen und der Nachweis aktenkundig zu machen, bedeutet dies nach meiner Auffassung nicht, daß grundsätzlich der Beleg in Kopie oder die Höhe des Einkommens durch schriftlichen Vermerk in der Akte festgehalten werden muß. Um dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz Rechnung zu tragen, der bei jedem Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung und ihr Grundrecht auf Datenschutz zu beachten ist, genügt ein Vermerk, der Nachweis über ein ausreichendes Einkommen habe vorgelegen. Meinen entsprechenden Empfehlungen an zwei Gemeinden, in dieser Weise zu verfahren, wurde bisher nicht gefolgt.

5.4.2 Erkennungsdienstliche Maßnahmen bei Erfassung von Asylbewerbern

Zahlreichen Presseberichten war zu entnehmen, daß beabsichtigt sein sollte, bei allen Ausländern, die die Anerkennung als Asylberechtigte beantragen, zu Identifizierungszwecken erkennungsdienstliche Maßnahmen bestehend aus einem Zehnfingerabdruck durchzuführen, um u. a. mehrfache Asylanträge oder den Mehrfachbezug von Sozialhilfe zu unterbinden.

Als gesetzliche Grundlage kommt nur § 13 Asylverfahrensgesetz (Asyl VfG) in Betracht. Danach ist die erkennungsdienstliche Behandlung eines Asylbewerbers zulässig, wenn seine Identität nicht eindeutig bekannt ist. Daraus folgt, daß eine generelle erkennungsdienstliche Behandlung aller Asylbewerber allein auf Grund ihres Status nicht zulässig ist. Darüber hinaus wäre eine solche lückenlose Erfassung wegen einzelner Mißbräuche mit dem Gebot der Verhältnismäßigkeit nicht vereinbar.

Sinn und Zweck der erkennungsdienstlichen Behandlung ist die zweifelsfreie Feststellung der Identität des Betroffenen. Wenn diese Identität aus anderen Gründen feststeht, etwa durch Vorlage eines fälschungssicheren Personalausweises oder sonstiger die Identität beweisender Urkunden, ist die Aufnahme von Fingerabdrücken unzulässig. Dagegen mag es hinnehmbar sein, wenn Asylbewerber aus Gegenden, in denen auf Grund polizeilicher Erfahrung häufig gefälschte Identitätspapiere in Gebrauch sind oder auch legale Möglichkeiten eines vereinfachten Wechsels der Identität bestehen, im Rahmen einer generalisierten Prüfung einer erkennungsdienstlichen Behandlung unterzogen werden.

Das Innenministerium des Landes Nordrhein-Westfalen hat die von mir vorgetragenen Bedenken aufgegriffen und beabsichtigt, den Runderlaß vom 8. Mai 1984 in dem o. a. Sinne zu überarbeiten.

5.4.3 Zentrale Anlauf- und Beratungsstelle für ethnische Minderheiten

Durch Presseberichte bin ich auf mögliche Datenschutzverstöße im Zusammenhang mit der Datenverarbeitung der von einer Gemeinde eingerichteten „Zentralen Anlauf- und Beratungsstelle für ethnische Minderheiten“ (A+B-Stelle) aufmerksam gemacht worden. Dabei wurden teilweise im Wege der fotografischen Wiedergabe in den Presseartikeln Fälle von Datenspeicherung, -weitergabe und -übermittlung dargestellt, die eine Überprüfung notwendig machten.

In mehreren Auskunftsersuchen und erläuternden Besprechungen wurde die Gemeinde auf die besonderen Datenschutzprobleme aufmerksam gemacht, die bei einer Stelle mit einer alle Lebensbereiche der Betroffenen umfassenden Aufgabenstellung entstehen können. Gegenstand der Überprüfung ist insbesondere die in mehreren Aktenordnern über einen Zeitraum von mehreren Monaten dokumentierte Datenverarbeitungspraxis der A+B-Stelle.

In ihrer Stellungnahme geht die Gemeinde davon aus, daß die gesamte Datenverarbeitung der A+B-Stelle rechtmäßig war: Rechtsgrundlage hierfür sei die Einwilligung der Betroffenen gewesen. Gleichwohl seien die Daten bis zum Abschluß der Überprüfung durch den Landesbeauftragten für den Datenschutz gesperrt. Danach würden die Daten dem kommunalen Archiv zur Übernahme angeboten.

Demgegenüber habe ich darauf verwiesen, daß ich mich dem Vorschlag der Abgabe der Unterlagen an das Archiv nur anschließen könnte, wenn unzulässig gespeicherte Daten zuvor gelöscht würden (§ 19 Abs. 3 Buchstabe a i.V.m. Abs. 4 DSG NW). Insoweit bietet sich eine Prüfung an, ob die Vorgänge letztlich nicht insgesamt einer Löschung zugeführt werden können. Zu berücksichtigen blieben dabei mögliche Rechte Betroffener, etwa aus § 20 DSG NW oder § 839 BGB, sowie mögliche Verfahren, etwa nach § 34 DSG NW, die die Frage nach weiterer Sperrung der Daten bis zum Ablauf bestimmter Fristen aufwerfen (vgl. hierzu auch § 19 Abs. 2 Buchstabe c und d DSG NW).

Zweifelhaft dürfte vor allem sein, ob für die Datenerhebung und weitere Datenverarbeitung der A+B-Stelle in dem Zeitraum, über den die Akten Auskunft geben, eine wirksame Einwilligung der Betroffenen nach § 4 DSG NW jeweils vorliegt. Eine Globaleinwilligung, die alle nur denkbaren Datenverarbeitungsvorgänge bei der A+B-Stelle umfassen sollte, wäre unzulässig.

Zu begrüßen war allerdings, daß die Gemeinde im übrigen die Notwendigkeit einer äußeren und inneren Abschottung der A+B-Stelle anerkannte. Die von ihr vorgesehenen Maßnahmen zur inneren Abschottung sind allerdings nicht ausreichend geeignet, Verstöße gegen Vorschriften über den Datenschutz durch die Arbeitsweise der Mitarbeiter der A+B-Stelle auszuschließen.

Soweit die Gemeinde für ihr Organisationsmodell auf die Organisationshoheit der Gemeinden abstellt, bleibt darauf hinzuweisen, daß die Grenzen der Organisationshoheit bei der Einrichtung der A+B-Stelle in den bestehenden gesetzlichen Bestimmungen liegen dürften, denen auch die Fachämter unterworfen sind und die durch eine organisatorische Zusammenfassung zu einer neuen Verwaltungseinheit nicht umgangen werden dürfen. Dies dürfte insbesondere dann gelten, wenn die Zusammenführung von Aufgaben in einer Stelle die Notwendigkeit einer inneren Abschottung der Verwaltungsarbeit erst bedingt, die gleichzeitig vorgesehene Personalausstattung aber so gering ist, daß eine wirksame Abschottung nicht zu verwirklichen ist. Gerade bei der von der Gemeinde zutreffend herausgestellten Notwendigkeit, einen des Lesens und Schreibens weitgehend unkundigen Personenkreis umfassend betreuen zu müssen, sollte nach meiner Auffassung ein organisatorischer Weg gewählt werden, der insbesondere die Entstehung von Personenprofilen vermeidet.

Zur Vermeidung von Verstößen gegen Vorschriften über den Datenschutz und unter Berücksichtigung der von der Gemeinde herausgestellten Schwierigkeiten, eine innere Abschottung durch Personalvermehrung zu gewährleisten, habe ich neben anderen Verbesserungen des Datenschutzes empfohlen, in der noch zu erlassenden Dienstanweisung der A+B-Stelle u. a. fest-

zulegen, bei der A+B-Stelle personenbezogene Daten nur über die Identität der Betroffenen und über die erfolgte Belehrung im Sinne von § 4 Satz 1 Buchstabe b DSG NW zu speichern und Daten aus den Beratungsgesprächen, soweit sie zulässigerweise schriftlich festgehalten werden, urschriftlich an das jeweils betroffene Fachamt weiterzureichen, ohne daß bei der A+B-Stelle hierüber irgendwelche Unterlagen zurückbleiben. Auch im übrigen ist der Schriftverkehr mit den Fachämtern so abzuwickeln, daß bei der A+B-Stelle keine Unterlagen verbleiben.

Bei entsprechender Berücksichtigung meiner Empfehlungen habe ich eine innere Abschottung in der A+B-Stelle nicht mehr für erforderlich gehalten. Das Ergebnis meiner Bemühungen bleibt abzuwarten.

5.5 Bau- und Wohnungswesen

5.5.1 Wohnungsbauförderung

Aufgrund von Bürgereingaben bestand Anlaß, die Erhebung personenbezogener Daten durch Fragebögen der Wohnungsbauförderungsanstalt des Landes Nordrhein-Westfalen zu überprüfen. Anders als bei dem in meinem 9. Tätigkeitsbericht (Seite 48/49) dargestellten Problem einer wirksamen Einwilligung fehlte es bei dieser Datenerhebung jeweils bereits an einer normenklaren Aufgabenzuweisungsnorm.

Bei der Verwendung der Fragebögen war insbesondere zu bemängeln, daß die Datenerhebung wegen unklarer Fragestellungen zu weitgehend erfolgte und der Behörde eine Prüfkompetenz für die erhobenen Daten zum Teil nicht zustand. Da die Wohnungsbauförderungsanstalt nicht bereit war, nach meinen Empfehlungen die Datenerhebung einzuschränken und die Fragebögen entsprechend zu ändern, war eine förmliche Beanstandung geboten.

Zweifel an der datenschutzrechtlichen Zulässigkeit bestanden auch gegenüber Nr. 7.21 der Wohnungsbauförderungsbestimmungen 1984 – WFB 1984 –, die festlegt, daß **Anträge** auf Bewilligung **bei der Gemeindeverwaltung** des Bauortes einzureichen sind, und zwar auch dann, wenn die Antragsannahmestelle nicht Bewilligungsbehörde ist. Hierdurch werden einer solchen Gemeinde erheblich mehr Daten, vor allem aus dem Bereich der familiären und finanziellen Verhältnisse des Bürgers offenbart, als zur Aufgabenerfüllung erforderlich ist. Zu dem Vorhaben selbst hat eine solche Gemeinde nur eine Stellungnahme in landesplanerischer und städtebaulicher Hinsicht abzugeben.

Nach Auskunft des Ministeriums für Stadtentwicklung, Wohnen und Verkehr des Landes Nordrhein-Westfalen findet die Regelung der Nr. 7.21 WFB 1984 – Antragsannahme – ihre Grundlage in § 6 a Abs. 3 GO NW. Damit sollen den Einwohnern Wege zu den eigentlich zuständigen, aber ortsfernen Behörden erspart werden. Die Regelung dient der Bürgernähe und der Vereinfachung der Antragstellung im Interesse des Bürgers und darüber hinaus der Verfahrensbeschleunigung, da die Gemeindeverwaltung mit der Weiterleitung des Antrages an die Bewilligungsbehörde ihre Stellungnahme in lan-

desplanerischer und städtebaulicher Hinsicht abzugeben hat, die anderenfalls gesondert anzufordern wäre.

Soweit ein Antragsteller seinen Antrag auf Gewährung von Wohnungsbauförderungsmitteln unmittelbar bei der Bewilligungsbehörde stellen will, ist er hieran durch Nr. 7.21 WFB 1984 nicht gehindert. Der Antrag würde sodann der Gemeinde zugeleitet, um die Stellungnahme in landesplanerischer und städtebaulicher Hinsicht einzuholen. Bei der Weiterleitung des Antrags durch die Bewilligungsbehörde an die Gemeinde könnten Unterlagen über familiäre oder finanzielle Verhältnisse des Antragstellers zurückbehalten werden, die für die Beurteilung des Bauwerks nicht benötigt werden. Das zuständige Ministerium hat eine entsprechende Präzisierung der Bestimmung in Aussicht gestellt.

Im Rahmen eines Kontrollbesuchs habe ich bei einer Gemeinde, die nicht Bewilligungsbehörde ist, die Praxis festgestellt, eine vollständige **Kopie des Antrags** zu behalten und für eine unbestimmte Zeit **aufzubewahren**. Nach meiner Auffassung ist eine derartige Datenspeicherung ohne Rechtsgrundlage. Unter Beachtung von § 6 a GO NW ist die Datenverarbeitung bei einer solchen Gemeinde auf den Vermerk zu beschränken „Gesehen und weitergereicht".

Ich habe deshalb empfohlen, die gespeicherten Unterlagen zu vernichten und für die Zukunft derartige Anträge nur entgegenzunehmen und an die zuständige Behörde weiterzureichen. Diese Empfehlung dürfte auch im Einklang mit der Auslegung von Nr. 7.21 WFB 1984 durch das Ministerium für Stadtentwicklung, Wohnen und Verkehr des Landes Nordrhein-Westfalen stehen. Die Gemeinde hat bereits erklärt, daß sie meiner Empfehlung folgen wird.

5.5.2 Vorkaufsrecht der Gemeinden

Bei mehreren Kontrollbesuchen von Gemeinden bin ich auf umfangreiche **Sammlungen von notariellen Kaufverträgen** gestoßen. Zum Zwecke der Entscheidung über die Ausübung des gemeindlichen Vorkaufsrechts übersenden die Notare nach § 28 Abs. 1 Satz 1 des Baugesetzbuchs (BauGB) eine vollständige Ausfertigung des Kaufvertrages an die jeweilige Gemeinde.

Nach einer Umfrage der Bundesnotarkammer ist etwa in den Jahren 1980 bis 1984 bundesweit bei nur 0,07 Prozent aller angezeigten Kaufverträge das Vorkaufsrecht ausgeübt worden. Diese Zahlen entsprechen auch den Angaben, die mir bei meinen Kontrollbesuchen gemacht wurden. Bei dieser Sachlage begegnet die Übermittlung der in den Kaufverträgen enthaltenen personenbezogenen Daten und die Speicherung dieser Daten bei den Gemeinden in der Form einer Sammlung von Kaufverträgen erheblichen datenschutzrechtlichen Bedenken, da fast immer (99,03 Prozent bei der Umfrage) der vollständige Kaufvertrag zur Aufgabenerfüllung der jeweiligen Gemeinde nicht erforderlich ist.

Nach Auffassung des Bundesministeriums für Raumordnung, Bauwesen und Städtebau könnte die Mitteilungspflicht des Verkäufers nach § 28 Abs. 1 Satz 1 BauGB in zwei Teilschritten erfolgen. In einem ersten Schritt sollte der Verkäufer die Gemeinde über die Tatsache der Veräußerung und den

vereinbarten Preis in Kenntnis setzen; der übrige Inhalt des Kaufvertrages sollte erst auf Verlangen der Gemeinde mitgeteilt werden. Das Ministerium für Stadtentwicklung, Wohnen und Verkehr hat mir auf meine Bitte um Stellungnahme mitgeteilt, daß es diese Auffassung teile. Es hat weiter darauf verwiesen, daß eine solche Verfahrensweise weitgehend der kommunalen Praxis, z. B. in Bayern und Berlin, entspreche.

Da ich eine derartige Praxis in Nordrhein-Westfalen nicht feststellen konnte, habe ich das Innenministerium und das Justizministerium gebeten, sich entsprechend der Auffassung des Ministeriums für Stadtentwicklung, Wohnen und Verkehr im Rahmen ihrer Zuständigkeit für die Einführung einer solchen Praxis bei den Notaren und den Kommunalverwaltungen einzusetzen. Hierzu dürfte auch gehören, die Gemeinden zu veranlassen, die dort im Laufe von Jahren aufgebauten umfangreichen Sammlungen von Kaufverträgen unverzüglich auszusondern und zu vernichten.

5.5.3 Planung

Ein Bürger wandte sich dagegen, daß in einer öffentlichen Bekanntmachung im Rahmen eines Planfeststellungsverfahrens für den Bau einer Straße bei Anträgen und Eingaben, die von mehr als 50 Personen auf **Unterschriftslisten** unterzeichnet werden, von dem nach § 17 Abs. 1 des Verwaltungsverfahrensgesetzes des Landes Nordrhein-Westfalen (VwVerfG) als Vertreter geltenden Person die Angabe auch des Berufs verlangt wird.

Gegen die Erhebung von Angaben über den Beruf eines Betroffenen bestehen Bedenken, da diese Angabe in der Regel, wenn die Identität des Vertreters feststeht, zur Aufgabenerfüllung nicht erforderlich ist. Darüber hinaus bestehen Zweifel, ob die Angabe des Berufs überhaupt zur Identifizierung eines Betroffenen geeignet ist.

Der von mir zur Stellungnahme aufgeforderte Regierungspräsident hat mein Schreiben zum Anlaß genommen, dem Ministerium für Stadtentwicklung, Wohnen und Verkehr vorzuschlagen, die Bekanntmachung dahingehend zu ergänzen, daß hinter dem Wort Beruf der Text eingeführt wird: „– Soweit dies zur Vermeidung von Verwechslungen erforderlich ist –". Das Innenministerium ist von mir auf die Notwendigkeit einer Änderung von § 17 VwVerfG hingewiesen worden. Ein Ergebnis liegt noch nicht vor.

Zur Durchführung der frühzeitigen Bürgerbeteiligung im Bauleitplanverfahren nach § 3 Abs. 1 des Baugesetzbuches veranstaltete eine Gemeinde eine öffentliche Bürgerversammlung, in der sie eine **Anwesenheitsliste** herumgehen ließ und den anwesenden Bürgern empfohlen wurde, Wortmeldungen mittels bereitliegender Handzettel dem Verhandlungsleiter anzuzeigen. Bürger befürchteten einen Mißbrauch dieser Daten durch die Gemeinde und haben mich um Überprüfung gebeten.

Dabei stellte sich heraus, daß auch nach Auffassung der Gemeinde ein Zwang zur Eintragung in die Anwesenheitsliste nicht besteht. Auch die Benutzung der Handzettel ist freiwillig. Sie werden nach Abschluß des Diktates zum Protokoll vernichtet.

Um Unklarheiten und Mißverständnissen vorzubeugen, habe ich der Gemeinde empfohlen, durch einen entsprechenden Aufdruck im Kopf der Anwesenheitsliste und im Kopf der Handzettel auf die Freiwilligkeit der Eintragung bzw. der Benutzung hinzuweisen. Die Gemeinde hat mitgeteilt, daß sie meiner Empfehlung folgt.

5.6 Kommunalwesen

5.6.1 Datenweitergabe an Rat und Ausschüsse

Nach wie vor entstehen in vielen Gemeinden bei der Bekanntgabe personenbezogener Daten an Rats- und Ausschußmitglieder datenschutzrechtlich Probleme. Gleiches gilt für die Bekanntgabe von personenbezogenen Daten an Zuhörer und Presse während einer öffentlichen Sitzung. Als Rechtsgrundlage für eine Datenweitergabe kommen je nach Beratungsgegenstand verschiedene gesetzliche Grundlagen in Betracht.

Selbst bei Vorliegen einer gesetzlichen Grundlage ist der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz zu beachten. Unter mehreren für die Erreichung des Zwecks geeigneten Mitteln ist dasjenige zu wählen, das den Betroffenen am wenigsten belastet. Besteht der zu erreichende Zweck darin, die Öffentlichkeit über die Tagesordnungspunkte einer Ratssitzung zu informieren, ist eine allgemeine Bezeichnung ohne personenbezogene Daten als das Mittel geeignet, das die Betroffenen am wenigsten belastet.

Bei der Beratung über Einwendungen und Beschwerden von Bürgern ist nicht grundsätzlich die Angabe des Namens des Beschwerdeführers erforderlich. In der Regel reichen sachbezogene Daten aus. Auch bei der Beratung im Zusammenhang mit Bebauungsplänen ist die Bekanntgabe personenbezogener Daten nicht grundsätzlich erforderlich.

Das Innenministerium hat mir zu einem Fall der Behandlung von Einwendungen im Rahmen eines Bebauungsplanverfahrens mitgeteilt, daß, sofern in Unterlagen, die in Ratssitzungen vorgelegt werden sollen, persönliche Daten von Verfahrensbeteiligten enthalten sind, seitens der Verwaltung im Wege einer konkreten Erforderlichkeitsprüfung festzustellen ist, ob auch ohne diese Daten die Ratsmitglieder eine ausreichende Grundlage für sachgerechte Entscheidungen zur Verfügung haben. Es wird für eine pragmatische und den Forderungen des Datenschutzes genügende Lösung gehalten, wenn in derartigen Fällen die Verwaltung aus den Sitzungsunterlagen die persönlichen Daten von Verfahrensbeteiligten herausfiltert (z. B. durch Abdecken bei Fotokopien). Nur dann, wenn seitens der Mandatsträger aus plausiblen Gründen eine Bekanntgabe für erforderlich gehalten wird, sind diese nachzuliefern. In derartigen Fällen kann es dann geboten sein, gemäß § 33 Abs. 2 der Gemeindeordnung für das Land Nordrhein-Westfalen in nicht-öffentlicher Sitzung zu beraten.

An die Erforderlichkeit der Bekanntgabe personenbezogener Daten ist ein strenger Maßstab anzulegen. Es genügt nicht, wenn die Bekanntgabe der Daten zur Aufgabenerfüllung nur dienlich ist; sie muß vielmehr hierfür unbe-

dingt notwendig sein. Dies macht eine Entscheidung in jedem einzelnen Fall erforderlich. Es ist nicht zu verkennen, daß die Angabe personenbezogener Daten in manchen Fällen zwar nicht erforderlich, aber dienlich oder nützlich sein kann. Um solche dienlichen oder nützlichen Daten an Rats- oder Ausschußmitglieder weitergeben zu können, kann die Einwilligung der Betroffenen nach § 4 Satz 1 Buchstabe b DSG NW eingeholt werden. Bei der Einholung der Einwilligung sind die Voraussetzungen des § 4 Satz 2 bis 4 DSG NW zu beachten. In diesen Fällen ist auch ausdrücklich auf die Öffentlichkeit der Sitzungen hinzuweisen.

Die Weitergabe der Daten mit Einwilligung der Betroffenen gilt jedoch nicht ohne weiteres auch für die Weitergabe an die Presse und die Zuhörer bei öffentlichen Sitzungen. Die Öffentlichkeit von Rats- und Ausschußsitzungen begründet auch keinen Anspruch der Presse auf vollständige Vorlage der in der Sitzung behandelten Unterlagen. Die Behörden sind nur verpflichtet, den Vertretern der Presse unter den Voraussetzungen des § 4 des Landespressegesetzes (LPG) die zur Erfüllung ihrer öffentlichen Aufgabe dienenden Auskünfte zu erteilen. § 4 LPG trifft insoweit eine abschließende bereichspezifische Regelung. Der Grundsatz der Öffentlichkeit erfordert nicht die Überlassung vollständiger Unterlagen an die Presse oder die Zuhörer.

5.6.2 Meinungsumfragen

Aufgrund von Beratungsersuchen und Bürgereingaben bestand verschiedene Male die Notwendigkeit, zu Meinungsumfragen von Städten in Nordrhein-Westfalen Stellung zu nehmen. So ließ etwa eine Stadt ihr Fremd-Image bei den Bürgern der Umlandgemeinden durch eine Universität untersuchen, eine andere eine Untersuchung zur Struktur und zu den anzustrebenden Entwicklungsmöglichkeiten des Einzelhandels durch Befragung der Bürger aus den Umlandgemeinden von einer privaten Firma durchführen, oder es erfolgte eine Meinungsumfrage unter den eigenen Bürgern zur Lebensqualität in der Stadt, sowie in einem anderen Fall zur Situation älterer Mitbürger.

Ein Datenschutzproblem bei derartigen Meinungsumfragen ist die Rechtsgrundlage für die Ermittlung der Anschriften der zu befragenden Bürger. So ist zweifelhaft, ob die Übermittlung der Meldedaten von Bürgern aus Umlandgemeinden an die jeweilige Stadt auf § 31 Abs. 1 des Meldegesetzes NW (MG NW) gestützt werden kann. Nach § 31 Abs. 1 MG NW darf die Meldebehörde personenbezogene Daten an Behörden übermitteln, wenn dies zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit oder der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist. An die Erforderlichkeit ist ein strenger Maßstab anzulegen. Es genügt nicht, wenn die Kenntnis der Daten nur dienlich ist. Sie muß vielmehr zur Aufgabenerfüllung unbedingt notwendig sein. Im Hinblick darauf, daß es eine Reihe anderer Möglichkeiten gibt, etwa das Fremd-Image einer Stadt festzustellen, ohne daß es hierzu der Übermittlung von Daten der Bürger anderer Gemeinden bedarf, bestehen an der Erforderlichkeit der Datenübermittlung Zweifel.

Gleiches gilt, wenn die Anschriften der Bürger an das die Untersuchung durchführende private Unternehmen übermittelt werden sollen. Die Über-

mittlung personenbezogener Daten über eine Vielzahl nicht namentlich bezeichneter Einwohner (Gruppenauskunft) an eine nicht-öffentliche Stelle ist nach § 34 Abs. 3 MG NW zu beurteilen. Nach dieser Vorschrift darf die Meldebehörde nicht-öffentlichen Stellen eine Melderegisterauskunft nur dann erteilen, wenn sie im öffentlichen Interesse liegt. Durch die Übermittlung der personenbezogenen Daten dürfen schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Das Vorliegen eines öffentlichen Interesses muß zumindest von einer obersten Bundes- oder Landesbehörde bestätigt werden.

Nicht zu verkennen ist allerdings, daß derartige Befragungen von Bürgern für die Aufgabenerfüllung der jeweiligen Stadt dienlich oder nützlich sein können. Insoweit kann die Datenübermittlung an die jeweilige Stadt auf § 4 Satz 1 Buchstabe b DSG NW gestützt werden. Danach ist die Verarbeitung personenbezogener Daten zulässig, wenn der Betroffene eingewilligt hat. Das setzt voraus, daß vor einer Datenübermittlung die schriftliche Einwilligung der Betroffenen von der jeweiligen Gemeinde einzuholen ist. Dabei sind auch § 4 Satz 3 und 4 DSG NW zu beachten. Der Betroffene ist entsprechend eingehend über die Verarbeitung seiner Daten zu informieren.

Datenschutzrechtlich bedenklich ist auch, daß entgegen den von den untersuchenden Stellen abgegebenen Erklärungen die Anonymität der Befragten in der Regel nicht gewährleistet ist. Durch eine Kombination verschiedener Angaben aus den Erhebungsbögen sind etwa Betroffene möglicherweise zu identifizieren. Zudem wird auch, wenn die Fragebögen vor Ort durch Beschäftigte der untersuchenden Stelle abgeholt oder gar eine mündliche Befragung vor Ort vorgesehen ist, die Anonymität wesentlich in Frage gestellt. Ein Hinweis, wie etwa daß Anonymität garantiert sei, ist deshalb irreführend. Auf das Risiko, daß der Bürger als Person bei der Befragung bestimmbar bleibt, sollte der Betroffene bei der Einholung seiner Einwilligung deshalb ausdrücklich hingewiesen werden.

Deshalb hat nach meiner Auffassung die jeweilige Stadt, um bei der Durchführung der Untersuchung einen ausreichenden Datenschutz zu gewährleisten, der untersuchenden Stelle verschiedene Auflagen zu machen:

- Der Betroffene ist über den Zweck der Meinungsumfrage und über die vorgesehene Datenverarbeitung aufzuklären.
- Der Betroffene ist ausdrücklich auf die Freiwilligkeit der Teilnahme an der Befragung hinzuweisen und darauf aufmerksam zu machen, daß ihm aus der Verweigerung der Teilnahme keine Nachteile entstehen. Entsprechend ist ihm auch die Beantwortung jeder einzelnen Frage freizustellen.
- Die von der untersuchenden Stelle erhobenen Daten dürfen nur für die bestimmungsgemäßen Zwecke verwandt werden.
- Name und Anschrift der Befragten dürfen nicht gespeichert werden.
- Soweit an Hand der Interviewunterlagen eine Reidentifizierung der Betroffenen möglich ist, sind die Bürger auf dieses Risiko hinzuweisen.

- Die Erhebungsbögen sind unmittelbar nach Ermittlung der Befragungsergebnisse bei der untersuchenden Stelle ersatzlos zu vernichten. Über die Vernichtung ist ein Protokoll anzufertigen.

- Die Erhebungsbögen dürfen zu keiner Zeit der jeweiligen Stadt und/oder den Umlandgemeinden zugänglich gemacht werden.

- Bei der Befragung dürfen keine Mitarbeiter der untersuchenden Stelle aus den Gemeinden der befragten Bürger eingesetzt werden.

Im Interesse der betroffenen Bürger wäre es wünschenswert, wenn auf bevorstehende Meinungsumfragen durch öffentliche Bekanntmachung und Information im redaktionellen Teil der örtlichen Presse hingewiesen würde. Dabei sollte auch auf die Datenschutzrechte der Betroffenen aufmerksam gemacht werden.

5.7 Rechtswesen

5.7.1 Strafverfahren

Bedauerlich ist nach wie vor, daß von Amtsgerichten des Landes Nordrhein-Westfalen immer noch im Rahmen von Ermittlungsverfahren Beschlüsse mit sog. **Sammelrubren** erlassen werden. In einem solchen Beschluß sind mehrere Personen mit Namen, Anschrift, Geburtsdatum und Geburtsort aufgeführt, die in einem Ermittlungsverfahren etwa von einer Durchsuchungsanordnung betroffen sind. Jeder der Betroffenen bekommt durch die gesetzlich vorgesehene Aushändigung des Beschlusses Kenntnis von den personenbezogenen Daten der anderen Betroffenen. Besonders bedenklich war in einem von mir konkret überprüften Fall, daß die Staatsanwaltschaft in Kenntnis der Datenschutzprobleme beim Ermittlungsrichter sogar beantragt hatte, mehrere Durchsuchungsbeschlüsse zu erlassen und gleichwohl der Ermittlungsrichter nur einen gemeinsamen Durchsuchungsbeschluß erlassen hat.

Als erfreulich ist in diesem Zusammenhang allerdings festzuhalten, daß es der Landesregierung, wie in der Stellungnahme zu meinem 8. Tätigkeitsbericht (S. 38) angekündigt, offenbar in der Zwischenzeit gelungen ist, die Staatsanwaltschaft anzuhalten, in Ermittlungsverfahren gegen mehrere Beschuldigte bei Gericht darauf hinzuwirken, daß bei der Fassung von Entscheidungen nach Möglichkeit von „Sammelrubren" abgesehen wird.

Der geringe bürotechnische Aufwand für mehrere Beschlüsse mit der Folge, daß der Richter statt eines Beschlusses mehrere gleichartige unterzeichnen muß, bedeutet für den Bürger einen deutlich besseren Schutz seiner Privatsphäre. Demgegenüber kann ein gemeinsamer Beschluß für ihn schwerwiegende Auswirkungen haben. So auch in dem von mir überprüften Fall, bei dem nach Aktenlage klar war, daß von mehreren Betroffenen möglicherweise nur einer Täter sein konnte und es sich deshalb bei den anderen um völlig unbescholtene Bürger handeln mußte.

Eine Änderung dürfte auch nach Einschätzung des Justizministeriums erst nach einer entsprechenden Novellierung der Strafprozeßordnung möglich sein.

Offenbar bedarf es auch erst der Klarstellung durch die Novellierung der Strafprozeßordnung, um den **Datenschutz von Zeugen** zu verbessern. So haben Betroffene, die an ihrem Arbeitsplatz mehrfach Opfer eines Raubüberfalls geworden waren, mir gegenüber ihre Bestürzung geäußert, daß dem Täter über die Anklageschrift ihre Privatanschrift mitgeteilt wurde und dieser dies zur Kontaktaufnahme genutzt hatte.

Nach meiner Auffassung ist eine Rechtsgrundlage für die Aufnahme der Anschrift von Zeugen in die Anklageschrift oder auch im Strafbefehlsverfahren nicht vorhanden. Anzugeben ist lediglich der Wohn**ort**. Unter Beachtung des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes sollte in derartigen Fällen als ladungsfähige Anschrift in die Akten nur die Anschrift des Arbeitgebers aufgenommen werden. Üblich ist dies nach meiner Kenntnis bereits jetzt schon für Zeugen aus dem Polizeibereich. Die schutzwürdigen Belange von Zeugen, die an ihrem Arbeitsplatz als Opfer die Gewalttätigkeit des Täters hautnah erleben durften, dürften gleichwertig sein.

Auszugehen ist dabei davon, daß die Bekanntgabe der Privatanschriften von Zeugen durch die Übersendung der **Anklageschrift** an den Angeklagten einen Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung sowie in ihr Grundrecht auf Datenschutz darstellt, der einer gesetzlichen Grundlage bedarf. Dabei ist auch der Verhältnismäßigkeitsgrundsatz zu beachten.

Nach § 200 Abs. 1 StPO hat die Anklageschrift den Angeschuldigten, die Tat, die ihm zur Last gelegt wird, Zeit und Ort ihrer Begehung, die gesetzlichen Merkmale der Straftat und die anzuwendenden Strafvorschriften zu bezeichnen. In ihr sind u. a. die Beweismittel anzugeben. Nach § 222 Abs. 1 StPO hat das Gericht die geladenen Zeugen und Sachverständigen der Staatsanwaltschaft und dem Angeklagten rechtzeitig namhaft zu machen und ihren Wohn- oder Aufenthaltsort anzugeben. Die Angabe der genauen Anschrift der Zeugen ist nicht vorgesehen. Auch aus Nr. 110 Abs. 1 Buchstabe d und Nr. 118 der Richtlinien für das Strafverfahren und das Bußgeldverfahren kann die Aufnahme der genauen Anschrift von Zeugen in die Anklageschrift nicht hergeleitet werden.

Selbst bei Vorliegen einer gesetzlichen Grundlage für derartige Angaben wäre der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz zu beachten. Das bedeutet, bei mehreren für die Erreichung des Zwecks geeigneten Mitteln ist dasjenige zu wählen, das den Betroffenen am wenigsten belastet. Für die Erreichung des Zwecks – Information des Angeklagten über vorhandene Beweismittel – reicht die Angabe des Wohnortes der Zeugen aus und belastet die Zeugen am wenigsten.

Auf jeden Fall wäre die Angabe von Zeugen mit vollständiger Anschrift im **Strafbefehlsverfahren** unverhältnismäßig. Dem berechtigten Interesse des Angeschuldigten auf Information dahingehend, ob ihm die zur Last gelegte

Tat nachzuweisen sein wird, kann dadurch genügt werden, daß ihm die Namen der Zeugen – mithin das Vorhandensein und die Anzahl der Zeugen – mitgeteilt werden, ohne daß die Anschrift der Zeugen in diesem Stadium des Verfahrens von Bedeutung sein müßte. Falls der Angeschuldigte der Auffassung ist, daß ihm die Straftat nicht nachzuweisen sein wird oder er mit der Rechtsfolge nicht einverstanden ist, wird er Einspruch einlegen.

Sofern er hingegen durch den Hinweis auf vorhandene Zeugen keine Erfolgsaussichten für einen Freispruch in der Hauptverhandlung sieht, wird er von der Einlegung eines Einspruchs Abstand nehmen. Wenn somit ein begründetes Interesse des Angeschuldigten an der Mitteilung der Anschrift der Zeugen im Strafbefehlsverfahren nicht ersichtlich ist, so sollte andererseits bei der Prüfung der berechtigten Belange der Zeugen an der zurückhaltenden Mitteilung ihrer Anschriften an andere Personen, insbesondere die Möglichkeit einer Gefährdung des Zeugen in Betracht gezogen werden.

Gerade bei der Verfolgung von Delikten wie Körperverletzung, Sachbeschädigung, Bedrohung oder Beleidigung im Strafbefehlsverfahren ist es durchaus möglich, daß einerseits der Strafbefehl zwar angenommen wird, sich andererseits jedoch aggressive Rachegedanken gegen den Belastungszeugen richten können. Die Angabe der vollständigen Anschrift des Zeugen im Strafbefehl erleichtert in solchen Fällen unnötig Reaktionen gegen den Zeugen.

Wegen der grundsätzlichen Bedeutung habe ich das Justizministerium um Stellungnahme gebeten.

Ähnliche datenschutzrechtliche Bedenken bestehen, wenn eine Ordnungsbehörde im **Bußgeldbescheid** wegen einer Verkehrsordnungswidrigkeit in Fällen von sog. Drittanzeigen den Namen und die Wohnanschrift des Anzeigenerstatters angibt. Die Behörde stützt sich hierbei insbesondere auf die Vorschrift des § 222 StPO. Danach dürfte die Ordnungsbehörde allerdings nur den Wohn**ort** des Anzeigenerstatters angeben.

Bei Angabe des Namens und der Wohnanschrift des Anzeigenerstatters im Bußgeldbescheid wird dem Betroffenen die Möglichkeit eröffnet, ggf. gegen den Anzeigenerstatter Repressalien auszuüben. Aus Gründen des Persönlichkeitsschutzes bestehen erhebliche Bedenken gegen diese Praxis, auch unter dem Gesichtspunkt, daß in Anzeigefällen von Polizeibeamten und Mitarbeitern der Ordnungsbehörden grundsätzlich nur deren Namen mitgeteilt werden. Zu verweisen ist in diesem Zusammenhang auf das Urteil des Bundesgerichtshofs vom 5. April 1990 (NJW 1990, 1860). Darin wird ausgeführt, daß die Bekanntgabe des Wohnortes oder gar der Wohnanschrift von Zeugen einen Eingriff in ihren durch Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 des Grundgesetzes geschützten Persönlichkeitsbereich darstelle, der nur im überwiegenden Allgemeininteresse im Rahmen der Verhältnismäßigkeit hinzunehmen sei.

Das Innenministerium ist der Auffassung der Ordnungsbehörde, generell die Wohnanschrift des Anzeigeerstatters im Bußgeldbescheid anzugeben, beigetreten. Diesen Ansichten vermag ich nicht zu folgen, weil sie den Grundsatz der Verhältnismäßigkeit, insbesondere im Hinblick auf die Bedeutung des Vorwurfs bei Verkehrsordnungswidrigkeiten, die überwiegend geringfü-

gige Verfehlungen im Straßenverkehr betreffen, nicht ausreichend berücksichtigen. Darüber hinaus gehe ich davon aus, daß die Mehrzahl der Betroffenen von einer Rechtsverteidigung absieht, so daß in diesen Fällen die Angabe der Wohnanschrift eine unverhältnismäßige Belastung des Anzeigenerstatters darstellt. Damit werden in einer Vielzahl von Fällen Angaben über Wohnort, Straße und Hausnummer des Anzeigenerstatters gemacht, ohne daß dies erforderlich ist.

Nach alledem bin ich der Auffassung, daß für Bußgeldverfahren wegen Verkehrsordnungswidrigkeiten das Gebot der Verhältnismäßigkeit eine Abstufung der im Strafverfahren gebotenen Mittel (§ 222 StPO) verlangt, so daß grundsätzlich bei Verkehrsordnungswidrigkeiten auf Grund einer „Drittanzeige" die Bekanntgabe lediglich des Namens des Anzeigenerstatters und des Wohnortes in dem Bußgeldbescheid als erforderlich aber auch ausreichend anzusehen ist.

Auf Verlangen eines Bürgers hatte ich den **Umfang eines Beweisantrages** der Staatsanwaltschaft im Rahmen eines Strafprozesses zu überprüfen. Der Beweisantrag enthielt mehrere umfangreiche Zitate aus anderen Verfahren, die beigezogen und durch Verlesen zum Gegenstand der Verhandlung gemacht werden sollten.

Die Rechtsgrundlage für die Weitergabe personenbezogener Daten im Rahmen eines Beweisantrages dürfte sich aus §§ 244, 245 StPO ergeben. Insoweit bestehen gegen die Stellung des Beweisantrages, auch wenn das Gericht den Antrag in seinem Beschluß als für die Entscheidung ohne Bedeutung abgelehnt hat, grundsätzlich im Ergebnis keine durchgreifenden datenschutzrechtlichen Bedenken.

Hinsichtlich des Umfangs der bekanntzugebenden Daten ist allerdings auch bei Vorliegen einer gesetzlichen Grundlage der Erforderlichkeitsgrundsatz zu beachten. An die Erforderlichkeit ist ein strenger Maßstab anzulegen. Es genügt nicht, wenn die Kenntnis der Daten zur Aufgabenerfüllung nur dienlich ist, sie muß vielmehr hierfür unbedingt notwendig sein.

Die Abfassung des schriftlichen Beweisantrages, wie er zu Protokoll genommen wurde, entsprach diesen Anforderungen nicht. Die Verlesung des schriftlich formulierten Beweisantrages in der öffentlichen Sitzung der Strafkammer mit der Möglichkeit der Kenntnisnahme des Inhalts durch beliebige Zuhörer war deshalb ebenfalls nicht zulässig. Wie der Verteidiger und das Gericht ausgeführt haben, hat der Beweisantrag sich durch seine Verlesung weitgehend erledigt. Daraus ergibt sich, daß der Antrag bereits weitgehend den Beweis selbst enthielt. Damit wurden mit dem Antrag deutlich mehr personenbezogene Daten weitergegeben, als zur Antragstellung und zur Entscheidung des Gerichts über den Antrag erforderlich waren. Insbesondere die Darstellung der Zitate war danach nicht notwendig.

Zur Vermeidung von Verstößen gegen Vorschriften über den Datenschutz habe ich empfohlen, in derartigen Fällen die Datenweitergabe im Rahmen der Stellung von Beweisanträgen auf die hierfür unbedingt notwendigen An-

gaben zu beschränken. Der Leitende Oberstaatsanwalt teilt meine Auffassung. Er wird darauf hinwirken, daß nach diesem Grundsatz verfahren wird.

In mehreren Fällen hatte ich die Gewährung von **Akteneinsicht an Dritte** nach § 406 e StPO in datenschutzrechtlicher Hinsicht zu überprüfen. Die Betroffenen wandten sich vor allem dagegen, daß auf diesem Wege von der Staatsanwaltschaft beschlagnahmte Unterlagen zur Kenntnisnahme Dritter gelangten und von diesen zu privaten Zwecken genutzt wurden.

Gesetzliche Grundlage für die Gewährung von Akteneinsicht durch den Rechtsanwalt ist die genannte Vorschrift. Nach Absatz 1 kann ein Rechtsanwalt für den Verletzten Akteneinsicht nehmen, soweit er hierfür ein berechtigtes Interesse darlegt. Eine darüber hinausgehende Einsichtnahme ist nur mit dem Einverständnis des Betroffenen zulässig.

Der Begriff des berechtigten Interesses ist weit gefaßt. Berechtigt ist jedes Interesse, das im Einklang mit der Rechtsordnung steht. Dabei kann es sich um ein ideelles oder ein wirtschaftliches Interesse handeln. Nicht erforderlich ist, daß die Daten zur Rechtsverfolgung oder Rechtsverteidigung benötigt werden oder im Zusammenhang mit einem Rechtsverhältnis des Auskunftsuchenden stehen.

Allerdings bestimmt § 406 e Abs. 2 StPO, daß die Einsichtnahme in die Akten zu versagen ist, soweit überwiegende schutzwürdige Interessen des Beschuldigten oder anderer Personen entgegenstehen. Daraus folgt, daß in jedem Einzelfall eine entsprechende Interessenabwägung vorzunehmen ist.

Aus den mir vorgelegten Unterlagen, einschließlich der staatsanwaltschaftlichen Ermittlungsakten, vermochte ich nicht zu ersehen, ob eine solche Interessenabwägung auch stattgefunden hat. Sie ist jedenfalls nicht nachvollziehbar aktenkundig gemacht worden.

Darüber hinaus ist nicht ersichtlich, weshalb dem Rechtsanwalt und über diesen auch einer dritten Person der gesamte Akteninhalt zugänglich gemacht wurde. Im Rahmen der Interessenabwägung wäre zu prüfen gewesen, ob es ausgereicht hätte, dem Rechtsanwalt nur die Teile aus den Ermittlungsakten zur Einsichtnahme auszuhändigen, die für das Verfahren unmittelbar von Bedeutung sind. Auch für eine derartige Prüfung durch die Staatsanwaltschaft ergaben sich nach Aktenlage keine Anhaltspunkte.

Zur Vermeidung von Verstößen gegen Vorschriften über den Datenschutz habe ich daher der Staatsanwaltschaft empfohlen, künftig in derartigen Verfahren einem Rechtsanwalt Einsicht nur nach erfolgter und aktenkundig gemachter Interessenabwägung zu gewähren und dies auch nur für diejenigen Teile der Akten, die für das Verfahren erforderlich sind. Eine Stellungnahme der Staatsanwaltschaft liegt hierzu bisher nicht vor.

5.7.2 Zwangsvollstreckung

Bei der Durchführung eines Konkursverfahrens warf ein Konkursverwalter Geschäftsakten, Kassenbücher, Kundenquittungen und Bankauszüge des Gemeinschuldners in einen Container, der für Dritte zugänglich auf der

Straße stand. Teile dieser Unterlagen flogen auf der Straße herum, und Passanten blätterten in den privaten und geschäftlichen Unterlagen.

Im Hinblick darauf, daß der Konkursverwalter nach § 83 der Konkursordnung (KO) unter der Aufsicht des Konkursgerichts steht, habe ich mich an das Konkursgericht gewandt und um Stellungnahme zu der Verfahrensweise des Konkursverwalters gebeten. Meine Bemühungen waren jedoch erfolglos. Der Präsident des Amtsgerichts hat mir mitgeteilt, daß er als Organ der Justizverwaltung nicht befugt sei, Anweisungen zum Einschreiten gegen den Konkursverwalter zu erteilen. Es stehe vielmehr im pflichtgemäßen Ermessen des Konkursgerichts (hier Rechtspfleger, § 9 des Rechtspflegergesetzes) inwieweit es von den ihm nach § 83 KO zustehenden Befugnissen Gebrauch mache.

Auch in einem Zwangsversteigerungsverfahren mußten meine datenschutzrechtlichen Bemühungen zunächst vor der unabhängigen Entscheidung des Rechtspflegers haltmachen. Ein Hausgrundstück im Wert von über einer halben Million DM sowie ein 1/22 Miteigentumsanteil im Wert von 300,– DM sollten versteigert werden.

Der Wert des gesamten zu versteigernden Grundbesitzes wurde vom Gericht nach § 74 a des Zwangsversteigerungsgesetzes festgesetzt. Der Beschluß über die Festsetzung des Verkehrswertes wurde allen Beteiligten des Zwangsversteigerungsverfahrens zugestellt. Zu den Beteiligten des Verfahrens gehörten wegen des zu versteigernden 1/22 Miteigentumsanteil auch die übrigen Miteigentümer.

Das Zwangsversteigerungsgesetz sieht zwar die Bekanntgabe personenbezogener Daten an Dritte vor, jedoch müßte auch hier der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz berücksichtigt werden. Die Bekanntgabe des vollständigen Wertgutachtens an alle Miteigentümer bei einem zu versteigernden Anteil von nur 1/22 im Wert von 300,– DM erschien jedoch unverhältnismäßig.

Erfolgreicher waren dagegen meine Bemühungen in einem Fall der Zustellung eines vorläufigen Zahlungsverbots. Auftraggeber des Zustellungsauftrags durch die Post war ein Gerichtsvollzieher. Auf dem Briefumschlag des zuzustellenden Schriftstücks war vermerkt „Vorl. Zahlungsverbot vom ...".

Der Postbedienstete beurkundet die Zustellung, indem er über die Zustellung eine Urkunde aufnimmt, die u. a. die Übergabe der ihrer Anschrift und ihrer Geschäftsnummer nach bezeichneten Sendung bezeugen muß. Eine ordnungsgemäße Beurkundung des Zustellungsvorgangs setzt allerdings voraus, daß ein Zweifel über die Identität (Nämlichkeit) des in der Postzustellungsurkunde bezeichneten und des übergebenen Schriftstücks ausgeschlossen ist. Es ist daher nicht nur auf der Zustellungsurkunde, sondern auch auf dem Briefumschlag der Inhalt der Sendung in einer Weise anzugeben, daß Zweifel über die Identität ausgeschlossen sind.

In Fällen, in denen ein Schriftstück mit einem bestimmten Datum zugestellt werden soll, reicht in aller Regel die Angabe des Datums als Zusatz zur Geschäftsnummer aus, um die Nämlichkeit der Sendung zu gewährleisten. Nur

soweit aus besonderen Gründen die Angabe des Datums zur Herstellung eines eindeutigen Zusammenhangs zwischen dem zu übergebenden Schriftstück und der Postzustellungsurkunde nicht ausreicht, etwa weil in einem Verfahren einem Betroffenen mehrere Schriftstücke mit dem gleichen Datum zugestellt werden sollen, bestehen keine Bedenken, die Nämlichkeit durch zusätzliche Abkürzungen zu gewährleisten.

Unzulässig ist aber auf jeden Fall die ausführliche Bezeichnung des zuzustellenden Schriftstücks auf dem Umschlag. Auch nach der Rundverfügung des Justizministers vom 1. Februar 1989 (1454 – I B. 327) über die Bezeichnung des zuzustellenden Schriftstücks auf der Postzustellungsurkunde müssen aus Gründen des Datenschutzes die zur näheren Kennzeichnung des Schriftstücks aufzunehmenden Zusätze neutral gefaßt sein und dürfen keine Rückschlüsse auf den Inhalt des zuzustellenden Schriftstücks zulassen.

Der Direktor des Amtsgerichts hat auf meine Veranlassung die Gerichtsvollzieher darauf hingewiesen, in Zukunft die zur näheren Kennzeichnung der zuzustellenden Schriftstücke aufzunehmenden Zusätze neutral zu fassen.

5.7.3 Nachlaßsachen

Das Recht auf informationelle Selbstbestimmung des Bürgers im Bereich der Rechtspflege ist oft sehr schwer durchzusetzen. Dies wird besonders in diesem Fall im Bereich der Nachlaßsachen deutlich. Eine Erblasserin reichte bei einem Amtsgericht ein handschriftliches Testament in einem verschlossenen Umschlag zur besonderen amtlichen Verwahrung ein.

Beim Amtsgericht wurde dieser verschlossene Testamentsumschlag geöffnet, um aus dem Testament Angaben für die Hinterlegung wie den Geburtsort und die Geburtsregisternummer der Erblasserin zu entnehmen, zu prüfen, ob das Testament den Vorschriften des § 2247 BGB entspricht und ob es einen hinterlegungsfähigen Inhalt hat. Die in dem verschlossenen Umschlag außer dem Testament enthaltenen Schriftstücke wurden der Erblasserin zurückgesandt, da diese Schriftstücke nach Auffassung des Gerichts keinen hinterlegungsfähigen Inhalt hatten.

Nach § 2248 BGB ist ein eigenhändiges Testament (§ 2247 BGB) auf Verlangen des Erblassers in besondere amtliche Verwahrung zu nehmen. Voraussetzung für die Aufnahme in die amtliche Verwahrung ist das Verlangen des Erblassers, nicht aber die Gültigkeit des Testaments. Wenn das Gericht das Testament in einem unverschlossenen Umschlag erhält, kann es nach meiner Auffassung prüfen, ob es den Formvorschriften entspricht, so wie ein Notar bei der Errichtung eines öffentlichen Testaments durch Übergabe einer offenen Schrift nach § 2232 BGB in Verbindung mit § 30 des Beurkundungsgesetzes das Testament prüfen soll.

Nach dem Tode des Erblassers ist jede amtlich verwahrte Urkunde, die sich äußerlich als Testament darstellt, zu öffnen, auch wenn sie formungültig ist. Über die Gültigkeit ist erst bei der Erbscheinserteilung zu entscheiden. Daraus kann geschlossen werden, daß für das Gericht bei der Annahme eines verschlossenen Umschlages zur Hinterlegung eines Testaments keine Ver-

pflichtung besteht, den Umschlag zu öffnen, um die Gültigkeit des Testaments festzustellen. Im übrigen sind die Angaben, die das Gericht für die Hinterlegung des Testaments braucht (Geburtstag, Geburtsort, Standesamt und Nummer des Geburtseintrags, Beruf, Staatsangehörigkeit) kaum in einem Testament enthalten. Diese Angaben müßte das Gericht bei dem Erblasser erfragen.

Das Justizministerium hat mir in dieser Angelegenheit mitgeteilt, die Frage, ob ein Umschlag, der ein zur besonderen amtlichen Verwahrung bestimmtes eigenhändiges Testament enthält, vom Gericht geöffnet werden darf, sei bisher weder in der Literatur noch in der Rechtsprechung behandelt worden. Bei einer Besprechung des Präsidenten des Oberlandesgerichts mit den nachgeordneten Gerichtspräsidenten sei im Ergebnis Übereinstimmung erzielt worden, daß bei der Auslegung der §§ 2247, 2248 BGB vieles dafür spreche, einem etwaigen Geheimhaltungsinteresse des Testators den Vorrang gegenüber Überlegungen zur zweckmäßigen Gestaltung des Hinterlegungsverfahrens einzuräumen.

Das Besprechungsergebnis wurde den für die Bearbeitung von Nachlaßsachen zuständigen Rechtspflegern des Amtsgerichts als Entscheidungshilfe zugänglich gemacht. Für weitere Maßnahmen im Verwaltungswege war mit Rücksicht auf die Selbständigkeit der Rechtspfleger nach § 9 des Rechtspflegergesetzes kein Raum.

Bei der Eröffnung eines Testaments verwenden die Nachlaßgerichte amtliche Vordrucke. Soweit bei der Eröffnung festgestellt wird, daß zum Nachlaß Grundbesitz gehört, ist in den Vordrucken vorgesehen, eine beglaubigte Abschrift des Testaments und der Niederschrift über die Eröffnung an das zuständige Grundbuchamt zu übersenden, damit ggf. das Grundbuchberichtigungsverfahren von Amts wegen eingeleitet werden kann.

Die beglaubigte Abschrift des Testaments verbleibt in der Regel bei den Grundakten. Dadurch besteht die Möglichkeit, durch Einsichtnahme in die Grundakte nach § 12 der Grundbuchordnung auch Kenntnis vom Inhalt des Testaments zu erhalten. Da ein Testament meist mehr Regelungen enthält als für eine Grundbuchberichtigung erforderlich sind, stellt die Übersendung einer vollständigen Abschrift des Testaments an das Grundbuchamt und insbesondere der Verbleib dieser Abschrift bei den Grundakten eine unverhältnismäßige Belastung der Erben dar.

In dem an mich herangetragenen Fall wurde deshalb die Abschrift des Testaments nach durchgeführter Grundbuchumschreibung an das Nachlaßgericht zurückgegeben. Das Justizministerium hat eine Änderung der bei einer Testamentseröffnung zu verwendenden Vordrucke veranlaßt.

5.7.4 Schuldnerverzeichnis

Durch einen Auszug aus ihren Unterlagen bei der Schufa stellte eine Bürgerin fest, daß dort der Erlaß eines Haftbefehls zur Abgabe der eidesstattlichen Versicherung eingetragen war. Von dem Erlaß eines solchen Haftbefehls hatte sie bis dahin keine Kenntnis. Meine Nachforschungen beim

Amtsgericht ergaben, daß die Ladung zur Abgabe der eidesstattlichen Versicherung ausweislich der Zustellungsurkunde an ihren damaligen Ehemann im Wege der Ersatzzustellung zugestellt worden war. Möglicherweise unterrichtete er sie nicht von dieser Ladung, so daß wegen ihres Nichterscheinens zum Termin der Haftbefehl erlassen wurde. Da seit dem Erlaß des Haftbefehls drei Jahre vergangen waren, habe ich ihr empfohlen, beim Amtsgericht einen Antrag auf Löschung dieser Eintragung im Schuldnerverzeichnis zu stellen.

In einem anderen Fall wurde auch die Löschung einer Eintragung im Schuldnerverzeichnis beantragt, dem Schuldner eine Löschungsbescheinigung erteilt und eine Löschungsverfügung erstellt. Versehentlich wurde aber die Löschungsverfügung nicht an die Schuldnerdatei zur Löschung der Eintragung weitergegeben. Als Folge blieb die Eintragung in der Datei bestehen. Auf mögliche Anfragen an die Schuldnerdatei hätten Auskünfte über die darin noch bestehende Eintragung zum Nachteil des Schuldners erteilt werden können. Seitens des Amtsgerichts wurden organisatorische Maßnahmen getroffen, um solche Vorkommnisse künftig zu verhindern.

5.7.5 Grundbuch

Das Justizministerium hat in der Rundverfügung vom 24. Februar 1988 (JMBl. NW. S. 73) die Verfahren festgelegt, die für die Bekanntmachung der Grundbucheintragungen nach § 55 der Grundbuchordnung (GBO) in Betracht kommen. Dazu gehört u. a. die Übersendung von Ablichtungen, die nach vorgenommener Eintragung von den in Betracht kommenden Seiten des Grundbuchblattes herzustellen sind. Das Ablichtungsverfahren darf jedoch nicht angewendet werden, wenn dadurch den Beteiligten Eintragungen bekanntgegeben werden, die sie nicht betreffen; insoweit kommt nur die Übersendung von Durchschriften der Eintragungen oder die wörtliche Wiedergabe der Eintragung in Betracht (vgl. 8. Tätigkeitsbericht, S. 43/44).

Bürgereingaben haben gezeigt, daß die Gerichte in vielen Fällen aus Gründen der Arbeitsvereinfachung dennoch vollständige Grundbuchablichtungen als Eintragungsnachrichten erteilen, auch wenn dadurch mehr personenbezogene Daten bekanntgegeben werden als erforderlich und zulässig sind. Auch dem Justizministerium liegen Berichte vor, wonach ein nicht unerheblicher Teil der gerichtlichen Praxis bei der Bekanntmachung von Grundbucheintragungen in der von mir beanstandeten Weise verfahren. Es hat daher mit Rundverfügung vom 19. Juni 1990 noch einmal darauf hingewiesen, daß Gegenstand der nach § 55 GBO vorgeschriebenen Bekanntmachung allein der Wortlaut der vorgenommenen Eintragung ist. Allerdings muß dem Empfänger der Benachrichtigungen, vor allem damit er diese seinem Sachvorgang zuordnen kann, auch der Name des Grundstückseigentümers mitgeteilt werden. Eine Verpflichtung oder Berechtigung des Grundbuchamtes, weitere Daten des Grundstückseigentümers bekanntzugeben, besteht dagegen nicht. Bei Bedarf hat jeder Miteigentümer oder Berechtigte im Rahmen des § 12 GBO die Möglichkeit, das Grundbuch einzusehen oder einen Grundbuchauszug zu beantragen.

5.7.6 Vernichtung von Akten und Altpapier

Verschiedene Male im Berichtszeitraum gelangten Akten und sonstige Unterlagen der Justiz mit sensiblen personenbezogenen Daten, die zur Vernichtung bestimmt waren, in die Hände unbefugter Dritter, die Kenntnis von diesen Daten genommen haben. Die Presse hat über die Vorfälle ausführlich berichtet. Wegen möglicher Verstöße gegen § 10 Abs. 3 DSG NW habe ich die betroffenen Stellen um eine Stellungnahme gebeten. Zu den daraufhin von diesen Stellen entworfenen Verfahren der Vernichtung von Schriftgut mit personenbezogenen Daten habe ich verschiedene Hinweise gegeben. Das Justizministerium hat die Vorfälle zum Anlaß genommen, eine Allgemeine Verfügung mit Bestimmungen über die Aufbewahrung, Aussonderung, Ablieferung und Vernichtung des Schriftguts der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden vorzubereiten.

Als Ergebnis meiner Überprüfungen konnte ich allerdings dem Justizministerium nur mitteilen, daß ich seinen Ausführungen und den Ausführungen der ihm nachgeordneten Behörden nicht zu entnehmen vermag, daß mit hinreichender Sicherheit beim Verfahren der Vernichtung von Akten und sonstigen Unterlagen mit personenbezogenen Daten eine unbefugte Kenntnisnahme Dritter ausgeschlossen ist. Auf die Verpflichtung der speichernden Stelle und ihrer Aufsichtsbehörde, auch insoweit einen ausreichenden Datenschutz sicherzustellen, habe ich ausdrücklich hingewiesen.

Von einer Beanstandung der von mir überprüften Fälle habe ich gleichwohl abgesehen, da eine Wiederholung der konkreten von der Presse aufgegriffenen Fälle durch die bisher vorgesehenen Maßnahmen der betroffenen Stellen ausgeschlossen sein dürfte.

Durch einen „Aktenfund" bin ich zudem auf die besondere Datensicherungsproblematik bei **Heimarbeit** aufmerksam gemacht worden. Wenn von der Justiz die Fertigung von Schriftgut mit personenbezogenen Daten in Heimarbeit vergeben wird, ist nicht ersichtlich, wie bei der Herausgabe von Akten in den ungeschützten Bereich eines privaten Haushalts ein ausreichender Datenschutz durch die Justiz überhaupt sichergestellt werden kann.

Auch auf Grund der Stellungnahme des Justizministeriums bleiben Zweifel, ob in einer privaten Wohnung eine dem sensiblen Bereich der Datenverarbeitung der Justiz entsprechende und dem Datensicherungsstandard in den Gebäuden der Justiz gleichwertige Datensicherung überhaupt möglich ist. Nach meiner Auffassung sollte daher die Datenverarbeitung in Heimarbeit auf Sonderfälle beschränkt bleiben.

Da davon auszugehen ist, daß der Einsatz von Heimarbeit nicht nur im Bereich der Justiz erfolgt, wurde das Innenministerium von mir entsprechend unterrichtet und um Erörterung der Problematik auf der Ebene der Landesregierung gebeten.

5.7.7 Strafvollzug

Aus den zahlreichen Eingaben von Gefangenen, die sich wie immer in der Hauptsache mit der Bekanntgabe ihrer personenbezogener Daten durch die Vollzugsanstalt an Dritte und die Kenntnisnahme durch Mitgefangene befaßten, greife ich an dieser Stelle nur einige Fälle heraus.

Im Rahmen eines Forschungsprojekts zur Abschöpfung von Vermögensvorteilen aus Straftaten soll eine **Befragung** Gefangener in Justizvollzugsanstalten aller Länder durchgeführt werden. In der Bundesrepublik sollen 40 Justizvollzugsanstalten in die Befragung einbezogen werden.

Es ist beabsichtigt, an jeden Leiter der beteiligten Vollzugsanstalten Fragebögen mit der Bitte zu übersenden, in Betracht kommende Gefangene, die wegen eines Vermögensdelikts im weiteren Sinne einsitzen, auszuwählen und diese zur Mitarbeit zu bewegen. Anschließend sollen die ausgefüllten Fragebögen an das Forschungsinstitut zurückgesandt werden, ohne daß dieses eine Liste der befragten Personen besäße oder nach Entnahme der Fragebögen aus dem Rücksendeumschlag auch nur wüßte, von welcher Vollzugsanstalt diese Fragebögen stammen.

Hierbei stellt sich die Frage, welches Verfahren innerhalb der Justizvollzugsanstalt zur Anwendung kommt, um dem informationellen Selbstbestimmungsrecht der in Betracht kommenden Gefangenen ausreichend Rechnung zu tragen. Aus der Sicht des Datenschutzes wäre ein Verfahren zu wählen, das

- gewährleistet, daß die betroffenen Gefangenen völlig freiwillig an der Befragung teilnehmen; dies schließt einen wie auch immer gearteten Druck seitens der Vollzugsanstalt aus. Es setzt vielmehr voraus, daß die Betroffenen ausdrücklich und deutlich auf die Freiwilligkeit der Teilnahme hingewiesen werden und ihnen Nachteile durch eine Verweigerung der Teilnahme nicht entstehen.
- aber auch gewährleistet, daß kein Bediensteter der Vollzugsanstalt vom Inhalt der ausgefüllten Fragebögen Kenntnis erhält. Bei den in den Fragebögen enthaltenen Angaben handelt es sich für den Bereich der Vollzugsanstalt um personenbezogene Daten der Gefangenen mit höchst sensiblem Inhalt. In diesem Zusammenhang erscheint es angemessen, daß die Rücksendung der ausgefüllten Fragebögen in Umschlägen erfolgt, die von den Gefangenen selbst verschlossen und die anschließend durch die Vollzugsanstalt nicht mehr geöffnet werden.

Das Justizministerium ist meinen Anregungen gefolgt.

Im Warteraum für Besucher in einer Vollzugsanstalt wurden die Namen der Gefangenen, die Besuch erhalten bzw. die **Namen der Besucher**, die einen Gefangenen besuchen, laut aufgerufen. Ich bin davon ausgegangen, daß das Ausrufen der Namen von Gefangenen und Besuchern im Besuchsraum nicht nur in dieser sondern auch in anderen Vollzugsanstalten erfolgt. Um den Datenschutzbelangen der Betroffenen Rechnung zu tragen, habe ich das Justizministerium gebeten, sich für eine datenschutzfreundlichere Lö-

sung einzusetzen, etwa ein Wartenummernsystem wie es auch in Wartezimmern von Ärzten angewendet wird.

Nach Mitteilung des Justizministeriums wird das vorgeschlagene Wartenummernsystem bereits in einigen Justizvollzugsanstalten des Landes praktiziert. In anderen Anstalten sei die Frage auf Grund der Vollzugsform (offener Vollzug) nicht aktuell oder durch andere organisatorische Maßnahmen gelöst. Soweit die von mir geschilderte Verfahrensweise in Vollzugsanstalten besteht, haben die Präsidenten der Vollzugsämter eine datenschutzfreundlichere Praxis der Besuchsabwicklung veranlaßt.

Bei der Ausstellung von **Lohnsteuerkarten** an Gefangene ergab sich das Problem, ob als Anschrift der Gefangenen die Anschrift der Justizvollzugsanstalt aufzunehmen ist. Die Eintragung der Anschrift einer Justizvollzugsanstalt als Wohnanschrift auf der Lohnsteuerkarte eines Gefangenen kommt in Nordrhein-Westfalen nach Auskunft des Finanzministeriums regelmäßig nur dann in Betracht, wenn dessen Lohnsteuerkarte zuständigerweise von der Gemeinde, in der sich die Vollzugsanstalt befindet, im allgemeinen Verfahren auszustellen ist. Wird die Ausstellung einer Lohnsteuerkarte erst nachträglich beantragt, sind die Gemeindebehörden in Nordrhein-Westfalen angewiesen worden, auf der Lohnsteuerkarte stets die im Zeitpunkt der Antragstellung maßgebende Anschrift des Arbeitnehmers einzutragen, d. h. regelmäßig die neue Wohnanschrift unter der ein ehemaliger Gefangener nach Haftentlassung gemeldet ist.

5.8 Polizei

5.8.1 Polizeiliche Informationssysteme

Bürger haben mir gegenüber verschiedentlich den Verdacht geäußert, daß Polizeibeamte für private Zwecke **unbefugt** personenbezogene Daten dieser Bürger aus dem Informationssystem der Polizei des Landes **abgefragt** und/oder unbefugt Einsicht in die Kriminalpolizeiliche personenbezogene Sammlung über diese Bürger genommen haben. Abgesehen von den Fällen, in denen nach dem Ergebnis meiner Ermittlungen davon auszugehen ist, daß Bürger nur versuchten, den von ihnen namentlich bezeichneten Beamten unberechtigterweise Schwierigkeiten zu bereiten, war zum Teil eine fehlende Klärung des Verdachtes auf die kurze Aufbewahrungsdauer von sechs Monaten für die Protokollbänder zurückzuführen. Die Aufbewahrung der Protokollbänder, auf denen jede einzelne Abfrage des polizeilichen Informationssystems festgehalten wird, ist in den einzelnen Bundesländern unterschiedlich geregelt. In Abwägung des Interesses an einer Aufklärung des Verdachts möglicher Datenschutzverstöße mit dem Interesse der übrigen Betroffenen auf baldige Löschung ihrer Daten auf den Protokollbändern dürften gegen eine Verlängerung der Aufbewahrungsdauer der Bänder auf ein Jahr keine datenschutzrechtlichen Bedenken bestehen.

Unbefugte Abfragen und Einsichtnahmen erschüttern das Ansehen der Polizei bei der Bevölkerung. Besondere Nachdenklichkeit löst deshalb auch die Begründung für die unzulässige Abfrage im System aus, die ein überführter

Bediensteter gab, er müsse, um ungefährdet leben zu können, schließlich wissen, wer in seinem privaten Wohnumfeld lebe. Es ist deshalb nicht verwunderlich, wenn Bürger den Verdacht äußern, das polizeiliche Informationssystem werde von einigen Bediensteten offenbar als „Selbstbedienungsladen" angesehen.

Durch eine Eingabe wurde ich bereits im Jahre 1989 auf einen Datenaustausch im Rahmen eines Verfahrens zur Verhinderung von **Störungen in Fußballstadien** beim Spielbetrieb einer Amateur-Oberliga aufmerksam gemacht. In dem konkreten Fall war dem „Fan" eines Fußballklubs vor einem Auswärtsspiel in einem Schreiben der Gemeinde des Austragungsortes ein Stadionverbot erteilt worden. Das Schreiben war von dem Gemeindedirektor und dem 1. Vorsitzenden des gastgebenden Fußballvereins gemeinsam unterschrieben worden. Die Anschrift des Betroffenen war von der für seinen Wohnort zuständigen Kreispolizeibehörde der für den Austragungsort zuständigen Kreispolizeibehörde auf Anforderung übermittelt worden. Diese hat dann die Gemeinde entsprechend unterrichtet.

Wie das Innenministerium mir auf Anfrage mitteilte, gibt es keine regelmäßige Datenübermittlung in Form eines Informationssystems der Polizei bezüglich der Störer in Fußballstadien oder bezüglich bereits erteilter Stadionverbote. Die Datenübermittlung zwischen den Polizeibehörden erfolge nach Prüfung des Einzelfalles. Unterschiede im Hinblick auf die einzelnen Fußball-Ligen bestünden nicht.

Mit dem Innenministerium bin ich der Auffassung, daß die Datenübermittlung zwischen den Polizeibehörden nunmehr auf § 27 Abs. 1 des Polizeigesetzes des Landes Nordrhein-Westfalen (PolG NW) gestützt werden kann. Auch der Umfang der Daten (Familienname, Vorname, Geburtsdatum, Geburtsort, Anschrift) ist zur Aufgabenerfüllung der Polizei, eine sichere Identifizierung der Störer vornehmen zu können, erforderlich. Die Datenübermittlung an die Gemeinde war nach § 28 Abs. 3 Nr. 1 PolG NW zulässig mit der Einschränkung, daß die Übermittlung von Geburtsdatum und -ort nicht erforderlich ist, um ein Stadionverbot zu erteilen.

Demgegenüber lagen für die in der Mitunterzeichnung durch den 1. Vorsitzenden des gastgebenden Fußballvereins liegende Datenübermittlung an private Dritte die Voraussetzungen des § 29 Abs. 2 PolG NW nicht vor. Die Datenübermittlung war daher unzulässig. Entsprechend hat das Innenministerium den zuständigen Regierungspräsidenten aufgefordert, dafür Sorge zu tragen, daß von Gemeindedirektoren als örtliche Ordnungsbehörde erlassene Stadionverbote nicht zugleich auch von den Vereinsvorsitzenden unterzeichnet werden.

In der Vergangenheit bin ich darauf aufmerksam gemacht worden, daß die Wasserschutzpolizei des Landes Nordrhein-Westfalen eine **„zentrale Schiffsbewegungsdatei"** als datengestütztes Informationssystem führe, in dem Verstöße von Schiffseignern und Schiffsbesatzungen gespeichert würden. Meine Überprüfungen haben ergeben, daß bis auf Hessen kein anderes Bundesland eine derartige Datei führt. Insoweit habe ich meine Zweifel

hinsichtlich der Erforderlichkeit einer solchen Datei für die polizeiliche Aufgabenerfüllung geäußert und auch im übrigen hinsichtlich der Speicherung einzelner Daten datenschutzrechtliche Bedenken geltend gemacht.

Die Wasserschutzpolizei hat daraufhin eine Umbenennung in „Schiffskontrolldatei" durchgeführt und den Zweck der Datei, Vermeidung von Doppelkontrollen, Überwachung von Mängelbeseitigung, Information über Gefahrguttransporte, einengend festgelegt. Weiter ist der Wegfall der Speicherung von personenbezogenen Daten, also auch der Namen der Schiffsführer, geregelt. Von den durchgeführten Kontrollen der Schiffe werden nur die letzten drei, zeitlich begrenzt, gespeichert. Eine jährliche Überprüfung der Speicherungen ist zudem festgeschrieben.

Gegen die Führung einer „Schiffskontrolldatei" entsprechend den Angaben der Wasserschutzpolizei bestehen nach meinem derzeitigen Erkenntnisstand keine durchgreifenden datenschutzrechtlichen Bedenken.

Wiederholt wurde auch in diesem Berichtszeitraum der Verdacht geäußert, die Polizei führe sog. **Rosa Listen** und beobachte Schwulenorganisationen. Wie in der Vergangenheit erwiesen sich die vorgelegten „Beweise" für eine derartige Tätigkeit der Polizei nach Überprüfung als unzutreffend. Deshalb hat mir das Innenministerium des Landes Nordrhein-Westfalen auch erneut mitgeteilt, es gebe bei der Polizei des Landes Nordrhein-Westfalen weder eine Homosexuellen-Kartei noch finde eine Beobachtung von Schwulenorganisationen statt (vgl. im übrigen 9. Tätigkeitsbericht, S. 54/55).

Die Praxis der Polizei, bei wichtigen Ereignissen eine Vielzahl von öffentlichen Stellen durch Meldungen zu informieren (sog. **WE-Meldung**), ist im Grundsatz aus datenschutzrechtlicher Sicht nicht zu beanstanden, soweit dies zur Aufgabenerfüllung der jeweiligen Stellen erforderlich ist und für die Übermittlung der personenbezogenen Daten eine Rechtsgrundlage in bereichspezifischen Vorschriften vorhanden ist (vgl. hierzu 6. Tätigkeitsbericht, S. 32/33).

Durch eine Eingabe bin ich auf die besonderen Datenschutzprobleme aufmerksam gemacht worden, die bestehen, wenn WE-Meldungen Vorfälle mit Bediensteten der Polizei betreffen, die möglicherweise zu personalrechtlichen Maßnahmen Anlaß geben können. Die Datenverarbeitung durch eine WE-Meldung hat dann auch § 29 DSG NW zu beachten.

Das Recht auf informationelle Selbstbestimmung verpflichtet die Behörden weiter zu technischen und organisatorischen Maßnahmen zum Schutz der Daten gegen unbefugte Kenntnisnahme durch Dritte. § 10 Abs. 2 Nr. 6 und 9 DSG NW stellt dies für die automatisierte Datenverarbeitung klar; § 10 Abs. 3 DSG NW für die konventionelle Datenverarbeitung. Dies könnte für WE-Meldungen über Vorfälle mit Bediensteten, die möglicherweise zu personalrechtlichen Maßnahmen Anlaß geben können, bedeuten, daß sie wie Personalsachen mit dem Vermerk einer vertraulichen Behandlung zu kennzeichnen und weiterzugeben wären.

Das Innenministerium, gegenüber dem ich entsprechende Empfehlungen gemacht habe, hat angekündigt, seinen Runderlaß über Meldung wichtiger Ereignisse vom 13. Mai 1971 zu ändern.

In ähnlicher Weise bestehen datenschutzrechtliche Bedenken, wenn eine **Kontrollmitteilung** über die Einspeicherung einer Notierung einer erkennungsdienstlichen Behandlung eines Polizeibeamten in die INPOL-Datei „Erkennungsdienst" als Fernschreiben offen durch die Dienststelle des Beamten läuft. Sinn einer solchen Mitteilung ist lediglich, die Stelle, die die erkennungsdienstliche Maßnahme durchgeführt hat, möglichst frühzeitig in Kenntnis zu setzen, daß die Dateieingabe erfolgt ist, mit der Gelegenheit, Eingabefehler rechtzeitig zu berichtigen.

Der mit der Überprüfung befaßte Regierungspräsident kam zu dem Ergebnis, daß die Versendung der Kontrollmitteilung nicht erforderlich war. Eine Überprüfung der Richtigkeit der Eingabe könne auch erfolgen, wenn der Vorgang von der Datenstation zurückkomme. Er hat die Kreispolizeibehörde angewiesen, zukünftig auf die Kontrollmitteilung zu verzichten.

Es bedarf nach meiner Auffassung keiner näheren Erörterung, daß es zur Aufgabenerfüllung der Polizei erforderlich sein kann, Telefongespräche über den **Notruf** 110, sowie den **polizeilichen Funkverkehr** aufzuzeichnen. Da es in der Praxis häufig unmöglich sein dürfte, zuvor die Einwilligung des Anrufers einzuholen, bedarf die Aufzeichnung als Eingriff in das Recht auf informationelle Selbstbestimmung (Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 des Grundgesetzes) und als Verletzung des Fernmeldegeheimnisses (Artikel 10 Abs. 1 des Grundgesetzes) einer normenklaren gesetzlichen Regelung.

Rechtzeitig vor den abschließenden Beratungen des Gesetzes zur Fortentwicklung des Datenschutzes im Bereich der Polizei und der Ordnungsbehörden habe ich das Innenministerium des Landes Nordrhein-Westfalen darauf hingewiesen, daß es dringend geboten sei, eine entsprechende gesetzliche Grundlage, etwa im Rahmen der beabsichtigten Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen zu schaffen. Meiner Aufforderung ist das Innenministerium leider nicht gefolgt.

Nach Inkrafttreten des Polizeigesetzes des Landes Nordrhein-Westfalen am 1. Mai 1990 kann die Aufzeichnung der Telefongespräche auch nicht auf einen wie auch immer gearteten „Übergangsbonus" nach der Rechtsprechung des Bundesverfassungsgerichts gestützt werden. Die Aufzeichnung derartiger Gespräche in den Notrufzentralen der Polizei erfolgt derzeit ohne Rechtsgrundlage. Die Schaffung entsprechender Rechtsgrundlagen ist nach wie vor dringend geboten.

Gleiches gilt für die Aufzeichnung von Telefongesprächen über den **Notruf** 112 der **Feuerwehr**. Auch hier ist die Schaffung einer gesetzlichen Grundlage für die notwendige Aufzeichnung dringend erforderlich.

Für die Beratung der Bürger in den Kriminalpolizeilichen Beratungsstellen führt die Polizei ein Firmenverzeichnis der Errichterfirmen von **Überfall- und Einbruchmeldeanlagen**. In einem bundesweit geltenden Pflichtenkatalog

ist festgelegt, welche Angaben Firmen, die in das Verzeichnis aufgenommen werden wollen, gegenüber der Polizei machen und welchen Überprüfungen durch die Polizei sie sich unterwerfen müssen.

Nach einer Überprüfung des Pflichtenkatalogs habe ich dem Innenministerium im Hinblick auf bestehende datenschutzrechtliche Bedenken empfohlen, zur Vermeidung von Verstößen gegen Vorschriften über den Datenschutz auf die Führung eines derartigen Firmenverzeichnisses zu verzichten. Nach meiner Auffassung fehlt es etwa für die im Pflichtenkatalog vorgesehene Verarbeitung von Daten der Firmen, deren Mitarbeitern und deren Kunden an einer normenklaren Aufgabenzuweisungs- sowie einer Befugnisnorm. Besonders zu beachten ist weiter, daß die Gewerbeüberwachung, in der Gewerbeordnung bereichspezifisch geregelt, eine derartige Datenverarbeitung nicht kennt. Auch die Führung eines Firmenverzeichnisses mit Warnfunktion ist in § 149 der Gewerbeordnung bereichspezifisch geregelt. Zweifel an der Erforderlichkeit der polizeilichen Tätigkeit bestehen schließlich auch, weil die Polizeien in den Ländern Schleswig-Holstein und Berlin das gleichartige Firmenverzeichnis des Verbandes der Sachversicherer zur Beratung ihrer Bürger ausreichen lassen.

Das Ergebnis meiner Bemühungen bleibt abzuwarten.

5.8.2 Bauliche Maßnahmen zum Datenschutz

Durch eine Reihe von Hinweisen bin ich auf den mangelhaften baulichen Datenschutz im Bereich der Polizei aufmerksam gemacht worden. So können etwa auf **Polizeiwachen** die Besucher den Telefon- und Funkverkehr mithören und die Terminalabfragen mitlesen. Dadurch erfolgt eine Preisgabe sensibler personenbezogener Daten an unbefugte Dritte. Die Durchführung des Wachbetriebs in derartigen Polizeiwachen ist nur unter ständiger Verletzung der Anforderungen des § 10 DSG NW möglich. Auch für eine weitere Übergangszeit erscheint mir ein derartiger Zustand nicht mehr hinnehmbar. Gerade im Bereich der polizeilichen Datenverarbeitung sollte der Bürger in besonderer Weise vor unbefugter Kenntnisnahme unbeteiligter Dritter geschützt sein.

In Einzelfällen konnte durch Neu-, Um- und Erweiterungsbauten Abhilfe geschaffen werden. Insgesamt allerdings ist deutlich geworden, daß auch nach über zehn Jahren seit Inkrafttreten des Datenschutzgesetzes Nordrhein-Westfalen der bauliche Datenschutz im Polizeibereich mit seinen besonders sensiblen Daten nicht den bestehenden gesetzlichen Bestimmungen entspricht. Ich habe das Innenministerium des Landes deshalb um Stellungnahme gebeten, in welchem Umfang in Polizeiwachen im Lande Nordrhein-Westfalen auf Grund der derzeitigen baulichen Gegebenheiten ein Betrieb entsprechend den Vorschriften über den Datenschutz nicht gewährleistet ist, wann mit einer abschließenden Änderung jeweils zu rechnen ist und auf welche Weise jeweils für die Übergangszeit ein ausreichender Datenschutz sichergestellt wird.

Eine Antwort liegt mir immer noch nicht vor. Eine vordringliche Bereinigung der baulichen Datenschutzmängel im Polizeibereich erscheint angezeigt.

Durch eine Eingabe wurde ich darauf aufmerksam gemacht, daß auch durch die Art und Weise der Durchführung von **Blutentnahmen** Datenschutzbelange der Bürger berührt sein können. So etwa, wenn der Bürger gemeinsam mit den eingesetzten Polizeibeamten in einem jedermann zugänglichen Wartezimmer eines Krankenhauses auf die Blutentnahme durch den Krankenhausarzt warten muß. Jedermann, d. h. auch Nachbarn, Freunde, Bekannte, kann den Betroffenen dort sehen und sich den Zusammenhang zusammenreimen.

Auf meinen Hinweis hat das Innenministerium des Landes diese Angelegenheit in einem Erlaß gegenüber den Polizeibehörden dahingehend geregelt, daß in Absprache mit den Krankenhäusern Betroffene mit den Polizeibeamten nach Möglichkeit in separaten Zimmern auf die Blutentnahme warten können.

5.8.3 Datenschutzkontrolle

Zu meinen Empfehlungen nach Schaffung einer für die interne Kontrolle in den einzelnen Kreispolizeibehörden jeweils zuständigen Stelle (vgl. 9. Tätigkeitsbericht, S. 56 bis 58) hat die Landesregierung in ihrer Stellungnahme (Drucksache 10/5055) Übereinstimmung festgestellt. So sei für den Polizeibereich beabsichtigt, in einem verbindlichen Organisationsplan, der im Anschluß an die Geschäftsordnung noch für die Kreispolizeibehörden zu erlassen sei, eine besondere **Organisationseinheit „Datenschutz/-sicherheit"** in der Verwaltungs- bzw. Zentraleinheit vorzusehen. Eine derartige Regelung ist mir bisher nicht zugegangen.

Verwirrend ist in diesem Zusammenhang, daß das Innenministerium durch Runderlaß vom 23. Juni 1989 – IV D4–875 – festgelegt hat, daß zur Kontrolle der Regelungen des Mitarbeiter-Datenschutzes in jeder Behörde/Einrichtung ein Mitarbeiter zu bestellen ist. Da ich es für wenig glücklich halte, jeweils für einen Teilbereich (z. B. Personalstelle) eine darin eingebundene interne Kontrolle zu schaffen, habe ich das Innenministerium um Stellungnahme zum Verhältnis der beiden organisatorischen Festlegungen zueinander gebeten. Eine Äußerung des Innenministeriums liegt mir hierzu bisher noch nicht vor.

In einigen Eingaben haben sich Bürger bei mir danach erkundigt, ob ihr Fernmeldeverkehr durch Behörden des Landes überwacht wird bzw. worden ist. Unter Hinweis auf § 22 Abs. 1 i.V.m. § 26 Abs. 1 Satz 1 und 2 DSG NW habe ich daraufhin das Landeskriminalamt um Auskunft gebeten, ob eine **Überwachung** des genannten **Telefonanschlusses** stattgefunden hat oder noch stattfindet und wenn ja, zu welchem Zweck und auf welcher Rechtsgrundlage überwacht wurde/wird. Das Landeskriminalamt hat mir auf meine Anfrage unter Hinweis auf die §§ 100 a, 100 b und 101 Abs. 1 StPO mitgeteilt, es sei weder für die Anordnung noch für die Benachrichtigung der Beteiligten zuständig. Bei der Überwachung des Fernmeldeverkehrs handele es sich um eine richterliche bzw. staatsanwaltschaftliche Maßnahme nach den spezialgesetzlichen Regelungen der Strafprozeßordnung. Polizeibehörden könnten demzufolge nicht Normadressat nach § 22 Abs. 1 i.V.m. § 26 Abs. 1 Satz 1 und 2 DSG NW sein. Eine Auskunft könne mir deshalb nicht erteilt werden.

Die Auffassung des Landeskriminalamtes teile ich nicht. Das Landeskriminalamt ist eine der Kontrolle durch den Landesbeauftragten für den Datenschutz unterliegende öffentliche Stelle im Sinne des § 2 Abs. 1 DSG NW. Zur Durchführung dieser Kontrolle sind die öffentlichen Stellen verpflichtet, ihn bei der Erfüllung seiner Aufgaben zu unterstützen und ihm Amtshilfe zu leisten. Er hat gegenüber diesen Stellen ein Auskunfts-, Einsichts- und Zutrittsrecht.

Inzwischen habe ich das Innenministerium des Landes gebeten, das Landeskriminalamt anzuweisen, in den Fällen, in denen keine Telefonüberwachung durchgeführt wird, eine Negativerklärung abzugeben, in den übrigen Fällen die für den Wohnsitz zuständige Staatsanwaltschaft sowie das Aktenzeichen mitzuteilen. Für eine Übergangszeit bis zu einer grundsätzlichen Regelung im Strafverfahrensänderungsgesetz hat das Innenministerium in Abstimmung mit dem Justizministerium des Landes Nordrhein-Westfalen zu erkennen gegeben, meiner Bitte um Auskunft im Einzelfall entsprechen zu wollen.

5.8.4 Verfolgung von Verkehrsverstößen

Ein Bürger wandte sich gegen die Erhebung verschiedener Daten in einem Anhörungsbogen für die Verkehrsordnungswidrigkeiten-Anzeige. Die Überprüfung ergab, daß die Kreispolizeibehörde **veraltete Formulare** verwandte. Mit Erlaß vom 1. Oktober 1987 hatte das Innenministerium bereits neue Vordrucke vorgegeben. Nach meiner Auffassung kann der Hinweis unter Nr. 4.1.1 des Erlasses „Noch vorhandene alte Vordrucke sind aufzubrauchen" nicht dahin ausgelegt werden, daß auch die Datenerhebungspraxis im bisherigen Umfang fortgesetzt werden kann, nachdem der neue Erlaß auf die Erhebung gerade der Daten verzichtet hatte, gegen deren Preisgabe der Bürger sich gewandt hatte.

In einem Verkehrsordnungswidrigkeitenverfahren wurde dem betroffenen Bürger ein Auszug aus dem **Meßprotokoll** mit dem Hinweis auf Datenschutzgründe verweigert. Das Innenministerium des Landes Nordrhein-Westfalen hat daraufhin mit Erlaß vom 12. Oktober 1989 allen in Betracht kommenden Polizeibehörden und -einrichtungen folgendes mitgeteilt: „Sofern im Ordnungswidrigkeitenverfahren die Einsichtnahme in Meßprotokolle erforderlich ist, werden diese nur auszugsweise zur Verfügung gestellt. Die personenbezogenen Daten werden bis auf die des Betroffenen ggf. geschwärzt."

Mit diesem Verfahren ist sichergestellt, daß Datenschutzrechte Dritter nicht verletzt werden. Zu bedauern ist, daß die betreffende Polizeibehörde auch nach dieser klaren Entscheidung des Innenministeriums noch weitere neun Monate und drei Erinnerungsschreiben des Landesbeauftragten für den Datenschutz benötigte, um dem Bürger endlich den Auszug aus dem Meßprotokoll zuzusenden.

Die Verwendung eines Formblatts durch eine Staatsanwaltschaft mußte ich gegenüber dem Justizministerium beanstanden. Die Staatsanwaltschaft hatte die Kreispolizeibehörde ihres Bezirks veranlaßt, in Verkehrsvergehenssachen das **Formblatt** „Anlage zum Vernehmungsbogen für Vergehen ..." als Ergänzung zum polizeilichen Vernehmungsbogen beizufügen oder

bei mündlichen Vernehmungen um Beantwortung der Fragen des Formblatts zu bitten. In dem Formblatt werden von der Polizei detaillierte Angaben über die Einkommensverhältnisse des Betroffenen sowie seines Ehegatten erfragt.

Eine gesetzliche Grundlage für die Frage nach den Einkommensverhältnissen bei der erstmaligen Vernehmung durch die Polizei im Rahmen einer Verkehrsvergehensanzeige liegt weder für den Betroffenen noch für seinen Ehepartner vor. Die Erforschung der Einkommensverhältnisse in diesem Stadium des Ermittlungsverfahrens kann nicht auf § 160 Abs. 3 StPO gestützt werden, da diese Vorschrift nur auf das staatsanwaltschaftliche Ermittlungsverfahren Anwendung findet. Bei der Bearbeitung von Verkehrsvergehensanzeigen wird die Polizei im Rahmen ihres gesetzlichen Auftrags ohne konkrete Weisung der Staatsanwaltschaft tätig. Diese Erforschungspflicht ist als sog. erster Zugriff der Polizei speziell in § 163 StPO geregelt.

Eine Verweisung auf § 160 StPO enthält § 163 StPO nicht. Der Auffassung, § 160 Abs. 3 StPO sei auf die polizeilichen Ermittlungen im Rahmen des § 163 StPO analog anzuwenden, kann nicht gefolgt werden. Zwar ist die Staatsanwaltschaft „Herrin des Verfahrens" und die Polizei als Ermittlungsorgan der Staatsanwaltschaft tätig, wobei sie – wie sich aus dem Verhältnis zwischen § 160 und § 163 StPO ergibt – auf das staatsanwaltschaftliche Ermittlungsverfahren hinarbeitet. Aus dieser Stellung der Staatsanwaltschaft ergibt sich auch ihre Sachleitung und Grundverantwortung für das Verfahren. Dieser Rahmen wäre aber durchbrochen, wenn für bestimmte Deliktsgruppen eine generelle Weisung der Staatsanwaltschaft an die Polizei ergehen würde. Eine generelle Weisung darf nicht zu einer Umgehung der eindeutigen Gesetzeslage führen. Eine Ermittlung der Umstände für die Rechtsfolgen durch die Polizei nach § 160 Abs. 3 StPO in diesem Verfahrensstadium bedarf daher stets einer konkreten Weisung im Einzelfall.

Unstreitig ist, daß sich die Ermittlung bei Verkehrsvergehensanzeigen durch die Polizei nach § 163 a Abs. 4 i.V.m. § 136 Abs. 3 StPO richtet.

Es bestehen jedoch datenschutzrechtliche Bedenken, wenn Umstände, die für den Rechtsfolgenzumessungssachverhalt von Bedeutung sein können, bei der polizeilichen Ermittlung auf Grund genereller Weisung der Staatsanwaltschaft für bestimmte Deliktsgruppen erfragt werden ohne Prüfung, ob die Kenntnis dieser Umstände im konkreten Einzelfall für die Bestimmung der Rechtsfolgen tatsächlich notwendig ist. Eine Datenerhebung ist immer nur zulässig, wenn und soweit sie zur Aufgabenerfüllung der erhebenden öffentlichen Stelle im Einzelfall erforderlich ist. Praktikabilitätsgründe können eine Datenerhebung nicht rechtfertigen. Zwar ist in § 136 Abs. 3 StPO geregelt, daß bei der ersten Vernehmung des Beschuldigten zugleich auf die Ermittlung seiner persönlichen Verhältnisse Bedacht zu nehmen ist. Dieser Auftrag ist jedoch unter dem generellen Vorbehalt zu sehen, daß die persönlichen Verhältnisse nicht ein nach der Schwere des Vorwurfs und dem Grad des Verdachts unverhältnismäßiges Eindringen in die Privatsphäre bedeuten. Das schließt eine generelle Erforschung der Vermögensverhältnisse ohne Erforderlichkeit im Einzelfall in diesem Verfahrensstadium aus.

Auch für die Frage nach den Einkommensverhältnissen des Ehegatten durch die Polizei ohne dessen Kenntnis oder ausdrückliche Einwilligung gibt es keine gesetzliche Grundlage. Die herangezogenen Vorschriften §§ 163 Abs. 1 i.V.m. 160, 163 a Abs. 4, 5 StPO reichen als gesetzliche Grundlage nicht aus. Die Begründung, die Vernehmung von Beschuldigten und Zeugen sei notwendigerweise auch Mittel der Erkenntnisgewinnung von Informationen über Dritte, was sich aus der Natur der Sache ergebe, steht nicht im Einklang mit den Ausführungen, die das Bundesverfassungsgericht in ständiger Rechtsprechung über eine normenklare gesetzliche Grundlage gemacht hat. Das Justizministerium ist meiner Empfehlung, zu veranlassen, daß das Formular nicht mehr verwendet wird, nicht gefolgt. Es hat die Staatsanwaltschaft lediglich gebeten, die Belehrung in dem Formblatt noch konkreter zu fassen.

5.8.5 Polizeiliche Daten an Dritte

Im Rahmen von Ermittlungen über einen Wohnungseinbruch bei einem Bürger hat die Polizei bei der Vernehmung der Vermieterin als Zeugin dieser die Einleitung eines Verfahrens gegen den Bürger wegen Verdachts des Versicherungsbetruges mitgeteilt. Da die Bekanntgabe dieser sensiblen Daten an die Vermieterin zur Durchführung des Ermittlungsverfahrens wegen Wohnungseinbruchs nicht erforderlich war und im übrigen auch keine Rechtsgrundlage für eine derartige Datenübermittlung erkennbar ist, habe ich die Weitergabe der **Information über ein Ermittlungsverfahren** wegen Versicherungsbetruges gegenüber dem Innenministerium beanstandet.

Das Innenministerium ist meiner Empfehlung, die Kreispolizeibehörde anzuweisen, in derartigen Fällen von einer Bekanntgabe personenbezogener Daten an Dritte abzusehen, nicht gefolgt. Er hält die Bekanntgabe als Belehrung gemäß § 69 Abs. 1 Satz 2 StPO für geboten.

Da die Mitteilung an die Vermieterin bereits vor einer Belehrung und Vernehmung als Zeugin im Ermittlungsverfahren wegen Versicherungsbetruges erfolgte, bedeutet die Anwendung des § 69 StPO eine doppelte Analogie. Dies ist nach meiner Auffassung nicht möglich. Zudem ist die polizeiliche Befragung im Rahmen eines Ermittlungsverfahrens **vor** einer eventuellen Zeugenbefragung vom Gesetzgeber in der Strafprozeßordnung – im Gegensatz zu § 9 PolG NW – gerade nicht geregelt. Meine Beanstandung habe ich daher unverändert aufrecht gehalten.

In mehreren Bürgereingaben und Beratungsersuchen wurde ich darauf aufmerksam gemacht, daß öffentliche Stellen sich etwa zur Durchführung von Vollstreckungsmaßnahmen im Rahmen von „Amtshilfeersuchen" an die Polizeibehörden mit der Bitte wenden, den **Aufenthalt** für eine bestimmte Person zu ermitteln, da die Anschrift über das Einwohnermeldeamt nicht festzustellen ist. In einem der Fälle kam es dabei wegen Namensgleichheit und fehlenden Abgleichs des Geburtsdatums zu einer für den Betroffenen in finanzieller Hinsicht schwerwiegenden Personenverwechslung.

Meine Bitte an das Innenministerium des Landes um Stellungnahme wurde dahingehend beantwortet, daß die Auskunft aus der Zentralen Haftdatei der

Polizei nur noch unter besonderen Voraussetzungen erfolgt. Die Auskunfterteilung richtet sich nach den §§ 27 bis 29 PolG NW, soweit nicht spezialgesetzliche Regelungen vorgehen.

5.8.6 Sicherheitsüberprüfung auf Flughäfen

Bereits in meinem 6. Tätigkeitsbericht (S. 33/34) habe ich darauf hingewiesen, daß gegen eine **Sicherheitsüberprüfung** von Personen, die im Rahmen ihrer Tätigkeit Sicherheitsbereiche auf einem Flughafen betreten sollen, aus der Sicht des Datenschutzes keine grundsätzlichen Bedenken bestehen. Gleichzeitig habe ich deutlich gemacht, daß die Überprüfung vom Verfahren her nicht in rechtlich einwandfreier Weise erfolgt. Vor allem bestanden Bedenken dagegen, daß die notwendigen Sicherheitsüberprüfungen von einer **unzuständigen** Behörde durchgeführt wurden.

Mit Wirkung vom 01.01.1990 hat das Ministerium für Wirtschaft, Mittelstand und Technologie des Landes Nordrhein-Westfalen Grundsätze zur Durchführung von Sicherheitsüberprüfungen von Personen, die Sicherheitsbereiche auf dem Flughafen betreten müssen, und Grundsätze für die Sicherheitsüberprüfung von Personal von Luftfahrtunternehmen in Kraft gesetzt. Bei der Abfassung sind eine ganze Reihe von meinen Vorschlägen zur Verbesserung des Datenschutzes berücksichtigt worden, so daß nach dem derzeitigen Erkenntnisstand keine durchgreifenden datenschutzrechtlichen Bedenken gegen die getroffenen Regelungen vorhanden sind.

Auf die nach wie vor bestehende Notwendigkeit der Schaffung bereichspezifischer normenklarer Grundlagen für die Sicherheitsüberprüfungen nach Ablauf des vom Bundesverfassungsgericht anerkannten Übergangsbonus habe ich das Ministerium für Wirtschaft, Mittelstand und Technologie wiederholt hingewiesen.

5.8.7 Polizeifälle in der Presse

Ein Bürger, dessen Kind bei einem Verkehrsunfall ums Leben gekommen war, sah in der Weitergabe des vollen Namens und der Adresse seines Kindes durch die Polizei an die Presse einen Verstoß gegen die Bestimmungen über den Datenschutz und hat insoweit um Überprüfung gebeten.

Wegen der grundsätzlichen Bedeutung der Angelegenheit habe ich mich an das Innenministerium gewandt und darauf hingewiesen, daß die Bekanntgabe des Namens und der Adresse eines **Unfallopfers** durch die Polizei an die Presse ohne Einwilligung des Betroffenen oder – im Falle des Todes – der nächsten Angehörigen ein Eingriff in das Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung sowie in das Recht auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 des Grundgesetzes ist. Ein derartiger Eingriff ist nur im überwiegenden Allgemeininteresse zulässig und bedarf einer gesetzlichen Grundlage.

Dabei kommt es nicht darauf an, ob das Unfallopfer verstirbt oder nicht. Das Recht auf informationelle Selbstbestimmung wird, obwohl höchstpersönlich, unübertragbar und unvererblich, für ein tödlich verletztes Unfallopfer von

den jeweils nächsten Angehörigen wahrgenommen. Darüber hinaus können auch die Angehörigen selbst Betroffene sein.

Inzwischen hat das Innenministerium durch Runderlaß die Polizei des Landes Nordrhein-Westfalen angewiesen, Anschrift und Namen von Personen, die durch einen Verkehrsunfall verletzt oder geschädigt worden sind, grundsätzlich nicht ohne Einwilligung der Betroffenen den Medien zu übermitteln. Entsprechendes gelte auch für die Bekanntgabe der Daten von tödlich verletzten Unfallopfern. Ein Auskunftsanspruch der Presse bestehe insoweit nicht, da der Persönlichkeitsschutz, der im Falle des Todes des Betroffenen in bestimmtem Rahmen von den Angehörigen wahrgenommen werden kann, ein schutzwürdiges privates Interesse im Sinne des § 4 Abs. 2 Nr. 3 Landespressegesetz NW ist. Über sog. Personen der Zeitgeschichte seien jedoch entsprechende Angaben im erforderlichen Umfang zulässig.

Zu begrüßen ist, daß das Innenministerium diese Grundsätze für die Bekanntgabe von Namen und Anschriften von **Geschädigten einer Straftat** entsprechend gelten läßt.

In einem weiteren Fall einer Presseberichterstattung unter Preisgabe der Identität der Opfer hat der von mir zur Stellungnahme aufgeforderte Polizeipräsident darauf hingewiesen, daß die Presse bekanntlich den **Polizeifunk illegal mithört**, dies aber im Einzelfall schwer nachzuweisen sei. An das Recherchiervermögen der Journalisten würden daher in solchen Fällen keine hohen Anforderungen gestellt. Eine aus Datenschutzgründen dringend erwünschte Erschwernis der Mithörgelegenheit werde erst dann gegeben sein, wenn der Polizei ein leistungsfähiges Chiffriersystem zur Verfügung gestellt werde.

Es dürfte dem Bürger nur schwer verständlich zu machen sein, daß eine Polizei, zu deren Aufgabenerfüllung es in präventiver und repressiver Hinsicht gehört, die Bürger zur Befolgung bestehender Gesetze anzuhalten, selbst die von den Gesetzen geforderten Datensicherungen im Polizeibereich nicht einrichtet oder die Einrichtung nicht mit dem notwendigen Nachdruck betreibt. Auch hier erscheint ein Zeitraum von nunmehr über zehn Jahren als nicht mehr plausibel.

5.9 Verfassungsschutz

5.9.1 Kontrollen

Wegen der besonderen Sensibilität der im Bereich des Verfassungsschutzes gespeicherten Daten ist für mich jede Bürgereingabe Anlaß, eine Kontrolle vor Ort beim Verfassungsschutz des Landes Nordrhein-Westfalen durchzuführen. Nach wie vor bemerkenswert ist die aufgeschlossene Haltung der Verfassungsschutzbehörde meinen Kontrollwünschen gegenüber und die Bereitschaft, meinen Vorschlägen nach Auskunft über und/oder Löschung der gespeicherten Daten einzelner Betroffener nachzukommen. Es bleibt zu hoffen, daß diese Praxis auch Eingang in das zu erwartende Verfassungsschutzgesetz Nordrhein-Westfalen finden wird.

5.9.2 Sicherheitsüberprüfungen

Derzeit gibt es keine besonderen gesetzlichen Regelungen für die Sicherheitsüberprüfungen in der Privatwirtschaft. Es besteht Übereinstimmung darüber, daß derartige Regelungen erforderlich sind. So hat etwa der Bundesrat auf Anregung des Landes Nordrhein-Westfalen am 25. Januar 1989 den Beschluß gefaßt, die Bundesregierung aufzufordern, unverzüglich den Entwurf eines Gesetzes, welches die Sicherheitsüberprüfungen zu Zwecken des Geheimschutzes und des Sabotageschutzes regelt, vorzulegen. Ein derartiges Gesetz ist bisher nicht verabschiedet worden.

An der Mitwirkung der Verfassungsschutzbehörde an derartigen Sicherheitsüberprüfungen bestehen daher ohne Einwilligung der Betroffenen Bedenken. Zwar ist in § 2 Abs. 2 Nr. 2 des Verfassungsschutzgesetzes Nordrhein-Westfalen (VSG NW) geregelt, daß die Verfassungsschutzbehörde bei der Überprüfung von Personen, die an sicherheitsempfindlichen Stellen von lebens- und verteidigungswichtigen Einrichtungen beschäftigt sind oder werden sollen, mitwirkt, jedoch ist diese Vorschrift nicht normenklar. Aus ihr kann der Bürger nicht ersehen, in welchen Bereichen der Wirtschaft und unter welchen Voraussetzungen er mit einer Sicherheitsüberprüfung rechnen muß.

Auf meine datenschutzrechtlichen Bedenken hin hat das Innenministerium mitgeteilt, daß es Personenüberprüfungen bis zu einer gesetzlichen Regelung grundsätzlich nur noch vornehmen werde, wenn ihm die Firmen das Einverständnis der Betroffenen nachweisen.

5.9.3 Erfassung von Rechtsanwälten

In einer Pressemeldung war berichtet worden, daß der Berliner Verfassungsschutz in der Vergangenheit 144 Rechtsanwälte und 82 Referendare erfaßt habe. Nach Überprüfung sehe der Verfassungsschutz selbst die Erfassung und Speicherung als rechtswidrig an. In diesem Zusammenhang bestand Veranlassung zu prüfen, ob diese Speicherungen auch in die Dateien des Landes Nordrhein-Westfalen eingegangen sind.

Im Rahmen des polizeilichen Staatsschutzes in Nordrhein-Westfalen käme für eine Speicherung der hier in Frage stehenden Daten lediglich die Arbeitsdatei PIOS – Innere Sicherheit – (APIS) in Betracht. Hierbei handelt es sich um eine Verbunddatei des Bundeskriminalamtes, an die das Land Nordrhein-Westfalen über das Landeskriminalamt angeschlossen ist. In dieser Datei befinden sich keine Daten des Verfassungsschutzes Berlin.

Eine Überprüfung der vom Land Nordrhein-Westfalen in die Datei APIS eingespeicherten Datenbestände hat ergeben, daß eine derartige Erfassungs- und Speicherungspraxis hier nicht stattgefunden hat.

Nach Auskunft der Verfassungsschutzbehörde sind die Speicherungen des Berliner Verfassungsschutzes in die hiesigen Dateien nur eingegangen, sofern extremistische Bestrebungen im Sinne des § 3 Abs. 1 VSG NW vorlagen und ein Bezug zu Nordrhein-Westfalen gegeben war. Soweit noch fest-

zustellen war, sind die Daten nicht an andere Stellen weitergegeben worden. Sie sind nach § 12 Abs. 2 Satz 2 VSG NW gelöscht, die Akten wurden vernichtet.

Wie die Verfassungsschutzabteilung des Innenministeriums Nordrhein-Westfalen weiter mitteilt, hat sich die hiesige Erfassungs- und Speicherungspraxis an folgenden Grundsätzen orientiert:

Rechtsanwälte sind unabhängige Organe der Rechtspflege, an die sich jedermann – also auch Träger verfassungsfeindlicher oder sicherheitsgefährdender Bestrebungen – zu Zwecken der Beratung und Vertretung in allen Rechtsangelegenheiten wenden kann (§§ 1, 3 der Bundesrechtsanwaltsordnung). Soweit Rechtsanwälte in diesem Bereich ausschließlich in Wahrnehmung der ihnen obliegenden Berufspflichten handeln, verfolgen oder unterstützen sie nicht Bestrebungen (§ 4 BVerfSchG) gegen die in § 3 Abs. 1 VSG NW genannten Schutzgüter. Sie sind daher nicht Gegenstand der Beobachtung und der Datenverarbeitung durch die Verfassungsschutzbehörde NW.

Anders sei der Sachverhalt zu beurteilen, wenn Rechtsanwälte entweder außerhalb ihres beruflichen Wirkungskreises oder unter Mißbrauch des Mandates (sh. §§ 138 a, 138 b StPO) eindeutig verfassungsfeindliche Aktivitäten entfalten. Hier werde sich zumindest eine zeitlich begrenzte Speicherung personenbezogener Daten als notwendig erweisen. Sofern einer Abgrenzung in der Praxis Schwierigkeiten begegneten, sei in Zweifelsfällen von dem Grundsatz auszugehen, daß mit einem Mandat versehene Anwälte im Rahmen ordnungsgemäßer Geschäftsbesorgung handeln.

Gegen ein derartiges Vorgehen bestehen nach dem derzeitigen Erkenntnisstand im Ergebnis keine durchgreifenden datenschutzrechtlichen Bedenken.

5.9.4 Datei Adressen und Objekte Ost (ADOS)

Erhebliche Bedenken haben verschiedene Datenschutzbeauftragte gegen die Errichtung der Datei Adressen und Objekte Ost (ADOS) erhoben. Sie bestand aus Datensätzen, die der Bundesgrenzschutz in Amtshilfe für die Verfassungsschutzbehörden des Bundes und der Länder erhoben und übermittelt hat. Betroffen hiervon waren insbesondere Aus- und Übersiedler aus Ostblockländern.

Das Innenministerium des Landes Nordrhein-Westfalen hatte daraufhin schon Anfang 1990 öffentlich gefordert, die von Aussiedlern und DDR-Übersiedlern erhobenen Objektadressen der sog. ADOS-Datei zu löschen, da ohnehin die Erhebung für ADOS längst gestoppt worden sei.

Als Ergebnis dieser Bemühungen kann festgehalten werden, daß die Datei ADOS inzwischen ersatzlos aufgelöst worden ist. Die Datensätze sind gelöscht und die dazugehörigen Unterlagen ausgesondert und vernichtet.

5.10 Sozialwesen

5.10.1 Geltung der formellen Vorschriften des DSG NW für Leistungsträger

Anläßlich eines Kontrollbesuchs bei einem Krankenkassenverband kam es zu einer Kontroverse über die Anwendbarkeit der formellen Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen. Der Verband war der Auffassung, daß er für die bei ihm geführten Dateien mit Sozialdaten Übersichten nach den Vorschriften des Bundesdatenschutzgesetzes (§ 15 Satz 2 Nr. 1 BDSG) und nicht Dateibeschreibungen nach den Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen (§ 8 DSG NW) zu erstellen habe.

Dieser Auffassung stehen insbesondere verfassungsrechtliche Gründe entgegen. Die Ausführung von Bundesrecht ist grundsätzlich Ländersache (Artikel 83 des Grundgesetzes). Aus dieser Kompetenzverteilung zwischen Bund und Ländern folgt, daß es Angelegenheit der Länder ist, eigene Datenschutzkontrollinstanzen einzurichten und mit Befugnissen zu versehen. Für die Durchführung der Datenschutzkontrolle bestimmt daher § 79 Abs. 3 Satz 2 SGB X ausdrücklich, daß an die Stelle des Bundesbeauftragten für den Datenschutz die nach Landesrecht zuständige Stelle, also der Landesbeauftragte für den Datenschutz tritt. Damit wird aber der Landesbeauftragte für den Datenschutz nicht etwa zum „Statthalter" des Bundesbeauftragten für den Datenschutz ernannt. Vielmehr ergibt sich aus der Verweisung in § 79 Abs. 3 Satz 1 SGB X auf § 7 Abs. 2 Satz 1 BDSG („mit Ausnahme der §§ 15 bis 21"), daß für die Kontrollbefugnisse des Landesbeauftragten für den Datenschutz Landesdatenschutzrecht gilt.

Demnach haben Sozialleistungsträger des Landesbereichs Dateibeschreibungen nach § 8 DSG NW zu erstellen und dem Landesbeauftragten für den Datenschutz die Beschreibung aller automatisiert geführten Dateien, in denen personenbezogene Daten gespeichert sind, mit den Angaben der Dateibeschreibung vorzulegen. Diese Auffassung wird vom Innenministerium geteilt.

5.10.2 Durchführung des Gesundheitsreformgesetzes

Nachdem das Gesundheitsreformgesetz am 1. Januar 1989 in Kraft getreten ist, liegen mir inzwischen auf Grund verschiedener Eingaben erste Erfahrungen über die Anwendung der neuen Vorschriften in der Praxis vor. Umsetzungsprobleme haben sich insbesondere dadurch ergeben, daß häufig zwar die Befugnis zur Datenerhebung eindeutig normiert ist, eine korrespondierende gesetzliche Offenbarungsbefugnis der Leistungserbringer jedoch fehlt. Nach Erörterung im Kreise der Datenschutzbeauftragten des Bundes und der Länder gilt dies insbesondere in den nachfolgenden gravierenden Fällen.

5.10.2.1 Angabe der Diagnose auf Krankenscheinen

Im Gesundheitsreformgesetz ist geregelt, welche personenbezogenen Daten die an der kassen- und vertragsärztlichen Versorgung teilnehmenden Ärzte zum Zwecke der Abrechnung ihrer Leistungen den Krankenkassen

und den Kassenärztlichen Vereinigungen zu offenbaren haben. Dies sind: die von ihnen erbrachten Leistungen, der Tag der Behandlung, die Arztnummer und die Krankenversichertennummer (§ 295 Abs. 1 SGB V). Die Diagnose ist, anders als in der Übermittlungsvorschrift für Krankenhäuser (§ 301 SGB V), nicht genannt. Somit ist eine ausreichende Grundlage für die Angabe der Diagnose auf Krankenscheinen im Gesundheitsreformgesetz nicht vorhanden.

Vereinbarungen der Spitzenverbände der Krankenkassen und der Kassenärztlichen Bundesvereinigungen können die für Eingriffe in das informationelle Selbstbestimmungsrecht erforderliche gesetzliche Offenbarungsbefugnis nicht ersetzen; sie würden im übrigen die Versicherten nicht binden.

Demgegenüber vertritt das Bundesministerium für Arbeit und Sozialordnung und ihm folgend das Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen die Auffassung, die Offenbarung der Diagnose sei gerechtfertigt, weil sie Bestandteil einer ordnungsgemäßen Leistungsbeschreibung sei. Dies kann jedoch im Hinblick auf den im Gesetz zum Ausdruck gelangten Willen des Gesetzgebers, durch Enumeration der Daten normenklare Befugnisse für deren Offenbarung zu schaffen, nicht überzeugen. Die Diagnose ist m. E. von den „erbrachten Leistungen" eindeutig zu unterscheiden. Soweit die Krankenkassen zur Erfüllung ihrer Aufgaben nach dem Sozialgesetzbuch auf die Angabe der Diagnose angewiesen sind, wird der Gesetzgeber das Gesundheitsreformgesetz um eine entsprechende Offenbarungsbefugnis ergänzen müssen. Hierfür hat sich im Hinblick auf die andauernde Kontroverse auch das Ministerium für Arbeit, Gesundheit und Soziales gegenüber dem Bundesministerium für Arbeit und Sozialordnung ausgesprochen.

5.10.2.2 Anforderung von Krankenhaus-Entlassungsberichten durch Krankenkassen

Im Gesundheitsreformgesetz (§ 301 SGB V) ist enumerativ aufgeführt, welche Angaben die Krankenhäuser an die Krankenkassen zwecks Prüfung ihrer Leistungsverpflichtung übermitteln dürfen. Danach sind die Krankenhäuser befugt, bei Krankenhausbehandlung folgende Angaben zu übermitteln: Krankenversichertennummer, Tag und Grund der Aufnahme sowie Aufnahmediagnose, Arztnummer des einweisenden Arztes, Tag und Grund der Entlassung oder Verlegung sowie Entlassungsdiagnose und die nach der Bundespflegesatzverordnung berechneten Entgelte. Da es sich hierbei um eine abschließende Regelung handelt, ist die Übersendung von ärztlichen Entlassungsberichten, deren Inhalt weit über die genannten Angaben hinausgeht, nicht gestattet.

Auch auf § 100 SGB X kann die Übersendung ärztlicher Entlassungsberichte nicht gestützt werden, weil nach dieser Vorschrift zum einen eine Verpflichtung zur Offenbarung personenbezogener Daten nur besteht, soweit es – wie in § 301 SGB V – gesetzlich zugelassen ist, zum anderen die Verpflichtung des Arztes lediglich auf Erteilung von Auskunft gegenüber der Krankenkasse gerichtet ist. Auskunfterteilung setzt aber begrifflich eine gezielte Fragestellung voraus.

Die Überprüfung der Notwendigkeit und Dauer der stationären Behandlung im Krankenhaus durch die Krankenkasse ist nur über den Medizinischen Dienst möglich. Dabei ist jedoch sicherzustellen, daß die Übersendung von Krankenhausentlassungsberichten an den Medizinischen Dienst nur in begründeten Einzelfällen erfolgt und nicht zur Regel wird. Wenn auch das Gesundheitsreformgesetz ausdrücklich nur ein Einsichtsrecht des Medizinischen Dienstes innerhalb des Krankenhauses regelt (§ 276 Abs. 4 SGB V), so kann die Übersendung von Krankenhausentlassungsberichten an den Medizinischen Dienst in den begründeten Einzelfällen bis zu einer in Aussicht genommenen Gesetzesänderung toleriert werden, da dies einen geringeren Eingriff darstellt als der im Gesetz vorgesehene Weg. Dabei dürfen Krankenhausentlassungsberichte nur unmittelbar an den Medizinischen Dienst übersandt werden.

5.10.2.3 Qualitätssicherung in der Röntgendiagnostik

Gestützt auf ihre Gewährleistungspflicht verlangten die Kassenärztlichen Vereinigungen bisher von behandelnden Ärzten die Übersendung von Röntgenaufnahmen ihrer Patienten zwecks Durchführung von Prüfungen zur Qualitätssicherung. Eine entsprechende Vorlagepflicht der Ärzte besteht nach Inkrafttreten des Gesundheitsreformgesetzes nicht mehr. Der Gesetzgeber hat als Ausprägung der Gewährleistungspflicht drei unterschiedliche Prüfungstypen geschaffen, und zwar Plausibilitätskontrollen (§ 83 Abs. 2 SGB V), Wirtschaftlichkeitsprüfungen (§ 106 SGB V) und Qualitätsprüfungen (§ 136 SGB V) und diese je eigenen Regelungen unterworfen. Im Gegensatz zur Wirtschaftlichkeitsprüfung (§§ 294 ff. SGB V) enthält das Gesundheitsreformgesetz für die Durchführung von Qualitätsprüfungen keine Befugnisnorm für die Datenübermittlung durch den behandelnden Arzt. Demnach verstoßen behandelnde Ärzte bei der Übersendung von Röntgenaufnahmen zur Durchführung von Prüfungen zur Qualitätssicherung ohne Einwilligung der Patienten gegen die ärztliche Schweigepflicht.

Die Richtlinien der Kassenärztlichen Bundesvereinigung für Radiologie und Nuklearmedizin können die fehlende gesetzliche Offenbarungsbefugnis für die Anforderung der Röntgenaufnahmen nicht ersetzen, weil sie keine Rechtsvorschriften sind und auf jeden Fall die Versicherten nicht binden.

Soweit die Kassenärztlichen Vereinigungen zur Durchführung ihrer Aufgaben nach dem Sozialgesetzbuch, insbesondere zur Durchführung von Qualitätsprüfungen auf die Offenbarung von Patientendaten durch Ärzte angewiesen sind, bleibt bis zu einer entsprechenden Ergänzung des Gesundheitsreformgesetzes nur der Weg, die schriftliche Einwilligung der Patienten einzuholen.

5.10.3 Krankenhaus-Entlassungsberichte an Sozialämter

Ein Krankenhausarzt wandte sich dagegen, daß ein Sozialamt von ihm ohne ausdrückliche Einwilligung der Patienten Krankenhaus-Entlassungsberichte zur Entscheidung über die Kostenübernahme verlangte.

Das Sozialamt räumte zwar ein, daß die Anforderung von Krankenhaus-Entlassungsberichten für die Entscheidung über die Erstattung der Kosten sta-

tionärer Maßnahmen grundsätzlich nicht erforderlich war. Es hielt jedoch zur Klärung der Frage, ob im konkreten Fall der örtliche oder der überörtliche Sozialhilfeträger sachlich zuständig war, die Kenntnis der Krankenhaus-Entlassungsberichte für unentbehrlich.

Mag auch die gebotene Zuständigkeitsabgrenzung allein mit Hilfe der Einweisungsdiagnose nicht immer eindeutig getroffen werden können, so ist es dennoch nicht erforderlich, hierfür auf den kompletten Krankenhaus-Entlassungsbericht zurückzugreifen.

Insbesondere rechtfertigt § 100 SGB X die Anforderung von Krankenhaus-Entlassungsberichten zum Zwecke der Zuständigkeitsprüfung nicht. Zwar korrespondiert mit der in dieser Vorschrift geregelten Verpflichtung des Arztes ein Anspruch des Leistungsträgers gegenüber dem Arzt. Dieser Anspruch ist jedoch nur auf die Erteilung von Auskunft gerichtet. Auskunfterteilung setzt begrifflich eine präzise Fragestellung voraus. Zudem gestattet diese Vorschrift die Anforderung und Erteilung von Auskunft nur insoweit, als es für die Durchführung von Aufgaben des Leistungsträgers erforderlich ist. Das Erforderlichkeitsprinzip zwingt den Leistungsträger, sich auf die Anforderung der Auskunft zu beschränken, die er für die Erfüllung seiner Aufgaben (hier für die Klärung der sachlichen Zuständigkeit) unbedingt kennen muß. Krankenhaus-Entlassungsberichte, die der Information des weiterbehandelnden Arztes zu dienen bestimmt sind und dementsprechend eine Fülle personenbezogener Daten des Patienten und seiner Angehörigen enthalten, gehen weit über den Rahmen der Erkenntnisse hinaus, die der Sozialhilfeträger für die Klärung der Zuständigkeit benötigt. Aus diesem Grunde kann der Sozialhilfeträger auch nicht die Einwilligung des Hilfeempfängers in die Übersendung der Krankenhaus-Entlassungsberichte verlangen. Zwar hat derjenige, der Sozialleistungen beantragt oder erhält, eine Mitwirkungspflicht gegenüber dem Leistungsträger. Der Betroffene hat aber auf Verlangen des zuständigen Leistungsträgers nur der Erteilung der **erforderlichen** Auskünfte durch Dritte zuzustimmen. Da die Anforderung der Krankenhaus-Entlassungsberichte durch den Sozialhilfeträger über dessen Auskunftsanspruch hinausgeht und die Berichte mehr Daten enthalten, als der Sozialhilfeträger für seine Aufgabenerfüllung benötigt, ist die Anforderung unzulässig.

Ich räume allerdings ein, daß die Feststellung, ob der überörtliche Träger der Sozialhilfe für die Übernahme der Krankenhausbehandlungskosten zuständig ist, in Einzelfällen nicht ohne Einholung einer ärztlichen Stellungnahme möglich sein dürfte. Dabei ist jedoch zu beachten, daß eine derartige Stellungnahme nur auf Grund gezielter Fragestellung, die sich im Rahmen des für die Zuständigkeitsprüfung Erforderlichen hält, angefordert werden darf. Zudem ist für die Anforderung einer solchen Stellungnahme die Zustimmung des Betroffenen einzuholen.

5.10.4 Offenbarung zur Durchführung berufsrechtlicher Maßnahmen

Ein Kassenzahnarzt hat sich darüber beschwert, daß die Kassenzahnärztliche Vereinigung (KZV) ihr von der Krankenkasse übersandte Unterlagen, die den Vorwurf der Verletzung kassenzahnärztlicher Pflichten enthielten

und Grundlage für ein Zulassungsentziehungsverfahren waren, teilweise an die Zahnärztekammer (ZÄK) zwecks Durchführung berufsrechtlicher Maßnahmen weitergegeben hat.

Die Bekanntgabe von Einzelheiten aus dem Verfahren über die Entziehung der Kassenzahnarztzulassung durch die KZV an die ZÄK ist zur Aufgabenerfüllung der KZV nach dem Sozialgesetzbuch nicht erforderlich und deshalb unzulässig. Auf die Frage, ob die Kenntnis von Einzelheiten aus dem Entziehungsverfahren für die Aufgabenerfüllung der ZÄK erforderlich ist, kann nicht abgehoben werden, weil die ZÄK nicht zu den in § 35 SGB I genannten Stellen gehört und somit keine Aufgaben nach dem Sozialgesetzbuch wahrnimmt.

Demgegenüber vertritt das Ministerium für Arbeit, Gesundheit und Soziales die Auffassung, daß die KZV den gesetzlichen Auftrag habe, die kassenzahnärztliche Versorgung zu gewährleisten. Dieser Auftrag umfasse zugleich die Verpflichtung, die Erfüllung der den Kassenzahnärzten obliegenden Pflichten zu überwachen (§ 75 Abs. 2 SGB V). Aus dieser umfassenden Gewährleistungspflicht ergebe sich als deren untrennbarer Bestandteil für die KZV auch die Verpflichtung, die Einhaltung der berufsrechtlichen Erfordernisse durch ihre Kassenzahnärzte zu gewährleisten und die Ahndung berufsrechtlicher Verstöße sicherzustellen.

Es trifft zu, daß die KZV nach § 75 Abs. 1 Satz 1 SGB V gegenüber den Krankenkassen und ihren Verbänden die Gewähr dafür zu übernehmen hat, daß die kassenzahnärztliche Versorgung den gesetzlichen und vertraglichen Erfordernissen entspricht, und nach § 75 Abs. 2 Satz 2 SGB V die Erfüllung der den Kassenzahnärzten obliegenden Pflichten zu überwachen hat. Allerdings kann die KZV die Kassenzahnärzte zur Erfüllung ihrer kassenzahnärztlichen Pflichten, soweit notwendig, nur unter Anwendung der im Fünften Buch des Sozialgesetzbuchs vorgesehenen Maßnahmen anhalten. Maßnahmen in diesem Sinne sind je nach Schwere der Verfehlung Verwarnung, Verweis, Geldbuße bis 20 000,– DM, Anordnung des Ruhens der Zulassung oder der vertragsärztlichen Beteiligung bis zu zwei Jahren (§ 81 Abs. 5 SGB V). Zu diesen im Gesetz enumerativ aufgeführten Maßnahmen gehört nicht die Offenbarung personenbezogener Daten zum Zwecke der Durchführung berufsrechtlicher Maßnahmen an die Ärztekammer.

Zudem besteht die Möglichkeit, dem Kassenzahnarzt die Zulassung zu entziehen, wenn er u. a. seine kassenzahnärztlichen Pflichten gröblich verletzt (§ 95 Abs. 6 Satz 1 SGB V). Für die Entziehung zuständig ist allerdings nicht die KZV, sondern der von der KZV und den Landesverbänden der Krankenkassen errichtete Zulassungsausschuß für Zahnärzte.

Somit hat die KZV nach den Vorschriften des Sozialgesetzbuchs nicht einmal die Aufgabe, selbst über die Entziehung der Zulassung als Kassenzahnarzt zu entscheiden. Erst recht ist es nicht ihre Aufgabe, personenbezogene Daten, die dem Sozialgeheimnis unterliegen, anderen Stellen, die nicht Leistungsträger sind, zu deren Aufgabenerfüllung zu offenbaren.

Entsprechendes gilt für die Offenbarung personenbezogener, dem Sozialgeheimnis unterliegender Daten durch die KZV gegenüber dem Regierungspräsidenten zum Zwecke des Widerrufs der Approbation.

Das Ministerium für Arbeit, Gesundheit und Soziales hält dennoch an seiner Auffassung fest. Die Gewährleistungspflicht bestehe in mehreren Richtungen: einmal in bezug auf ihre Mitglieder in ihrer Tätigkeit in der speziell kassenzahnarztspezifischen Bezogenheit, zum anderen außerdem – jedoch untrennbar damit verbunden – in bezug auf ihre Mitglieder bei jeder kassenzahnärztlichen Tätigkeit zugleich in der allgemeinspezifischen Bezogenheit als Zahnarzt schlechthin. Diese Ausführungen kann ich nicht nachvollziehen; sie finden im Gesetz auch keine Stütze.

5.10.5 Offenbarung von Sozialdaten an den Rat

Mehrere Gemeinden äußerten Bedenken gegen eine ergänzende Regelung der Rechnungsprüfungsvorschriften in der Gemeindeordnung, die zur Folge hat, daß in Gemeinden ohne eigenes Rechnungsprüfungsamt die Mitglieder des Rechnungsprüfungsausschusses in sämtliche sozialhilferechtlichen Vorgänge einschließlich amtsärztlicher Gutachten Einsicht nehmen können.

Zu den in § 35 SGB I genannten Stellen gehören auch die rechnungsprüfungsberechtigten Behörden (§ 35 Abs. 1 Satz 2 SGB I). Daraus folgt, daß auch diese Stellen eine gesetzliche Aufgabe nach dem Sozialgesetzbuch erfüllen. Im Hinblick auf die neue Aufgabenzuweisungsnorm des § 99 Abs. 1 Satz 2 GO gilt dies auch für den Rechnungsprüfungsausschuß, so daß ihm die für seine Aufgabenerfüllung erforderlichen Sozialdaten befugt offenbart werden (§ 69 Abs. 1 Nr. 1 SGB X). Allerdings dürfen die rechnungsprüfungsberechtigten Stellen nur im erforderlichen Maße Einsicht in die Sachakten nehmen. Insofern wäre zu prüfen, ob wirklich alle Mitglieder des Rechnungsprüfungsausschusses die Akte einsehen müssen. Nach meiner Auffassung reicht es aus, wenn nur der Vorsitzende (ggf. zusammen mit einem weiteren Ausschußmitglied) die Prüfung vornimmt und den Ausschuß über das Ergebnis unterrichtet. Dabei wäre auch zu überlegen, ob nicht auf die Offenbarung von Name und Anschrift des Betroffenen in der Regel verzichtet werden kann.

5.10.6 Offenbarung von Sozialdaten an die Presse

Förmlich beanstanden mußte ich, daß ein Oberkreisdirektor der Presse Angaben über einen Asylbewerber offenbart hat, aus denen hervorging, daß der Betroffene seinen Lebensunterhalt durch Bezug von Sozialhilfe bestritten hat und ihm Krankenhilfe gewährt wurde. Dieser Presseinformation war eine auf Angaben der anderen Seite beruhende Veröffentlichung in der Presse vorausgegangen, die den Sachverhalt aus der Sicht des Oberkreisdirektors unvollständig und zum Teil unzutreffend wiedergegeben hatte. Der Oberkreisdirektor wollte dem Eindruck entgegenwirken, als habe die Verwaltung unmenschlich und willkürlich ohne Rücksicht auf den Gesundheitszustand des Betroffenen gehandelt.

Das Sozialgesetzbuch sieht zwar eine Offenbarungsbefugnis zur Richtigstellung unwahrer Tatsachenbehauptungen des Betroffenen vor (§ 69 Abs. 1 Nr. 3 SGB X), hierzu bedarf es jedoch der vorherigen Genehmigung durch die zuständige oberste Landesbehörde. Hieran fehlte es.

Auch im Rahmen der gesetzlichen Aufgabenerfüllung nach dem Sozialgesetzbuch (§ 69 Abs. 1 Nr. 1 SGB X) war es nicht erforderlich, die genannten Daten gegenüber der Presse zu offenbaren. Entgegen der Auffassung des Oberkreisdirektors läßt die Offenbarungsbefugnis zur gesetzlichen Aufgabenerfüllung keinen Raum für eine Abwägung zwischen dem Interesse des Betroffenen an der Geheimhaltung seiner dem Sozialgeheimnis unterliegenden personenbezogenen Daten und dem Interesse des Leistungsträgers an einer sachgerechten Unterrichtung der Öffentlichkeit. Entscheidend ist allein, ob die Offenbarung zur Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch erforderlich ist. Dies war hier ersichtlich nicht der Fall. Da der Oberkreisdirektor an seiner Auffassung, daß hier ein Informationsinteresse der Öffentlichkeit höher zu bewerten sei als das Interesse des Betroffenen, festhielt und somit die Gefahr bestand, daß in vergleichbaren Fällen auch künftig personenbezogene Daten Betroffener an die Presse offenbart würden, war die förmliche Beanstandung geboten.

Der Oberkreisdirektor hat zudem bestritten, daß es sich überhaupt um eine Offenbarung gehandelt habe, da der Presse die Tatsache der Sozialhilfeleistung bereits bekannt war. Dabei hat er jedoch übersehen, daß Gegenstand des Sozialdatenschutzes nicht mehr „Geheimnisse", sondern personenbezogene Daten schlechthin sind. Das Merkmal der Offenbarung stellt allein auf den Umgang mit personenbezogenen Daten ab und setzt kein Geheimhaltungsinteresse des Betroffenen voraus. Es kommt deshalb nicht darauf an, ob die Daten dem Empfänger bereits bekannt waren oder ob sie offenkundig sind.

5.10.7 Datenspeicherung über geringfügig Beschäftigte

Mit Inkrafttreten des Gesetzes zur Einführung eines Sozialversicherungsausweises und zur Änderung anderer Sozialgesetze zum 01.01.1990 sind die Arbeitgeber verpflichtet, geringfügig Beschäftigte zu melden. Mehrere Krankenkassen fragten daraufhin an, ob es zulässig sei, die an die Datenstelle der Rentenversicherungsträger zu übermittelnden Meldungen von geringfügig Beschäftigten auch für Prüfungszwecke der Einzugsstellen zu speichern. Die Krankenkassen waren der Auffassung, daß eine Speicherung in einer eigenen Datei erforderlich sei, um ihrem Prüfungsauftrag gegenüber den Arbeitgebern nachkommen zu können.

Eine Speicherung der Meldung durch die Einzugsstellen ist in den Vorschriften des Vierten Buches des Sozialgesetzbuchs nicht vorgesehen. Die Krankenkassen als Einzugsstellen erhalten von den Arbeitgebern die Meldung geringfügig Beschäftigter allein zu dem Zweck, sie binnen sieben Tagen an die Datenstelle der Rentenversicherungsträger zu übermitteln. Nur die Datenstelle der Rentenversicherungsträger darf die Daten geringfügig Beschäftigter in einer gesondert geführten Datei speichern. Eine Speicherung

dieser Daten durch die Krankenkassen für deren eigene Zwecke ist nach der Zweiten Datenerfassungs-Verordnung sogar untersagt.

5.10.8 Versorgungsangelegenheiten von Beschäftigten

Mit Inkrafttreten des Zehnten Buches des Sozialgesetzbuchs ist die Regelung des § 46 Abs. 2 des Gesetzes über das Verwaltungsverfahren der Kriegsopferversorgung entfallen, nach der die Bearbeitung und Entscheidung des Versorgungsfalles eines Antragstellers oder Versorgungsberechtigten, der bei einem Versorgungsamt beschäftigt ist, durch dasselbe Versorgungsamt ausgeschlossen war. Anstelle des ausgeschlossenen Versorgungsamtes war ein anderes bestimmt. Nach § 16 Abs. 1 Nr. 5 SGB X ist die Bearbeitung der Versorgungsangelegenheiten der im örtlich zuständigen Versorgungsamt Beschäftigten zulässig. Dies bedeutet, daß die amtsangehörigen Antragsteller oder Versorgungsberechtigten den Sachbearbeitern, die zugleich Kollegen sind, äußerst sensible Daten offenbaren müssen. Selbst dann, wenn die Bearbeitung der Versorgungsangelegenheiten der Amtsangehörigen nur bestimmten Personen eines anderen Teilbereiches zugewiesen und diese zur besonderen Vertraulichkeit verpflichtet worden sind, bleibt es datenschutzrechtlich bedenklich, wenn ein Amtsangehöriger gezwungen ist, sensible Daten einem ihm bekannten Kollegen zu offenbaren. Aus datenschutzrechtlicher Sicht ist deshalb die Abwicklung von Versorgungsangelegenheiten der Beschäftigten durch ein anderes Versorgungsamt im Wege des Auftrages nach § 88 SGB X zu fordern.

5.11 Gesundheitswesen

5.11.1 Listen über ärztliches Personal

Ein Gesundheitsamt verlangte von den Medizinischen Einrichtungen einer Universität folgende Angaben über die dort beschäftigten Ärzte: Name, Vorname, Anschrift, Datum und Aussteller der Approbation sowie Datum der Einstellung. Außerdem sollten dem Gesundheitsamt etwaige Veränderungen quartalsweise gemeldet werden. Der Kanzler der Universität hatte gegen die Datenübermittlung Bedenken, die ich geteilt habe.

Eine gesetzliche Grundlage für die Meldung der angeforderten Daten ist nicht vorhanden. Zwar hat das Gesundheitsamt nach der Dritten Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens (3. DVO) für Zwecke der Gesundheitsaufsicht Listen über in Berufen des Gesundheitswesens tätige Personen zu führen. Grundlage dieser Listenführung ist jedoch das Melderegister (§ 1 Abs. 1 Satz 2 der 3. DVO). Demnach werden den Gesundheitsämtern die für die Listenführung erforderlichen Daten jeweils von der zuständigen Meldebehörde übermittelt. Eine Datenübermittlung durch die Krankenhäuser als Arbeitgeber ist nicht vorgesehen und kann auch nicht, worauf sich das Gesundheitsamt berufen hatte, aus der Befugnis der Gesundheitsämter zur Prüfung der Berechtigungsausweise (§ 1 Abs. 1 Satz 4 der 3. DVO) hergeleitet werden.

5.11.2 Meldedaten zu Forschungszwecken

Ein Oberstadtdirektor fragte bei mir an, ob es zulässig sei, einem Krankenhaus aus dem Einwohnermelderegister das etwaige Todesdatum von bestimmten Patienten zu übermitteln, die dort wegen einer Erkrankung, deren Erforschung Gegenstand einer Studie der Medizinischen Fakultät einer Universität war, operativ behandelt worden waren. Zur Durchführung des Vorhabens hatte die Universität Kontakt zu dem Krankenhaus aufgenommen. Die Erhebung der für die Studie erforderlichen Daten erfolgte im Wege der Akteneinsichtnahme durch einen Arzt des Krankenhauses, der die benötigten Daten anonymisiert auf einen Erfassungsbogen übertrug, so daß dem Forscher keine personenbezogenen Daten übermittelt wurden. Um Aussagen über den postoperativen Verlauf machen zu können, wurde für die Studie auch das etwaige Todesdatum benötigt.

Nach § 28 Abs. 2 DSG NW dürfen öffentliche Stellen unter den dort genannten Voraussetzungen personenbezogene Daten ohne Einwilligung für ein bestimmtes Forschungsvorhaben übermitteln. Die Anwendung dieser Vorschrift scheitert hier bereits daran, daß es sich nicht um ein Forschungsvorhaben des Krankenhauses, sondern um ein solches der Medizinischen Fakultät handelt. Auch die Vorschriften des Meldegesetzes NW (MG NW) gestatten eine Übermittlung des Todesdatums an das Krankenhaus nicht. Auf § 31 Abs. 1 MG NW kann die Datenübermittlung nicht gestützt werden, da das Datum Nr. 13 (Sterbetag) nicht zur Aufgabenerfüllung des Krankenhauses erforderlich ist. Eine Datenübermittlung nach § 34 Abs. 2 Nr. 8 MG NW scheidet schon deshalb aus, weil die Daten hier an das Krankenhaus und nicht an den mit der Datenerhebung betrauten Arzt zwecks Durchführung eines **eigenen** Forschungsvorhabens übermittelt werden sollen.

Zudem würden bei einer Anforderung des Todesdatums durch das Krankenhaus dem Einwohnermeldeamt inzident Patientendaten offenbart, die der ärztlichen Schweigepflicht unterliegen. Eine solche Offenbarung ist weder nach § 28 DSG NW noch nach den Bestimmungen der ärztlichen Berufsordnung zulässig, weil es sich zum einen nicht um ein Forschungsvorhaben des Krankenhauses handelt, zum anderen eine Offenbarung zum Schutz eines höheren Rechtsguts hier nicht in Betracht kommt.

5.11.3 Einsichtnahme in Gesundheitsamtsakten

Ein Oberstadtdirektor hatte einer Betroffenen die von ihr begehrte Einsicht in die beim Gesundheitsamt über sie geführte Akte, in der sich ein im Auftrag des Sozialamtes gefertigtes amtsärztliches Gutachten befand, mit der Begründung verwehrt, das Gutachten dürfe nur an den Auftraggeber herausgegeben werden; im übrigen enthalte die Akte ärztliche, speziell jugendpsychiatrische Befunde und Begutachtungen, die nicht generell als einfache Daten betrachtet werden könnten. Zum größeren Teil handele es sich um Berichte mit subjektiven Äußerungen Dritter, deren Schutz die Akteneinsicht verbiete. Zudem sei der Einblick in das dem Sozialamt erstattete Gutachten nicht unproblematisch, da es Aussagen zu dem früheren Entwicklungszu-

stand und dem psychischen Verhalten der Betroffenen enthalte, deren Kenntnis für die Betroffene sehr belastend wäre.

Grundsätzlich besteht nach den Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen für jede speichernde Stelle die Verpflichtung, dem Betroffenen Akteneinsicht zu gewähren. Diese Verpflichtung entfällt nur unter den im Gesetz ausdrücklich geregelten Voraussetzungen, die hier jedoch nicht vorlagen. Wenngleich die Akte zum größeren Teil Berichte mit subjektiven Äußerungen Dritter enthält, kann der Betroffenen die Akteneinsicht nicht schlechthin verwehrt werden. Dies gilt auch, soweit dritte Personen – wie z. B. Amtsärzte oder Gutachter – im amtlichen Auftrag tätig geworden sind. Zudem kann den berechtigten Interessen Dritter (wie z. B. Informanten) an der Geheimhaltung ihrer Daten dadurch entsprochen werden, daß Unterlagen, soweit sie geheimzuhalten sind, entweder vorübergehend aus der Akte entfernt oder, wenn dies nicht möglich ist, kopiert und die zu schützenden Angaben in den Kopien unkenntlich gemacht werden.

Die Tatsache, daß die Akte ärztliche, speziell jugendpsychiatrische Befunde und Begutachtungen enthält, kann dem Akteneinsichtsrecht der Betroffenen nicht entgegengehalten werden. § 18 DSG NW stellt – abgesehen von den im Gesetz geregelten, hier nicht in Betracht kommenden Ausnahmen – nicht auf den Akteninhalt und die Sensitivität der Daten ab. Aus diesem Grunde kann auch der Umstand, daß die Kenntnis des in der Akte befindlichen Gutachtens für die Betroffene belastend sein könnte, nicht zur Versagung der Akteneinsicht führen. Das Akteneinsichtsrecht ist eine verfassungsrechtlich gebotene Folge des Rechts auf informationelle Selbstbestimmung, das generell zu respektieren ist und nicht durch bevormundende Fürsorge unterlaufen werden darf (vgl. BVerwG, NJW 1989, 2960).

Dem stünde allerdings nicht entgegen, wenn entsprechend den aus § 25 Abs. 2 SGB X sich ergebenden Grundsätzen der Inhalt der beim Gesundheitsamt geführten Akten der Betroffenen durch einen Arzt vermittelt wird. Besteht aber die Betroffene auf Akteneinsicht, ist sie ihr zu gewähren.

Soweit das Gesundheitsamt von anderen Stellen (hier Sozialamt) ersucht wird, ein Gutachten zu erstellen, braucht sich die Betroffene nicht darauf verweisen zu lassen, ihr Recht auf Akteneinsicht statt beim Gesundheitsamt bei dem Auftraggeber des Gutachtens wahrzunehmen. Das Akteneinsichtsrecht besteht gegenüber jeder aktenführenden Stelle, d. h. die Betroffene kann ihr Einsichtsrecht sowohl bei der begutachtenden als auch bei der auftraggebenden Stelle ausüben. Diese Wahlmöglichkeit ist im Hinblick auf die in der Regel unterschiedlichen Inhalte des in der Gesundheitsamtsakte verbleibenden und des an den Auftraggeber übersandten Gutachtens von erheblicher Bedeutung für das informationelle Selbstbestimmungsrecht.

5.11.4 Qualitätssicherung bei Röntgeneinrichtungen

Durch ein Beratungsersuchen wurde mir bekannt, daß Röntgenaufnahmen, die die Ärztekammern zum Zwecke der Qualitätssicherung nach der Rönt-

genverordnung bei den Ärzten anfordern, oft mit personenbezogenen Daten der Patienten übersandt werden.

Gegen die Übersendung nichtanonymisierter Röntgenaufnahmen an die für Qualitätssicherung zuständige Stelle der Ärztekammer bestehen Bedenken, da diese Stelle ihre Kontrollfunktion auch an Hand anonymisierter Röntgenbilder wahrnehmen kann. Zur Erfüllung ihrer gesetzlichen Aufgabe ist es erforderlich, aber auch ausreichend, mit der Röntgenaufnahme den Monat ihrer Fertigung sowie das Geschlecht und das Alter des Patienten nach Dekade zu übermitteln. Bei Weitergabe dieser Daten kann von einer hinreichenden (faktischen) Anonymisierung ausgegangen werden, und zwar auch unter Berücksichtigung der Inzidentoffenbarung der Tatsache, daß es sich um einen Patienten des übersendenden Arztes handelt und an welcher Krankheit er leidet.

Da ich es für geboten hielt, schon bei der Anforderung von Röntgenaufnahmen die Ärzte darauf hinzuweisen, daß sie bei deren Übersendung nur den Monat ihrer Fertigung sowie Geschlecht und Alter des Patienten nach Dekade anzugeben haben, habe ich das Ministerium für Arbeit, Gesundheit und Soziales gebeten, entsprechend auf die Ärztekammern einzuwirken. Dieser Bitte ist das Ministerium mit Erlaß vom 11. September 1990 nachgekommen.

5.11.5 Einschulungsuntersuchung

Erneut haben sich Eltern gegen die Datenerhebung mit dem von Gesundheitsämtern bei der Einschulungsuntersuchung verwendeten Vordruck „Angaben für den Schularzt" gewandt.

Mit der Erhebung von Angaben für die Einschulungsuntersuchung habe ich mich schon früher, zuletzt in meinem 8. Tätigkeitsbericht (S. 75) befaßt. Nach meiner Auffassung, die von der Landesregierung geteilt wird (Drucksache 10/2676, S. 39 sowie Erlaß des MAGS vom 17. November 1988), ist die Erhebung des Geburtstages der Eltern für den Gesundheitszustand und dessen Beurteilung für die Einschulung unwesentlich; sie dient vielmehr schulischen Informationsbedürfnissen.

Gleichwohl verwenden Gesundheitsämter immer noch die alten Vordrucke, die den Anforderungen des Datenschutzes nicht genügen. Zudem werden Angaben zu Schwangerschaft und Geburtsverlauf sowie zur Familienanamnese der Großeltern, Eltern und Geschwister hinsichtlich bestimmter Krankheiten erhoben.

Wenngleich sich medizinische Fragen einer datenschutzrechtlichen Überprüfung grundsätzlich entziehen, so hatte ich doch gewisse Zweifel schon an der Dienlichkeit dieser Angaben im Hinblick auf den Zweck der Untersuchung. Die Gesundheitsämter hielten mir entgegen, daß die genannten Angaben aus medizinischer Sicht wichtig und daher weiterhin als erforderlich zu beurteilen seien. So wurde z. B. geltend gemacht, daß Krankheiten in der Familie bei manchen Symptomen des Kindes Bedeutung hätten und zur Diagnose führen könnten. Viele Störungen des Kindes seien auf Störungen während der Schwangerschaft und des Geburtsverlaufs zurückzuführen.

Meines Erachtens wird hier nicht hinreichend zwischen den Aufgaben des Gesundheitsamtes und dem Tätigkeitsfeld behandelnder Ärzte unterschieden.

Das Ministerium für Arbeit, Gesundheit und Soziales, das ich unter Hinweis auf meine Bedenken um Stellungnahme gebeten habe, teilt meine Auffassung, daß eine derartig weitgehende Ausforschung sensibler Daten des Kindes und seiner Angehörigen anläßlich der Einschulungsuntersuchung deren Rahmen sprengt. Die Einschulungsuntersuchung diene der Beurteilung der Schulfähigkeit aus medizinischer Sicht. Eine Familien- oder Sozialanamnese sei überzogen, da der körperliche Ist-Zustand des Kindes zu beurteilen sei und nicht die soziale und psychische Reife.

Widersprechen mußte ich dem Ministerium allerdings, soweit es die Mitarbeit der Sorgeberechtigten in Form der elterlichen Auskunft bei der Einschulungsuntersuchung für erforderlich hält, weil sonst der Schularzt zu keinem Ergebnis kommen könne, das dem Kind nütze und das ordnungsgemäß sei. Aus den einschlägigen schulrechtlichen Vorschriften läßt sich nach meiner Auffassung lediglich die Verpflichtung der Erziehungsberechtigten herleiten, ihre schulpflichtig werdenden Kinder dem Schularzt zur Schuleingangsuntersuchung vorzustellen. Die Verpflichtung, über die Identifikation hinausgehende Angaben über das Kind zu machen, kann den Vorschriften auch nicht andeutungsweise entnommen werden. Dementsprechend muß ich daran festhalten, daß Angaben über das Kind nur auf freiwilliger Grundlage erhoben werden dürfen. Dies gilt sowohl für die (schriftlichen) Angaben in dem Elternfragebogen wie auch für entsprechende (mündliche) Angaben gegenüber dem Schularzt. Nach meiner Einschätzung läßt sich der die Schulfähigkeit begründende körperliche Ist-Zustand durch eine ärztliche Untersuchung (Erhebung objektiver Befunde) einschließlich der im Rahmen dieser Untersuchung auf Grund der erforderlichen Mitwirkung des Kindes für die Beurteilung des **gegenwärtigen** Gesundheitszustandes gewonnenen Erkenntnisse feststellen.

Inzwischen hat das Ministerium für Arbeit, Gesundheit und Soziales mit Erlaß vom 18. September 1990 gegenüber den Gesundheitsämtern klargestellt, daß der Schularzt auf die freiwillige Mitarbeit der Betroffenen und der Angehörigen bei allen Schuluntersuchungen, auch bei der Einschulungsuntersuchung, angewiesen sei. Das Gesundheitsamt müsse durch entsprechende Aufklärungsmaßnahmen die Bevölkerung auf den Nutzen und den Vorteil der Schuluntersuchungen hinweisen und entsprechend bürgerfreundlich vorgehen, somit „hoheitliches" Vorgehen vermeiden. Eine vorherige Erhebung gesundheitlicher, häufig sensibler Daten des Kindes und seiner Angehörigen im Rahmen der Einschulungsuntersuchung sei einer Akzeptanz eher hinderlich. Deshalb sei zu prüfen, ob auf die Versendung von Fragebogen zur Einschulungsuntersuchung verzichtet werden könne.

Einen Verzicht auf die vorherige Erhebung von Angaben für den Schularzt würde ich begrüßen; er darf aber nicht dazu führen, daß die Erziehungsberechtigten während der schulärztlichen Untersuchung mit unzulässigen Fragen überrumpelt werden. Vielmehr ist darauf zu achten, daß nur die für den Untersuchungszweck, nämlich die Beurteilung der Schulfähigkeit aus medizinischer Sicht erforderlichen Daten zum status praesens erhoben werden.

5.11.6 Genomanalyse

Auf Grund eines Beschlusses der Konferenz der Justizminister und -senatoren hat sich die Bund-Länder-Arbeitsgruppe „Genomanalyse" unter dem Vorsitz des Bundesministers der Justiz mit Fragen der Humangenetik, insbesondere der Genomanalyse befaßt. Der Abschlußbericht dieser Bund-Länder-Arbeitsgruppe berücksichtigt die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 26./27.10.1989 über Genomanalyse und informationelle Selbstbestimmung (vgl. Anlage 4, S. 173 bis 175) und stimmt mit ihr in der grundsätzlichen Bewertung überein, daß die Genomanalyse das Persönlichkeitsrecht des einzelnen in besonderer Weise beeinträchtigen kann.

Aus dem Abschlußbericht der Arbeitsgruppe wie auch aus der Entschließung der Datenschutzbeauftragten ergibt sich eindeutig die Notwendigkeit, Grundsätze für die Zulässigkeit sowie Art und Umfang von Genomanalysen in den verschiedenen Bereichen wie auch für die Durchführung genomanalytischer Untersuchungen und die Verarbeitung der durch die Untersuchung gewonnenen genetischen Daten gesetzlich normenklar festzulegen.

5.11.7 Bundeskrebsregister

Das Bundesministerium für Jugend, Familie, Frauen und Gesundheit beabsichtigt die Schaffung eines Bundeskrebsregistergesetzes. Die Notwendigkeit hierfür ergebe sich insbesondere daraus, daß keine Einheitlichkeit der Erfassung bestehe und es seit dem GMK-Beschluß von 1983 zu keiner nennenswerten Ausweitung der erfaßten Bevölkerung gekommen sei. Die angestrebte Flächendeckung solle allerdings nicht durch **ein** zentrales Register, sondern durch eine ausreichende Zahl regionaler Register erreicht werden. Dies bedeutet, daß die in einigen Ländern bereits vorhandenen epidemiologischen Krebsregister, denen zum Teil unterschiedliche Erfassungsmodalitäten zugrunde liegen, vergleichbar gemacht werden müssen. Dabei sind die schon bestehenden Lösungen, nämlich Meldeberechtigung, Einwilligung, dezentrale Verschlüsselung, Meldepflicht daraufhin zu prüfen, inwieweit damit das Ziel einer effektiven Krebsregistrierung bei Wahrung des größtmöglichen Schutzes personenbezogener Daten der Patienten erreicht wird.

Die Datenschutzbeauftragten des Bundes und der Länder haben in ihrem Beschluß vom 4./5. Oktober 1990 die Auffassung vertreten, daß die Einrichtung eines Krebsregisters auf der Grundlage einer namentlichen Meldung der Patienten ohne deren Einwilligung einen äußerst schwerwiegenden Eingriff in ihr informationelles Selbstbestimmungsrecht, verbunden mit einer weiteren Durchbrechung der ärztlichen Schweigepflicht darstellen würde. Darüber hinaus kann auf Grund zentraler Registrierung die registerführende Stelle feststellen, welche Personen an Krebs erkrankt und zum Register gemeldet worden sind. Die Datenschutzbeauftragten sind deshalb nach wie vor der Meinung, daß Krebsregister nur mit Einwilligung der Patienten oder auf anonymer Basis geführt werden können.

5.12 Personalwesen

5.12.1 Polizeiärztlicher Dienst

Aus dem Bereich der Polizei mehren sich Beschwerden von Polizeivollzugsbeamten über den Umgang mit ihren Gesundheitsdaten durch Polizeiärzte. Eine nähere datenschutzrechtliche Prüfung der Datenverarbeitung durch den Polizeiärztlichen Dienst zeigt, daß außer den Vorschriften der §§ 194 Abs. 1 und 2 i.V.m. § 45 Abs. 1 Satz 3 sowie § 189 Abs. 2 Satz 2 und 3 des Landesbeamtengesetzes (LBG) sowie der Verordnung über die freie Heilfürsorge der Polizeivollzugsbeamten keine weiteren bereichspezifischen gesetzlichen Regelungen bestehen, die etwa besondere Vorkehrungen für den Umgang mit den sensiblen Gesundheitsdaten durch Polizeiärzte und deren Zusammenarbeit mit den Dienstvorgesetzten der Betroffenen vorsehen. Auch § 29 Abs. 1 Satz 1 DSG NW kommt als bereichspezifische Rechtsgrundlage nicht in Betracht, soweit für einen derart tiefen Eingriff in das Persönlichkeitsrecht der Polizeivollzugsbeamten keine näheren Bestimmungen (wie etwa in § 29 Abs. 2 DSG NW) getroffen sind.

Diese Gesetzeslage wird den Anforderungen des Grundrechts der Polizeivollzugsbeamten auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung sowie ihres Rechts auf informationelle Selbstbestimmung und der hieraus abgeleiteten verfassungsrechtlichen Grundsätze nicht gerecht. Der Polizeivollzugsbeamte steht zwar in einem freiwillig übernommenen Dienst- und Treueverhältnis zu seinem Dienstherrn und unterliegt deshalb besonderen, über die allgemeinen Bürgerpflichten hinausgehenden Pflichten gegenüber dem Staat. Zugleich kann er jedoch wie jeder Bürger seine Grundrechte gegenüber dem Staat, also auch gegenüber seinem Dienstherrn, geltend machen. Der Konflikt zwischen dem Schutz des Persönlichkeitsrechtes und der Garantie eines für die Erhaltung dieses Schutzes unentbehrlichen Staatsapparates, insbesondere einer funktionstüchtigen Polizei, kann – wie bei anderen Grundrechten auch – nur in der Weise gelöst werden, daß Grundrechtsbeschränkungen nur zulässig sind, soweit Sinn und Zweck des Dienst- und Treueverhältnisses des Polizeivollzugsbeamten dies im konkreten Fall unter Beachtung des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes erfordern. Dies wird, wie mehrere Eingaben zeigen, in der Praxis nicht hinreichend beachtet.

Wenngleich nicht zu verkennen ist, daß die Funktionsfähigkeit der Polizei ohne Feststellung und Erhaltung der Polizeidienstfähigkeit ihrer Vollzugsbeamten nicht gewährleistet werden kann, so darf dies wiederum nicht dazu führen, daß in den beim Polizeiärztlichen Dienst geführten **Krankenakten** Datensammlungen über den gesamten Polizeidienst der Vollzugsbeamten entstehen, die eine Fülle von Gesundheitsdaten aus allen Vorsorge-, Eignungs- und Überwachungsuntersuchungen, aber auch aus allen Krankmeldungen und allen Abrechnungen der freien Heilfürsorge (bei freier Arztwahl werden die abgerechneten Behandlungsscheine zur Krankenakte genommen), aus Kur- oder Sanatoriumsaufenthalten sowie aus fachärztlichen Gutachten enthalten, – und dies alles, ohne daß Umfang, Dauer der Datenspeicherung, Aufbewahrung der Krankenakten und Zugriffs- sowie Einsichts-

rechte gesetzlich geregelt sind. Ich habe erhebliche Zweifel, ob derartig umfassende Datensammlungen mit ihrer durchgängigen und nahezu lückenlosen Registrierung der gesundheitlichen Befindlichkeit aller Polizeivollzugsbeamten dem Verhältnismäßigkeitsgebot noch entsprechen.

Dabei darf nicht übersehen werden, daß eine derartige Datenfülle auch Aussagen gegenüber dem Dienstvorgesetzten ermöglicht, die sich von der eigentlichen Zweckbestimmung der Feststellung und Erhaltung der Polizeidienstfähigkeit entfernen. So hat in einem mir vorgetragenen Fall der Leiter einer Kreispolizeibehörde vom Polizeiarzt **Auskunft** darüber verlangt, ob der Polizeivollzugsbeamte trotz seiner Erkrankung, die zur Dienstunfähigkeit geführt hatte, einer Nebentätigkeit nachgehen konnte. Die polizeiärztliche Stellungnahme sollte in einem Disziplinarverfahren gegen den Polizeivollzugsbeamten verwertet werden. Für derartige Zweckänderungen fehlt es an einer gesetzlichen Grundlage.

In einem anderen Fall wies eine Kreispolizeibehörde mit Verfügung vom Juli 1989 die Polizeivollzugsbeamten an, die mit der Diagnose versehenen Durchschriften der ärztlichen **Arbeitsunfähigkeitsbescheinigungen** mit dem Aufdruck „zur Vorlage bei der Krankenkasse" unverzüglich an den Polizeiarzt zu übersenden. Der Polizeiärztliche Dienst werde durch die Zusendung der Arbeitsunfähigkeitsbescheinigungen mit Diagnose, die für die Anerkennung von Heil- und Hilfsmitteln sowie anderen Heilmaßnahmen notwendig sei, keine zusätzlichen Informationen erhalten, da der Behandlungsschein ebenfalls die Diagnose enthalte. Da der Behandlungsschein aber erst ein bis zwei Quartale nach der Behandlung übersandt werde, erfordere die „reibungslose polizeiärztliche Tätigkeit" eine umgehende Übersendung. Das Innenministerium teilte mir auf meine Bitte um Stellungnahme mit, daß sein diesbezüglicher Runderlaß vom 9. Dezember 1983 mit Ablauf des Jahres 1988 außer Kraft getreten sei. Das Innenministerium ging davon aus, daß eine Weiterleitung der Arbeitsunfähigkeitsbescheinigung mit Diagnose an den Polizeiärztlichen Dienst nur noch freiwillig erfolge.

Hiervon kann jedoch, wie die Verfügung der Kreispolizeibehörde zeigt, nicht die Rede sein. Außerdem bestehen schwerwiegende Bedenken dagegen, daß ohne bereichspezifische und normenklare gesetzliche Grundlage und ohne Prüfung des Erforderlichkeits- und Verhältnismäßigkeitsgrundsatzes eine Arbeitsunfähigkeitsbescheinigung in dieser Form verlangt wird, wie dies im übrigen öffentlichen Dienst – aber auch im gesamten arbeitsrechtlichen Bereich – unbekannt ist und rechtswidrig wäre.

Erhebliche Bedenken habe ich auch gegen eine Verquickung der Abrechnungsstelle für die freie Heilfürsorge mit dem Polizeiärztlichen Dienst durch Übersendung aller **Behandlungsscheine** nach Abrechnung und Überprüfung. Meiner Auffassung, daß dieses Verfahren eine Durchbrechung des im öffentlichen Dienst vorherrschenden Gebotes einer strikten Abschottung der Heilfürsorge – wie bei der Beihilfe – von der Personalverwaltung, aber auch vom Amtsarzt darstellt, hat das Innenministerium entgegengehalten, daß der Abschottung der Heilfürsorge durch den Runderlaß vom 9. November 1960 (SMBl. NW. 203030) Rechnung getragen werde. Daß dem nicht so ist,

wird durch die Darstellung der Aufgaben des Polizeiarztes belegt. Das Innenministerium sieht durch die Vorschriften der §§ 194 und 189 Abs. 2 LBG sowohl die Behandlung erkrankter Polizeibeamter, die vorbeugende Gesundheitsvorsorge und die arbeitsmedizinische Betreuung als auch die amtsärztliche Funktion sowie die Beurteilung der Notwendigkeit und Angemessenheit der Aufwendungen in der freien Heilfürsorge aus medizinischer Sicht datenschutzrechtlich mit „hinreichender Klarheit" abgedeckt. Auch das vom Innenministerium angezogene Gesetz über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit deckt die unterschiedlichen Funktionen des Polizeiarztes nicht ab und rechtfertigt die damit verbundenen Eingriffe in das Persönlichkeitsrecht der Polizeivollzugsbeamten keinesfalls. Nach diesem Gesetz unterliegen die Betriebsärzte im Einzelfall neben ihrer Schweigepflicht auch einer besonderen Geheimhaltungspflicht gegenüber dem Arbeitgeber; sie dürfen vor allem keine Befunde der Arbeitnehmer an ihn weitergeben (vgl. § 3 Abs. 1). Außerdem behandeln Betriebsärzte nicht und üben keine vertrauensärztliche Funktion aus.

Ein weiterer Fall verdeutlicht die Problematik fehlender gesetzlicher Regelungen. Ein Polizeiarzt, der vom Dienstvorgesetzten eines Polizeivollzugsbeamten (telefonisch!) um Stellungnahme zu dessen Dienstunfähigkeit im Rahmen dienstrechtlicher Überprüfung nach § 79 Abs. 1 Satz 2 LBG gebeten worden war, nahm ebenfalls telefonisch Kontakt mit dem behandelnden Arzt auf, ohne daß der Beamte hiervon und von der angeordneten Untersuchung Kenntnis hatte. Der Polizeiarzt, der dem **Hausarzt** mitteilte, daß der Betroffene wegen der langen Dienstausfallzeit polizeiärztlich zu untersuchen sei und daß er an Hand der Untersuchungsbefunde über den weiteren dienstlichen Einsatz oder die Dienstunfähigkeit zu entscheiden habe, bat darum, dem Betroffenen die ärztlichen Untersuchungsbefunde zur polizeiärztlichen Untersuchung mitzugeben. Durch die aus diesem Telefonat entstandenen Mißverständnisse zwischen Hausarzt und betroffenem Polizeivollzugsbeamten wurde das Vertrauensverhältnis gestört und die Behandlung abgebrochen. Die unmittelbare Kontaktaufnahme mit dem Hausarzt sollte nach Aussage des Polizeiarztes wegen des kurzfristig anberaumten Untersuchungstermins der Verwaltungsvereinfachung dienen. Während sich der Dienstvorgesetzte hinsichtlich der Anordnung der polizeiärztlichen Untersuchung auf § 79 LBG berief, meinte der Polizeiarzt nach § 194 Abs. 2 LBG untersuchen zu müssen. Daneben war dem Polizeiarzt nicht bewußt, daß die ärztliche Schweigepflicht auch unter Ärzten gilt. Der ärztlichen Schweigepflicht unterliegen nicht nur medizinische Daten, sondern auch – wie hier – die Tatsache, daß und aus welchen Gründen der Betroffene polizeiärztlich untersucht werden sollte.

Ein anderer Polizeiarzt nutzte bei seiner Untersuchung zur Feststellung der Polizeidienstfähigkeit nicht nur den Inhalt der Krankenakten, insbesondere Entlassungsberichte aus einer Krankenhausbehandlung sowie früher eingeholte **fachärztliche Gutachten**, die er im Rahmen einer von ihm selbst durchgeführten Behandlung erhalten hatte; er übersandte dem Dienstvorgesetzten zur Untermauerung der eigenen Feststellungen auch noch die fachärztlichen Gutachten, die er anläßlich eines von ihm behandelten Dienstunfalles des Betroffenen bei einer Universitätsklinik eingeholt hatte.

Wiederum ein anderer Polizeiarzt hat das ihm vom Polizeivollzugsbeamten zur Beurteilung der Notwendigkeit einer Anschlußheilbehandlung überlassene Gutachten einer neurologischen Universitätsklinik ohne Wissen und Einwilligung des Betroffenen an die **Kurklinik** zur Durchführung einer Kneipp-Kur übersandt. Und schließlich wurde von einem Polizeiarzt ohne Kenntnis des Betroffenen der ärztliche Befund über eine Krankenhausbehandlung unmittelbar bei der Klinik angefordert.

Sämtliche Fälle zeigen eindringlich, daß die Tätigkeit des Polizeiarztes ohne bereichspezifische und normenklare Rechtsgrundlage, die alle für den Datenschutz notwendigen Vorkehrungen trifft, auf erhebliche Bedenken stoßen muß. Ich halte es nicht für überzeugend, wenn das Innenministerium zwar einräumt, daß die Vorschriften des Landesbeamtengesetzes (§§ 45 und 194 LBG) keine ausreichende Rechtsgrundlage für eine regelmäßige Übermittlung aller anläßlich der Untersuchung gewonnenen Gesundheitsdaten an den Dienstvorgesetzten darstellen, andererseits aber die Zulässigkeit der Übermittlung auch von Einzelergebnissen der Untersuchung, ergänzenden Befunden und Diagnosen damit zu begründen versucht, daß bei einem Polizeivollzugsbeamten immer zu prüfen sei, ob im Bereich des Polizeivollzugsdienstes eine Tätigkeit vorhanden sei, die der Beamte trotz seiner gesundheitlichen Einschränkung noch ausüben könne. Ungeachtet dieser Auffassung hat das Innenministerium allerdings angekündigt, die Zusammenarbeit zwischen Dienstvorgesetzten und Polizeiarzt neu regeln zu wollen. Ich halte an meiner Auffassung fest, daß es hierzu einer bereichspezifischen gesetzlichen Regelung bedarf.

5.12.2 Amtsärztliche Untersuchung

In meinem 9. Tätigkeitsbericht (S. 68) habe ich mich bereits mit der Einstellungsuntersuchung und dem dabei verwendeten Fragebogen auseinandergesetzt. Im Berichtszeitraum gaben mehrere Eingaben Anlaß, die recht unterschiedliche Verfahrensweise der Dienstvorgesetzten bei der Einholung amtsärztlicher Gutachten sowie der Amtsärzte bei der Erstattung von Gutachten zur Feststellung der **Dienstunfähigkeit** zu überprüfen. So hat in einem mir zur Prüfung vorgelegten Fall der Amtsarzt unzulässigerweise dem Dienstvorgesetzten ein zwölfseitiges Gutachten vorgelegt, das neben der Vorgeschichte einschließlich Familienanamnese auch eine ausführliche Befunderhebung wiedergab. In einem anderen Fall wurden vom Amtsarzt neben dem eigenen Gutachten weitere fachärztliche Gutachten, die mit der Untersuchung nicht einmal im Zusammenhang standen, dem Dienstvorgesetzten übersandt, ohne daß auch hier der Betroffene Kenntnis davon hatte.

Rechtsgrundlage für eine amtsärztliche Untersuchung zur Feststellung der Dienstunfähigkeit ist § 45 Abs. 1 Satz 3 des Landesbeamtengesetzes (LBG) bzw. § 7 Abs. 2 des Bundes-Angestelltentarifvertrages (BAT). Aus diesen Vorschriften ergibt sich für den im öffentlichen Dienst Beschäftigten zwar die Verpflichtung, sich einer amtsärztlichen Untersuchung zu stellen; es fehlen jedoch die bereichspezifischen normenklaren Regelungen, die auch den mit der Untersuchung verbundenen Eingriff in das informationelle Selbstbestim-

mungsrecht zulassen und die notwendigen Vorkehrungen zum Datenschutz enthalten. Auch § 29 DSG NW trifft – anders als für die Einstellungsuntersuchung (§ 29 Abs. 2 DSG NW) – die zur Feststellung der Dienstunfähigkeit notwendigen datenschutzrechtlichen Regelungen nicht. Ob § 29 Abs. 2 DSG NW für die Feststellung der Dienstunfähigkeit entsprechend herangezogen werden kann, erscheint mir zweifelhaft. Während der Bewerber um Einstellung in den öffentlichen Dienst sich der amtsärztlichen Untersuchung freiwillig stellt, ist der im öffentlichen Dienst Beschäftigte zur Untersuchung verpflichtet (§ 45 Abs. 1 Satz 3 LBG und § 7 Abs. 2 BAT). Wenn er demnach nicht selbst darüber entscheiden kann, ob im Zusammenhang mit dem Untersuchungsergebnis auch Gesundheitsdaten an den Dienstvorgesetzten übermittelt werden, so darf er bei Untersuchungen auf Grund gesetzlicher Verpflichtung oder entsprechender tarifrechtlicher Bestimmung keinesfalls der Übermittlung seiner Gesundheitsdaten an den Dienstvorgesetzten schutzlos ausgeliefert sein.

Datenerhebung und Datenübermittlung unterliegen auch bei Feststellung der Dienst- oder Arbeitsunfähigkeit dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit. Dies bedeutet, daß nur diejenigen Daten vom Amtsarzt erhoben werden dürfen, die zur Erstattung des Gutachtens im Rahmen des Untersuchungsauftrages unbedingt notwendig sind. Voraussetzung hierfür ist vor allem ein vom Dienstvorgesetzten an den Amtsarzt gerichteter **präziser Untersuchungsauftrag**, der auch dem Betroffenen bekannt sein muß (vgl. § 12 Abs. 2 DSG NW). Mit der Präzisierung des Untersuchungsauftrages wird die Voraussetzung dafür geschaffen, daß es nicht zu einer übermäßigen Erhebung medizinischer Daten kommt und nur diejenigen Daten an den Dienstvorgesetzten weitergegeben werden, die nach dem Zweck der Untersuchung erforderlich sind. Die gutachtliche Äußerung des Amtsarztes hat sich demzufolge in aller Regel auf die Beantwortung der gestellten Fragen, also das Ergebnis der Untersuchung – dienstfähig bzw. nicht dienstfähig – und erforderlichenfalls die festgestellten Einschränkungen der Dienstfähigkeit zu beschränken. Bei der Untersuchung erhobene Einzeldaten (Vorgeschichte, Untersuchungsbefunde und Diagnose) sind grundsätzlich nicht erforderlich und dürfen nicht mitgeteilt werden.

Außerdem ist zu berücksichtigen, daß die bei der Untersuchung erhobenen Gesundheitsdaten der ärztlichen Schweigepflicht unterliegen, die auch für Amtsärzte gilt. Eine Offenbarung dieser Daten ist nach § 2 Abs. 5 der ärztlichen Berufsordnung nur zulässig, wenn dem Betroffenen vor der Untersuchung bekannt ist oder eröffnet wurde, inwieweit die vom Amtsarzt getroffenen Feststellungen zur Mitteilung an den Auftraggeber des Gutachtens bestimmt sind.

Nach allem halte ich es für geboten, gesetzlich festzulegen, daß vom untersuchenden Arzt grundsätzlich nur das Ergebnis der Untersuchung verlangt werden kann. Darüber hinaus darf die Mitteilung von Risikofaktoren verlangt werden, soweit dies zur Begründung einer Entscheidung im Einzelfall erforderlich ist. Außerdem muß gesetzlich geregelt werden, unter welchen Voraussetzungen Ärzte, Krankenhäuser und Versicherungen vom Arzt nach Vorerkrankungen oder den Ergebnissen und Unterlagen früherer ärztlicher

Untersuchungen und Maßnahmen befragt werden und diese offenbaren dürfen. Eine Offenbarung ist, wie auch die medizinische Untersuchung, unzulässig, wenn sie zum Zweck der Feststellung der Dienstunfähigkeit erfolgen soll und der Bedienstete nicht zuvor unterrichtet worden ist.

In diesem Gesetz muß auch klargestellt werden, daß der Betroffene ein Recht auf Einsicht in die beim Gesundheitsamt verbliebenen Untersuchungsunterlagen hat (oben S. 28). Schließlich ist festzulegen, daß diese Unterlagen nicht mit solchen (z. B. im Gesundheitsamt) vermengt werden dürfen, die anderen Zwecken dienen, daß sie nicht für andere Zwecke verwendet werden dürfen und nach einer bestimmten Frist zu löschen oder zu vernichten sind.

5.12.3 Psychologische Eignungstests

Ein Oberkreisdirektor, der sich bei der Auswahl seiner Bewerber der Deutschen Gesellschaft für Personalwesen (DGP) bedient, hat mich gefragt, ob die Übermittlung der Testergebnisse von der DGP an die Einstellungsbehörde und deren Nutzung der schriftlichen Einwilligung des Bewerbers bedarf.

In meinem 4. Tätigkeitsbericht (S. 82) bin ich auf Grund der Ausführungen des Innenministers davon ausgegangen, daß die DGP als sonstige öffentliche Stelle des Landes anzusehen ist, da sie bei der Mitwirkung an dem Auswahlverfahren eine Aufgabe der öffentlichen Verwaltung wahrnimmt (§ 22 Abs. 3 BDSG). Dementsprechend finden auf die Erhebung, Speicherung, Auswertung und Übermittlung der personenbezogenen Daten von Bewerbern durch die DGP die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen Anwendung.

Dabei ist die DGP speichernde Stelle. Die Übermittlung der Testergebnisse an die Einstellungsbehörde ist daher eine Weiterverarbeitung im Sinne des § 29 Abs. 2 Satz 1 DSG NW, die der schriftlichen Einwilligung des Bewerbers bedarf.

Eine wirksame Einwilligung setzt voraus, daß der Bewerber über das Ergebnis des Tests und den Umfang der zu übermittelnden Testdaten in Kenntnis gesetzt worden ist, damit er in Kenntnis dieses Ergebnisses über seine Einwilligung in die Übermittlung an die Einstellungsbehörde entscheiden kann. Er ist aber auch unter Darlegung der Rechtsfolgen darauf hinzuweisen, daß er die Einwilligung verweigern und mit Wirkung für die Zukunft widerrufen kann (§ 4 Satz 4 DSG NW).

Die Aufklärung über den Verwendungszweck der Daten hat bereits vor deren Erhebung, am besten in der Einladung zu dem Auswahltermin, zu erfolgen (§ 12 Abs. 2 Satz 1 DSG NW). Dabei ist dem Bewerber zu eröffnen, daß im Rahmen des Auswahlverfahrens die Teilnahme an einem Test der DGP vorgesehen ist, die Daten zum Zwecke der Einstellung nach § 29 Abs. 1 Satz 1 DSG NW erhoben werden und vor einer Übermittlung der Testergebnisse an die Einstellungsbehörde die schriftliche Einwilligung des Bewerbers eingeholt wird. Zur Aufklärung über den Verwendungszweck gehört außerdem, daß der Bewerber über den Verbleib der Testdaten bei der DGP und die Dauer ihrer Speicherung informiert wird.

Dementsprechend sollte die Einstellungsbehörde sicherstellen, daß auch von der DGP die erforderlichen Maßnahmen zum Datenschutz und zur Datensicherung getroffen werden. Diese Problematik wird noch Gegenstand einer Erörterung mit dem Innenministerium sein.

5.12.4 Bewerbungs- und Personalfragebogen

Viele Personalverwaltungen verlangen bereits bei der Bewerbung um Einstellung in den öffentlichen Dienst – neben den üblichen Bewerbungsunterlagen – einen ausgefüllten Personalfragebogen. Nach meinem Eindruck wird bei dieser Verfahrensweise nicht zwischen erforderlicher Datenerhebung für die Entscheidung über Bewerbungen und derjenigen für die Einstellung unterschieden. Insbesondere wird häufig verkannt, daß das Fragerecht des Dienstherrn bzw. öffentlichen Arbeitgebers im Stadium der Bewerbung nicht so weit geht wie bei der beabsichtigten Einstellung.

Nach § 29 Abs. 1 Satz 1 DSG NW dürfen personenbezogene Daten nur erhoben werden, soweit sie zur Eingehung eines Dienst- oder Arbeitsverhältnisses erforderlich sind. An die Erforderlichkeit ist im Hinblick darauf, daß Personaldaten einer besonderen Geheimhaltung unterliegen, ein entsprechend strenger Maßstab anzulegen. Es reicht nicht aus, wenn die Kenntnis von personenbezogenen Daten bei der Personalauswahl und zur beabsichtigten Einstellung dienlich oder nützlich ist, vielmehr muß ihre Kenntnis unbedingt notwendig sein und unter Beachtung des verfassungsrechtlichen Grundsatzes der Verhältnismäßigkeit den Schutz des Persönlichkeitsrechts der Beschäftigten ausreichend berücksichtigen.

Für die verschiedenen Sparten des öffentlichen Dienstes sind daher bereichspezifische **Bewerbungsfragebogen** zu entwickeln und verbindlich einzuführen. In diese Fragebogen gehören keine Angaben, die erst später für Personalfragebogen, Personalbogen (auch Personalstammblätter) oder Besoldungsbogen benötigt werden. Vielmehr muß sich nach den genannten Grundsätzen die Erhebung der einzelnen Daten auf die Angaben beschränken, auf die es für die Entscheidung über die Bewerbung ankommt. Unzulässige Datenerhebungen sind z. B. Fragen nach Geburtsdatum und Vornamen des Ehegatten, dessen Beruf, Namen der Ehegatten aus früheren Ehen, Sozialversicherungsnummer, privater Krankenversicherung, Art und Höhe finanzieller Verpflichtungen und Schulden, Beruf von Vater und Mutter, Geburtsdaten und Vornamen der Kinder sowie deren Rechtsstellung. Grundsätzlich darf dem Bewerber keine Frage vorgelegt werden, auf die es entweder gar nicht oder erst in einem späteren Stadium des Einstellungsverfahrens oder sogar erst nach positiver Entscheidung über die Einstellung ankommt. Unzulässig ist daher die Frage nach krankheitsbedingten Ausfallzeiten in einer bisherigen Tätigkeit oder nach gesundheitlichen Dauerschäden bzw. schweren Krankheiten; dies ist allenfalls Sache des Amtsarztes bei der medizinischen Einstellungsuntersuchung. Ebenso haben Fragen nach Vorstrafen oder der Verfassungstreue im Bewerbungsfragebogen zu unterbleiben, da diese Angaben erst erforderlich werden, wenn die Einstellung beabsichtigt ist.

Die Frage nach einer **Schwangerschaft** im Bewerbungsfragebogen dürfte nach meiner Auffassung in der Regel auch dann unzulässig sein, wenn sich nur Frauen bewerben (anders Urteil des Bundesarbeitsgerichts vom 20.02.1986, 2 AR 244/85). Bewerben sich Frauen und Männer, so könnte in der Frage eine unzulässige Benachteiligung wegen des Geschlechts und damit ein Verstoß gegen Artikel 3 des Grundgesetzes zu sehen sein; bewerben sich nur Frauen, so könnte ein Verstoß gegen Artikel 6 des Grundgesetzes vorliegen. Die Frage kann allerdings erforderlich und zulässig sein, wenn der Einsatz einer Schwangeren auf der in Aussicht genommenen Stelle gegen mutterschutzrechtliche Bestimmungen verstoßen würde und ein vorübergehender anderer Einsatz nicht möglich ist. Bei Zeitverträgen darf nach der Schwangerschaft gefragt werden, wenn sie dazu führen würde, daß der Arbeitsplatz praktisch unbesetzt bliebe.

Bei Bewerbungen um Einstellung in besondere Bereiche des öffentlichen Dienstes (beispielsweise Justizvollzugsdienst, Sparkassen) können mehr oder auch weniger und andere Fragen erforderlich sein als bei einer Bewerbung um Einstellung in die allgemeine innere Verwaltung. Auch hier sollte von vornherein sorgfältig unterschieden werden zwischen Bewerbungsfragebogen, Personalfragebogen und Besoldungsfragebogen. Unter strikter Beachtung des Erforderlichkeitsgrundsatzes muß sichergestellt werden, daß keiner dieser Fragebogen im Falle der Einstellung automatisch zum **Personalbogen** (Vorblatt zur Personalakte Unterordner A) wird; dieser muß vielmehr gesondert angelegt werden. Zur schnellen Information mittels Personalbogen sind andere Angaben erforderlich, als sie z. B. in der Besoldungs- oder in der Beihilfeakte (z. B. Kontonummer) stehen müssen. Eine Erhebung von Gesundheitsdaten im zulässigen Umfang durch einen Personal**fragebogen** – um ein Beispiel aus meiner Überprüfungspraxis anzuführen – setzt voraus, daß diese besonders sensiblen Daten Dritten, die diese Daten nicht benötigen, nicht zugänglich gemacht werden. Sie müssen auch nicht bei jeder Personalsachbearbeitung zur Kenntnis genommen werden. Deshalb sollen derartige Angaben nicht im Personalbogen stehen, der als Bestandteil der Personalakte bei jedem Bearbeitungsvorgang einsehbar ist.

Förmlich beanstanden mußte ich die Erhebung des Familiennamens von **Adoptivkindern** im Personalbogen nach Anl. 2 der Richtlinien für die äußere Form und Gliederung der Personalakten in der allgemeinen und inneren Verwaltung (RdErl. des Innenministers vom 19.01.1965 – SMBl. NW. 203034), der im Geschäftsbereich des Innenministeriums verwandt wird.

Der Vordruck sah die Erhebung von Rufnamen und Geburtsdaten der Kinder sowie bei Adoptivkindern zusätzlich die Erhebung des Familiennamens vor. Dies stellt einen Verstoß gegen § 1758 Abs. 1 BGB dar. Nach dieser Vorschrift dürfen Tatsachen, die geeignet sind, die Annahme eines Kindes und ihre Umstände aufzudecken, ohne Zustimmung des Annehmenden und des Kindes nicht offenbart oder ausgeforscht werden, es sei denn, daß besondere Gründe des öffentlichen Interesses dies erfordern.

Das Innenministerium ist meiner Empfehlung, von der Erhebung des Familiennamens bei Adoptivkindern abzusehen, nicht gefolgt, weil es eine geson-

derte Änderung des Personalbogens vor der geplanten Neuregelung des gesamten Personalaktenrechts nicht für zweckmäßig hielt. Da jedoch der Zeitpunkt, zu dem die Änderung des Personalaktenrechts in Kraft treten soll, nicht absehbar ist und die weitere Erhebung und Speicherung des Familiennamens des Adoptivkindes nicht länger hinnehmbar war, mußte ich die Erhebung des Familiennamens des Adoptivkindes förmlich beanstanden. Das Innenministerium hat inzwischen die anderen Ressorts und die nachgeordneten Behörden darauf hingewiesen, daß die Angabe des Familiennamens bei Adoptivkindern nicht mit der Vorschrift des § 1758 BGB vereinbar ist und eine Änderung des Personalbogens angekündigt. Meiner Empfehlung an die Ressorts, auch die Löschung der unzulässigen Angaben zum Familiennamen bei Adoptivkindern nach § 19 Abs. 3 Satz 1 Buchstabe a DSG NW zu veranlassen, ist bisher nur das Kultusministerium gefolgt.

5.12.5 Personalnebenakten

Die in meinem 9. Tätigkeitsbericht (S. 78) kritisierte Praxis der Führung unzulässiger Personalnebenakten durch Vorgesetzte scheint in der öffentlichen Verwaltung weiter verbreitet zu sein, als ich befürchtet hatte. Im Berichtszeitraum haben sich mehrmals Beschäftigte des öffentlichen Dienstes darüber beschwert, daß neben der personalverwaltenden Stelle auch Vorgesetzte, beispielsweise Schulleiter, Institutsleiter an einer Universität, Klinikleiter oder die Pflegedienstleitung eines Kreiskrankenhauses zum Teil in erheblichem Umfang Datensammlungen über ihre Mitarbeiter führen.

Eine gesetzliche Grundlage, die dem Vorgesetzten das Recht zugesteht, personalaktengleiche Datensammlungen zu führen, ist nicht ersichtlich. Nach § 29 Abs. 1 Satz 1 DSG NW darf er lediglich die zu seiner Aufgabenerfüllung erforderlichen personenbezogenen Daten erheben, speichern und nutzen. Hierzu gehört zwar auch die Kenntnisnahme von personenbezogenen Daten der Mitarbeiter, soweit sie ihm über den Dienstweg zugänglich gemacht werden. Es muß aber gewährleistet sein, daß diese Daten nicht über die erforderliche Zeitdauer hinaus beim Vorgesetzten gespeichert bleiben. Insoweit erscheint mir die in vielen Verwaltungen übliche Praxis, Durchschriften von personalrechtlichen Entscheidungen auch für den Vorgesetzten zu fertigen, datenschutzrechtlich problematisch, weil diese Praxis dazu verführt, eine unzulässige Personalnebenakte anzulegen.

Zwar ist es beispielsweise zur Aufgabenerfüllung für den Vorgesetzten erforderlich, Kenntnis über die Abwesenheit seiner Mitarbeiter zu erhalten. Dagegen dürfte das Festhalten derartiger Daten über den Zeitraum der Abwesenheit hinaus grundsätzlich unzulässig sein. Es ist nicht Aufgabe des Vorgesetzten, über die unmittelbare Anwesenheitskontrolle hinaus etwa eine Jahresstatistik über die Fehlzeiten seiner Mitarbeiter zu führen. Weiterhin dürfte es zwar erforderlich sein, den Vorgesetzten über dienstrechtliche Verfügungen gegen seine Mitarbeiter zur Leistungs- bzw. Verhaltenskontrolle in Kenntnis zu setzen. Dagegen halte ich es für bedenklich, wenn der Vorgesetzte diese Kenntnisse in seinen Unterlagen festhält und ohne jede weitere Kontrolle speichert.

Nach meiner Erfahrung nutzen manche Dienststellenleiter, die nicht zugleich Dienstvorgesetzte der Angehörigen ihrer Dienststelle sind, sogenannte Personalfragebogen oder Personalstammblätter, wie sie von Verlagen bezogen werden können und eigentlich für die Anlage von Personalakten gedacht sind. Sie lassen diese Vordrucke ohne Einschränkung von ihren Mitarbeitern ausfüllen, um so an die für ihre Aufgabenerfüllung als Vorgesetzte vermeintlich erforderlichen Daten zu gelangen. Auf diese Weise werden in großem Umfang Daten erhoben, die für die Vorgesetzten zwar interessant oder nützlich sein können, für ihre Aufgabenerfüllung aber nicht unbedingt notwendig sind. Hierzu zählen etwa Angaben über Religionszugehörigkeit, Anzahl und Geburtsdaten der Kinder, Beruf der Ehefrau und ähnliche Daten, die den Vorgesetzten nichts angehen. Ich halte es für erforderlich, die Verarbeitung von Personaldaten durch Vorgesetzte in einer Dienstanweisung zu regeln.

Dementsprechend habe ich das Kultusministerium gebeten, im Schulbereich auch für die nicht automatisierte Datenverarbeitung durch den Schulleiter in einer Dienstanweisung zu regeln, welche Daten der Lehrkräfte wo und wielange von ihm gespeichert und genutzt werden dürfen. Nach meiner Auffassung ist eine solche Dienstanweisung aber auch in anderen Verwaltungsbereichen notwendig. Der Auffassung des Kultusministeriums, daß es nach dem in Nordrhein-Westfalen geltenden Personalaktenrecht „kein absolutes Verbot des Inhalts gibt, Abschriften oder Durchschriften von Personalakten in anderen Teilen der Verwaltung als bei der personalaktenführenden Dienststelle aufzubewahren, sofern dies für eine ordnungsgemäße Personalverwaltung zweckdienlich ist", kann ich nicht folgen. Zum einen ist nicht jeder Vorgesetzte gleichzeitig auch personalverwaltende Stelle, sondern nur derjenige, auf den personalrechtliche Entscheidungsbefugnisse delegiert sind, wie z. B. die Schulaufsichtsbeamten der Schulämter oder die Leiter der Finanzämter. Zum anderen reicht es nicht aus, wenn die Datenspeicherung nur zweckdienlich ist, sie muß erforderlich sein, denn nur dann ist sie auch zulässig. Nicht das Verbot des Umgangs mit personenbezogenen Daten bedarf einer Rechtfertigung, sondern der Umgang selbst.

In einem von mir zu kontrollierenden Fall hat die Pflegedienstleitung eines Kreiskrankenhauses im Zeitraum von fast zehn Jahren in erheblichem Umfang „Personalnebenakten" geführt, die nicht nur komplette Bewerbungsunterlagen, sondern auch Stellungnahmen zu Alkoholproblemen, handschriftliche Vermerke über die Eignung von Pflegekräften sowie Angaben über strafrechtliche Vorgänge enthielten. Diese völlig unzulässige Aktensammlung wurde nach ihrer Aufdeckung durch Kreisverwaltung und Personalrat auf meinen Rat hin nicht sofort vernichtet. Vielmehr wurden die Akten von einem hierzu besonders beauftragten Beamten unter Verschluß genommen und den Betroffenen Gelegenheit gegeben, zur Wahrung etwaiger Rechtsansprüche in **ihre** Akte einzusehen. Insoweit konnten die Betroffenen nach § 19 Abs. 2 Satz 1 Buchstabe b DSG NW zur Geltendmachung von Rechtsansprüchen eine Sperrung an Stelle der Löschung verlangen. Erst nach Ablauf der für die Einsichtnahme eingeräumten Frist wurden die Akten ordnungsgemäß vernichtet.

5.12.6 Einsichtnahme in die Personalakte

In einer Behörde wurde auch die Einsichtnahme in die Personalakte durch den Betroffenen selbst aktenkundig gemacht, indem ein entsprechender Vermerk zur Akte genommen wurde. Eine solche Dokumentation ist unzulässig, weil der Betroffene dadurch von der Wahrnehmung seines Einsichtsrechts abgehalten werden kann.

Demgegenüber halte ich es unter dem Gesichtspunkt der Transparenz der Datenverarbeitung für geboten, daß **jede** Einsichtnahme durch Personen, die mit der Personalsachbearbeitung befaßt sind, aber auch die Einsichtnahme durch deren Vorgesetzte oder durch Dritte innerhalb oder außerhalb der Behörde dokumentiert wird. Diese zugleich der Datensicherung dienende Dokumentation muß auf dem dafür vorgesehenen, der Personalakte vorgehefteten Aktenausgabeblatt (vgl. Anlage 1 zu Nr. 1.2 der Richtlinien über die äußere Form und die Gliederung der Personalakte in der allgemeinen und inneren Verwaltung (RdErl. des Innenministers vom 19.01.1965 – SMBl. NW. 203034) erfolgen.

In diesem Zusammenhang ist anzumerken, daß das Bundesarbeitsgericht (NJW 1988, 791) den Arbeitgeber auf Grund des verfassungsrechtlich gewährleisteten Persönlichkeitsschutzes für verpflichtet hält, für die vertrauliche Behandlung der Personalakten durch die Sachbearbeiter Sorge zu tragen, wie auch den Kreis der mit Personalakten befaßten Mitarbeiter möglichst eng zu halten. Sensible Daten, zu denen insbesondere auch solche über den körperlichen, geistigen und seelischen Gesundheitszustand und allgemeine Aussagen über die Persönlichkeit des Beschäftigten gehörten, bedürften des verstärkten Schutzes.

Das Innenministerium, dem ich empfohlen habe, im Zuge der Neuregelung des Personalaktenwesens auch eine Dokumentationspflicht für die Einsichtnahme in die Personalakte durch Dritte vorzusehen, hat sich meiner Auffassung nicht angeschlossen. Wegen der bereits bestehenden Regelungen hielt es eine weitergehende Kontrolle der Zugangsberechtigung zu den Personalakten nicht für erforderlich. Ich werde mich für eine Dokumentationspflicht, die im übrigen aus § 10 Abs. 3 i.V.m. Abs. 2 Nr. 6 DSG NW herzuleiten ist, im Rahmen der Novellierung der landesrechtlichen Vorschriften zum Personalaktenrecht weiterhin einsetzen.

5.12.7 Entfernung von Vorgängen aus der Personalakte

In mehreren Fällen ging es um die Frage, ob der Betroffene eine Entfernung von Unterlagen aus der Personalakte verlangen kann, wenn die Speicherung unzulässig oder zur Aufgabenerfüllung nicht mehr erforderlich ist und der Betroffene in unangemessener Weise beeinträchtigt wird (§ 19 Abs. 3 DSG NW). Einem solchen Anspruch wird immer noch entgegengehalten, daß in die Personalakte nach § 102 Abs. 1 Satz 1 Halbsatz 2 LBG alle den Beamten betreffenden Vorgänge mit Ausnahme der Prüfungsakten gehörten. In die Personalakte seien also sämtliche Vorgänge aufzunehmen, die in einem inneren Zusammenhang mit dem Beamtenverhältnis stünden. Der

Grundsatz der Kontinuität und Vollständigkeit von Personalakten gebiete ein lückenloses und chronologisches Festhalten sämtlicher beamtenrechtlich relevanter Vorgänge, um auch später jederzeit ein lückenloses Bild über die berufliche Entwicklung des jeweiligen Beamten gewinnen zu können.

Die Neuregelung im Personalaktenrecht läßt erwarten, daß der von Verwaltung und Rechtsprechung lange gehegte Grundsatz der Vollständigkeit und Lückenlosigkeit der Personalakte, der mit dem Recht auf informationelle Selbstbestimmung des Beamten jedenfalls in dieser Ausprägung nicht vereinbar ist, endlich durchbrochen wird (oben S. 20). Der Grundsatz kann nämlich zu einer Dokumentation sämtlicher Vorgänge eines Beamtenlebens führen, wie sie den Zielsetzungen eines historischen Archives entsprechen mag, aber nach Sinn und Zweck des beamtenrechtlichen Dienst- und Treueverhältnisses nicht erforderlich ist. Nach § 56 e des Entwurfes eines Neunten Gesetzes zur Änderung dienstrechtlicher Vorschriften (oben S. 19) müssen Unterlagen, die sich als unbegründet oder falsch erwiesen haben, unverzüglich aus der Personalakte entfernt und vernichtet werden. Ebenso sind Unterlagen, die für den Beamten ungünstig sind oder ihm nachteilig werden können, soweit sie u. a. für die nächste dienstliche Beurteilung nicht benötigt werden, nach drei Jahren aus der Personalakte zu entfernen. Dementsprechend müssen nach meiner Auffassung auch Unterlagen, deren Speicherung datenschutzrechtlich unzulässig war, unverzüglich aus der Personalakte entfernt werden.

In einem besonders problematischen Fall aus dem Bereich der Finanzverwaltung habe ich eine weitere Speicherung von sensiblen, den Betroffenen besonders belastenden Beihilfedaten in der Personalakte als Verstoß gegen Vorschriften über den Datenschutz angesehen. Die Daten standen in fachärztlichen Gutachten, die zu Zwecken der Beihilfegewährung angefertigt waren, und wurden unzulässigerweise vom Beihilfesachbearbeiter an die Personalverwaltung weitergegeben. Entgegen meiner Empfehlung sind diese Unterlagen zwar aus der Beihilfeakte entfernt, aber in einem verschlossenen Umschlag weiterhin bei der Personalakte aufbewahrt worden. Hierzu wurde die Auffassung vertreten, daß die Beihilfedaten zu Recht weitergegeben worden seien; u. a. wurde die Weitergabe auf § 29 Abs. 1 Satz 1 DSG NW gestützt, den ich hier allerdings nicht für anwendbar halte.

Unabhängig von der weiteren Auseinandersetzung in dieser Frage halte ich es auch für einen groben Verstoß gegen den Datenschutz, wenn der gesamte Vorgang über den Widerspruch, den der Betroffene gegen die Ablehnung seines Antrages auf Entfernung der unzulässig gespeicherten Beihilfedaten aus seiner Personalakte eingelegt hatte, in der Personalakte aufbewahrt wird, während sich die Beihilfedaten selbst in einem verschlossenen Umschlag bei der Personalakte befinden. Durch die Aufbewahrung der das Streitverfahren betreffenden Unterlagen in der Personalakte wird auf Kosten des Persönlichkeitsrechts des Betroffenen ein zwar lückenloses, aber im Ergebnis zwiespältiges Bild über den Betroffenen festgehalten, das ihn unverhältnismäßig belastet. In diesem Fall ist der Vorgang als Sachakte – wie bei anderen gegen beamtenrechtliche Entscheidungen gerichteten Verwaltungsverfahren auch – getrennt von der Personalakte aufzubewahren.

5.12.8 Datenweitergabe an den Personalrat

Mit Beschluß vom 1. Juli 1987 hatte der Bayerische Verwaltungsgerichtshof festgestellt, daß die Speicherung personenbezogener Daten von Beschäftigten in einem elektronischen Datenverarbeitungsgerät, das dem Personalrat von einem Personalratsmitglied zur Verfügung gestellt wurde, unzulässig ist. Im Hinblick auf diesen Beschluß hat mich das Innenministerium gebeten, unter datenschutzrechtlichen Gesichtspunkten zu prüfen, ob Personalratsmitglieder befugt sind, die ihnen in Listenform zur Verfügung gestellten Daten zu verarbeiten und wie sichergestellt werden kann, daß Informationen aus den Listen nicht an Dritte gelangen.

Ich habe keine Bedenken, wenn personenbezogene Daten, die Personalvertretungen zur Erfüllung ihrer Aufgaben im Rahmen des § 65 Abs. 1 des Landespersonalvertretungsgesetzes in Form einer aktuellen Liste erhalten haben, gespeichert, verändert und genutzt werden, wenn und solange eine solche Datenverarbeitung zur Aufgabenerfüllung nach dem Landespersonalvertretungsgesetz unbedingt notwendig ist. Beispielsweise halte ich die Übermittlung in Listenform zusammengestellter Daten der Beschäftigten mit den Angaben von Namen, Vorname, Geburtsjahr, abgeschlossene Berufsausbildung, Eintritt in den Vorbereitungsdienst, Ernennungsdaten, Abteilungs- oder Dezernatszugehörigkeit, Beurlaubung und Ermäßigung der Arbeitszeit bei Beamten bzw. Datum der letzten Eingruppierung, Vergütungs- oder Lohngruppe und Fallgruppe sowie feste Zulagen bei Arbeitnehmern für erforderlich und damit zulässig. Allerdings ist der Personalrat, soweit das Landespersonalvertretungsgesetz keine abschließenden datenschutzrechtlichen Regelungen trifft, den Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen unterworfen. Er hat daher das Gebot der Zweckbindung zu beachten und muß die Daten löschen, sobald deren Speicherung nicht mehr erforderlich ist. Außerdem ist er verpflichtet, für die von ihm geführten Dateien in einer Dateibeschreibung Einzelheiten der Datenverarbeitung festzulegen und die Beschreibung aller automatisiert geführten Dateien mit den Angaben der Dateibeschreibung dem Landesbeauftragten für den Datenschutz zur Aufnahme in das Dateienregister vorzulegen.

Die inzwischen ergangene Entscheidung des Bundesverwaltungsgerichts im o. g. Fall, nach der ein Speichern von personenbezogenen Daten, die anläßlich konkreter beteiligungspflichtiger Angelegenheiten weitergegeben werden, durch den Personalrat nur für das laufende Mitbestimmungsverfahren und nicht auf Dauer im automatisierten Verfahren zulässig ist (vgl. BVerwG, NJW 1991, 375), steht meiner Auffassung nicht entgegen, sondern stützt sie sogar. Denn das Gericht verweist ausdrücklich auf die Möglichkeit, dem Personalrat die jeweils erforderlichen Grunddaten in Form einer aktuellen Liste zu überlassen.

Darüber hinaus teile ich grundsätzlich die Bedenken des Bundesverwaltungsgerichts gegen eine auf Dauer angelegte – automatisierte oder nicht automatisierte – Speicherung von personenbezogenen Daten, die aus den zu konkreten Mitbestimmungsfällen vorgelegten Unterlagen oder deren Bekanntgabe erfaßt sind. Die damit zusammenhängenden weiteren Fragen

wie beispielsweise die Vernichtung der dem Personalrat vorgelegten Schreiben zur Durchführung konkreter Mitbestimmungsverfahren, Art und Dauer der Aufbewahrung von Tagesordnung und Protokoll, die Zugangsberechtigung der Personalratsmitglieder zu den Protokollen sowie die Aufbewahrung der den Personalratsmitgliedern übersandten Tagesordnungen, die bereits personenbezogene Daten enthalten, sollte der Gesetzgeber durch bereichspezifische datenschutzrechtliche Regelungen im Landespersonalvertretungsgesetz entscheiden (oben S. 28).

Was die Datensicherheit der beim Personalrat vorhandenen Daten betrifft, so ist neben der Personalvertretung auch der Leiter der Dienststelle für die Einhaltung der Vorschriften über den Datenschutz in seiner Dienststelle verantwortlich (§ 10 Abs. 1 DSG NW). Da der Personalrat Teil der Dienststelle ist, untersteht er grundsätzlich auch der Dienst- und Fachaufsicht des Leiters der Dienststelle. Die Aufsicht ist jedoch insoweit eingeschränkt, als der Personalrat in Erfüllung seiner personalvertretungsrechtlichen Aufgaben nicht an Weisungen und Aufträge gebunden ist (vgl. BVerfGE 51, 77, 87). Aus dieser Entscheidung läßt sich zwar ableiten, daß der Leiter der Dienststelle gegenüber dem Personalrat hinsichtlich der ihm durch das Landespersonalvertretungsgesetz übertragenen Aufgaben keine Kontrollkompetenz hat. Damit bleiben aber Kontrollbefugnisse, die diese Rechtspositionen nicht tangieren, unberührt.

Dies bedeutet, daß der Leiter der Dienststelle

- einer Organisationseinheit in seiner Dienststelle die Überprüfung von Art und Umfang der getroffenen Datensicherungsmaßnahmen übertragen muß (vgl. § 10 Abs. 2 Nr. 10 DSG NW);
- in einer Dienstanweisung die erforderlichen Datensicherungsmaßnahmen darzustellen und die zu kontrollierenden Anweisungen festzulegen hat, insbesondere beim Einsatz eines persönlichen Computers;
- darüber hinaus an den Besonderheiten einer Datenverarbeitung durch den Personalrat orientierte technische und organisatorische Maßnahmen prüfen muß;
- in die interne Kontrolle die Datenverarbeitung bei dem Personalrat einzubeziehen hat.

Bei Verwendung eines privaten persönlichen Computers wird der Personalrat den Anforderungen, die für eine Datei der öffentlichen Stelle zu gelten haben, kaum entsprechen (unten S. 147). Daher halte ich die Nutzung eines privaten persönlichen Computers durch Personalratsmitglieder oder den Personalratsvorsitzenden für unzulässig.

5.12.9 Datenweitergabe an Gleichstellungsbeauftragte

Auf Anfragen – insbesondere von Berufsverbänden – habe ich dargelegt, daß ein Recht der Gleichstellungsbeauftragten auf Einsichtnahme in Personalakten keine gesetzliche Grundlage findet. Weder § 102 des Landesbeamtengesetzes noch das Gesetz zur Förderung der beruflichen Chancen für

Frauen im öffentlichen Dienst enthält eine normenklare gesetzliche Regelung, die einen Eingriff in das Recht der Beschäftigten auf informationelle Selbstbestimmung insoweit zuläßt, als die Gleichstellungsbeauftragte auch ohne Einwilligung des Betroffenen Zugang zu dessen Personalakte erhalten soll.

Ebensowenig kann § 29 Abs. 1 Satz 1 DSG NW als Rechtsgrundlage für ein Einsichtsrecht der Gleichstellungsbeauftragten in Betracht kommen, da dem Anwendungsbereich dieser Vorschrift enge Grenzen gesetzt sind. Jedenfalls dürfte die Heranziehung von Personalakten durch die Gleichstellungsbeauftragte zur Feststellung gleichwertiger Qualifikation bei Beförderungen, Versetzungen und Umsetzungen einen anderen Verwendungszweck verfolgen als dies durch die gesetzliche Festlegung des Verwendungszweckes auf die Durchführung oder Abwicklung eines Dienst- oder Arbeitsverhältnisses oder Personalplanung und Personaleinsatz durch die Personalreferate geschehen ist.

Ein Akteneinsichtsrecht kann nach meiner Einschätzung auch nicht einfach dadurch begründet werden, daß die Gleichstellungsbeauftragte als eine mit der Bearbeitung von Personalangelegenheiten beauftragte Bedienstete ausgewiesen wird. Aus der Funktion der Gleichstellungsbeauftragten ergibt sich nicht zwangsläufig die Notwendigkeit, mit der Bearbeitung von Personalangelegenheiten befaßt zu sein. Viel eher scheint mir ihre Aufgabenstellung, insbesondere Ansprechpartnerin für alle Bediensteten in Fragen der Gleichstellung von Frau und Mann zu sein, für eine Funktionstrennung zu sprechen. Die Mitwirkung an Personalmaßnahmen stellt jedenfalls keine Bearbeitung von Personalangelegenheiten dar. Im übrigen reicht eine bloße organisatorische Zuordnung der Gleichstellungsbeauftragten zur Personalverwaltung wie auch eine Übertragung von Aufgaben der Personalverwaltung nicht aus, wenn ihr damit Befugnisse übertragen werden sollen, die die informationelle Selbstbestimmung der Beschäftigten berühren; hierzu bedürfte es einer gesetzlichen Grundlage. Nach Erörterung dieser Problematik im Innenministerium gehe ich davon aus, daß eine solche gesetzliche Grundlage geschaffen werden soll. Mit Erlaß vom 22. Mai 1990 hat das Innenministerium die Akteneinsicht wenigstens teilweise eingeschränkt und der Gleichstellungsbeauftragten insoweit lediglich ein Auskunftsrecht zugestanden.

5.12.10 Videoüberwachung

In einer Universität war geplant, verschiedene Bereiche durch Video-Überwachungsanlagen zu sichern. Im einzelnen handelte es sich um einen Klinikparkplatz, auf dem es zu Beeinträchtigungen durch vorschriftswidrig fahrende Kraftfahrer und unbefugte Nutzung kam, sowie um den Eingangsbereich zu den im Keller gelegenen Umkleideräumen für das Personal und um einen Küchenbereich, in dem größere Diebstähle vermutet wurden; in diesem Bereich wurde die Video-Überwachung verdeckt durchgeführt.

Gegen die Sicherungsmaßnahmen im Bereich des Parkplatzes und vor den Umkleideräumen hatte ich keine durchgreifenden datenschutzrechtlichen Bedenken, soweit die Maßnahme ausschließlich zum Schutz der Beschäftigten und zum Schutz der Einrichtungen gegen unbefugten Zutritt erfolgen

sollte. Ich habe den Verwaltungsdirektor allerdings gebeten, in einer Dienstanweisung klare Regelungen über den Zweck der Überwachung, die Dauer der Speicherung der Videobänder, deren sichere Verwahrung, die Berechtigung des Zugangs zu den Bandaufnahmen sowie die Kontrolle der Einhaltung dieser Regelungen zu treffen. Außerdem habe ich ihn gebeten, ungeachtet einer etwaigen Beteiligung des Personalrates nach dem Landespersonalvertretungsgesetz auch die Beschäftigten über die Einrichtung der Video-Überwachungen zu informieren.

Die versteckte Installation von Videokameras im Küchenbereich war dagegen geeignet, zumindest einen Teil der dort Beschäftigten ständig zu überwachen. Eine derartige arbeitsplatzbezogene Überwachung ohne Kenntnis der Beschäftigten stellt einen schwerwiegenden Eingriff in das Recht der Beschäftigten auf informationelle Selbstbestimmung sowie in ihr Grundrecht auf Datenschutz dar, der einer normenklaren gesetzlichen Grundlage bedarf.

Eine solche Rechtsgrundlage ist nicht ersichtlich. Auch nach der allenfalls in Betracht zu ziehenden Vorschrift über die Verarbeitung von Personaldaten (§ 29 Abs. 1 DSG NW) wäre eine versteckte Überwachung der Beschäftigten nicht zulässig. Danach dürfen nur Daten von Beschäftigten erhoben und gespeichert 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. Weder diente die versteckte Überwachung den genannten Zwecken, noch war sie erforderlich.

Ich habe allerdings auch erhebliche Zweifel daran, daß eine Überwachung durch offen montierte Videokameras in diesem Falle zulässig gewesen wäre. Im Hinblick auf die mit der ständigen Beobachtung der Beschäftigten am Arbeitsplatz verbundene permanente Kontrolle ist von einer nachhaltigen Beeinträchtigung der Beschäftigten auszugehen, so daß eine solche Maßnahme unverhältnismäßig wäre. Gegenüber derartigen Eingriffen in das Persönlichkeitsrecht der Beschäftigten überwiegt in diesem Fall nicht das schutzwürdige Interesse des Arbeitgebers an der Verhinderung weiterer Diebstähle im Küchenbereich, zumal nicht auszuschließen war, daß die vermißten Gegenstände auch außerhalb des Küchenbereichs abhanden gekommen sein konnten.

In einem anderen Fall hat ein Schulträger in Turnhallen Videokameras sichtbar angebracht, um Diebstähle und Beschädigungen von Sportgeräten zu verhindern. Auch dies halte ich für problematisch, weil dadurch die Verhaltensweisen der Schüler und der Lehrer, die die Aufsichtspflicht wahrnehmen, ständiger Beobachtung unterliegen. Deshalb ist unter Berücksichtigung des verfassungsrechtlichen Grundsatzes der Verhältnismäßigkeit besonders zu prüfen, ob die Installation von Videokameras das zur Abhilfe allein geeignete und erforderliche Mittel darstellt, dem dann die schutzwürdigen Interessen der Schüler und Lehrer unterzuordnen wären. Darüber hinaus muß für den Fall einer Aufzeichnung sichergestellt sein, daß die Videoaufnahmen nur zu dem festgelegten Zweck genutzt werden können, nur für eine bestimmte Dauer gespeichert und sicher verwahrt werden sowie nur den berechtigten

Personen zugänglich sind. Dazu gehört im übrigen auch die Bestimmung darüber, wer die Einhaltung dieser Regelungen zu kontrollieren hat.

5.12.11 Übermittlung an private Versicherungen

Seit Jahren treten Beamtenanwärter – insbesondere Lehramtsanwärter, aber auch solche aus anderen Bereichen – und Berufsanfänger im öffentlichen Dienst an mich heran und beklagen, daß ihre Personaldaten ohne ihre Einwilligung an private Versicherungsunternehmen weitergegeben werden. In allen Fällen erhielten die Betroffenen, noch bevor sie selbst über die bevorstehende Einstellung in den Vorbereitungsdienst unterrichtet worden waren, entweder Werbematerial mit unmittelbarem Bezug auf die Einstellung in den öffentlichen Dienst oder direkten Vertreterbesuch einer Versicherung. Hierüber habe ich zuletzt in meinem 7. Tätigkeitsbericht (S. 97) berichtet.

Aus den mir vorliegenden Unterlagen ergibt sich, daß Versicherungen über Anschriften und Angaben zur Berufslaufbahn der Betroffenen verfügen, die aus dem Datenbestand der öffentlichen Stellen stammen. Auf Grund der Vielzahl der Eingaben muß ich davon ausgehen, daß personenbezogene Daten von Berufsanfängern landesweit von Bediensteten öffentlicher Stellen an Versicherungen weitergegeben werden. Dabei liegt die Annahme nahe, daß dies vielfach aus Bereicherungsgründen geschieht.

Soweit diese Taten nicht nach anderen Vorschriften mit Strafe bedroht sind, können sie den Straftatbestand des § 33 Abs. 1 Satz 1 DSG NW erfüllen. Wer danach gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern, entgegen den Vorschriften des Datenschutzgesetzes Daten, die nicht offenkundig sind, zweckwidrig verwendet, weitergibt oder sich verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Für Mitarbeiter der Versicherungsunternehmen bedeutet dies, daß auch sie möglicherweise eine Straftat begehen oder sich an einer solchen beteiligen.

Alle Bemühungen in der Vergangenheit, die Vorfälle aufzuklären, waren mit geringen Ausnahmen bisher erfolglos. Es scheint weiterhin gängige Praxis zu sein, daß zu jedem Einstellungstermin die personenbezogenen Daten der Bewerber an private Versicherungsunternehmen fließen und durch deren Versicherungsvertreter zur Geschäftsanbahnung genutzt werden.

Ich halte diesen Zustand einer ständig wiederkehrenden Verletzung von Datenschutzvorschriften in bestimmten Aufgabenbereichen für untragbar und habe daher dem Innenministerium folgende Vorschläge zur Sicherstellung des Schutzes der Daten von Berufsanfängern im öffentlichen Dienst unterbreitet:

- Die Versicherungsunternehmen als Nutznießer solcher Straftaten sollten darauf aufmerksam gemacht werden, daß sich ihre Mitarbeiter, die Daten aus derartigen Quellen beziehen, möglicherweise selbst strafbar machen. Es sollte eingehend geprüft werden, ob die Gewinnung neuer Versicherungsnehmer auf Grund eines aus Straftaten gewonnenen Adreßmaterials nicht auch ein Fall zur Einschaltung der Versicherungsaufsicht ist.

- Den Berufsanfängern im öffentlichen Dienst sollte mit den Bewerbungsunterlagen ein schriftlicher Hinweis übersandt werden. Darin sollte dargelegt werden, daß sie im zeitlichen Zusammenhang mit dem Einstellungsverfahren möglicherweise von Versicherungsvertretern angesprochen werden. Es sei nach bisherigen Erfahrungen nicht auszuschließen, daß ihre Daten über Straftaten in den Besitz der Versicherung gelangt seien. Um solche Straftaten nicht zu belohnen, solle daher der Versicherungsvertreter genau befragt werden, aus welcher Quelle die Anschriften und die Angaben zum beruflichen Status jeweils stammten. Im Zweifel sollte der Fall zur Abklärung an die Staatsanwaltschaft gemeldet werden.
- Den mit der Verarbeitung von Personaldaten betrauten öffentlichen Bediensteten ist deutlich zu machen, daß die Weitergabe derartiger Angaben unter den Voraussetzungen des § 33 DSG NW kein „Kavaliersdelikt", sondern eine Straftat und ein schwerwiegender Verstoß gegen Datenschutzvorschriften ist.

Ich habe das Innenministerium darum gebeten, die anderen betroffenen Ressorts entsprechend zu unterrichten.

5.13 Statistik

5.13.1 Anonymisierung

Gegenstand meiner Prüfung war eine interessante, in ihrer Zielsetzung begrüßenswerte wissenschaftliche Untersuchung zur Zuverlässigkeit der faktischen Anonymisierung. Eine Universität beabsichtigte, durch Simulationsexperimente die wichtigsten Gefährdungssituationen für eine potentielle Deanonymisierung zu überprüfen, die sich bei Lieferung von anonymisierten Einzelangaben aus der amtlichen Statistik für die wissenschaftliche Forschung, insbesondere im Hinblick auf verfügbares Zusatzwissen ergeben kann. Dies sollte an Hand von zwei unterschiedlichen Datensätzen mit aus dem Mikrozensus 1987 in Nordrhein-Westfalen gewonnenen Einzelangaben und Daten, über die die Sozialwissenschaftler auf Grund eigener Untersuchungen verfügten, sowie unter Zuhilfenahme von Informationen aus Handbüchern näher untersucht werden.

Aus datenschutzrechtlichen Erwägungen war vorgesehen, die Datensätze aus der Mikrozensuserhebung unterschiedlich zu sortieren und mit unterschiedlichen Ordnungsnummern zu versehen. Eine tatsächliche Zuordnung von Datensätzen zu bestimmten Personen sollte nicht stattfinden. Sichergestellt werden sollte dies dadurch, daß das Landesamt für Datenverarbeitung und Statistik einen Treuhänder einsetzte, der ohne Kenntnis der Einzelangaben feststellen sollte, ob eine Zuordnung der übermittelten Datensätze zu einer bestimmten, ihm namentlich jedoch nicht bekannten Person, gelungen war.

An die Durchführung des Vorhabens wurde die Erwartung geknüpft, Erkenntnisse über die Zuverlässigkeit einer faktischen Anonymisierung zu gewinnen und dabei herauszufinden, ob die Voraussetzung des § 16 Abs. 6

des Bundesstatistikgesetzes für eine Übermittlung von Statistikdaten für wissenschaftliche Zwecke erfüllt werden kann.

Unter der Voraussetzung, daß entsprechend der vorgesehenen Konzeption verfahren wurde, bestanden gegen das Vorhaben keine durchgreifenden datenschutzrechtlichen Bedenken.

5.13.2 Übermittlung von Daten aus der Volkszählung 1987

Eine Übermittlung von Daten aus der Volkszählung 1987 an Dritte, Unternehmen oder sonstige Interessenten ist nach einhelliger Auffassung der Datenschutzbeauftragten des Bundes und der Länder nur in anonymisierter Form zulässig. Dabei kann von einer (faktischen) Anonymisierung dann ausgegangen werden, wenn die Einzelangaben nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft den in der Volkszählung Befragten zugeordnet werden können (vgl. § 16 Abs. 6 des Bundesstatistikgesetzes). Bei der Aggregierung von Einzelangaben nach § 15 Abs. 4 Satz 4 des Volkszählungsgesetzes (VZG) durch das von den Statistischen Landesämtern entwickelte Blockprogramm, das Dritten zur Verfügung gestellt werden soll, ist deshalb sicherzustellen, daß es nur zur Weitergabe und Veröffentlichung bestimmte Merkmale enthält. Dabei ist auch zu berücksichtigen, daß Zusatzwissen in Form von Gemeindelisten, Straßenschlüsseln und Blockbeschreibungen vorhanden ist, das sich der Empfänger beschaffen kann. Soweit dies nicht ausgeschlossen werden kann, muß geprüft werden, ob eine Übermittlung von Merkmalen bezogen auf die Blockseitenebene zulässig ist, oder ob nur Merkmale, die zu einer höheren Einheit zusammengefaßt sind, weitergegeben werden dürfen (vgl. § 15 Abs. 4 Satz 5 VZG).

5.13.3 Statistikdienststellen

Anfragen entnehme ich, daß insbesondere in den Statistikdienststellen kleinerer Gemeinden Schwierigkeiten dadurch auftreten, daß das Gebot der personellen Abschottung einen Einsatz der Mitarbeiter in anderen Verwaltungsbereichen ausschließt. Vielfach üblich, aber datenschutzrechtlich besonders bedenklich ist der Einsatz von Mitarbeitern in Statistikdienststellen bei Wahlen. Manche Gemeinden helfen sich so, daß sie dabei nur solche Mitarbeiter der Statistikdienststelle einsetzen, die dort ausschließlich mit aggregierten Daten arbeiten. Einen solchen Einsatz würde ich nicht beanstanden.

5.13.4 Mikrozensus

Der im Berichtszeitraum in ausgewählten Bezirken von Nordrhein-Westfalen durchgeführte Mikrozensus, der einen gegenüber der Volkszählung wesentlich umfangreicheren Fragenkatalog aufwies, hat zwar zahlreiche Anfragen bei mir ausgelöst; zu nennenswerten datenschutzrechtlichen Pannen bei der Durchführung ist es jedoch nicht gekommen. Die Anfragen basierten hauptsächlich auf mangelnder Sensibilität einzelner Interviewer, aber auch auf der Überforderung der Befragten: In dem umfangreichen Informationsmaterial waren für die Befragten wesentliche Hinweise nur schwer erkenn-

bar; dies wurde besonders deutlich bei den Unsicherheiten der Betroffenen hinsichtlich der verschiedenen Möglichkeiten, der Auskunftspflicht nachzukommen. Im Hinblick auf das Transparenzgebot und die daraus folgende Unterrichtungspflicht halte ich es für erforderlich, die Betroffenen bei künftigen Erhebungen deutlicher (z. B. durch drucktechnische Hervorhebung) auf ihre Rechte und Pflichten hinzuweisen.

5.14 Wissenschaft und Forschung

5.14.1 Nachweis der Prüfungsunfähigkeit

Welche Angaben ein **ärztliches Attest** enthalten muß, das die Prüfungsunfähigkeit eines Prüfungskandidaten bescheinigen soll, wird von den Hochschulen des Landes unterschiedlich beurteilt. Während ein Teil der Hochschulen ein einfaches ärztliches Attest als Nachweis der Prüfungsunfähigkeit akzeptiert, verlangen andere von dem jeweils behandelnden Arzt detaillierte Angaben zur Erkrankung des Prüfungskandidaten. Es begegnet nach meiner Auffassung datenschutzrechtlichen Bedenken, soweit Angaben gefordert werden, die für die Entscheidung des Prüfungsausschusses, ob eine Prüfungsunfähigkeit als Grund für den Rücktritt oder das Versäumnis anerkannt werden kann, nicht erforderlich sind.

Hierzu liegt mir ein von einer Universität entwickelter Vordruck „Ärztliches Attest zur Vorlage beim Prüfungsausschuß" vor, welcher von dem behandelnden Arzt auszufüllen ist. Das Erheben von Angaben, wie sie in diesem Vordruck erfragt werden, umfaßt auch sensible Gesundheitsdaten wie z. B. die Bezeichnung der Krankheit (Diagnose) und die Darstellung der krankheitsbedingten Beeinträchtigung.

Nach der mir vorliegenden Diplomprüfungsordnung für einen Studiengang der betreffenden Universität, die sich als Universitätssatzung auf § 91 des Gesetzes über die wissenschaftlichen Hochschulen des Landes Nordrhein-Westfalen stützt, ist in § 8 Abs. 2 bestimmt, daß die für den Rücktritt oder das Versäumnis geltend gemachten Gründe dem Prüfungsausschuß unverzüglich schriftlich angezeigt und glaubhaft gemacht werden müssen. Bei Krankheit des Kandidaten kann nach dieser Vorschrift die Vorlage eines ärztlichen Attestes verlangt werden. Entsprechende Regelungen sehen auch die mir aus Urteilen des Verwaltungsgerichts Düsseldorf bekannten Prüfungsordnungen anderer Universitäten vor. Diese Prüfungsordnungen verlangen weder die Bezeichnung der Krankheit noch die Darstellung der krankheitsbedingten Beeinträchtigung.

Nach § 8 Abs. 2 der Diplomprüfungsordnung obliegt also den Kandidaten, die Gründe für den Rücktritt oder das Versäumnis glaubhaft darzulegen und auf Verlangen ein ärztliches Attest vorzulegen. Dies bedeutet aus datenschutzrechtlicher Sicht, daß nicht in allen Fällen eines Prüfungsrücktritts oder eines Versäumnisses ein ärztliches Attest verlangt werden darf. Außerdem darf nach meiner Auffassung das ärztliche Attest nur diejenigen Angaben enthalten, die für die Anerkennung der Gründe unbedingt erforderlich sind. Danach kann es erforderlich, aber in den meisten Fällen auch ausrei-

chend sein, wenn aus ärztlicher Sicht bestätigt wird, daß der Prüfungskandidat zur Zeit der Prüfung bzw. für die Zeit der vorgesehenen Prüfungstermine auf Grund körperlicher oder geistiger Beeinträchtigungen in seiner Prüfungsfähigkeit erheblich eingeschränkt war oder ist.

Die Prüfungsbehörden sind allenfalls dann berechtigt, vom Prüfungskandidaten die Offenlegung seiner Krankheitsdaten zu verlangen, wenn im Einzelfall Zweifel bestehen. Ich halte deshalb den von der betreffenden Universität entwickelten Vordruck für datenschutzrechtlich bedenklich, wenn er in allen Fällen eines Rücktritts von der Prüfung oder des Versäumnisses eines Prüfungstermines vorgelegt werden muß.

Wegen der grundsätzlichen Bedeutung der Angelegenheit habe ich das Ministerium für Wissenschaft und Forschung des Landes Nordrhein-Westfalen um Stellungnahme zu der Problematik gebeten. Es hat sich meiner Auffassung insoweit angeschlossen, als die Forderung nach Bekanntgabe der Diagnose im ärztlichen Attest unzulässig ist. Die regelmäßige Vorlage eines ärztlichen Attestes mit Angaben über krankheitsbedingte Beeinträchtigungen (Krankheitssymptome) wird dagegen in allen Fällen einer Prüfungsunfähigkeit für notwendig erachtet. Schon im Hinblick auf die Rechtslage – Regelung in den Diplomprüfungsordnungen sowie das Fehlen einer weitergehenden Ermächtigung – kann ich dieser Ansicht nicht folgen. Ich werde daher dem Ministerium empfehlen, darauf hinzuwirken, daß ein ärztliches Attest nicht in allen Fällen und weitere Angaben über krankheitsbedingte Beeinträchtigungen der Prüfungsfähigkeit durch den Arzt nur in Zweifelsfällen verlangt werden.

5.14.2 Akteneinsicht zu Forschungszwecken

Verschiedene Forschungsvorhaben mit besonderen Eingriffen in das Recht der Betroffenen auf informationelle Selbstbestimmung ließen im Berichtszeitraum die Problematik der Anwendbarkeit des § 28 Abs. 2 DSG NW, wie ich sie bereits in meinem 9. Tätigkeitsbericht (S. 19) dargestellt habe, deutlich werden. Ich halte an meiner Auffassung fest, daß in bestimmten Bereichen, in denen Forschungsvorhaben eine besondere Eingriffstiefe aufweisen, erst spezialgesetzliche Forschungsklauseln eine Ermächtigung zur Durchführung der Forschungsvorhaben schaffen können. Anderenfalls dürfen die mit solchen Forschungsvorhaben verbundenen Datenverarbeitungen nur mit Einwilligung der Betroffenen durchgeführt werden.

Im Rahmen des vom Bundesminister für Jugend, Familie, Frauen und Gesundheit in Auftrag gegebenen Forschungsvorhabens „Ursachen von **Ehescheidungen** in der Bundesrepublik Deutschland" sollten Akten von Scheidungsverfahren, die im Jahre 1983 von nordrhein-westfälischen Familiengerichten erledigt worden sind, analysiert werden. Das Justizministerium des Landes Nordrhein-Westfalen hat Wissenschaftlerinnen der Freien Universität Berlin Einsicht in die nach dem Zufallsprinzip ausgewählten Verfahrensakten gewährt und eine Datenübermittlung ohne Einwilligung der Betroffenen nach § 28 Abs. 2 Satz 1 Buchstabe c DSG NW als zulässig erachtet, da eine Einholung der Einwilligung den Forschungszweck gefährdet hätte. Die Gefährdung habe sich aus einer bei Verweigerung der Einwilligung bedingten Verände-

rung der Stichprobe – 480 aus 2 038 ausgewählten Akten – und der damit verbundenen Verzerrung des Aussagewerts hinsichtlich der sozialen Schichtung wie auch der zur Scheidung führenden Konfliktsituation ergeben. Aller Wahrscheinlichkeit nach wäre die Einwilligung nur von solchen Betroffenen erteilt worden, die auf Grund ihres sozialen Status Verständnis für das Forschungsvorhaben aufgebracht hätten. Oder sie wäre von Betroffenen verweigert worden, bei denen Härtegründe wie z. B. Gewalt oder Alkoholmißbrauch zur Scheidung geführt hätten. Daneben wäre – zumindest für einen Teil der Betroffenen – den Ehepartnern, die aus Härtegründen geschieden worden seien, eine Konfrontation mit dem Scheidungsfall nach Jahren kaum zumutbar gewesen.

In den zur Durchführung der Aktenanalyse benutzten Erhebungsbogen wurden Daten zur ökonomischen und sozialfamiliären Situation der Ehegatten vor der Scheidung, zur sozioökonomischen Situation durch das Scheidungsverfahren sowie zu den die Scheidung herbeiführenden besonderen Härtegründen u.a. Alkoholismus, Gewalttätigkeit, eheliche Untreue und Impotenz, also Angaben aus dem intimsten Bereich der Privatsphäre, erhoben und gespeichert. Hierzu vertrat ich entsprechend meinen Ausführungen im 9. Tätigkeitsbericht (S. 19/20) die Auffassung, daß § 28 DSG NW mit seiner allgemein gehaltenen Datenschutzregelung für Forschungsvorhaben in Bereichen mit einer besonderen Eingriffsintensität nicht anwendbar ist. Deshalb konnte das Forschungsvorhaben nur dann ohne Einwilligung der Betroffenen durchgeführt werden, wenn dies eine bereichspezifische Regelung – in der Zivilprozeßordnung – zugelassen hätte.

Auch für eine Übergangszeit bis zum Erlaß einer bereichspezifischen Regelung konnte die Durchführung eines solchen Forschungsvorhabens ohne Einwilligung der Betroffenen nicht hingenommen werden. Unter Anlegung eines besonders strengen Maßstabes an die Zulässigkeit eines Vorhabens auf der Grundlage eines Übergangsbonus wog der Eingriff in die Persönlichkeitsrechte der Betroffenen schwerer als die Nachteile, die für die Durchführung dieses Forschungsvorhabens durch die Einholung der Einwilligung entstanden wären. In diesen Fällen muß eben der Gesetzgeber durch eine spezifische Erlaubnisnorm unter Beachtung des Verhältnismäßigkeitsgrundsatzes das informationelle Selbstbestimmungsrecht der Betroffenen insoweit einschränken.

Im übrigen war wegen der im Erhebungsbogen angegebenen allgemeinen Kennzeichen, wie Angaben des Familiengerichts im Landgerichtsbezirk, des Datums des Urteils, der Daten von Eheschließung und Ehescheidung sowie der Geburtsdaten der Eheleute höchst zweifelhaft, ob nach Auswertung der Akten davon ausgegangen werden konnte, daß im weiteren Verlauf der Datenverarbeitung im Rahmen des Forschungsvorhabens kein Personenbezug mehr gegeben war. Mit der Speicherung derart vieler persönlicher Angaben würde auch bei Verarbeitung der Daten ohne Namen der Betroffenen ihre Bestimmbarkeit in nicht seltenen Fällen möglich sein.

Bei diesen Forschungsvorhaben zeigt sich im übrigen, daß § 28 Abs. 2 DSG NW zur Lösung der besonderen datenschutzrechtlichen Problematik ungeeignet ist. Die Unzumutbarkeit der Einwilligung und die Gefährdung des For-

schungszweckes wegen fehlender Einwilligungen sind gerade bei solchen Forschungsvorhaben mit besonderer Eingriffsintensität anzunehmen, so daß regelmäßig in allen diesen Fällen die Voraussetzung des § 28 Abs. 2 Satz 1 Buchstaben b oder c DSG NW als gegeben angesehen werden müßten. Dadurch wäre aber Sinn und Zweck dieser Vorschrift, das Recht der Betroffenen auf informationelle Selbstbestimmung und ihr Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung zu gewährleisten, in das Gegenteil verkehrt.

In einem hinsichtlich seiner Eingriffstiefe noch problematischeren Forschungsvorhaben wurden die Akten sämtlicher in einem Amtsgerichtsbezirk geführten **Vormundschaften** (400 Fälle) und **Pflegschaften** (1 300 Fälle) von der Forschungsgruppe einer Fachhochschule eingesehen. Dieser Forschungsgruppe gehörten auch Studenten an. Die Erhebungsbogen enthielten u. a. eine Vielzahl von persönlichen Angaben über die psycho-soziale Situation der Betreuten, von der körperlichen Befindlichkeit über Suchtverhalten und soziale Auffälligkeiten bis zum sozio-kulturellen Verhalten sowie ihrer religiösen Einbindung. Auch hier habe ich die Gewährung der Akteneinsicht durch das Justizministerium wegen fehlender bereichspezifischer Ermächtigungsnorm als unzulässig angesehen. Selbst unter Anwendung der Grundsätze des Übergangsbonus konnte die Akteneinsicht nicht ohne Einwilligung der Betroffenen gewährt werden, da es bei diesem Vorhaben offensichtlich möglich war, die Einwilligung des Vormundes oder Pflegers, soweit sich dessen Wirkungskreis auf die Personensorge erstreckte, einzuholen. Da für das Forschungsvorhaben auch die personenbezogenen Daten des Vormunds oder Pflegers erhoben wurden, mußte ohnehin dessen Einwilligung eingeholt werden. Mit dem Recht zur Personensorge hatte nach meiner Auffassung der Vormund oder Pfleger auch in dem ihm übertragenen Bereich das Entscheidungsrecht, ob er für die Daten seines Mündels bzw. Pfleglings dessen Recht auf informationelle Selbstbestimmung zu Gunsten der Durchführung des Forschungsvorhabens zurückstellen wollte. Darüber hinaus war bei den von Sozialämtern geführten Vormundschaften oder Pflegschaften zu berücksichtigen, daß die in den Akten des Vormundschaftsgerichts enthaltenen Daten nach § 78 Satz 2 des Zehnten Buches des Sozialgesetzbuchs (SGB X) auch dem Sozialgeheimnis unterliegen. Nach § 75 Abs. 1 Satz 2 SGB X durften die Sozialdaten nur mit Einwilligung offenbart werden, da die Einholung der Einwilligung nach dem Vorstehenden zumutbar war.

Das Justizministerium kam zwar gegenüber meinen Bedenken zu der grundsätzlichen Bewertung der Forschungsklausel des § 28 DSG NW zu dem Ergebnis, daß die Datenverarbeitung zu Forschungszwecken ohne Einwilligung des Betroffenen unter den Voraussetzungen des § 28 Abs. 2 Satz 1 DSG NW nur selten zulässig ist. Es erkannte auch die Notwendigkeit bereichspezifischer Regelungen für besonders sensible Bereiche an, hat dies aber nur als gesetzgeberisches Programm für die Zukunft verstanden. Außerdem war nach seiner Auffassung die Eingriffstiefe nicht am Grad der Sensibilität der Daten, sondern an den mit der Datenverarbeitung verbundenen Nachteilen für den Betroffenen zu messen. Nachteile wären dann besonders gering einzuschätzen, wenn das Forschungsinteresse die betroffe-

nen Personen nur beiläufig zur Kenntnis nehmen würde und aus dieser Kenntnis keine diese Personen berührenden Konsequenzen gezogen würden. Damit wurde bei beiden Forschungsvorhaben das öffentliche Interesse an der Durchführung der Forschungsprojekte höher als das Geheimhaltungsinteresse der Betroffenen eingeschätzt, insbesondere weil die Angaben der Betroffenen bereits bei der Erfassung der Daten in den Erhebungsbogen anonymisiert würden und damit eine Beeinträchtigung schutzwürdiger Belange zu verneinen wäre.

Dieser Auffassung konnte ich mich nicht anschließen, da sie im Ergebnis zu einer weniger restriktiven Interpretation des § 28 Abs. 2 DSG NW führte. Außerdem sah ich mich durch die Stellungnahme der Landesregierung zu meinen Ausführungen im 9. Tätigkeitsbericht (S. 19) vielmehr darin bestärkt, daß in diesen Bereichen nur bereichspezifische Lösungen möglich und dringend erforderlich sind.

Demgegenüber hatte ich bei einem weiteren Forschungsvorhaben, das die polizeiliche Bearbeitung von **Insolvenzkriminalität** untersuchte und als Ergebnis wesentliche Hinweise zu Effizienzsteigerung, Vereinheitlichung und Vereinfachung der polizeilichen und staatsanwaltschaftlichen Ermittlungstätigkeit bringen sollte, im Hinblick auf die mit dem Regierungsentwurf des Strafverfahrensänderungsgesetzes 1989 verfolgte Absicht einer bereichspezifischen Regelung eine Akteneinsicht in die Verfahrensakten abgeschlossener strafrechtlicher Verfahren nach den Grundsätzen des Übergangsbonus für die Zeit bis zum Inkrafttreten dieser Vorschrift als zulässig erachtet. Aus denselben Gründen war auch das Forschungsvorhaben zur polizeilichen Bearbeitung von **Umweltdelikten** nach meiner Auffassung zulässig. Nach dem Ablauf der Legislaturperiode des 11. Deutschen Bundestages, in der das Strafverfahrensänderungsgesetz nicht mehr verabschiedet worden ist, habe ich allerdings gegen eine fortdauernde Anwendung des Übergangsbonus in diesen Fällen erhebliche Bedenken.

5.15 Schule

5.15.1 Lehrerdaten

Zu der Frage, in welchem Umfang personenbezogene Daten von Lehrern an den **Schulträger** übermittelt werden dürfen, habe ich zuletzt in meinem 9. Tätigkeitsbericht (S. 93) Stellung genommen. Über diese Problematik habe ich ein Gespräch mit dem Kultusministerium und den kommunalen Spitzenverbänden geführt. Dabei wurde nochmals darauf hingewiesen, daß gegen eine auf Dauer angelegte Sammlung personenbezogener Daten von Lehrern beim Schulträger (Schulverwaltungsamt) datenschutzrechtliche Bedenken bestehen, da eine gesetzliche Grundlage hierfür nicht ersichtlich ist. Die Gesprächsteilnehmer waren sich jedoch einig, daß der Schulträger im Rahmen eines Verfahrens nach § 23 des Schulverwaltungsgesetzes (SchVG) – Einstellung, Beförderung und Versetzung von Lehrern – personenbezogene Daten von Lehrern in dem hierfür erforderlichen Umfang und für eine bestimmte Zeitspanne verarbeiten darf. Dazu gehört auch die Dokumentation der in diesem Verfahren geführten Beratungen kommunaler Gremien und der dort ge-

faßten Beschlüsse. Außerdem muß nach Beendigung des Beteiligungsverfahrens nach § 23 SchVG eine angemessene Nachlauffrist zugestanden werden, soweit mit gerichtlicher Anfechtung der getroffenen Entscheidung oder ähnlichem zu rechnen ist. Im übrigen gilt nach Abschluß des Verfahrens das Löschungsgebot des § 19 Abs. 3 DSG NW. Die Vertreter der kommunalen Spitzenverbände haben ihre Mitglieder auf diese Grundsätze hingewiesen. Wie sich die Anwendung in der Praxis darstellt, bleibt abzuwarten.

Wiederholt mußte ich mich auch in diesem Berichtszeitraum mit der Frage beschäftigen, welche Lehrerdaten der **Schulleiter** speichern darf. Nach meiner Auffassung ist davon auszugehen, daß der Schulleiter Vorgesetzter aller Lehrer seiner Schule, aber weder Dienstvorgesetzter noch personalverwaltende Behörde (wie beispielsweise das Schulamt) ist. Insofern steht ihm kein Recht zu, Personalnebenakten zu führen. Deshalb darf er neben den zur Erledigung der inneren Schulangelegenheiten erforderlichen Personaldaten allenfalls noch den Entwurf seines Leistungsberichts und sonstige für seine rechtmäßige Aufgabenerfüllung erforderlichen Unterlagen führen. Dagegen dürfen Unterlagen wie z. B. ein vierseitiges Personalstammblatt, das Abiturzeugnis, Zeugnis des ersten und zweiten Staatsexamens, Fachlehrergutachten aus dem Vorbereitungsdienst, der Arbeitsvertrag für eine kurzfristige Angestelltentätigkeit, Anträge auf Sonderurlaub oder Durchschriften personalrechtlicher Entscheidungen wie Abordnung, Beurlaubung, Nebentätigkeitsgenehmigung nicht aufbewahrt werden, wenn sie zur Aufgabenerfüllung des Schulleiters nicht erforderlich sind. Soweit die bloße Kenntnisnahme von Daten, die dem Schulleiter über den Dienstweg bekanntgegeben werden, ausreicht, ist die Speicherung dieser Daten unzulässig. Unzulässig ist nach meiner Auffassung auch die Erhebung von umfangreichen Daten in sog. Personalfragebogen, wie sie – über Verlage beziehbar – von Schulleitern häufig benutzt werden. Diese Problematik wird mit dem Kultusministerium erörtert.

Aus dem **Vertretungsplan** eines Gymnasiums war auch der Grund für die Abwesenheit der vertretenen Lehrer ersichtlich (z. B. Erkrankung, Beurlaubung). Dieser Plan wurde sowohl im Lehrerzimmer als auch – zur Unterrichtung der Schüler – am Schwarzen Brett der Schule ausgehängt. Dort konnte er außerdem von allen vorbeigehenden Personen eingesehen werden. Eine Bekanntgabe dieser Daten ist nach § 29 Abs. 1 DSG NW weder an Lehrer und Schüler noch an Dritte zulässig. Ich habe daher dem Schulleiter empfohlen, künftig nur noch einen Vertretungsplan auszuhängen, aus dem der Grund für die Abwesenheit nicht hervorgeht.

5.15.2 Schüler- und Elterndaten

Ein Stadtdirektor ließ sich die **Namen und Anschriften** aller Schülerinnen und Schüler geben, die mit dem neuen Schuljahr zur Gesamtschule der Nachbargemeinde wechseln wollten. Nach Ansicht des Stadtdirektors hatte die Nachbargemeinde in der örtlichen Tageszeitung falsche Informationen über die Ausbildungsmöglichkeiten an der Gesamtschule verbreitet. Die Erhebung von Namen und Anschriften der zukünftigen Schüler sollte dem Zweck dienen, die betroffenen Eltern gezielt ansprechen und informieren zu können.

Nach meiner Auffassung war die Erhebung nicht zulässig. Sie konnte weder auf § 10 Abs. 2 des Schulverwaltungsgesetzes (SchVG) noch auf § 12 DSG NW gestützt werden. § 10 Abs. 2 SchVG ließ eine Datenerhebung allenfalls zur Feststellung eines Bedürfnisses für die Errichtung einer Gesamtschule zu. Nach § 12 DSG NW war die Erhebung unzulässig, weil es ihr an der Erforderlichkeit fehlte. Es mag zwar zu den Aufgaben der Gemeinde gehören, die betroffenen Eltern über die Ausbildungsmöglichkeiten an einer bestimmten Schule zu informieren bzw. Falschinformationen zu berichtigen. Eine Unterrichtung des betroffenen Personenkreises hätte jedoch auch auf anderem Weg erfolgen können, etwa durch ausführliche Informationen in der Zeitung oder an den Schulen verteilte Handzettel.

Darüber hinaus wurden die Daten an die Mitglieder des Haupt- und Finanzausschusses zur Unterrichtung weitergegeben. Auch hier gilt, daß die Übermittlung nach § 14 Abs. 1 DSG NW nicht erforderlich und damit unzulässig war. Eine Information der Ausschußmitglieder ohne Namensnennung der Betroffenen hätte nach meiner Auffassung ausgereicht. Der Stadtdirektor ist meiner Empfehlung, künftig derartige Datenerhebungen und -übermittlungen zu unterlassen, gefolgt.

Die bei der Einschulung verwendeten **Schülerstammblätter** einer Grundschule entsprachen nicht den Vorgaben der Verwaltungsvorschriften zu § 5 Abs. 4 der Allgemeinen Schulordnung (ASchO). Es wurden weitere, über den in Nr. 3.2 der Verwaltungsvorschriften festgelegten maximalen Datenbestand hinausgehende Angaben erhoben u. a. Beruf und Staatsangehörigkeit der Eltern sowie Krankenkasse und Hausarzt der Betroffenen. Diese unzulässig erhobenen Daten waren gemäß § 19 Abs. 3 Satz 1 Buchstabe a DSG NW zu löschen. Da bei einer Löschung der Daten z. B. durch Schwärzen die Gefahr besteht, daß sie auch weiterhin lesbar bleiben, habe ich empfohlen, den Datenschutzvorschriften entsprechende Stammblätter zu entwerfen, den vorhandenen Bestand – soweit zulässig – zu übertragen und die alten Stammblätter zu vernichten.

Auch das Führen von **Beobachtungsbogen** an den Schulen war Gegenstand mehrerer Eingaben. Dabei wurde festgestellt, daß die verwendeten Vordrucke in der Wahl der Beobachtungskriterien und der Formulierungen erheblich voneinander abwichen. In den Beobachtungsbogen werden sensible personenbezogene Daten erhoben; einige dieser Angaben, insbesondere zum sozialen Verhalten des einzelnen Schülers, beinhalten Beschreibungen charakterlicher Eigenschaften.

Ich habe das Kultusministerium darauf hingewiesen, daß für einen derartigen Eingriff in das Recht der Schüler auf informationelle Selbstbestimmung § 12 DSG NW als Rechtsgrundlage keinesfalls ausreicht. Auch die Verwaltungsvorschriften zu § 5 Abs. 4 ASchO können einen solchen Eingriff nicht rechtfertigen. Wie ich bereits mehrfach ausgeführt habe, ist für die Datenverarbeitung in der Schule eine gesetzliche Grundlage überfällig (auch oben S. 29). Darüber hinaus halte ich in Anbetracht der Verwendung und Verbreitung unterschiedlicher Beobachtungsbogen in den Schulen eine Anweisung zum Umgang mit diesen Unterlagen – insbesondere bezüglich Art und Dauer der

Speicherung, Verwendungszweck, Zugang zu den Unterlagen, Umfang der Verwendung in Konferenzen, Auskunfts- und Einsichtsrechten von Schülern und Eltern, Art und Dauer der Aufbewahrung sowie des Zeitpunktes der Löschung der Daten bzw. Vernichtung der Bogen – für dringend erforderlich.

5.15.3 Schulmitwirkung

Datenübermittlungen im Rahmen der Schulmitwirkung sind nach den Vorschriften des DSG NW zu beurteilen, da das Schulmitwirkungsgesetz hierzu keine normenklaren Bestimmungen enthält. Die Zulässigkeit der Übermittlung von Namen, Anschriften und Telefonnummern von Mitgliedern eines Schulmitwirkungsorgans an ein anderes richtet sich nach § 14 Abs. 1 DSG NW. Danach ist die Übermittlung zulässig, wenn sie zur rechtmäßigen Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist und das Gebot der Zweckbindung beachtet wird. Nach § 14 Abs. 5 DSG NW gilt dies entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.

Nach meiner Auffassung ist die Übermittlung der Daten erforderlich, um eine wirksame Zusammenarbeit der Mitwirkungsorgane der Eltern in der Schule zu ermöglichen. Dabei ist jedoch das Gebot der Zweckbindung zu beachten. Eine Liste mit diesen Angaben ist daher ausschließlich für Mitwirkungszwecke zu verwenden. Sie sollte entsprechend gekennzeichnet und gesichert aufbewahrt werden.

5.15.4 Schulträger und Einsatz von ADV

Eine Stadt hat mir die Frage gestellt, inwieweit dem Schulträger ein **Organisationsrecht** in Bezug auf die Verwendung von ADV-Geräten und -Programmen in den Schulen zusteht bzw. welche Pflichten sich für ihn ergeben. Soweit der kommunale Schulträger als Träger der datenverarbeitenden Stelle (der Schule) über die Anschaffung und Verwendung von ADV-Geräten und -Programmen entscheidet, trägt er die Verantwortung nach § 10 Abs. 1 DSG NW und hat für die erforderlichen technischen und organisatorischen Maßnahmen zu sorgen. In äußeren Schulangelegenheiten besteht das Organisationsrecht des Schulträgers uneingeschränkt; nach § 20 Abs. 4 des Schulverwaltungsgesetzes (SchVG) sind die Anordnungen des Schulträgers für den Schulleiter verbindlich. Soweit im Rahmen dieser äußeren Schulangelegenheiten auch personenbezogene Daten (z. B. der Schulsekretärin) verarbeitet werden, unterliegt der Schulleiter ebenfalls der Anordnungsbefugnis des Schulträgers.

Dagegen ist im Bereich der inneren Schulangelegenheiten der Schulleiter nach § 20 Abs. 2 SchVG für die ordnungsgemäße Verarbeitung personenbezogener Daten selbst verantwortlich. Insoweit hat er die nach § 10 Abs. 1 DSG NW erforderlichen Maßnahmen zu treffen. Dabei ist er an die Regelungen in der Dienstanweisung für die automatisierte Verarbeitung von personenbezogenen Daten in der Schule (RdErl. des Kultusministers vom 15.09.1988) gebunden. Eine datenschutzrechtliche Verantwortung für die Sicherstellung des Datenschutzes liegt hier nach § 7 DSG NW auch bei den

Schulaufsichtsbehörden. Das schließt nicht aus, daß der kommunale Schulträger im Zusammenhang mit der Anschaffung und Verwendung von ADV-Geräten und -Programmen Maßnahmen zur Verbesserung der Datensicherheit treffen kann.

5.15.5 Akteneinsicht durch minderjährige Schüler

Die Ausübung des Rechts auf Auskunft und Akteneinsicht in einem laufenden Verwaltungsverfahren richtet sich nach den Regeln des Verwaltungsverfahrensgesetzes für das Land Nordrhein-Westfalen (VwVfG NW). Nach § 12 Abs. 1 Nr. 1 VwVfG NW ist die mit der Volljährigkeit verbundene Geschäftsfähigkeit nach bürgerlichem Recht zur Ausübung des Rechts auf Akteneinsicht erforderlich. Nach § 12 Abs. 1 Nr. 2 VwVfG NW sind außerdem solche natürlichen Personen handlungsfähig, die nach bürgerlichem Recht in der Geschäftsfähigkeit beschränkt sind, soweit sie für den Gegenstand des Verfahrens durch Vorschriften des öffentlichen Rechts als handlungsfähig anerkannt sind. Derartige Regelungen bestehen jedoch für die Ausübung des Auskunfts- und Akteneinsichtsrechts nach § 18 DSG NW nicht.

In der Kommentarliteratur werden zur Wahrnehmung des Rechts auf Auskunft und Akteneinsicht nach § 18 Abs. 1 Satz 1 bzw. Abs. 2 Satz 1 DSG NW unterschiedliche Auffassungen vertreten. Nach meiner Ansicht sollte – wenn immer dies möglich ist – die Schule auch einem minderjährigen Schüler, der die für die Ausübung seines Rechts erforderliche Einsichtsfähigkeit besitzt, nach § 18 DSG NW Auskunft und Akteneinsicht gewähren. Die in Nr. 6 der Verwaltungsvorschrift zu § 5 Abs. 4 der Allgemeinen Schulordnung getroffene Regelung sollte deshalb geändert werden.

5.16 Finanzwesen

5.16.1 Anwendung der Abgabenordnung

Mit dem Steuerbereinigungsgesetz 1986 vom 19.12.1985 (BGBl. I S. 2436) wurde § 93 a in die Abgabenordnung eingefügt. Die zur Ausführung dieser Vorschrift erforderliche **Kontrollmitteilungsverordnung** ist jedoch bisher noch nicht erlassen worden. Im Hinblick auf den aus § 93 a der Abgabenordnung (AO) erkennbaren Willen des Gesetzgebers, zur Sicherung der Besteuerung Kontrollmitteilungen zuzulassen, hatte ich zunächst im Zusammenhang mit Bürgereingaben und Beschwerden zum Kontrollmitteilungsverfahren von Beanstandungen abgesehen. Nachdem die dazu erforderliche Kontrollmitteilungsverordnung aber auch in diesem Jahr nicht verabschiedet worden ist, kann ich die Verfahrensweise nicht länger hinnehmen.

Kontrollmitteilungen, die ohne die erforderliche gesetzliche Grundlage ergehen, sind rechtswidrig. Das Finanzministerium hat hierzu die Auffassung vertreten, daß sie gleichwohl durch die Finanzämter ausgewertet werden dürfen. Dieser Auffassung kann ich mich nicht anschließen. Der Grundsatz der Gesetzmäßigkeit der Verwaltung nach Artikel 20 Abs. 3 des Grundgesetzes verbietet nach meiner Auffassung die Auswertung von Daten, die von öffentlichen Stellen unzulässigerweise den Finanzbehörden übermittelt werden. Ich

habe deshalb empfohlen, die Finanzbehörden anzuweisen, daß eine Auswertung von personenbezogenen Daten, die mittels Kontrollmitteilung zur Kenntnis der Finanzbehörden gelangt sind, nur insoweit erfolgen darf, als die Kontrollmitteilung im Einzelfall auf eine besondere Rechtsgrundlage gestützt werden kann. Dieser Regelung vorzuziehen wäre es jedoch, wenn die absendenden Stellen durch die Finanzbehörden gebeten würden, Kontrollmitteilungen bis zum eventuellen Inkrafttreten einer Kontrollmitteilungsverordnung nicht mehr zu übersenden, sofern die Mitteilung nicht im konkreten Fall durch besondere Rechtsvorschriften gerechtfertigt ist. Damit würden unzulässige Eingriffe in Grundrechte der Betroffenen schon im Ansatz vermieden.

Das Finanzministerium hat zwar die Ressorts darauf hingewiesen, daß – unbeschadet spezialgesetzlicher Regelungen – derzeit für öffentliche Stellen keine Verpflichtung besteht, der Finanzverwaltung Kontrollmitteilungen zu übersenden. Meiner Auffassung zum Verwertungsverbot bezüglich der bisher übersandten Kontrollmitteilungen konnte es sich jedoch nicht anschließen.

Vom Finanzministerium ist mir der Entwurf einer **Steuerdatenabrufverordnung** nach § 30 Abs. 6 AO zur Prüfung zugeleitet worden. Nachdem sich die Datenschutzbeauftragten des Bundes und der Länder über mehrere Jahre um datenschutzrechtliche Verbesserungen im Steuerdatenabrufverfahren bemüht haben, bestehen nunmehr gegen die Verordnung in der jetzigen Fassung keine durchgreifenden datenschutzrechtlichen Bedenken mehr. Der Datenabruf durch die Oberfinanzdirektionen im Rahmen der Dienst- und Fachaufsicht sollte jedoch auf Einzelfälle beschränkt werden. Darüber hinaus habe ich dem Finanzministerium zwei Änderungsvorschläge im Interesse der Datensicherheit unterbreitet. Sie betrafen zum einen die Identitätsprüfung beim Datenabruf und zum anderen Aufbau und Änderungsfristen von Paßwörtern.

5.16.2 Neutrale Absenderangabe

Mit der Verordnung des Finanzministers vom 12.09.1986 (GV. NW. S. 639) sind u. a. Finanzämter für **Steuerstrafsachen und Steuerfahndung** errichtet worden (§ 2 der Verordnung).

Schreiben dieser Dienststellen wurden gemäß der Festlegung in der Verordnung mit dem Absender „Finanzamt für Steuerstrafsachen und Steuerfahndung" verschickt. Diese Bezeichnung auf dem Briefumschlag war Gegenstand mehrerer Eingaben betroffener Bürger. Sie befürchteten, aus diesem Absender könne geschlossen werden, daß der Empfänger in ein Steuerstrafverfahren oder eine Steuerfahndungsangelegenheit verwickelt sei.

Ich habe beim Finanzministerium angeregt, für diesen Finanzamtstyp eine neutrale Bezeichnung einzuführen. Daraufhin wurden die Finanzämter angewiesen, Schreiben an Steuerpflichtige mit der neutralen Absenderangabe „Finanzverwaltung Nordrhein-Westfalen" zu verschicken.

5.16.3 Steuerangelegenheiten der Beschäftigten in der Steuerverwaltung

Nach § 23 Abs. 1 Nr. 4 der bundeseinheitlich geltenden Geschäftsordnung für die Finanzämter (FAGO) zeichnet der Vorsteher eines Finanzamtes abschließend Steuerangelegenheiten von Amtsangehörigen. Diese Regelung führt dazu, daß der Dienstvorgesetzte weitreichende Einblicke in die persönlichen Verhältnisse und die Lebensführung bis hin beispielsweise zu gesundheitlichen Gebrechen, religiösen Bindungen, Ehe- und Familienverhältnissen oder politischen Verbindungen erhält. Dies wird von Angehörigen der Finanzverwaltung kritisiert und die Befürchtung geäußert, daß die im steuerlichen Bereich erlangten Kenntnisse Entscheidungen des Vorgesetzten im beamten- und personalrechtlichen Bereich beeinflussen könnten. Die Betroffenen sehen in der Regelung des § 23 Abs. 1 Nr. 4 FAGO eine unverhältnismäßige Beeinträchtigung ihres informationellen Selbstbestimmungsrechts und eine Benachteiligung gegenüber den Angehörigen von Behörden, deren steuerliche Angelegenheiten bei anderen Ämtern bearbeitet werden.

§ 23 Abs. 1 Nr. 4 FAGO dürfte auf der Überlegung beruhen, daß der Gefahr einer unzulässigen kollegialen Bevorzugung bei der Bearbeitung von Steuerangelegenheiten vorzubeugen ist. Ich halte jedoch die gegen die Regelung des § 23 FAGO vorgebrachten Bedenken für beachtlich. Der beabsichtigte Zweck der Vorbeugung könnte nach meiner Auffassung auch dadurch erreicht werden, daß für die Bearbeitung der Steuerangelegenheiten Amtsangehöriger ein anderes Finanzamt für zuständig erklärt wird. Diese Beurteilung wird auch von den anderen Landesbeauftragten für den Datenschutz geteilt.

Das Finanzministerium hat mir hierzu mitgeteilt, daß bei einer Besprechung der obersten Finanzbehörden der Länder vereinbart wurde, Vorschläge für eine bundesweite Änderung der FAGO zu erarbeiten. Dabei werde daran gedacht, den Zeichnungsvorbehalt des Vorstehers wegfallen zu lassen. Für den Fall, daß eine Änderung der FAGO in absehbarer Zeit nicht zustande kommen sollte, wird in Aussicht gestellt, für die betroffenen Fälle Zuständigkeitsvereinbarungen nach § 27 der Abgabenordnung zuzulassen. Letzteres würde von mir im Interesse der Betroffenen begrüßt.

5.16.4 Kommunalabgaben

Beanstanden mußte ich gegenüber einem Stadtdirektor den Versand von Bescheiden über Grundbesitzabgaben als „Briefdrucksache – Gebühr geprüft". Der Bescheid enthielt z. B. die Festsetzung der Grundsteuer und der Gebühren für Müllabfuhr und Straßenreinigung.

Die Angaben zur Grundsteuer unterliegen gemäß § 12 Abs. 1 Nr. 1 c des Kommunalabgabengesetzes (KAG) dem **Steuergeheimnis** nach § 30 der Abgabenordnung (AO). Das Steuergeheimnis wird durch jede unbefugte Offenbarung verletzt. Die übrigen Angaben sind durch das allgemeine Amtsgeheimnis gemäß § 3 a des Verwaltungsverfahrensgesetzes für das Land Nordrhein-Westfalen geschützt.

Wie ich in meinem 8. Tätigkeitsbericht (Seite 158) ausgeführt habe, kann ein Umschlag dann als verschlossen angesehen werden, wenn er nur bei bleibender nachträglich erkennbarer Beschädigung geöffnet werden kann. Dies gilt auch für Briefumschläge mit Adhäsionsverschluß. Ein Briefumschlag, der als verschlossen gelten soll, darf allerdings nicht als Briefdrucksache oder Drucksache gekennzeichnet sein, weil er in diesem Fall von der Post für Kontrollzwecke geöffnet werden darf. Die Eigenschaft als verschlossener Brief wird durch den Aufdruck – d. h. durch das Einverständnis des Absenders mit der Öffnung – insoweit aufgehoben. Die damit geschaffene Möglichkeit einer Kenntnisnahme von Daten durch die Bundespost stellt eine unzulässige Übermittlung dar, weil eine Offenbarungsbefugnis nicht besteht.

Ich hatte daher dem Stadtdirektor empfohlen, Schriftstücke mit derartigen sensiblen personenbezogenen Daten nicht mehr als Briefdrucksache zu versenden. Der vom Stadtdirektor um Weisung gebetene Innenminister teilte ihm nur mit, daß die Bundespost nicht bereit sei, auf ihr Öffnungs- und Prüfungsrecht zu verzichten. Daraufhin erklärte der Stadtdirektor, daß er die Abgabenbescheide im Januar 1991 wiederum als Briefdrucksache zustellen werde. Auf meine Beanstandung hin wird der Stadtdirektor die Bescheide als normale Briefe zustellen.

Auf Grund verschiedener Eingaben ist mir bekanntgeworden, daß in Fällen der Veräußerung eines Hundes oder des Wohnsitzwechsels des Hundehalters die Wohngemeinde des Erwerbers bzw. die neue Wohngemeinde des Halters über diesen Tatbestand im Wege einer schriftlichen Mitteilung unterrichtet wird. Die datenschutzrechtliche Zulässigkeit solcher **Mitteilungen zur Hundesteuer** von Gemeinde zu Gemeinde ist zweifelhaft. Als Eingriff in das Recht der Beteiligten auf informationelle Selbstbestimmung sind derartige Mitteilungen nur zulässig, wenn dafür eine normenklare Rechtsgrundlage besteht, die auch dem Verhältnismäßigkeitsgrundsatz Rechnung trägt.

Für die Meldepflicht des Veräußerers bzw. Hundehalters ist nach § 11 Abs. 2 der von den Gemeinden nach Vorgabe der Hundesteuermustersatzung des Innenministers (RdErl. vom 01.10.1970, SMBl. NW. 61215) erlassenen Hundesteuersatzungen die Rechtsgrundlage vorhanden. Daher bestehen keine Bedenken, wenn eine Gemeinde diese Daten für ihre eigenen steuerlichen Zwecke verwertet und insoweit an den Erwerber eines Hundes, der mit der Anmeldung säumig ist, herantritt.

Datenschutzrechtlich problematisch dagegen ist die Übermittlung der Daten über Veräußerung oder Wohnortwechsel von einer Gemeinde zur anderen. Da die Gemeinden die Kenntnis dieser Daten in Zusammenhang mit der Hundesteuerpflicht erlangt haben, ist insoweit das Steuergeheimnis zu beachten (§ 12 Abs. 1 Nr. 1 KAG). Nach § 30 Abs. 2 AO verletzt ein Amtsträger das Steuergeheimnis, wenn er Verhältnisse eines anderen, die ihm in einem Verfahren in Steuersachen bekanntgeworden sind, unbefugt offenbart oder verwertet. Eine Offenbarung dieser Kenntnisse ist nur unter bestimmten Voraussetzungen zulässig. Ob im vorliegenden Fall dafür § 30 Abs. 4 Nr. 1 i.V.m. Abs. 2 Nr. 1 Buchstabe a AO herangezogen werden kann, halte ich jedenfalls in den Fällen für zweifelhaft, in denen es sich um die Verhältnisse

eines anderen (z. B. Hundekäufers) handelt. Aber auch im Hinblick auf § 93 a AO sowie auf den Grundsatz der Verhältnismäßigkeit sind Kontrollmitteilungen über den Zuzug eines Hundehalters unzulässig.

Zwar sieht das Kommunalabgabengesetz des Landes Nordrhein-Westfalen die Anwendung des § 93 a AO auf Kommunalabgaben nicht vor. Mit der Aufnahme des § 93 a in die Abgabenordnung hat sich der Gesetzgeber jedoch der Auffassung der Datenschutzbeauftragten angeschlossen, daß Kontrollmitteilungsverfahren einer besonderen gesetzlichen Grundlage bedürfen. So wollen die Länder Niedersachsen und Rheinland-Pfalz in den dort gleichfalls bestehenden Hundesteuermustersatzungen klarstellen, daß im Fall der Veräußerung eines Hundes bzw. des Wohnsitzwechsels eines Hundehalters die neue Gemeinde über diesen Umstand unterrichtet wird und der Hundehalter im voraus oder doch spätestens gleichzeitig mit der Mitteilung über das Kontrollmitteilungsverfahren unterrichtet wird. Eine nachträgliche, mit der Aufforderung zur Anmeldung verbundene Unterrichtung des Betroffenen, wie sie laut Auskunft des Innenministeriums des Landes Nordrhein-Westfalen regelmäßig vorgenommen wird, entspricht nach meiner Auffassung nicht dem Gebot zur Herstellung von Transparenz in der Informationsverarbeitung öffentlicher Stellen.

5.17 Umweltschutz

5.17.1 Zugang zu Umweltdaten

Gegenüber der im 9. Tätigkeitsbericht (S. 94 bis 97) dargestellten Situation des Informationszuganges zu Umweltdaten im Abfall- und Wasserrecht ist der **freie Zugang zu Informationen über die Umwelt** durch die vom Rat der Europäischen Gemeinschaft am 3. Juli 1990 verabschiedete Richtlinie weiterentwickelt worden. Danach sollen die Mitgliedstaaten grundsätzlich gewährleisten, daß allen natürlichen oder juristischen Personen auf Antrag ohne Nachweis eines Interesses Informationen über die Umwelt zur Verfügung gestellt werden. Allerdings kann der Zugang zu solchen Informationen beschränkt werden, die beispielsweise Geschäfts- und Betriebsgeheimnisse, die **Vertraulichkeit personenbezogener Daten** oder den Schutz staatlichen Handelns betreffen. Der Öffentlichkeit sollen durch regelmäßige Veröffentlichung von Zustandsberichten allgemeine Informationen über den Zustand der Umwelt zur Verfügung gestellt werden. Bis zum 31. Dezember 1992 müssen in den Mitgliedstaaten die dazu erforderlichen Rechts- und Verwaltungsvorschriften erlassen sein.

In diesem Zusammenhang stehen folgende vier vom Bundesgesetzgeber verabschiedete Gesetze, die unterschiedliche Informationszugänge regeln:

Das Gesetz zur Umsetzung der Richtlinie des Rates vom 27. Juni 1985 über die Umweltverträglichkeitsprüfung bei bestimmten öffentlichen und privaten Projekten – UVPG – vom 12. Februar 1990 (BGBl. I S. 205) verlangt die Beteiligung der Öffentlichkeit bei der Zulassung bestimmter Vorhaben mit Auswirkungen auf die Umwelt in Form einer **Anhörung**. Das Anhörungsverfahren muß den Anforderungen des § 73 Abs. 3 bis 7 des Verwaltungsverfah-

rensgesetzes für Planfeststellungsverfahren entsprechen (§ 9 UVPG). Dabei müssen die Rechtsvorschriften über Geheimhaltung und Datenschutz beachtet werden (§ 10 UVPG).

Den Behörden hat das Dritte Gesetz zur Änderung des Bundes-Immissionsschutzgesetzes – BImSchG – vom 11. Mai 1990 (BGBl. I S. 870) eine bessere Beurteilungsgrundlage für die **Veröffentlichung** von Einzelangaben aus der vom Anlagenbetreiber abzugebenden Emissionserklärung geschaffen (§ 27 BImSchG). Nunmehr muß der Betreiber einer Anlage der zuständigen Behörde bei Abgabe der Emissionserklärung mitteilen und begründen, welche Einzelangaben der Emissionserklärung Rückschlüsse auf Betriebs- oder Geschäftsgeheimnisse erlauben und demnach nicht veröffentlicht werden dürfen. Bisher oblag allein der Behörde die Prüfung, ob Betriebs- oder Geschäftsgeheimnisse unzulässigerweise offenbart werden; insoweit trägt also jetzt der Anlagenbetreiber die Darlegungslast. Außerdem ist die Bundesregierung zur Erfüllung von Beschlüssen der Europäischen Gemeinschaft ermächtigt, in Rechtsverordnung zu regeln, wie die Bevölkerung zu unterrichten ist (§ 48 a BImSchG).

Das Gesetz über die Umwelthaftung – UmweltHG – vom 10. Dezember 1990 (BGBl. I S. 2634) sieht in den §§ 8 und 9 einen **Auskunftsanspruch** des Geschädigten gegen den Inhaber der Anlage bzw. die Behörde zur Geltendmachung seines Schadensersatzanspruches vor. Dieser Auskunftsanspruch besteht gegenüber dem Inhaber der Anlage nicht, soweit Vorgänge auf Grund gesetzlicher Vorschriften geheimzuhalten sind oder die Geheimhaltung einem überwiegenden Interesse des Inhabers der Anlage oder eines Dritten entspricht (§ 8 Abs. 2 UmweltHG). Desgleichen ist der Auskunftsanspruch gegenüber den Behörden beschränkt (§ 9 Satz 2 UmweltHG). Aber auch dem Inhaber einer Anlage wird gegenüber dem Geschädigten und dem Inhaber einer anderen Anlage ein entsprechender Auskunftsanspruch zugestanden.

Demgegenüber bedarf der mit Änderung des Chemikaliengesetzes beabsichtigte Aufbau einer **Gefahrstoffdatenbank** beim Umweltbundesamt noch einer gesetzlichen Grundlage, die den datenschutzrechtlichen Anforderungen genügt. Die zu dieser Datei regelmäßig zu übermittelnden Daten sollen Angaben enthalten, die der Hersteller eines neuen Stoffes, den er in Verkehr bringt, anzumelden hat. Die Daten können somit auch personenbezogene Herstellerangaben sowie Betriebs- und Geschäftsgeheimnisse betreffen. Das vom Ministerium für Umwelt, Raumordnung und Landwirtschaft des Landes Nordrhein-Westfalen entwickelte Informations- und Kommunikationssystem **gefährliche und umweltrelevante Stoffe** enthält dagegen ausschließlich Daten, die keinen Personenbezug aufweisen.

In Nordrhein-Westfalen laufen Vorarbeiten zum Aufbau eines **Bodeninformationssystems** unter der Federführung des Bodenschutzzentrums. Geplant ist die Einrichtung eines ADV-Systems zur Vermittlung und Auswertung von Fachdaten des Bodenschutzes (Bodeninformationssystem des Landes Nordrhein-Westfalen – BIS NRW). Dabei werden auch die Vorschläge der Sonderarbeitsgruppe „Informationsgrundlagen Bodenschutz" des Bund-Länder-Arbeitskreises „Bodenschutz" berücksichtigt.

In diesem Informationssystem sollen die im Land vorliegenden Daten zu geowissenschaftlichen Grundlagen, zum Natur- und Landschaftsschutz und insbesondere zu anthropogenen Einwirkungen auf den Boden verfügbar gemacht und für das Daten- und Informationssystem des Ministeriums für Umwelt, Raumordnung und Landwirtschaft ausgewertet werden. Demzufolge müssen Daten aus unterschiedlichen Bereichen zum Zweck der Risikovorhersage, der Vorsorge und der Sanierung miteinander verknüpft werden. Im ersten Schritt ist an die Einbeziehung nur der datenerhebenden Stellen bei den Landeseinrichtungen gedacht; u. a. sollen das Bodenbelastungskataster der Landesanstalt für Ökologie, Landschaftsentwicklung und Forstplanung, das Immissions-, Emissions- und Bodenkataster der Landesanstalt für Immissionsschutz, die Datenbank Sonderabfall-Lizenz, das Informationssystem-Altlasten und die Direkteinleiterüberwachung des Landesamtes für Wasser und Abfall, die Bodendatenbank des Geologischen Landesamtes aber auch das Liegenschaftskataster des Landesamtes für Datenverarbeitung und Statistik genutzt werden. Später sollen auch andere Informationssysteme insbesondere auf kommunaler Ebene einbezogen werden. Nutzer des BIS NRW werden neben den öffentlichen Stellen auch Kammern, Verbände, private Institutionen und Firmen sein.

Da davon auszugehen ist, daß in diesem umfangreichen Informationssystem personenbezogene Daten – auch mit Zugriffsberechtigung Dritter – verarbeitet sowie Betriebs- und Geschäftsgeheimnisse berührt werden, halte ich eine bereichspezifische Regelung für erforderlich, die einmal die Voraussetzung für die Zulässigkeit der Datenverarbeitung im Bodeninformationssystem schafft und außerdem Vorkehrungen zur Gewährleistung des Datenschutzes trifft.

5.17.2 Einwendungen im Planfeststellungsverfahren

Im Rahmen eines Planfeststellungsverfahrens nach dem Abfallgesetz wurden über 4 000 Einwendungen erhoben. Der zuständige Regierungspräsident hat der Antragstellerin des Planfeststellungsverfahrens bereits vor dem Erörterungstermin alle Einwendungen übersandt und dadurch generell die **Namen und Anschriften** der Einwender bekanntgegeben.

Zu diesem Problem habe ich bereits in meinem 7. Tätigkeitsbericht (S. 140/141) im Rahmen eines Genehmigungsverfahrens nach dem Bundes-Immissionsschutzgesetz Stellung genommen. Die dort angestellten Erwägungen gelten auch hier. Ich habe dem Regierungspräsidenten empfohlen, künftig die Namen und Anschriften der Einwender nur dann an die Beteiligten des Planfeststellungsverfahrens zu übermitteln, wenn die Kenntnis dieser Daten für deren Rechtsverfolgung erforderlich ist. In der Regel reicht eine ungefähre Angabe der Wohnlage des Einwenders zum Vorhaben aus. Das Ministerium für Umwelt, Raumordnung und Landwirtschaft hat sich meiner Auffassung zwar angeschlossen, aber nur dann ein Unkenntlichmachen von Name und Anschrift des Einwenders für notwendig erachtet, wenn der Einwender dies verlangt hat. Dies halte ich nicht für ausreichend, da ein bloßes Widerspruchsrecht dem Recht auf informationelle Selbstbestimmung hier nicht genügt.

Inzwischen habe ich zur Novellierung des § 12 der 9. Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes – Genehmigungsverfahren – Stellung genommen. Die dort vorgesehene Klarstellung, daß die Einwendungen dem Antragsteller bekanntzugeben sind, ist ebenfalls unzureichend. Es muß bei einer den Datenschutz berücksichtigenden Formulierung beachtet werden, daß eine pauschale, undifferenzierte Übermittlung der Namen und Anschriften aller Einwender unverhältnismäßig ist. Daher darf deren Bekanntgabe nur in den Fällen erfolgen, in denen der Antragsteller diese Daten zur Vorbereitung des **Erörterungstermins** dringend benötigt. Den Einwendern muß die Möglichkeit erhalten bleiben, ihre Einwendungen bis zum Erörterungstermin zurückzunehmen, ohne daß ihre Identität gegenüber dem Antragsteller aufgedeckt wird.

5.18 Verkehr

5.18.1 Verstöße im ruhenden Straßenverkehr

Von einer Stadt bin ich um datenschutzrechtliche Beurteilung des dort geübten Verfahrens gebeten worden, nach dem **wiederholte Verstöße** im ruhenden Verkehr mit erhöhter Geldbuße geahndet wurden. Die Stadt erhob zu dem im Normalfall fälligen Verwarnungsgeld einen „Zuschlag", bei dessen Höhe jeweils die Zahl der Wiederholungsfälle berücksichtigt wurde. Beispielsweise betrug der „Zuschlag" ab dem 20. bis 29. Fall je Fall 50,– DM. Bei der Überprüfung, wieviele Verwarnungen oder Bußgelder gegen einen Betroffenen wegen vergleichbarer Verstöße in der Vergangenheit verhängt worden waren, machte sich die Stadt das automatisierte Verfahren zur Bearbeitung der Verkehrsordnungswidrigkeiten zunutze.

Hierbei ging sie folgendermaßen vor: Die Mitarbeiter des Außendienstes der Ordnungsbehörde gaben in die bei der Überwachungstätigkeit mitgeführten Handcomputer das Zeichen „J" (= Ja) ein, wenn es sich bei dem falsch geparkten Kraftfahrzeug „nach ihrer Erinnerung" um ein Fahrzeug handelte, das ihnen durch wiederholtes falsches Parken aufgefallen war. Die im Handcomputer gespeicherten Daten einschließlich des Wiederholungsmerkmals wurden in die automatisierte Datei der Falschparker übernommen. Diese Datei diente der Erteilung von schriftlichen Verwarnungen und der Erstellung von Anhörungsbogen sowie dem etwaigen Erlaß von Bußgeldbescheiden. In den mit „J" gekennzeichneten Fällen wurde dann durch den Aufruf des jeweiligen Kfz-Kennzeichens festgestellt, ob und wie häufig das Fahrzeug innerhalb einer Frist von zwei Jahren falsch geparkt worden war. Auf Grund der Dateiauskünfte wurde ein Bußgeldbescheid mit einer Geldbuße nach der jeweiligen Regelstaffel erlassen.

Da in der Zwischenzeit Zweifel an der Zulässigkeit der geschilderten Verfahrensweise aufgetreten sind, hat die Stadt das Verfahren zur Festsetzung einer erhöhten Geldbuße in Wiederholungsfällen bei Verkehrsverstößen zunächst ausgesetzt.

In meinem 2. Tätigkeitsbericht (S. 44/45) habe ich bereits dargelegt, daß das Führen örtlicher „Verkehrssünderkarteien" unzulässig ist. Zur Erkennung

von Wiederholungsfällen von Verkehrsverstößen darf lediglich auf die ohne dieses Hilfsmittel vorhandenen Erkenntnisse insbesondere der Außendienstmitarbeiter des Ordnungsamtes zurückgegriffen werden. Auch eine systematische Auswertung der vorhandenen Dateien zur erhöhten Ahndung von Wiederholungsfällen bei Verstößen im ruhenden Verkehr ist einer unzulässigen Verkehrssünderkartei gleichzusetzen.

Wegen der bundesweit aufgetretenen Problematik in dieser Frage hat sich der Bund-Länder-Fachausschuß „Straßenverkehrsordnungswidrigkeiten" mit den damit zusammenhängenden Fragen beschäftigt. Nach seiner Auffassung gehört das Erkennen wiederholter Ordnungswidrigkeiten im ruhenden Verkehr zu den Aufgaben der Verfolgungsbehörde. Wiederholtes Begehen sei ein Indiz für die Schwere des Schuldvorwurfs, der ein wesentliches Zumessungskriterium für die Geldbuße bilde. Die Verwertung von Erinnerungswissen sei problemlos. Aber die Hinzuziehung technischer Hilfsmittel (manuelle Kartei oder elektronische Datei) begegne auch in den Fällen der Verifizierung von Erinnerungswissen Bedenken, solange keine Sicherungen gegen ausforschungsähnliches Vorgehen bestünden.

Nach diesem Erkenntnisstand habe ich gegen das von der Stadt praktizierte Verfahren insoweit Bedenken, als mit dem bloßen Eingeben des Zeichens „J" durch die Mitarbeiter des Außendienstes in ihre bei der Überwachungstätigkeit mitgeführten Handcomputer nicht bloßes „Erinnerungswissen" verwertet wird, sondern eine automatisierte Dateiauskunft eingeholt wird. Daher halte ich es für erforderlich aber auch für ausreichend, wenn der Außendienstmitarbeiter sein Erinnerungswissen durch nähere Angaben etwa zum Tattag und Tatort präzisiert. Dabei muß sichergestellt werden, daß nicht durch technische Hilfsmittel eine weitere systematische Auswertung erfolgt.

Die Angelegenheit konnte bisher noch nicht zum Abschluß gebracht werden. Die Stadt hat den Städtetag Nordrhein-Westfalen um Erörterung der Problematik gebeten.

5.18.2 Mitteilungen über Fahreignung

Zu den regelmäßigen Mitteilungen des Ordnungsamtes an die Straßenverkehrsbehörde über Unterbringungen nach dem Gesetz über Hilfen und Schutzmaßnahmen bei **psychischen Krankheiten** (PsychKG) habe ich immer wieder gefordert, daß die datenschutzrechtlichen Belange der Betroffenen stärker berücksichtigt werden müssen (3. Tätigkeitsbericht, S. 107; 5. Tätigkeitsbericht, S. 133/134). Meine Bemühungen haben im Ergebnis zu dem Runderlaß des Ministers für Arbeit, Gesundheit und Soziales über Mitteilungen der Ordnungsämter an die Straßenverkehrsämter bei Unterbringungen nach dem PsychKG vom 16. März 1984 geführt, der im Einvernehmen mit dem Innenminister ergangen ist. In diesem Erlaß ist ausgeführt, daß durch regelmäßige Mitteilungen der Grundsatz der Verhältnismäßigkeit evident außer acht gelassen wird. Mitteilungen an die Straßenverkehrsämter seien nur dann geboten, wenn Fahruntüchtigkeit oder ein begründeter Anhalt für die Fahruntüchtigkeit einer Person gegeben sei. Hierzu ist in einem späteren Erlaß des Ministers für Arbeit, Gesundheit und Soziales vom 29. März 1985 näher erläu-

tert worden, daß dann eine Mitteilung der Ordnungsbehörde an die Straßenverkehrsbehörde zu erfolgen hat, wenn der Unterbringung des psychisch Kranken eine konkrete Gefahr, die im Straßenverkehr zu Tage getreten ist, zugrunde liegt oder im Einzelfall hinreichende Anhaltspunkte für eine zu erwartende Gefährdung des Straßenverkehrs gegeben sind.

Durch den Hinweis eines Vereins für Suchtkrankenberatung und durch die Eingabe eines ärztlichen Direktors einer Nervenklinik wurde mir bekannt, daß es entgegen der Erlaßregelungen eine weit verbreitete Praxis der Ordnungsbehörden in Nordrhein-Westfalen gibt, jede wegen Trunksucht entmündigte und nach dem PsychKG zwangseingewiesene Person regelmäßig der Straßenverkehrsbehörde zu melden, ohne im Einzelfall die Notwendigkeit dieser Maßnahme geprüft und ohne den Betroffenen darüber informiert zu haben. Von einer Ordnungsbehörde ist mir hierzu mitgeteilt worden, daß bei der Unterbringung von Personen nach dem PsychKG immer Eigen- bzw. Fremdgefährdung vorliege, und daher in diesen Fällen die Information an die Straßenverkehrsbehörde zum Schutze Dritter geboten sei. Dementsprechend finde eine „dezidierte Einzelfallprüfung" in aller Regel nicht statt. Auf diese unzulässige Praxis habe ich das Ministerium für Arbeit, Gesundheit und Soziales hingewiesen und angeregt, ggf. mit einem klarstellenden Erlaß die Mitteilungspraxis der Ordnungsämter auf das erforderliche Maß zu beschränken.

Gegen die regelmäßige Mitteilung der Gerichte über die Anordnung einer **Vormundschaft** oder vorläufigen Vormundschaft sowie einer **Pflegschaft** wegen geistiger oder körperlicher Gebrechen nach Abschnitt XIII/2 der Mitteilungen in Zivilsachen (MiZi) an das Straßenverkehrsamt habe ich ebenfalls erhebliche datenschutzrechtliche Bedenken. Hierzu werden mir immer wieder Beschwerden von Betroffenen sowie deren Pfleger aber auch von Fachärzten vorgetragen. Insbesondere die Fachärzte weisen in ihren Eingaben auf den o. g. Runderlaß vom 16. März 1984 über Mitteilungen der Ordnungsämter an die Straßenverkehrsämter hin.

Ab 1. Januar 1992 gilt für die Zulässigkeit der genannten Mitteilungen nach Abschnitt XIII/2 MiZi die Vorschrift des § 69 k des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit (FGG) in der Fassung des Betreuungsgesetzes (oben S. 16). Nach Absatz 1 dieser Vorschrift teilt das Vormundschaftsgericht Entscheidungen anderen Gerichten, Behörden oder sonstigen öffentlichen Stellen mit, soweit dies unter Beachtung berechtigter Interessen des Betroffenen nach den Erkenntnissen im gerichtlichen Verfahren erforderlich ist, um eine erhebliche Gefahr für das Wohl des Betroffenen, für Dritte oder für die öffentliche Sicherheit abzuwenden. Zu dieser Regelung wird in der Begründung zum Gesetz darauf hingewiesen, daß das Gericht prüfen muß, ob das öffentliche Interesse an der Aufgabenerfüllung des Empfängers das Schutzinteresse des Betroffenen überwiegt.

Mit Inkrafttreten des Betreuungsgesetzes gelten für die Unterrichtung der Straßenverkehrsbehörden durch das Vormundschaftsgericht Regelungen, die unter Anlegung eines strengen Maßstabes nach den Erfordernissen der Verkehrssicherheit einerseits und andererseits nach dem verfassungsrechtlichen Verständnis des Persönlichkeitsschutzes festgelegt worden sind. Da-

gegen erfüllen die Regelungen in Abschnitt XIII/2 MiZi diese Voraussetzungen nicht. Daher habe ich das Justizministerium des Landes Nordrhein-Westfalen gebeten, bereits vor Inkrafttreten des Betreuungsgesetzes vorzusehen, daß die genannten Mitteilungen des Vormundschaftsgerichts an das Straßenverkehrsamt nur nach Maßgabe einer Prüfung und Abwägung erfolgen dürfen, wie sie in § 69 k FGG vorgesehen ist. Dabei sollte auch der Betroffene bzw. für diesen handelnde Personen über die Mitteilung unterrichtet werden. Das Justizministerium hat mir mitgeteilt, daß es in Erwägung ziehe, unmittelbar nach Verkündung dieses Gesetzes die Mitteilungspflicht nach Abschnitt XIII/2 MiZi insgesamt aufzuheben und den Richtern zu empfehlen, ab sofort nach den neuen Mitteilungsregelungen zu verfahren.

Demgegenüber halte ich das Verfahren der regelmäßigen Mitteilungen über die Anordnung eines **Fahrverbots** nach § 25 des Straßenverkehrsgesetzes (StVG) durch die Ordnungsbehörde an die Straßenverkehrsbehörde grundsätzlich für zulässig. Nach § 28 Abs. 2 des Polizeigesetzes des Landes Nordrhein-Westfalen, der nach § 24 des Ordnungsbehördengesetzes entsprechend anwendbar ist, sind Mitteilungen über das Fahrverbot durch die Ordnungsbehörde an die Straßenverkehrsbehörde zulässig, wenn die Kenntnis von dem Fahrverbot zur Aufgabenerfüllung der Straßenverkehrsbehörde erforderlich erscheint. Die Straßenverkehrsbehörde benötigt die Mitteilung, um Maßnahmen gegen den Fahrerlaubnisinhaber wegen Bedenken gegen seine Kraftfahreignung zu prüfen. Für regelmäßige Mitteilungen müssen allerdings zusätzlich die Voraussetzungen des § 9 Abs. 8 i.V.m. Abs. 2 DSG NW vorliegen. Danach muß insbesondere die regelmäßige Datenübermittlung durch Rechtsverordnung zugelassen sein. Eine dementsprechende Rechtsverordnung liegt nicht vor. Deshalb habe ich dem Innenministerium empfohlen, eine Rechtsverordnung für das Verfahren der regelmäßigen Mitteilung über ein Fahrverbot nach § 25 StVG zu erlassen.

5.18.3 Frühere Straftaten

Zuletzt habe ich in meinem 9. Tätigkeitsbericht (S. 100/101) dargelegt, daß die gegenwärtige Praxis zur Anwendung des § 52 Abs. 2 des Bundeszentralregistergesetzes (BZRG) allgemein als unbefriedigend angesehen wird. Die „Kann-Bestimmung" des § 52 Abs. 2 BZRG ermöglicht in Fahrerlaubnisangelegenheiten eine **zeitlich unbegrenzte Verwertung** von Straftaten auch nach Tilgung dieser Delikte im Bundeszentralregister und im Verkehrszentralregister.

Bei der Anwendung des § 52 Abs. 2 BZRG wird in der Praxis der Länder unterschiedlich verfahren. In Rheinland-Pfalz gilt die Regelung, daß bei Berücksichtigung zurückliegender Verkehrsstraftaten nicht über zehn Jahre hinausgegangen werden darf. In den Ländern Niedersachsen und Schleswig-Holstein haben die für den Verkehr zuständigen Ministerien entschieden, Verurteilungen nicht mehr zu verwerten, wenn sie der Tilgung unterliegen. Die Länder Hamburg, Berlin und Nordrhein-Westfalen halten dagegen ohne Rücksicht auf die Tilgung strafrechtlicher Entscheidungen diese dem Betroffenen im Verfahren über die Erteilung oder Entziehung einer Fahrer-

laubnis vor. Überwiegend wird jedoch die Auffassung vertreten, daß die Regelung in § 52 Abs. 2 BZRG dem Bewährungsgrundsatz in keiner Weise Rechnung trägt. Darüber hinaus sei eine unbegrenzte und damit lebenslängliche Verwertung früherer Straftaten in Fahrerlaubnisangelegenheiten aus Verkehrssicherheitsgründen nicht mehr erforderlich. Daher hat der Bundesminister der Justiz in seinen Vorschlägen zur Änderung des Bundeszentralregistergesetzes die Verwertung von Verurteilungen auf den Zeitpunkt bis zur Tilgung ihrer Eintragung im Verkehrszentralregister begrenzt.

Die Landesregierung Nordrhein-Westfalen vertritt in ihrer Stellungnahme zu meinem 9. Tätigkeitsbericht die Auffassung, daß bis zum Inkrafttreten der beabsichtigten Änderung des § 52 Abs. 2 BZRG weiterhin eine Verwertung früherer Straftaten ohne Rücksicht auf deren Tilgung im Verkehrszentralregister und Bundeszentralregister in Fahrerlaubnisangelegenheiten vorzunehmen ist. Demgegenüber halte ich es für geboten, durch Verwaltungsvorschriften sicherzustellen, daß nicht von einer unbegrenzten Verwertbarkeit früherer Straftaten ausgegangen werden darf.

5.18.4 Medizinisch-psychologische Untersuchung

Nach meinen Feststellungen übersenden Straßenverkehrsbehörden ausnahmslos die **komplette Führerscheinakte** an die medizinisch-psychologische Untersuchungsstelle zur Begutachtung der Kraftfahreignung bei Verfahren auf Neuerteilung einer Fahrerlaubnis.

Bei der Neuerteilung einer Fahrerlaubnis kann die Verwaltungsbehörde nach § 15 c Abs. 1 i.V.m. § 12 Abs. 1 der Straßenverkehrs-Zulassungs-Ordnung (StVZO) die Beibringung des Gutachtens einer amtlich anerkannten medizinisch-psychologischen Untersuchungsstelle fordern, wenn Tatsachen bekannt sind, die Bedenken gegen die Kraftfahreignung des Betroffenen begründen. War die Fahrerlaubnis entzogen worden, weil der Bewerber wiederholt gegen verkehrsrechtliche Vorschriften oder Strafgesetze verstoßen hatte, so hat die Verwaltungsbehörde vor der Neuerteilung der Fahrerlaubnis in der Regel die Beibringung eines derartigen Gutachtens anzuordnen (§ 15 c Abs. 3 Satz 1 StVZO).

Nach dieser Regelung kann die Eignungsbegutachtung durch eine medizinisch-psychologische Untersuchungsstelle nur mit Zustimmung des Betroffenen vorgenommen werden. Daher bedarf auch die Übersendung der für die Untersuchung erforderlichen Unterlagen an die Untersuchungsstelle der Einwilligung des Betroffenen. Dementsprechend ist in Nr. 5 der Eignungsrichtlinien des Bundesministers für Verkehr vom 1. Dezember 1982 (VkBl. 1983, S. 7) bestimmt, daß bei der Anforderung eines medizinisch-psychologischen Eignungsgutachtens die Verwaltungsbehörde der Untersuchungsstelle nach Zustimmung durch den Betroffenen die für die Begutachtung erforderlichen Verwaltungsvorgänge übersendet, d. h. die Vorgänge, die im Hinblick auf die gestellten Fragen Aufschluß über den Betroffenen geben können und deren Kenntnis für die Durchführung der Untersuchung erforderlich sind.

Danach ist also grundsätzlich die Übersendung der gesamten Führerscheinakte nicht zulässig. Vielmehr hat die Behörde im Einzelfall zu prüfen, welche Vorgänge für die Erstellung des Gutachtens von der medizinisch-psychologischen Untersuchungsstelle benötigt werden. Nach meiner Auffassung darf die Verwaltungsbehörde auch nur soweit die Einwilligung des Betroffenen zur Übersendung von Unterlagen an die Untersuchungsstelle einholen, als diese zur Erstellung des Gutachtens benötigt werden. Denn der Betroffene ist, wenn er seine Fahrerlaubnis wiedererlangen möchte, auf die Durchführung der medizinisch-psychologischen Untersuchung angewiesen. Ohne Unterlagen über den zu Untersuchenden wird die Untersuchungsstelle, jedenfalls in der bisherigen Praxis, nicht tätig. Der zur Abgabe der Einwilligungserklärung aufgeforderte Betroffene befindet sich somit in einer Zwangslage. Deshalb ist eine Einwilligung, die sich auch auf Unterlagen erstreckt, die für die Erstellung des Gutachtens nicht benötigt werden, insoweit unwirksam.

Somit darf die Straßenverkehrsbehörde nur die Unterlagen an die medizinisch-psychologische Untersuchungsstelle übersenden, die für die Erstellung des Gutachtens erforderlich sind. Sie darf auch nur insoweit die Einwilligung einholen.

5.18.5 Führerscheinakte

Ein Bürger hat mich gebeten, darauf hinzuwirken, daß die ihn belastenden Unterlagen aus seiner Führerscheinakte **vernichtet** werden. Die Behörde ist dem Begehren des Bürgers nicht gefolgt, weil sie sich nach § 52 Abs. 2 des Bundeszentralregistergesetzes (BZRG) zur weiteren Aufbewahrung dieser Unterlagen für verpflichtet hält. Im übrigen sei nicht auszuschließen, daß auch zukünftig eine Beurteilung der Kraftfahreignung des Betroffenen notwendig werden würde.

Die Führerscheinakte enthält Erkenntnisse über Vorgänge, die fast 30 Jahre zurückliegen. Der jüngste Vorgang betrifft das Verfahren auf Neuerteilung der Fahrerlaubnis im Jahr 1984. In dem zu diesem Zweck erstellten medizinisch-psychologischen Gutachten wird festgestellt, daß sich der Betroffene nach der letzten Trunkenheitsfahrt im Jahr 1977 um eine Stabilisierung seiner Lebensverhältnisse bemüht habe. Es sei zu erwarten, daß er sich in der Zukunft auch im Straßenverkehr angepaßter verhalten werde. Eine erhöhte Gefährdung beim Führen von Kraftfahrzeugen ließe sich daher bei ihm nicht nachweisen. Daraufhin hat die Behörde dem Betroffenen die Fahrerlaubnis im Jahr 1984 neu erteilt.

Zur Erfüllung der Aufgaben der Erteilung und Entziehung der Fahrerlaubnis kann das Speichern von Angaben über eine frühere Tat, wenn die Verurteilung wegen dieser Tat in das Verkehrszentralregister einzutragen war (§ 52 Abs. 2 BZRG), grundsätzlich als erforderlich angesehen werden. Dies gilt insbesondere für Angaben über alkoholbedingte Verkehrsvergehen der Vergangenheit wegen der Rückfallwahrscheinlichkeit von Alkoholtätern. Gleiches muß dementsprechend auch für die weiteren in der Führerscheinakte gespeicherten Angaben gelten. Eine Aufbewahrungspflicht läßt sich aus § 52 BZRG nicht herleiten.

Allerdings kann die Speicherung derartiger Sachverhalte in den Führerscheinakten dann nicht mehr als erforderlich angesehen werden, wenn diese keine wesentlichen Erkenntnisse zur Kraftfahreignung erwarten lassen. Bei alkoholbedingten Straßenverkehrsvergehen gilt dies, wenn auf Grund der Persönlichkeitsstruktur des Alkoholauffälligen eine Rückfallgefahr nicht mehr wahrscheinlich ist. Hierzu ermöglicht insbesondere die medizinisch-psychologische Eignungsbegutachtung Erkenntnisse, die auf eine derartige Einstellungs- und Verhaltensänderung schließen lassen.

Im konkreten Fall sind keine Anhaltspunkte ersichtlich, die auch zukünftig eine Beurteilung der Kraftfahreignung des Betroffenen notwendig erscheinen lassen. Insbesondere spricht dagegen, daß über den Betroffenen seit dem Jahr 1977 keine Auffälligkeiten mehr bekanntgeworden sind und er sich nach Neuerteilung der Fahrerlaubnis im Jahr 1984 offensichtlich auch bei der Teilnahme am Straßenverkehr bewährt hat. Die Speicherung der in der Führerscheinakte des Betroffenen enthaltenen Angaben über seine früheren Auffälligkeiten ist daher zur Erfüllung der Aufgaben der Straßenverkehrsbehörde nicht mehr erforderlich. Darüber hinaus stellt die weitere Datenspeicherung eine unverhältnismäßige Belastung des Betroffenen dar, da sie ein heute nicht mehr zutreffendes Persönlichkeitsbild festhält. Dementsprechend sind die Unterlagen nach § 24 des Ordnungsbehördengesetzes i.V.m. § 32 Abs. 2 Satz 1 Nr. 3 und Satz 3 des Polizeigesetzes des Landes Nordrhein-Westfalen aus der Führerscheinakte zu entfernen und zu vernichten. Dies kann im Einzelfall die Vernichtung der gesamten Führerscheinakte bedeuten. Es bleibt dann nur noch die Karteikarte über den Führerschein nach § 10 Abs. 2 Satz 2 der Straßenverkehrs-Zulassungs-Ordnung in der Datensammlung der Straßenverkehrsbehörde.

Ich habe in dieser Angelegenheit empfohlen, die Führerscheinakte zu vernichten.

5.18.6 Halterauskünfte

Mehrere Bürgereingaben haben wiederum die Schwierigkeit deutlich gemacht, Auskünfte über Kraftfahrzeughalter ohne erfolgte Aufzeichnungen durch die speichernde Stelle nachvollziehen zu können. Die Landesregierung vertritt in ihrer Stellungnahme zu meinem 9. Tätigkeitsbericht (S. 101) die Auffassung, daß eine Verpflichtung der Zulassungsstelle zur **Aufzeichnung** von Halterauskünften nicht besteht. Hierzu verweist sie auf die Vorschrift des § 35 Abs. 3 Satz 2 des Straßenverkehrsgesetzes, nach der eine Aufzeichnungspflicht nur für die ersuchende Behörde besteht. Diese Regelung gilt allerdings nicht, wenn die Zulassungsstelle Halterauskünfte auf Ersuchen von nicht-öffentlichen Stellen und Personen erteilt. In diesen Fällen würden keinerlei Aufzeichnungen über erteilte Halterauskünfte existieren. Damit wäre weder eine Überprüfung der Zulässigkeit der Halterauskunft durch die übermittelnde Zulassungsstelle zur Erfüllung ihrer Kontrollpflicht nach § 10 Abs. 2 Nr. 6 DSG NW noch eine Kontrolle durch den Landesbeauftragten für den Datenschutz möglich. Darüber hinaus würde das Recht des Betroffenen beschnitten, auf Antrag Auskunft über die Empfänger einer Datenübermittlung nach § 18

Abs. 1 Satz 1 Nr. 3 DSG NW zu erhalten. Deshalb halte ich an meiner Auffassung fest, daß die Zulassungsstelle zur Aufzeichnung von Halterauskünften an nicht-öffentliche Stellen und Personen verpflichtet ist. Ich werde das Fehlen der Aufzeichnungen künftig beanstanden.

5.19 Wirtschaft

5.19.1 Gewerbeüberwachung

Wiederholt habe ich auf Grund von Bürgereingaben und Beratungsersuchen festgestellt, daß vor Entscheidung über die Erteilung einer Erlaubnis nach dem Gaststättengesetz regelmäßig, d. h. bei jeder Antragstellung, auch die Vorlage eines **Führungszeugnisses des Ehegatten** oder des Lebensgefährten verlangt wird.

Nach § 2 Abs. 1 Satz 1 des Gaststättengesetzes (GastG) bedarf derjenige, der ein Gaststättengewerbe betreiben will, der Erlaubnis. Die Erlaubnis ist nach § 4 Abs. 1 Nr. 1 GastG zu versagen, wenn Tatsachen die Annahme rechtfertigen, daß der Antragsteller die für den Gewerbebetrieb erforderliche Zuverlässigkeit nicht besitzt. Auf die genannten Vorschriften kann das regelmäßige Verlangen der Vorlage eines Führungszeugnisses vom Ehegatten oder Lebensgefährten des Antragstellers wegen der fehlenden Normenklarheit nicht gestützt werden. Auch die Vorschrift des § 4 Abs. 2 Satz 1 Nr. 1 der Gaststättenverordnung, nach der bei einem Antrag auf Erteilung einer Gaststättenerlaubnis insbesondere Angaben und Unterlagen über die Person des Antragstellers und seines Ehegatten erforderlich sind, ermächtigt die Behörde nicht, in allen Fällen die Vorlage des Führungszeugnisses zu verlangen.

Nur in begründeten Einzelfällen, in denen Anhaltspunkte über die Unzuverlässigkeit des Ehegatten oder des Lebensgefährten des Antragstellers vorliegen und diese für die gewerberechtliche Entscheidung von Bedeutung sind, ist das Verlangen der Vorlage eines Führungszeugnisses für diese Personen zulässig.

5.19.2 Industrie- und Handelskammern

Ein Bürger übersandte mir mehrere **Schuldnerlisten**, die er bei einem Waldspaziergang aufgefunden hatte. Die Listen stammten von einer Industrie- und Handelskammer, die sie an ein Kammermitglied im Abonnement weitergegeben hatte.

Vom Beginn meiner Tätigkeit an habe ich die für die Erteilung von Auskünften und Abschriften aus dem Schuldnerverzeichnis der Amtsgerichte maßgebenden Rechtsgrundlagen als änderungsbedürftig angesehen (1. Tätigkeitsbericht, S. 45/46; 2. Tätigkeitsbericht, S. 46/47). Seit dem Volkszählungsurteil des Bundesverfassungsgerichts ist klargestellt, daß es an einer hinreichenden Rechtsgrundlage für die weitere Verwendung der aus dem Schuldnerverzeichnis regelmäßig übermittelten Daten durch die Kammer fehlt. Weder § 915 Abs. 4 ZPO noch § 1 Abs. 1 des Gesetzes zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern lassen eine regelmäßige Über-

mittlung der Abschriften aus dem Verzeichnis an die Mitglieder der Kammern zu. Als Rechtsgrundlage kann auch nicht das Datenschutzgesetz Nordrhein-Westfalen herangezogen werden. Der regelmäßigen Überlassung der Schuldnerlisten an die Bezieher steht schon § 9 Abs. 8 i.V.m. Abs. 5 DSG NW entgegen. Danach dürfen personenbezogene Daten an Stellen außerhalb des öffentlichen Bereichs nicht regelmäßig übermittelt werden.

Es bestehen bereits Zweifel, ob die Praxis der Überlassung von Schuldnerlisten durch die Industrie- und Handelskammern auf die Grundsätze des Übergangsbonus gestützt werden kann. Zudem ist wiederum eine Legislaturperiode des Deutschen Bundestages verstrichen, ohne daß eine gesetzliche Neuregelung zum Schuldnerverzeichnis erfolgt ist. Ohne eine derartige Regelung halte ich jede weitere Übermittlung von Schuldnerlisten an die Mitglieder der Industrie- und Handelskammern für unzulässig. Nach meiner Auffassung können derzeit nur noch Einzelauskünfte für zulässig angesehen werden, soweit ein rechtliches Interesse des Auskunftbegehrenden (§ 16 Abs. 1 Satz 1 Buchstabe c DSG NW) glaubhaft gemacht wird. Andernfalls ist das Kammermitglied an das Amtsgericht zu verweisen.

Ein mittelständischer Unternehmensverband hat sich in einer Eingabe dagegen gewandt, daß die Finanzämter auf Anfrage der Industrie- und Handelskammern die **Steuermeßbeträge** für die Gewerbesteuer mitteilen. An Hand dieser Angaben ermittelt die zuständige Industrie- und Handelskammer den Beitrag, den das jeweilige Mitglied an die Kammer zu entrichten hat. Die Vereinigung der Industrie- und Handelskammern in Nordrhein-Westfalen sowie das Ministerium für Wirtschaft, Mittelstand und Technologie halten die unmittelbare Erhebung der Gewerbesteuermeßbeträge durch die Kammern bei den Finanzämtern für zulässig.

Soweit für die Zulässigkeit dieser Datenerhebung die Vorschrift des § 31 der Abgabenordnung (AO) in Betracht gezogen wird, vermag ich diese Auffassung nicht zu teilen. Nach § 31 Abs. 1 AO sind die Finanzbehörden u. a. berechtigt, Steuermeßbeträge an Körperschaften des öffentlichen Rechts zur Festsetzung von solchen Abgaben mitzuteilen, die an diese Tatsache anknüpfen. Durch diese Regelung wird zwar das Steuergeheimnis eingeschränkt, aber keine Ermächtigung für die Industrie- und Handelskammern geschaffen, die Steuermeßbeträge unmittelbar bei den Finanzbehörden zu erheben. Auch soweit die Zulässigkeit der Datenerhebung durch die Kammern auf § 12 Abs. 1 Satz 3 i.V.m. der 2. Alternative des § 13 Abs. 2 Satz 1 Buchstabe a DSG NW gestützt wird, halte ich die Voraussetzungen nicht für gegeben. Nach dieser Vorschrift dürfen personenbezogene Daten ohne Kenntnis des Betroffenen bei anderen Stellen oder Personen und zu einem anderen Zweck nur erhoben werden, wenn die Wahrnehmung einer durch Gesetz oder Rechtsverordnung zugewiesenen einzelnen Aufgabe die Verarbeitung dieser Daten zwingend voraussetzt. Grundsätzlich bestehen Zweifel an der Normenklarheit dieser Ausnahmevorschrift. Selbst wenn diese Zweifel zurückgestellt werden, kommt jedenfalls nur eine besonders restriktive Handhabung in Frage (vgl. 9. Tätigkeitsbericht, S. 12).

Danach müßte im vorliegenden Fall die Erhebung der Meßbeträge – an den Mitgliedern der Kammern vorbei – unmittelbar bei den Finanzbehörden für die ordnungsgemäße Beitragsbemessung zwingend notwendig sein. Dies vermag ich nicht zu erkennen, da die Kammern ohne weiteres die Steuermeßbeträge bei den Mitgliedern selbst erheben können. Erst dann, wenn die Angaben verweigert werden, dürften die Meßbeträge unmittelbar beim Finanzamt erhoben werden. Sofern Zweifel an der Richtigkeit der von einem Mitglied gemachten Angaben bestehen, können die Kammern ebenfalls an das Finanzamt herantreten.

Nach alledem bin ich der Auffassung des Ministeriums für Wirtschaft, Mittelstand und Technologie und der Vereinigung der Industrie- und Handelskammern in Nordrhein-Westfalen entgegengetreten. Wenn an einer unmittelbaren Erhebung der Gewerbesteuermeßbeträge durch die Industrie- und Handelskammern bei den Finanzämtern festgehalten werden soll, müßte eine entsprechende Regelung in die Satzung der Industrie- und Handelskammern aufgenommen werden.

6. Organisatorische und technische Maßnahmen

6.1 Autonome Datenverarbeitung ohne arbeitsteilige Organisation

6.1.1 Problem

Fragen, die sich aus den Anforderungen der autonomen Datenverarbeitung und der Büroautomation des kommenden Jahrzehnts ergeben, haben für die Planung vor allem auch im kommunalen Bereich erhebliche Bedeutung. Im Rahmen mehrerer Kontrollbesuche bei Städten und Gemeinden wurden insbesondere die Anforderungen zum Gewährleisten der Datensicherheit bei autonomer Datenverarbeitung ohne arbeitsteilige Organisation, die bestehenden Möglichkeiten und auch eventuelle Einschränkungen eingehend erörtert. Dabei habe ich auf die Besonderheiten hingewiesen, die eine solche Organisationsform mit sich bringt, Möglichkeiten zur Beratung und Unterstützung kleinerer Verwaltungen aufgezeigt und weitere Empfehlungen und Hinweise gegeben.

6.1.2 Besonderheiten

Insbesondere wegen der geringen Zahl der für die automatisierte Datenverarbeitung eingesetzten Mitarbeiter lassen sich bei Einsatz kleinerer Datenverarbeitungsanlagen wesentliche Maßnahmen zur Datensicherung, die bei großen Rechenzentren heute als selbstverständlich und unverzichtbar angesehen werden, nicht verwirklichen. Funktionstrennungen und eine den Anforderungen der Datensicherheit entsprechend strukturierte Organisation bedürfen einer hinreichenden Mitarbeiterzahl. Falls nur wenige Mitarbeiter die Aufgaben des Rechenzentrums wahrnehmen, ist eine Strukturierung der Organisation im allgemeinen praktisch nicht möglich. Dadurch ist die Datensicherheit beim Betrieb kleinerer Datenverarbeitungsanlagen beeinträchtigt. Diese Beeinträchtigung ist im allgemeinen so stark, daß sie bei einem großen Rechenzentrum – jedenfalls für die Verarbeitung personenbezogener Daten nach verbindlich vorgegebener Verarbeitungslogik – als nicht hinnehmbar angesehen würde.

Auf die besonderen Schwierigkeiten, die einer angemessenen Datensicherung bei Einsatz kleinerer Datenverarbeitungsanlagen entgegenstehen, habe ich erstmals in meinem 4. Tätigkeitsbericht (März 1983) hingewiesen. In der Folgezeit sah ich mehrfach Veranlassung, in meinen Tätigkeitsberichten erneut diese Problematik herauszustellen. In einem Beschluß zur Datensicherheit beim Einsatz kleinerer Datenverarbeitungsanlagen vom 10. Oktober 1988, über den ich in meinem 9. Tätigkeitsbericht (S. 106 bis 108, 137/138) berichtete, betont die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, daß die Datensicherheit und die Ordnungsmäßigkeit der Verarbeitung personenbezogener Daten beim Einsatz kleinerer Datenverarbeitungsanlagen besondere Probleme bereiten. Die Datenschutzbeauftragten empfehlen, daß vor jeder Entscheidung, ob für die Arbeiten

eines Aufgabengebiets ein PC oder eine sonstige kleinere Datenverarbeitungsanlage eingesetzt werden kann, geprüft werden muß, ob die dabei erzielbare Datensicherheit ausreichend ist. Sofern die Datensicherheit mit den verfügbaren Maßnahmen nicht in dem erforderlichen Umfang gewährleistet werden kann, muß auf den Einsatz des PCs oder der kleineren Datenverarbeitungsanlage verzichtet werden.

Als Ergebnis zahlreicher Erörterungen kann ich heute feststellen, daß die eigentliche Schwierigkeit, eine angemessene Datensicherheit bei der Datenverarbeitung ohne arbeitsteilige Organisation zu gewährleisten, daher rührt, daß der datenverarbeitenden Stelle nur in beschränktem Umfang Instrumente zur Verfügung stehen, mit denen sie eine ordnungsgemäße Arbeit sicherstellen kann. Es bereitet keine besonderen Schwierigkeiten, eine Dienstanweisung aufzustellen, die dieser Organisationsform gerecht wird. Soweit auf eine arbeitsteilige Organisation verzichtet werden muß, sind aber die verfügbaren technischen und organisatorischen Hilfsmittel unbefriedigend, mit denen sichergestellt werden soll, daß gemäß der Dienstanweisung gearbeitet wird.

6.1.3 Beratung und Unterstützung

Eine Stelle, die eine kleinere Datenverarbeitungsanlage einsetzt, bedarf im allgemeinen der fachlichen Beratung und Unterstützung. Eine Zusammenstellung von Gebieten, auf denen häufig eine fachliche Beratung und Unterstützung gewünscht wird, und Vorschläge, wie sich eine derartige Beratung und Unterstützung verwirklichen lassen, enthält mein 7. Tätigkeitsbericht (S. 182/183). Für eine Stadt oder Gemeinde ist es naheliegend, die Beratung und Unterstützung bei einer **kommunalen Datenzentrale** zu suchen. Auf die Möglichkeit, daß Datenzentralen langfristig in starkem Umfang die Aufgabe der Beratung und Unterstützung von autonomen Anwendern kleinerer Datenverarbeitungsanlagen übernehmen, habe ich in meinen Tätigkeitsberichten bereits mehrfach hingewiesen.

Während verschiedener Kontrollbesuche wurde auch die Frage der möglichen Organisationsform erörtert, durch die in einer Datenzentrale die Wahrnehmung der fachlichen Beratung und Unterstützung autonom arbeitender Anwender gefördert werden könnte. Die Situation einer Datenzentrale, die ihre Auftraggeber in der autonomen Anwendung der automatisierten Datenverarbeitung fachlich berät und unterstützt, ist ähnlich derjenigen des ADV-Bereichs eines großen Unternehmens der Privatwirtschaft im Verhältnis zu den dortigen Anwendern, die auch in zunehmendem Umfang über eine gewisse Autonomie beim Einsatz der automatisierten Datenverarbeitung verfügen. In Großunternehmen der Privatwirtschaft wurde in diesem Zusammenhang die Organisationsform des **Information Center** eingeführt. Das Information Center ist im allgemeinen organisatorischer Bestandteil des ADV-Bereichs. Es ist dort der Leitung dieses Bereichs direkt zugeordnet und steht damit organisatorisch gleichrangig neben den Bereichen Entwicklung und Durchführung. Seine Aufgabe ist die Betreuung der Anwender des Unternehmens, soweit dort automatisierte Datenverarbeitung autonom durchgeführt wird.

In Analogie zu dieser in der Privatwirtschaft bewährten Organisationsform könnte man erwägen, auch bei einer kommunalen Datenzentrale eine entsprechende Organisationseinheit zur Unterstützung und Beratung autonomer Anwender einzurichten, falls diese Aufgabe langfristig von der Datenzentrale wahrgenommen werden soll. Ich gehe davon aus, daß es auch in diesem Fall günstig wäre, diese Organisationseinheit der Leitung der Datenzentrale direkt zuzuordnen und damit gleichrangig neben die bereits existierenden Bereiche Entwicklung und Durchführung in die bestehende Hierarchie einzuordnen.

6.1.4 Empfehlungen und Hinweise

Nicht bei jeder Anwendung ist es erforderlich, über die hohe Sicherheit zu verfügen, die bei einem großen Rechenzentrum erreichbar ist. Ein besonderer Grad an Verarbeitungssicherheit ist aber jedenfalls dann angemessen, wenn die Logik der Verarbeitung verbindlich vorgeschrieben ist oder wenn diese Logik verbindlich zugesagt wurde. In diesen Fällen der Verarbeitung mit verbindlicher Verarbeitungslogik muß durch die öffentliche Stelle sichergestellt werden, daß diese Verarbeitungslogik im Rahmen der automatisierten Datenverarbeitung eingehalten wird. Daraus ergeben sich insbesondere die Anforderungen, daß

- die bereitgestellten Programme einwandfrei sind und
- unverändert zum Einsatz kommen und daß
- die öffentliche Stelle in der Lage ist, diesen unveränderten Einsatz einwandfreier Programme zu gewährleisten.

Um trotz der oben (S. 134/135) begründeten Bedenken eine angemessene Datensicherheit zu gewährleisten, habe ich den autonom arbeitenden öffentlichen Stellen einige grundsätzliche Empfehlungen und Hinweise gegeben.

6.1.4.1 Bereitstellen einwandfreier Programme

Eine autonom arbeitende kleinere datenverarbeitende Stelle kann grundsätzlich mit der gleichen Sicherheit einwandfreie Programme bereitstellen wie eine große datenverarbeitende Stelle. Grundlage der Sicherheit der großen datenverarbeitenden Stelle ist die Funktionstrennung zwischen den Aufgabenbereichen Programmierung und Anwendung. Indem man die fachlich verantwortliche und die entwickelnde Stelle personell gegeneinander abgrenzt, erleichtert man die inhaltliche Kontrolle der Programme. Die Funktionstrennung zwischen fachlich verantwortlicher und entwickelnder Stelle ist daher im allgemeinen Bestandteil eines Sicherheitskonzeptes. Eine derartige Funktionstrennung kann auch die kleinere datenverarbeitende Stelle verwirklichen.

Diese Funktionstrennung muß organisatorisch durch Regelungen zur **Programmfreigabe** ergänzt werden. Ohne Programmfreigabe durch den fachlich zuständigen Auftraggeber ist dessen Verantwortlichkeit 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.

Der Gewinn an Sicherheit, den die Funktionstrennung bringen soll, würde ohne Programmfreigabe völlig aufgegeben. Die Funktionstrennung als Bestandteil des Sicherheitskonzeptes soll die Kontrolle erleichtern. Falls diese aber nicht wahrgenommen wird, bedeutet die Funktionstrennung nichts anderes als eine Verlagerung von Arbeiten auf die Programmierung. Erst mit der abschließenden Programmfreigabe durch die fachlich verantwortliche Stelle erhält eine Funktionstrennung zwischen dieser und der entwickelnden Stelle ihren Sinn im Rahmen des Sicherheitskonzeptes. Ohne Programmfreigabe hat die Funktionstrennung sogar ein Verringern der Sicherheit zur Folge, da in diesem Fall die Möglichkeiten der fachlich verantwortlichen Stelle, eventuelle Verarbeitungsfehler zu erkennen, deutlich reduziert sind.

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.

Bei autonomer Datenverarbeitung kann organisatorisch in der geschilderten Weise verfahren werden. Wegen der hohen Kosten der Programmentwicklung und wegen der Schwierigkeit, für die programmtechnischen Arbeiten die erforderliche Fachaufsicht zu gewährleisten, ist es einer autonom arbeitenden kleineren Stelle im allgemeinen nur auf wenigen Einsatzgebieten möglich, Programme selbst zu entwickeln. Sie wird daher überwiegend Fremdprogramme einsetzen, die an anderer Stelle entwickelt wurden. Dabei gibt es sehr unterschiedliche Möglichkeiten, Fremdprogramme zu erhalten. Die Programme könnten etwa in einer kommunalen Datenzentrale entwikkelt werden, sie könnten im Rahmen einer Entwicklungsgemeinschaft entstanden sein, sie könnten aber auch vom Hersteller der Datenverarbeitungsanlage oder einer sonstigen Firma bezogen worden sein.

In allen genannten Fällen läßt sich eine einwandfreie Funktionstrennung zwischen der programmierenden Stelle und dem Anwender verwirklichen. Der Anwender trägt auch bei dieser Organisationsform die uneingeschränkte Verantwortung für den logischen Inhalt der von ihm eingesetzten Programme. Damit er dieser Verantwortung gerecht werden kann, bedürfen die Programme der ordnungsgemäßen Freigabe durch den Anwender.

Allerdings ist ein Anwender häufig durch die Anforderungen des als Voraussetzung für eine Programmfreigabe erforderlichen Anwendertests überfordert. Es ist daher üblich, daß verschiedene Anwender kooperieren, um gemeinsam und arbeitsteilig die Anwendertests der bei ihnen eingesetzten Programme durchführen zu können. Gegen eine solche Arbeitsteilung bestehen dann keine Bedenken, wenn gewährleistet ist, daß der Anwendertest in jedem Falle ordnungsgemäß und unter alleiniger Verantwortung der Anwender durchgeführt wird.

Im allgemeinen ist es allerdings notwendig, nicht nur Freigabe und Einsatz von Fremdprogrammen verbindlich zu regeln, sondern auch festzulegen, ob, in welchem Umfang und durch welche Organisationseinheiten oder Mitarbeiter im eigenen Hause Programme entwickelt werden dürfen. Dabei stehen zwei Fragen im Vordergrund.

- Welche Befugnisse hat der ADV-Bereich oder der Systemverwalter? Hinweise zu dieser Frage werden unten (S. 140/141) gegeben.
- Ist individuelle Datenverarbeitung zugelassen? Fragen zur individuellen Datenverarbeitung werden unten (S. 150/151) behandelt.

6.1.4.2 Einsatz unveränderter Programme

Im Unterschied zu der Situation bei großen Rechenzentren ist es für eine autonom arbeitende kleinere datenverarbeitende Stelle im allgemeinen nicht leicht sicherzustellen, daß ausschließlich unveränderte Programme zum Einsatz kommen. Große Rechenzentren stützen sich für diese Aufgabe auf die Funktionstrennung zwischen Programmierung und Produktion. Insbesondere darf es dem Programmierer nicht möglich sein, freigegebene Programme unzulässigerweise zu ändern.

Bei der Funktionstrennung zwischen Programmierung und Produktion spielt in großen Rechenzentren im allgemeinen die Arbeitsvorbereitung eine wichtige Rolle. Es gehört üblicherweise zu den Aufgaben der Arbeitsvorbereitung, nach erfolgter Programmfreigabe die Programme einschließlich sämtlicher Unterlagen von der Programmierung zu übernehmen. Bei dieser Übernahme prüft die Arbeitsvorbereitung unter anderem die Ordnungsmäßigkeit der Freigabe und die Vollständigkeit der Unterlagen. Durch die Arbeitsvorbereitung werden die freigegebenen Programme dann für die Produktionsläufe bereitgestellt.

Vor ihrer Freigabe befinden sich Programme üblicherweise in maschinell geführten Testbibliotheken. Nach der Freigabe werden sie in die Bibliotheken der freigegebenen Programme übernommen. Für die Übernahme in die Bibliotheken der freigegebenen Programme ist in diesem Fall die Arbeitsvorbereitung zuständig. Aus Gründen der Datensicherheit ist im allgemeinen ausschließlich die Arbeitsvorbereitung für die Bibliotheken der freigegebenen Programme verantwortlich. Diese Funktionstrennung zwischen Programmierung, Arbeitsvorbereitung und Maschinenbedienung ist eine der wesentlichen Grundlagen der Datensicherheit in großen Rechenzentren.

Bei der autonom arbeitenden kleineren Stelle übernimmt der Maschinenbediener im allgemeinen in Personalunion die Aufgabe des Arbeitsvorbereiters. Eine Funktionstrennung scheidet wegen der geringen Mitarbeiterzahl aus. Sehr wünschenswert wäre es daher, wenn durch die Technik Hilfsmittel bereitgestellt würden, die es gestatten, diesen Mangel an Datensicherheit auszugleichen. So könnte etwa das Datenverarbeitungssystem der datenverarbeitenden Stelle eine Möglichkeit bieten sicherzustellen, daß bei der Eingabe neuer Programme und bei deren Änderung ein Vier-Augen-Prinzip eingehalten werden muß. Langfristig sollte angestrebt werden, durch ein ge-

eignetes technisches Verfahren zu gewährleisten, daß freigegebene Programme nur in unveränderter Form zum Ablauf kommen können.

Für die Anforderung, daß freigegebene Programme nur in unveränderter Form zum Ablauf kommen, würde die Möglichkeit des Versiegelns dieser Programme einen wesentlichen Fortschritt bedeuten. Unter Versiegeln wird das Zuordnen einer mehrstelligen Kennzahl zu einem Programm verstanden. Durch die Logik der Zuordnung muß gewährleistet sein, daß ein Ändern des Programms ohne Auswirkung auf die Kennzahl unmöglich ist. Ich hoffe, das Versiegeln von Programmen wird in einigen Jahren zu den selbstverständlichen Maßnahmen der Datensicherung gehören. Damit wäre ein Mittel verfügbar, um die bisher häufig unzureichende Datensicherheit bei kleineren Datenverarbeitungsanlagen wesentlich zu verbessern.

6.1.4.3 Auswertung der Systemnachrichten

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

Die aufgezeichneten Systemnachrichten müssen zusammen mit den bereits genannten Anforderungen an die technischen Möglichkeiten des Datenverarbeitungssystems (oben S. 138/139) hinreichende Voraussetzungen für die Revision der Datenverarbeitung bieten. Für kleinere Datenverarbeitungsanlagen sollte angestrebt werden, diese Voraussetzungen so zu verwirklichen, daß der Revisor kein Fachmann der automatisierten Datenverarbeitung sein muß. Die Summe aller Maßnahmen, die als Voraussetzung für die Revisionsfähigkeit eines Datenverarbeitungssystems verwirklicht sind, könnte man als dessen Revisionsoberfläche bezeichnen. Zu fordern ist daher, daß auch kleinere Datenverarbeitungsanlagen über eine aussagekräftige und **unmanipulierbare Revisionsoberfläche** verfügen und daß diese Revisionsoberfläche von einem Revisor genutzt werden kann, der kein Fachmann der automatisierten Datenverarbeitung ist.

Einige Voraussetzungen müssen erfüllt sein, damit die aufgezeichneten Systemnachrichten einen solchen wesentlichen Beitrag zur Datensicherheit leisten können.

- Die Systemnachrichten müssen hinreichend aussagekräftig sein. Es müssen alle wesentlichen Aktivitäten aufgezeichnet sein, und zu jeder

einzelnen Aktivität müssen die Aufzeichnungen alle für die Revision bedeutsamen Einzelangaben enthalten.

- Die Systemnachrichten müssen gegen Veränderung geschützt sein. Es muß gewährleistet sein, daß nachträgliche Änderungen an den aufgezeichneten Systemnachrichten ausgeschlossen sind.
- Die Systemnachrichten müssen vollständig sein. Es muß sichergestellt sein, daß die Aufzeichnung von Systemnachrichten nicht unterdrückt werden kann und daß aufgezeichnete Systemnachrichten nicht nachträglich gelöscht werden können.
- Es sollten Hilfsprogramme zum Auswerten der aufgezeichneten Systemnachrichten verfügbar sein. Aussagekräftig aufgezeichnete Systemnachrichten können einen sehr großen Umfang haben. Wichtig ist es daher, über Möglichkeiten zu verfügen, die Systemnachrichten mit Hilfe geeigneter Auswerteprogramme zu überprüfen. Die Systemnachrichten sollten dazu in maschinenlesbarer Form archiviert werden, und es sollten Programme für deren Auswertung verfügbar sein.

6.1.4.4 Festlegung der Aufgaben des ADV-Bereichs oder des Systemverwalters

Fragen der Verantwortung und Zuständigkeit sind von großer Bedeutung für die Datensicherheit. Sie müssen für die Betroffenen und für Dritte erkennbar unmißverständlich geregelt sein. Die Regelung sollte daher schriftlich erfolgen.

Bei jeder öffentlichen Stelle, die ihre automatisierte Datenverarbeitung autonom durchführt, gibt es einen ADV-Bereich oder wenigstens einen Mitarbeiter, er wird im folgenden als Systemverwalter bezeichnet, zu dessen Aufgaben die Betreuung der automatisierten Datenverarbeitung gehört. Festlegung und Abgrenzung der Zuständigkeit des ADV-Bereichs oder des Systemverwalters sind von erheblicher Bedeutung für die Datensicherheit.

Zu regeln sind insbesondere folgende Fragen:

- Unter welchen Voraussetzungen dürfen von den Mitarbeitern des ADV-Bereichs oder dem Systemverwalter Programme entwickelt oder geändert werden?
- Welche Aufgabe hat der ADV-Bereich oder der Systemverwalter im Zusammenhang mit der Beschaffung von Programmen?
- Unter welchen Voraussetzungen und wie hat die Eingabe von neuen Programmen oder von Programmänderungen in die Datenverarbeitungsanlage zu erfolgen?
- Welche Zuständigkeit hat der Leiter des ADV-Bereichs oder der Systemverwalter bezüglich der zu treffenden Maßnahmen zur Verbesserung der Datensicherheit?

- Welche Verantwortung und Verpflichtungen hat der ADV-Bereich oder der Systemverwalter im Zusammenhang mit der Bedienung der Datenverarbeitungsanlage?
- Welche Verantwortung und Verpflichtungen hat der Leiter des ADV-Bereichs oder der Systemverwalter im Zusammenhang mit der Kontrolle der Nutzung der Datenverarbeitungsanlage?

Ich habe jeweils empfohlen, Aufgabe und Verantwortung der Mitarbeiter des ADV-Bereichs oder des Systemverwalters umfassend schriftlich zu regeln.

6.1.4.5 Notwendigkeit und Inhalt einer Dienstanweisung für die automatisierte Datenverarbeitung

Es ist Aufgabe jeder öffentlichen Stelle, diejenigen Anweisungen zu erteilen, die erforderlich sind, damit die öffentliche Stelle die Datensicherheit bei Einsatz der automatisierten Datenverarbeitung gewährleisten kann. Darüber hinaus hat die öffentliche Stelle sicherzustellen, daß sich alle Mitarbeiter entsprechend den erteilten Anweisungen verhalten. Als Voraussetzung dazu ist es erforderlich, dieses erwartete Verhalten verbindlich vorzuschreiben. Bei der großen Bedeutung der Datensicherheit sollten Anweisungen, die der Datensicherheit dienen, schriftlich erfolgen. Mündliche Anweisungen werden häufig mißverstanden oder als weniger verbindlich angesehen.

Die Gesamtheit der Anweisungen zur Datensicherung sollte zu einer schriftlichen Dienstanweisung zusammengefaßt werden. Erfahrungsgemäß läßt sich nur auf diese Weise sicherstellen, daß jedem Mitarbeiter die ihn betreffenden Anweisungen bekannt sind. Auch kann dadurch vermieden werden, daß Zweifel über die Gültigkeit von Anweisungen entstehen, falls zu verschiedenen Zeiten unterschiedliche Anweisungen zu demselben Sachverhalt getroffen werden.

Die von mir herausgegebenen Organisationshilfen zur Datensicherung (unten S. 166/167) können Hinweise für den Inhalt der Dienstanweisung geben. Die Organisationshilfen enthalten jeweils Kataloge regelungsbedürftiger Sachverhalte für eine Dienstanweisung. Sie können daher genutzt werden, um zu überprüfen, ob in einer Dienstanweisung sämtliche im Rahmen der Datensicherung regelungsbedüftigen Sachverhalte geregelt werden.

6.1.4.6 Institutionalisierung einer internen Kontrolle

Die Einhaltung der Vorschriften zur Datensicherung bedarf der Kontrolle. Jede datenverarbeitende Stelle ist daher zur datenschutzrechtlichen Selbstkontrolle verpflichtet.

Zur Überwachung gibt es im wesentlichen die drei Möglichkeiten der Überwachung durch den Vorgesetzten, der Funktionstrennung und der institutionalisierten Kontrolle. Die Überwachung durch den Vorgesetzten ist zwar als selbstverständlich vorauszusetzen. Jedoch ist gerade bei öffentlichen Stellen, die eine kleinere Datenverarbeitungsanlage autonom betreiben, nicht auszuschließen, daß den für die Überwachung der automatisierten Daten-

verarbeitung zuständigen Vorgesetzten das dafür erforderliche Fachwissen fehlt. Die Möglichkeit der Selbstkontrolle der öffentlichen Stelle ist insoweit erheblich eingeschränkt. Auch Möglichkeiten zur Funktionstrennung sind jedenfalls insoweit nur sehr beschränkt vorhanden, als die Funktionstrennung die Arbeitsdurchführung betreffen soll (oben S. 134). Daher muß die dritte Möglichkeit der Überwachung, die institutionalisierte Kontrolle, verwirklicht werden.

Einer Stelle, die eine kleinere Datenverarbeitungsanlage einsetzt, ist es aber im allgemeinen nicht leicht, für die interne Kontrolle einen fachlich geeigneten Mitarbeiter mit der erforderlichen organisatorischen Unabhängigkeit zu finden. Bei Kontrollbesuchen im kommunalen Bereich wurden insbesondere folgende Möglichkeiten erörtert, die interne Kontrolle zu institutionalisieren.

- Die Aufgabe der internen Kontrolle könnte dem eigenen Rechnungsprüfungsamt übertragen werden. Diese Möglichkeit besteht allerdings nur, falls es die Revisionsoberfläche (oben S. 139) der Anwendungen dem Rechnungsprüfungsamt möglich macht, diese Aufgabe wahrzunehmen. In diesem Fall sollte der Rat der Stadt oder Gemeinde die Rechnungsprüfungsordnung um die Aufgabe der Prüfung der organisatorischen und technischen Maßnahmen zum Sicherstellen einer den Vorschriften und Weisungen entsprechenden Verarbeitung und zum Verhindern von Verlust, unzulässiger Verarbeitung oder Kenntnisnahme von Daten ergänzen.
- Es könnte ein Auftrag zur Durchführung der internen Kontrolle an das Rechnungsprüfungsamt des Kreises oder aber an eine kommunale Datenzentrale gegeben werden. Die Möglichkeit, externe Stellen mit der Durchführung der Kontrolle zu beauftragen, habe ich in meinen Tätigkeitsberichten mehrfach erörtert. Dabei bedarf allerdings die Abgrenzung der Verantwortungen einer unmißverständlichen Regelung, worauf ich bereits in meinem 7. Tätigkeitsbericht (S. 185) hingewiesen habe.
- Im Rahmen der interkommunalen Zusammenarbeit wäre es möglich, einen oder mehrere Mitarbeiter mit der Durchführung der internen Kontrolle bei einer Reihe von Städten und Gemeinden zu beauftragen. Die Mitarbeiter könnten organisatorisch einer der beteiligten Städte oder Gemeinden zugeordnet werden.

6.2 Spezielle Techniken oder Einsatzarten der Datenverarbeitung

6.2.1 Kleinere Datenverarbeitungsanlagen

Die Zahl der kleineren Datenverarbeitungsanlagen und insbesondere auch der persönlichen Computer (PCs), die zur Verarbeitung personenbezogener Daten eingesetzt werden, nimmt stark zu. Es erscheint angemessen, einige spezielle Beobachtungen und Empfehlungen ausdrücklich herauszustellen.

Besonderer Aufmerksamkeit bedarf die Sicherung von PCs gegen **Entwendung**. Gegen diese Anforderung wird leider in Einzelfällen verstoßen. Es sind bereits Fälle bekannt, in denen PCs, auf deren Festplatte personenbezogene Daten gespeichert waren, entwendet wurden.

Beim Kontrollbesuch einer Hochschule habe ich festgestellt, daß für die Verarbeitung personenbezogener Daten an verschiedenen Stellen PCs eingesetzt werden. Während des Kontrollbesuchs wurden zwei Einsatzfälle eingehend geprüft. In beiden Fällen sind die PCs mit Festplatten ausgerüstet, auf denen die personenbezogenen Daten auch außerhalb der Dienstzeit gespeichert sind. Im Hinblick auf diese Speicherung personenbezogener Daten ist eine zusätzliche Sicherung der Geräte außerhalb der Dienstzeit angemessen. Eine solche Sicherung erfolgt aber nicht. Das Fehlen der zusätzlichen Sicherung ist insbesondere bei einem der Einsatzfälle wegen der Empfindlichkeit der gespeicherten Daten besonders bedenklich.

Während des Kontrollbesuchs wurde erörtert, daß die Hochschule prüfen sollte, ob es möglich ist, die Sicherheit der PCs außerhalb der Dienstzeit zu erhöhen. Sollte eine derartige Möglichkeit nicht bestehen, wäre zu prüfen, ob die Verarbeitung der Dateien in die zentrale Datenverarbeitungsanlage der Verwaltung übernommen werden kann. Sofern die Datensicherheit mit den verfügbaren Maßnahmen nicht in dem erforderlichen Umfang gewährleistet werden kann, muß auf den Einsatz der PCs verzichtet werden. Der Hochschule wurde darüber hinaus empfohlen, alle weiteren Einsatzfälle von PCs zur Verarbeitung personenbezogener Daten daraufhin zu überprüfen, ob die Geräte außerhalb der Dienstzeit hinreichend gesichert sind.

Bezüglich des Einsatzes einer kleineren Datenverarbeitungsanlage in einer Schule wurde ich um Beratung gebeten. Zur Erörterung stand ein **Mehrplatzsystem**, das sowohl für Aufgaben der Verwaltung als auch für Übungsarbeiten im Rahmen des Unterrichts eingesetzt werden sollte. Der Zugriff sollte durch einen Paßwortschutz gesichert und die Verwaltungsdaten zusätzlich durch Umsetzen in ein anderes Format geschützt werden.

Gegen die vorgesehene Doppelnutzung einer kleineren Datenverarbeitungsanlage für die Abwicklung von Verwaltungs- und Übungsarbeiten in der Schule habe ich erhebliche Bedenken geäußert. Meine Bedenken beruhen zunächst auf Zweifeln an der Wirksamkeit der angeführten Sicherungen. Bei On-line-Zugriffen ist das Authentifizieren dessen, der einen Zugriff auf die Daten beabsichtigt, eine der zentralen Aufgaben der Datensicherung. Ein weit verbreitetes Verfahren, das den Zugriff über Datenendgeräte sichern soll, ist der in dem Beratungsersuchen genannte Paßwortschutz. Allerdings haben meine Erfahrungen bei Kontrollbesuchen gezeigt, daß der Paßwortschutz im allgemeinen nur unzulänglich verwirklicht ist und daher nur selten die erforderliche Authentifizierung mit hinreichender Sicherheit gewährleistet. Über entsprechende Bedenken berichtete ich bereits mehrfach in meinen Tätigkeitsberichten.

Aber auch die zweite vorgesehene Sicherungsmaßnahme, das Umsetzen von Daten in ein anderes Format, bietet keinen erheblichen Schutz gegen die unbefugte Kenntnisnahme der Daten. Selbst der Hinweis, Daten seien verschlüsselt, hat ohne ergänzende Ausführungen nur geringen Aussagewert bezüglich der erreichten Schutzwirkung. Unter „verschlüsseln" wird in vielen Fällen eine Maßnahme verstanden, die für den Fall, daß die verschlüsselten Daten in fremde Hände gelangen, keine angemessene Sicherheit gewährleistet.

Unabhängig von diesen speziellen Bedenken habe ich aber auch erhebliche Zweifel, ob im Einzelfall bei einer Anlage, die für den Unterricht bestimmt ist und die auch gleichzeitig für die schulinterne Verwaltung genutzt wird, durch die Nutzung technischer Sicherheitsvorrichtungen ein unbefugter Zugriff auf personenbezogene Daten ausgeschlossen ist. Die Kenntnisse und Fähigkeiten von Schülern im Umgang mit Datenverarbeitungsanlagen sollten nicht unterschätzt werden. Ich habe daher angeregt zu prüfen, ob für den Unterricht und für die schulinterne Verwaltung jeweils getrennte Datenverarbeitungsanlagen eingesetzt werden können.

Für einen Leitfaden „Datenschutz und Datensicherheit beim Einsatz von Personal-Computern im Bereich der gesetzlichen Krankenversicherung" habe ich ausdrücklich darauf hingewiesen, daß bei Einsatz von PCs die **Beratung der Anwender** eine wichtige Aufgabe ist. Die Auswahl der zweckmäßigen Maßnahmen zur Datensicherung und die Entscheidung darüber, welche Maßnahmen angemessen sind, setzen Fachwissen der automatisierten Datenverarbeitung voraus. Erfahrungsgemäß verfügen die Anwender häufig nicht oder nicht in hinreichendem Umfang über derartiges Fachwissen. Es sollte daher im Bereich der Krankenkassen Stellen geben, die solches Fachwissen in Form von Beratung und anderen Leistungen auf dem Gebiet der automatisierten Datenverarbeitung anbieten.

6.2.2 Privater persönlicher Computer (PC)

Beim Einsatz kleinerer Datenverarbeitungsanlagen, vor allem von PCs, bereitet das Gewährleisten der Datensicherheit und der Ordnungsmäßigkeit der Datenverarbeitung besondere Probleme (oben S. 142 bis 144). Zusätzliche Bedenken sind angebracht, wenn ein Mitarbeiter seinen privaten PC für dienstliche Zwecke einsetzt. Diese Bedenken werden auch von der Landesregierung geteilt. In ihrer Stellungnahme zu meinem 9. Tätigkeitsbericht teilt die Landesregierung darüber hinaus mit, daß die Ressorts deshalb in ihren Geschäftsbereichen die Nutzung privater PCs für dienstliche Zwecke grundsätzlich nicht gestatten werden (Drucksache 10/5055, S. 53).

Gegenwärtig ist der Einsatz privater PCs für dienstliche Zwecke innerhalb der Landesverwaltung unterschiedlich geregelt. So hat der Innenminister für den Bereich der Polizei durch Erlaß vom 24. August 1987 – IV D 4–182/1875 – angeordnet, daß keine privaten Computer für dienstliche Zwecke genutzt werden dürfen.

Mit Erlaß vom 31. Mai 1989 – V A 3–37.10 – hat der Innenminister den Regierungspräsidenten eine Musterdienstanweisung über Datenschutz und Datensicherheit beim Einsatz von DV-Geräten mit der Bitte übersandt, diese Regelung gemäß § 2 Nr. 6 der Geschäftsordnung für die Regierungspräsidenten zu erlassen. Nach § 3 Satz 1 dieser Musterdienstanweisung dürfen private DV-Geräte, Datenträger und Software für dienstliche Zwecke nicht eingesetzt werden. Dies gilt nach § 3 Satz 2 der Musterdienstanweisung nicht für private DV-Geräte, Datenträger und Software, die mit finanzieller Unterstützung eines öffentlichen Kostenträgers als Arbeitsmittel für Schwerbehinderte beschafft worden sind.

Mit Erlaß vom 7. März 1985–0 2200–1 – II B 1 – (Betr.: Benutzung privateigener automatischer Einrichtungen zur Erledigung dienstlicher Aufgaben) hatte der Finanzminister des Landes Nordrhein-Westfalen geregelt, daß dem Steuergeheimnis (§ 30 AO) unterliegende Daten in Dateien auf privateigenen externen Datenträgern (z.B. Magnetbandkassetten, Disketten, Magnetplatten) nicht gespeichert werden dürfen. Der Erlaß des Finanzministers vom 21. Februar 1990–0 2200–1 – II B 1 – zu demselben Betreff enthält diese einschränkende Regelung leider nicht mehr.

Mit Rücksicht auf die mögliche weitere Entwicklung in der Praxis halte ich es für angebracht, die folgenden Hinweise und Empfehlungen zu der angesprochenen Problematik zu geben.

6.2.2.1 Allgemeine Bewertung

Falls ein Mitarbeiter seinen privaten PC oder seinen privaten maschinenlesbaren Datenträger für dienstliche Zwecke nutzt, könnte diese Nutzung grundsätzlich im Rahmen einer Datenverarbeitung im Auftrag (§ 11 DSG NW, § 8 BDSG, § 80 SGB X) erfolgen. In diesem Fall müßte der Mitarbeiter als Privatperson von der öffentlichen Stelle mit der Durchführung eines Auftrags zur Datenverarbeitung beauftragt werden. Nach meinem derzeitigen Erkenntnisstand wird von dieser Möglichkeit aber kein Gebrauch gemacht. Falls für die Verarbeitung der Daten das Datenschutzgesetz Nordrhein-Westfalen zur Anwendung kommt, wäre die öffentliche Stelle bei Datenverarbeitung im Auftrag unter anderem verpflichtet sicherzustellen, daß sich der Mitarbeiter der Kontrolle des Landesbeauftragten für den Datenschutz Nordrhein-Westfalen unterwirft (§ 11 Abs. 3 Satz 1 DSG NW).

Die Nutzung eines privaten PCs oder eines privaten maschinenlesbaren Datenträgers wird also im allgemeinen keine Datenverarbeitung im Auftrag im Sinne von § 11 DSG NW, § 8 BDSG oder § 80 SGB X sein. Entscheidend für die Bewertung der Verarbeitung ist in dieser Situation die Frage, in welchem Umfang die öffentliche Stelle in der Lage ist, die rechtmäßige und sichere Verarbeitung der Daten zu gewährleisten. Von einer Verarbeitung der Daten durch die öffentliche Stelle kann hier nur dann ausgegangen werden, wenn die öffentliche Stelle selbst über die Daten und bei einer Verarbeitung mit verbindlicher Verarbeitungslogik auch über die Programme verfügt. Falls die Möglichkeiten der öffentlichen Stelle, über die Daten zu verfügen, zu stark eingeschränkt und die Daten in entsprechendem Ausmaß von dem Mitarbeiter in die Privatsphäre übernommen worden sind, wird sich die Frage stellen, ob noch von einer Weitergabe innerhalb der öffentlichen Stelle gesprochen werden kann.

Kriterien dafür, in welchem Umfang die öffentliche Stelle die Verfügungsgewalt über die Daten besitzt, sind etwa:

- Gültigkeit der Regelungen einer Dienstanweisung der öffentlichen Stelle in solcher Weise, als erfolge die Verarbeitung auf einer Anlage der öffentlichen Stelle,
- Kenntnis der öffentlichen Stelle von den gespeicherten Dateien,

- Kenntnis einer eventuellen Revisionsinstanz der öffentlichen Stelle von den gespeicherten Dateien,

- Vorlage einer Beschreibung der Dateien bei dem Landesbeauftragten für den Datenschutz und

- Gewährleisten der Kontrollmöglichkeit durch den Landesbeauftragten für den Datenschutz.

Wichtig ist insbesondere auch die Frage, ob das Eigentumsrecht des Mitarbeiters an dem PC oder dem Datenträger in einer ungewöhnlichen Situation verhindern könnte, daß die öffentliche Stelle über die Daten verfügt. Bei einem Unfall oder einer schweren Erkrankung des Mitarbeiters könnte diese Frage erhebliche praktische Bedeutung gewinnen.

Kriterien für eine Verfügungsgewalt der öffentlichen Stelle über die Programme sind darüber hinaus vor allem deren Freigabe durch die öffentliche Stelle und deren Aufnahme in ein Programmverzeichnis der öffentlichen Stelle.

Nach den mir vorliegenden Erkenntnissen gehe ich davon aus, daß bei der Verarbeitung von Daten auf einem privaten PC oder bei dem Speichern von Daten auf einem privaten maschinenlesbaren Datenträger die Möglichkeit der öffentlichen Stelle, selbst über die Daten zu verfügen, im allgemeinen sehr stark eingeschränkt ist, weil die Daten in erheblichem Umfang von dem Mitarbeiter in die Privatsphäre übernommen worden sind.

Man könnte daran denken, den Anforderungen des Datenschutzes bei Einsatz eines privaten PCs oder eines privaten maschinenlesbaren Datenträgers durch eine Regelung zu entsprechen, durch die die öffentliche Stelle rechtmäßiger Besitzer des PCs oder des Datenträgers wird, solange auf einem von diesen personenbezogene Daten gespeichert sind. In diesem Fall könnte grundsätzlich durch geeignete zusätzliche Maßnahmen gewährleistet werden, daß die Daten nicht die Verfügungsgewalt der öffentlichen Stelle verlassen. Dazu müßte allerdings eine entsprechende verbindliche Vereinbarung zwischen der öffentlichen Stelle und dem Mitarbeiter vorliegen, die schriftlich erfolgen sollte. Mir ist kein Fall bekannt, bei dem eine derartige Vereinbarung getroffen worden ist.

Nach meinen Erfahrungen gehe ich daher davon aus, daß von den Beteiligten bei der Benutzung eines privaten PCs oder eines privaten maschinenlesbaren Datenträgers zur Verarbeitung personenbezogener dienstlicher Daten weder unterstellt wird, es erfolge Datenverarbeitung im Auftrag noch unterstellt wird, die öffentliche Stelle sei rechtmäßiger Besitzer des PCs oder des Datenträgers.

Diese Aussagen gelten auch dann, wenn der Mitarbeiter in dienstlicher Eigenschaft Daten bei Dritten erhebt und in seinen eigenen PC oder auf seinen eigenen maschinenlesbaren Datenträger überträgt.

6.2.2.2 Einzelfragen des Datenschutzes

Unabhängig von der allgemeinen Bewertung des Einsatzes privater PCs oder privater maschinenlesbarer Datenträger durch Mitarbeiter öffentlicher Stellen ergeben sich zusätzliche Bedenken:

- Nach § 23 Abs. 1 Satz 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 DSG NW) vorzulegen. Ich habe erhebliche Zweifel, ob dies bei Einsatz eines privaten PCs geschieht.
- Dem Betroffenen (§ 3 Abs. 1 DSG NW) ist von der speichernden Stelle gemäß § 18 Abs. 1 Satz 1 DSG NW Auskunft zu erteilen. Bei Einsatz privater PCs oder privater maschinenlesbarer Datenträger wird die speichernde Stelle im allgemeinen nicht oder nur schwer in der Lage sein, die Möglichkeit der Auskunfterteilung zu gewährleisten.
- Die Einhaltung der Vorschriften zur Datensicherung bedarf der Kontrolle. Die öffentliche Stelle ist daher zur datenschutzrechtlichen Selbstkontrolle verpflichtet. In Bezug auf private PCs und private maschinenlesbare Datenträger werden derartige Kontrollen im allgemeinen nicht wahrgenommen.
- Bevor ein privater PC oder ein privater maschinenlesbarer Datenträger, der zur Verarbeitung personenbezogener dienstlicher Daten benutzt worden ist, wieder uneingeschränkt in den privaten Bereich des Mitarbeiters übernommen werden darf, sind alle gespeicherten personenbezogenen dienstlichen Daten zu löschen. Der Mitarbeiter hat aber häufig keine Möglichkeit zum Löschen der Magnetplatte seines PCs und eventuell auch seiner Disketten. Er mag sogar der Überzeugung sein, Magnetplatte und Disketten gelöscht zu haben, und die Daten sind dennoch unverändert auf diesen Speichern verfügbar (vgl. unten S. 151 bis 153). Manche Anwendungshandbücher sind in dieser Frage irreführend. Es ist keinesfalls selten, daß ein Befehl, der nach der Beschreibung im Anwendungshandbuch Daten löscht, kein Löschen bewirkt, sondern lediglich ein Freigeben der Datenblöcke, in denen die zu löschenden Daten gespeichert sind. Die Daten selbst sind nach Ausführung eines solchen Befehls „Löschen" unverändert gespeichert, und es gibt sogar Dienstprogramme, die auf solche Weise „gelöschte" Daten wieder verfügbar machen.

6.2.2.3 Zusammenfassende Wertung und Empfehlungen

Ich habe erhebliche Zweifel, ob der Einsatz privater PCs oder privater maschinenlesbarer Datenträger zur Verarbeitung dienstlicher personenbezogener Daten noch zugelassen werden kann. In deren Einsatz sehe ich grundsätzlich eine erhebliche Beeinträchtigung des Datenschutzes.

Im Hinblick auf seine Zuständigkeit für die Koordinierung der automatisierten Datenverarbeitung (§ 4 Abs. 1 Satz 1 ADVG NW) habe ich daher den Innenminister gebeten, sich für eine innerhalb der Landesverwaltung einheitliche

Lösung der angesprochenen Problematik unter Berücksichtigung der im folgenden genannten Empfehlungen einzusetzen.

- Bekanntlich wurden durch das Land Nordrhein-Westfalen in den letzten Jahren zahlreiche PCs beschafft. Die Zahl wird weiter zunehmen. Ich gehe daher davon aus, daß die dienstliche Nutzung privater PCs im Verhältnis zum Einsatz behördeneigener PCs von sehr geringer Bedeutung ist. Im Hinblick auf die erheblichen Bedenken, die gegen einen Einsatz privater PCs zur Verarbeitung dienstlicher personenbezogener Daten bestehen, habe ich empfohlen zu prüfen, ob ein derartiger Einsatz ausnahmslos untersagt werden kann. Meines Erachtens wäre es angemessen, in den wenigen Fällen, in denen man auf den Einsatz des privaten PCs zur Verarbeitung personenbezogener dienstlicher Daten nicht verzichten zu können glaubt, einen dienstlichen PC zu beschaffen.
- Mir ist kein Grund ersichtlich, der die Nutzung privater externer maschinenlesbarer Datenträger zum Speichern dienstlicher personenbezogener Daten erforderlich macht. Ich habe daher empfohlen, eine derartige Nutzung ausnahmslos zu untersagen.
- Falls es als unumgänglich angesehen werden sollte, Ausnahmen von dem Verbot zuzulassen, personenbezogene dienstliche Daten mit Hilfe privater PCs oder privater maschinenlesbarer Datenträger zu verarbeiten, sollte verbindlich vorgeschrieben werden, daß jeweils darzulegen ist, wie der Einsatz des privaten PCs oder Datenträgers zu bewerten ist (oben S. 145/146), ob die öffentliche Stelle – unter Berücksichtigung der oben angeführten Kriterien – über die gespeicherten Daten uneingeschränkt verfügen kann und wie den oben aufgeführten Beeinträchtigungen des Datenschutzes (oben S. 147) wirksam begegnet wird.

6.2.3 Lokales Netzwerk (LAN)

In meinem 7. Tätigkeitsbericht (S. 159 bis 162) hatte ich auf die Beeinträchtigung der Datensicherheit bei Einsatz des Schnittstellenvervielfachers SK 12 der Deutschen Bundespost hingewiesen. Die Beeinträchtigung der Datensicherheit liegt darin, daß der SK 12 Daten, die von einer Datenverarbeitungsanlage an ein hinter dem SK 12 angeschlossenes Datenendgerät gesendet werden, in alle hinter dem SK 12 angeschlossenen Leitungen überträgt. Die Daten werden daher jedem der an diese Leitungen angeschlossenen Datenendgeräte zum Empfang angeboten. In ihrer Stellungnahme zu meinem 7. Tätigkeitsbericht teilte die Landesregierung mit, daß die Frage der Beeinträchtigung der Datensicherheit beim Einsatz des SK 12 auf Veranlassung des Innenministers auch im Kooperationsausschuß ADV Bund/Länder/Gemeinden behandelt worden sei. Der Kooperationsausschuß halte es ebenfalls für erforderlich, daß bei Netznutzungen durch öffentliche Stellen die mit dem SK 12 verbundenen Gefahren untersucht und Alternativen geprüft werden.

Eine vergleichbare Auswirkung hat ein lokales Netzwerk (LAN, local area network). Es gibt unterschiedliche Techniken für den Betrieb lokaler Netz-

werke. Alle Techniken haben aber die Eigenart, daß eine Nachricht, die eines der angeschlossenen Geräte absendet, allen anderen angeschlossenen Geräten oder jedenfalls einer großen Zahl der angeschlossenen Geräte angeboten wird. Jedes Gerät, dem die Nachricht angeboten wird, überprüft, ob es Adressat der angebotenen Nachricht ist. Falls es Adressat ist, wird die Nachricht in das Gerät übernommen und möglicherweise gespeichert oder auf dem Bildschirm dargestellt. Falls das Gerät nicht Adressat ist, wird die Nachricht nicht übernommen. Bei einer solchen Technik besteht daher am Ort eines jeden angesprochenen Gerätes die Möglichkeit, die übertragene Nachricht zu lesen. Die Datensicherheit ist dadurch beeinträchtigt.

Mehrfach wurde mir während Kontrollbesuchen berichtet, es werde möglicherweise in Zukunft ein lokales Netzwerk installiert. Ich wies jeweils darauf hin, daß die öffentliche Stelle in eigener Verantwortung prüfen müsse, welche Maßnahmen zur Datensicherung im Hinblick auf dessen Technik erforderlich sind und ob eine angemessene Datensicherheit mit den realisierbaren Maßnahmen gewährleistet werden kann. An die zu treffenden Maßnahmen sind nur geringe Anforderungen zu stellen, wenn alle Mitarbeiter, die an den an ein lokales Netz angeschlossenen Geräten tätig sind, gleiche Zugriffsbefugnisse haben. In diesem Fall kann die Datensicherheit im allgemeinen angemessen gewährleistet werden. Einer besonderen Überprüfung bedarf die Datensicherheit aber jedenfalls dann, wenn unterschiedliche Organisationseinheiten an ein lokales Netzwerk angeschlossen sind. Diese Aussage gilt auch dann, wenn alle angeschlossenen Organisationseinheiten zu derselben öffentlichen Stelle gehören.

In jedem Fall muß auch bedacht werden, daß ein Wartungstechniker, der die Wartung eines Gerätes, das an ein lokales Netz angeschlossen ist, durchzuführen hat, im allgemeinen von der öffentlichen Stelle nicht fachlich beaufsichtigt werden kann. Es ist davon auszugehen, daß der Wartungstechniker Daten, die über eine Leitung übertragen werden, auch dann zur Kenntnis nehmen kann, wenn das zu wartende Gerät außer Betrieb oder defekt ist. Der Wartungstechniker kann damit über alle Daten verfügen, die auf einer Leitung, zu der er Zugriff hat, übertragen werden. Eine angemessene Maßnahme, um dieser Unsicherheit zu begegnen, kann darin bestehen festzulegen, daß personenbezogene Daten in dem lokalen Netz nicht übertragen werden dürfen, solange ein Wartungstechniker Zugang zu der Leitung oder zu einem der angeschlossenen Geräte hat.

Jede öffentliche Stelle sollte die durch die Technik des Netzes bedingte Unsicherheit bei der Überprüfung der Datensicherheit eines lokalen Netzes und bei der Entscheidung über die zu treffenden Maßnahmen berücksichtigen. Gegebenenfalls sollte die öffentliche Stelle darüber hinaus prüfen, in welchem Umfang die an ein lokales Netz angeschlossenen Stellen über die bestehende Gefährdung der Datensicherheit informiert sein müssen. Bedauerlicherweise fehlen Hinweise auf die durch die Technik bedingte Unsicherheit lokaler Netze in einer Bekanntmachung des Innenministeriums vom 22. August 1990 (MBl. NW. 1990, S. 1250) „Hinweise und Empfehlungen für die Verkabelung in Gebäuden beim Einsatz von Lokalen Netzen (LAN) und Ter-

minalnetzen – Verkabelungsempfehlungen –". In einem Schreiben an das Innenministerium habe ich angeregt, den Behörden und Einrichtungen des Landes baldmöglichst entsprechende Hinweise zu geben.

6.2.4 Individuelle Datenverarbeitung (IDV)

Von individueller Datenverarbeitung (IDV) wird bei der automatisierten Datenverarbeitung dann gesprochen, wenn der einzelne Mitarbeiter oder die einzelne Organisationseinheit des Anwenderbereichs für die eigene Arbeit Programme selbst entwickelt oder entsprechende Fremdprogramme selbst bezieht und die Verarbeitung von Daten mit diesen Programmen selbst durchführt. IDV ist sowohl auf einem PC als auch auf einer zentralen Datenverarbeitungsanlage möglich. Im Rahmen meiner Kontrolltätigkeit hatte ich wiederholt Gelegenheit, beide Arten von IDV zu prüfen und dazu Empfehlungen auszusprechen.

Beim Kontrollbesuch einer Stadt stellte ich fest, daß durch einen Mitarbeiter des Bauaufsichtsamts ein Programm zum Bearbeiten von Baugenehmigungen konzipiert worden war. Das Programm wurde in einer Programmiersprache geschrieben, die einen interpretativen Ablauf des Programms in der zentralen Datenverarbeitungsanlage des Amtes für automatisierte Informationsverarbeitung ermöglichte. Programmierarbeiten an dem Programm für das Bearbeiten von Baugenehmigungen wurden bisher ausschließlich von dem Mitarbeiter des Bauaufsichtsamts durchgeführt.

Ich habe darauf hingewiesen, daß der erforderliche, von dem Programmierertest unabhängige Anwendertest und die anschließende Anwenderfreigabe nicht Aufgaben dieses Mitarbeiters sein können. Diese Aufgaben müssen vielmehr solchen Mitarbeitern des Fachamts übertragen werden, die an der Programmierung nicht beteiligt waren.

Für die Datensicherheit ist es wichtig, daß die Arbeitsvorbereitung ihre Aufgaben uneingeschränkt wahrnehmen kann (oben S. 138). Ein Programm mit verbindlicher Verarbeitungslogik, das auf der zentralen Datenverarbeitungsanlage zum Ablauf kommen soll, sollte daher nach seiner Freigabe auch dann der Arbeitsvorbereitung des Amtes für automatisierte Informationsverarbeitung übergeben werden, wenn die Entwicklung durch einen Mitarbeiter des Fachamts erfolgte. Der Einsatz des Programms unterliegt dadurch wesentlichen Sicherungen eines großen Rechenzentrums.

Zum Gewährleisten der Datensicherheit sollte eine Regelung aller Einzelheiten zur individuellen Datenverarbeitung durch eine besondere Dienstanweisung erfolgen. Während verschiedener Kontrollbesuche wurden die Anforderungen an eine solche Dienstanweisung eingehend erörtert. Grundlage der Erörterung bildete die von mir herausgegebene Organisationshilfe zur Datensicherung bei individueller Datenverarbeitung (Organisationshilfe-IDV, unten S. 166/167).

Mehrfach machte ich gleichartige Feststellungen und sah mich zu entsprechenden Empfehlungen veranlaßt:

- Die Zulässigkeit von IDV für die Verarbeitung von personenbezogenen Daten ist nicht verbindlich geregelt. Im Hinblick auf die Verantwortung der öffentlichen Stelle sollte eine derartige Regelung jedenfalls für alle Verarbeitungen mit verbindlicher Verarbeitungslogik erfolgen.
- Es gibt keine schriftliche Dienstanweisung für den Einsatz von IDV. Eine solche Dienstanweisung sollte erstellt werden, bevor bei der öffentlichen Stelle erstmalig personenbezogene Daten im Rahmen von IDV verarbeitet werden. Der Organisationshilfe-IDV können Hinweise entnommen werden, welche Sachverhalte im Rahmen der Dienstanweisung zu regeln sind.
- Eine solche Dienstanweisung sollte unter anderem auch Aussagen zur Verantwortlichkeit der Vorgesetzten bei Einsatz von IDV enthalten.
- Insbesondere bei einer Datenverarbeitung mit verbindlicher Verarbeitungslogik ist es von besonderer Bedeutung, den Einsatz der IDV durch eine institutionalisierte interne Kontrolle (oben S. 141/142) laufend zu überwachen.
- Auch bei Einsatz von IDV ist eine Programmfreigabe in allen Fällen der Verarbeitung mit verbindlicher Verarbeitungslogik erforderlich. Die Freigabe ist Aufgabe der fachlich zuständigen Organisationseinheit und nicht des Mitarbeiters, der die Anwendung programmiert hat. Die Dienstanweisung sollte eine entsprechende Vorschrift enthalten.
- Im Hinblick auf die besondere Bedeutung von Programmen mit verbindlicher Verarbeitungslogik sollte die öffentliche Stelle über eine zentrale Übersicht entsprechender Programme verfügen, die im Rahmen von IDV eingesetzt werden.

6.2.5 Textverarbeitung

Bei einer Reihe von Kontrollbesuchen wurde von mir unter anderem die Sicherheit der Textverarbeitung geprüft. Immer wieder mußte ich dabei feststellen, daß der geprüften Stelle irreführende Aussagen bezüglich des Löschens gespeicherter Dokumente vorlagen. Es gab jeweils einen Löschbefehl für Dokumente, die auf der Festplatte eines Textverarbeitungssystems gespeichert waren. Dieser Löschbefehl sollte nach dem Inhalt der Bedienungsanleitung ein Dokument oder mehrere Dokumente auf der Festplatte löschen. In Wirklichkeit wurden die Dokumente aber nicht gelöscht, sondern nur der Verfügungsgewalt der Schreibkraft entzogen. Es wäre für Dritte mit entsprechenden Detailkenntnissen der automatisierten Datenverarbeitung möglich gewesen, in solcher Weise „gelöschte" Dokumente zu lesen.

Folgendes Beispiel ist repräsentativ für alle derartigen Feststellungen: Eine Stadt setzt auf ihrem Verwaltungsrechner ein Programm zur Textverarbeitung ein. Dieses Programm ermöglicht es, von den Datenendgeräten aus Schreib- und Archivierungsarbeiten durchzuführen. Die eingegebenen Dokumente werden auf dem Plattenspeicher des Verwaltungsrechners gespeichert.

Während des Kontrollbesuchs wurde die Frage erörtert, wann und durch welchen Vorgang gespeicherte Dokumente gelöscht werden. Die Stadt berichtete, es gebe einen Löschauftrag, der am Datenendgerät eingegeben werde

und das Löschen eines Dokuments bewirke. Um zu klären, welche Wirkung der Löschauftrag für ein gespeichertes Dokument hat, wurde während des Kontrollbesuchs eine entsprechende Frage an die Lieferfirma gerichtet.

Die Lieferfirma erteilte folgende Antwort: „Ein Dokument wird in 512 Byte Blöcken auf allen Platten des Verwaltungsrechners verteilt. Mit dem Löschauftrag werden neben dem Objekteintrag alle Querverbindungen zwischen den einzelnen Datenblöcken physisch gelöscht. Die freiwerdenden Plätze werden dynamisch von anderen Objektinhalten überschrieben. Somit ist eine Wiederherstellung von gelöschten Dokumenten praktisch unmöglich."

Aus dieser Antwort der Lieferfirma entnehme ich, daß ein Dokument nicht unmittelbar als Folge des auf dieses Dokument gerichteten Löschauftrags gelöscht wird. Nach Ausführung des Löschauftrags ist vielmehr der gesamte Text des Dokuments noch unverändert auf dem Plattenspeicher vorhanden. Er ist aufgeteilt in Blöcke von einer Länge von 512 Bytes. Die einzelnen Datenblöcke sind allerdings nicht mehr miteinander verbunden.

Die Ausführung des Löschauftrags für ein Dokument bewirkt also zunächst lediglich, daß die Datenblöcke, in denen das Dokument gespeichert ist, zum erneuten Beschreiben freigegeben werden und daß die Verbindung zwischen diesen Datenblöcken aufgelöst wird. Das Löschen eines solchen Datenblocks erfolgt erst durch Überschreiben bei der späteren Eingabe neuer Dokumente. Der Antwort der Lieferfirma kann nicht entnommen werden, durch welches neu eingegebene Dokument ein bestimmter gespeicherter Datenblock überschrieben und damit gelöscht wird.

Der Löschauftrag bewirkt also kein Löschen, sondern lediglich ein Freigeben der Datenblöcke, in denen das zu löschende Dokument gespeichert ist. Die Stadt hat keine Möglichkeit sicherzustellen, daß ein gespeichertes Dokument wirklich gelöscht wird. Ihr fehlt auch jegliche Information darüber, ob und wann das Löschen aller Datenblöcke, in denen ein bestimmtes Dokument gespeichert ist, erfolgt.

Die Datensicherheit ist dadurch beeinträchtigt. Während des Kontrollbesuchs wurde erörtert, daß folgende Maßnahmen zu treffen sind, um dennoch eine angemessene Datensicherheit zu gewährleisten:

- Die Stadt hat sicherzustellen, daß Unbefugte keine Möglichkeit haben, Dokumente aus der Festplatte auszulesen. Insbesondere sollte sichergestellt werden, daß die Festplatte nicht ungelöscht die Verfügungsgewalt der Stadt verläßt.
- Es sollte geklärt werden, ob es Dokumente gibt, die wegen ihrer Empfindlichkeit nicht in den Verwaltungsrechner eingegeben werden dürfen, solange keine Möglichkeit besteht, sie bei Bedarf zu löschen.
- Die Benutzer sollten darüber informiert werden, welche Auswirkungen ein Löschauftrag für ein gespeichertes Dokument hat. Die Benutzer sollten wissen, daß die einzelnen Datenblöcke, in denen ihr Dokument gespeichert ist, auch nach Ausführung des Löschauftrags inhaltlich unverändert auf dem Plattenspeicher verfügbar sind.

- Mit der Lieferfirma sollte geklärt werden, ob es Möglichkeiten gibt, einzelne Dokumente gezielt zu löschen oder aber die ganze Festplatte oder bestimmte Bereiche der Festplatte zu löschen. Unter Löschen ist dabei ein Vorgang zu verstehen, der bewirkt, daß vorher gespeicherte Daten nicht mehr auf der Platte aufgezeichnet sind und daher auch der Platte durch kein technisches Verfahren mehr entnommen werden können. Löschen erfolgt im allgemeinen durch Überschreiben mit einer anderen Information.

Die Stadt sollte über die Möglichkeit verfügen, einzelne Dokumente, einzelne Plattenbereiche oder die ganze Festplatte zu löschen.

6.2.6 Telefax

Der Telefaxdienst der Deutschen Bundespost Telekom, mit dessen Hilfe Abbildungen von Texten, Zeichnungen und Diagrammen als Fernkopie übertragen werden können, hat bereits weite Verbreitung gefunden. Es ist damit zu rechnen, daß seine Bedeutung in den kommenden Jahren erheblich zunimmt. Unter diesen Umständen halte ich es für geboten, auf bestehende Unsicherheiten hinzuweisen und Wege aufzuzeigen, wie diesen Unsicherheiten begegnet werden kann.

Mir wurden aus meinem Kontrollbereich bislang erst zwei Fälle mitgeteilt, in denen eine Fernkopie nicht an die vorgesehenen Empfänger, sondern an Dritte übertragen wurde.

Nach meiner Einschätzung ist aber zu befürchten, daß die Zahl der Übermittlungen von Fernkopien an einen falschen Anschluß mit zunehmender Nutzung des Telefaxdienstes ansteigen wird. Falsche Übermittlungen aus technischen Gründen werden möglicherweise sogar überproportional ansteigen; sie können immer dann erfolgen, wenn die angewählte Nummer in eine Nummer verfälscht wird, die eine Telefaxrufnummer ist.

Diese Entwicklung ist insbesondere deshalb bedenklich, weil der Absender einer Fernkopie nicht ohne besondere Maßnahmen feststellen kann, ob die Verbindung zu dem Telefaxanschluß des vorgesehenen Empfängers der Fernkopie hergestellt wurde. Es besteht leider nicht die vom Telefonieren bekannte Situation, bei der der Anrufende aus dem Gespräch im allgemeinen sofort erkennen kann, ob er mit dem vorgesehenen Partner verbunden ist.

Hinweisen möchte ich auch auf eine mögliche Unsicherheit beim Empfänger der Fernkopie. Eine Fernkopie ist bei dem Empfänger ohne weiteres lesbar, sobald sie an dem dortigen Fernkopierer ausgegeben ist. Die Mitarbeiter der Stelle, bei der der Fernkopierer aufgestellt ist, sind somit in der Lage, den Inhalt einer Fernkopie zur Kenntnis zu nehmen. Ob weitere Personen den Inhalt einer Fernkopie zur Kenntnis nehmen können, kann von dem Absender der Fernkopie mangels Kenntnis des organisatorischen Umfeldes bei dem Empfänger häufig nicht beurteilt werden. Der Datenschutz ist insoweit als beeinträchtigt anzusehen.

Angesichts der bestehenden Unsicherheiten sollte die Übertragung personenbezogener Daten als Fernkopie nur unter besonderen organisatorischen

Vorkehrungen erfolgen dürfen. Daher gebe ich folgende Anregungen und Empfehlungen:

a) Es sollte von jeder speichernden Stelle festgelegt werden, ob es in ihrem Bereich personenbezogene Daten gibt, die wegen ihrer Art nicht als Fernkopie übertragen werden dürfen. Diese sollten ausschließlich auf anderem Wege weitergegeben werden.

b) Es muß sichergestellt werden, daß beim Anwählen die Telefaxrufnummer des vorgesehenen Empfängers verwendet wird. Dazu könnte zum Beispiel die Anwendung des Vier-Augen-Prinzips vorgeschrieben werden.

c) Es muß sichergestellt werden, daß es sich bei dem Gerät, zu dem die Verbindung hergestellt wurde, um das Gerät des vorgesehenen Empfängers handelt. Hierzu sind folgende Voraussetzungen zu erfüllen:

   - Eine Übertragung sollte nur erfolgen, wenn der Fernkopierer des Empfängers seine Kennung an den Absender zurückgesandt hat. Ob es sich bei einer Rufnummer, die das sendende Gerät anzeigt, lediglich um die eingegebene Nummer oder um eine von dem angewählten Gerät zurückgesandte Kennung handelt, ist an den ersten Stellen zu erkennen. Eine zurückgesandte Kennung enthält in den ersten zwei Stellen die Landeskennzahl (Bundesrepublik Deutschland = 49). An Geräte, die über keine Kennung verfügen und die daher auch keine Kennung zurücksenden können, sollten keine personenbezogenen Daten übertragen werden.
   - Die angezeigte Kennung muß zuverlässig mit der anzuwählenden Telefaxrufnummer verglichen worden sein, bevor die Übertragung personenbezogener Daten beginnen darf. Erfahrungsgemäß ist es kaum möglich, den Vergleich bis zum Beginn der Übertragung mit hinreichender Sorgfalt durchzuführen. Am Anfang der Übertragung sollte daher ein Vorblatt mit Daten übertragen werden, die ihrer Art nach weniger sensibel sind. Die Übertragung des Vorblatts sollte so viel Zeit in Anspruch nehmen, daß in dieser Zeit ein sorgfältiger Vergleich der angezeigten Kennung mit der anzuwählenden Telefaxrufnummer möglich ist. Die Übertragung der Fernkopie ist selbstverständlich unverzüglich abzubrechen, falls bei dem Vergleich der Kennung des Fernkopierers des Empfängers mit der anzuwählenden Telefaxrufnummer eine Unstimmigkeit festgestellt wird.

     Als Voraussetzung für den hier empfohlenen Ablauf muß der Absender über einen Fernkopierer verfügen, bei dem die Kennung des angewählten Gerätes während der gesamten Übertragung der Fernkopie angezeigt wird. Für die Übertragung personenbezogener Daten sollten daher nur Geräte eingesetzt werden, die diese Eigenschaft besitzen.

     Die Kontrolle der Kennung könnte zuverlässiger erfolgen und würde erheblich erleichtert, wenn die Kennung nicht nur aus der Telefaxrufnummer, sondern zusätzlich aus einer Buchstabenfolge – etwa einer Kurzbezeichnung des angewählten Empfängers – bestehen würde. Die Sicherheit des Telefaxdienstes könnte durch eine derartige Erweiterung der Kennung erheblich verbessert werden. Wegen der in einer

erweiterten Kennung enthaltenen Redundanz wäre es sogar sinnvoll, im absendenden Gerät einen automatischen Vergleich der eingegebenen (erweiterten) Kennung mit der von dem angewählten Gerät zurückgesandten Kennung durchzuführen.

d) Es muß sichergestellt werden, daß personenbezogene Daten nur dann als Fernkopie übertragen werden, wenn dem Absender bekannt ist, daß die räumlichen und organisatorischen Gegebenheiten bei dem vorgesehenen Empfänger den Anforderungen des Datenschutzes entsprechen. Bei dem Empfänger muß sichergestellt sein, daß jede ankommende Fernkopie behandelt wird wie sonstige geöffnete Post, die noch nicht von dem dazu Berechtigten zur weiteren Bearbeitung ausgezeichnet ist.

6.3 Verarbeitung personenbezogener Daten im Auftrag

Mehrfach wurde ich von öffentlichen Stellen um Beratung im Zusammenhang mit der Verarbeitung personenbezogener Daten im Auftrag gebeten. Über einige Fälle, die von allgemeiner Bedeutung sind, wird im folgenden berichtet.

Eine Stadt, deren Daten im Rechenzentrum des Kreises gespeichert werden sollten, wollte wissen, welche Weisungen (§ 11 Abs. 1 Satz 3 DSG NW) sie zu erteilen und welche Überprüfungen des Auftragnehmers sie im Rahmen der **Auftragskontrolle** (§ 10 Abs. 2 Nr. 8 DSG NW) durchzuführen hat. Zu den erforderlichen Weisungen habe ich die Stadt auf folgendes hingewiesen:

- Das Speichern von Daten bei dem Kreis als Datenverarbeitung im Auftrag der Stadt bedarf eines schriftlichen Auftrages (§ 11 Abs. 1 Satz 5 DSG NW). In diesem Auftrag hat die Stadt festzulegen, welche Daten mit welchem Programm unter welchen Voraussetzungen zu verarbeiten sind. Darüber hinaus sollte das Auftragsschreiben eventuelle zusätzliche Anforderungen im Rahmen der Datensicherung nach § 10 Abs. 2 DSG NW enthalten.
- Die im Rahmen der Datenverarbeitung im Auftrag eingesetzten Programme müssen von der Stadt als Auftraggeber freigegeben sein. Durch die Programmfreigabe übernimmt die Stadt die Verantwortung für den logischen Inhalt der für sie eingesetzten Programme. Die Stadt bestimmt dadurch die Logik der in ihrem Auftrag erfolgenden Verarbeitung von Daten. Die Programmfreigabe ist daher ein wesentlicher Bestandteil der erforderlichen Weisungen.
- Welche Weisungen darüber hinaus erforderlich sind, muß die Stadt aus der dortigen Situation in eigener Verantwortung entscheiden.

Im Rahmen der Auftragskontrolle sind Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten geeignet sind zu gewährleisten, daß Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (§ 10 Abs. 2 Nr. 8 DSG NW). Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (§ 10 Abs. 1 Satz 2 DSG NW). Ein bloßer Hinweis auf § 10 DSG NW oder auf § 10 Abs. 2 Nr. 8 DSG NW ist zur Auftragskontrolle nicht ausreichend.

Im Hinblick auf die von der Stadt gestellte Frage habe ich einige Hinweise zu den im Rahmen der Auftragskontrolle erforderlichen Überprüfungen gegeben. Die Datensicherheit beruht im wesentlichen auf drei Arten von Maßnahmen:

- Es müssen die zur Datensicherung erforderlichen einzelnen technischen und organisatorischen Maßnahmen getroffen werden. Zu den möglichen Maßnahmen können etwa Funktionstrennungen im Datenverarbeitungsbereich, ein Zugangskontrollsystem für das Rechenzentrum oder auch automatisierte Aufzeichnungen über die Systemnutzung der Datenverarbeitungsanlage gehören.
- Es muß eine Dienstanweisung zur Datensicherung geben, in der festgelegt ist, wie der einzelne Mitarbeiter sich zu verhalten hat, damit die erforderliche Datensicherheit gewährleistet ist.
- Die datenverarbeitende Stelle muß sicherstellen, daß die Dienstanweisung befolgt wird. Dazu ist es im allgemeinen erforderlich, eine interne Kontrolle zu institutionalisieren. Diese interne Kontrolle prüft die Einhaltung organisatorischer Regelungen in ähnlicher Weise wie ein Rechnungsprüfungsamt die Einhaltung gegebener Vorschriften bei geldwirksamen Vorgängen überprüft.

Im Rahmen der Auftragskontrolle ist es jedenfalls erforderlich, daß sich die Stadt überzeugt, daß bei dem Kreis die Datensicherheit für die Auftragsdatenverarbeitung in angemessenem Umfang gewährleistet ist. Dazu müssen bei dem Kreis Maßnahmen getroffen sein, die sicherstellen, daß den oben genannten Anforderungen in angemessenem Umfang entsprochen wird.

In welchem Umfang zusätzliche Maßnahmen zur Überprüfung des Auftragnehmers im Rahmen der Auftragskontrolle erforderlich sind, die insbesondere dem Überprüfen des Ablaufs der Verarbeitung dienen, sollte in Kenntnis der dortigen Situation entschieden werden. Insbesondere könnte eine Vereinbarung mit dem Kreis getroffen werden, daß Berichte der internen Kontrolle, soweit sie für die Datenverarbeitung im Auftrag von Bedeutung sein können, der Stadt im Rahmen der Auftragskontrolle zugänglich gemacht werden.

In diesem Zusammenhang habe ich darauf hingewiesen, daß die einzelnen Auftraggeber ihre Auftragskontrolle nicht unabhängig voneinander wahrnehmen müssen. Es bestehen keine Bedenken gegen eine Vereinbarung der Auftraggeber, die eine gemeinsame Wahrnehmung der Auftragskontrolle zum Ziel hat. So könnte z. B. einer der Auftraggeber die Auftragskontrolle im Namen aller Auftraggeber wahrnehmen.

Ein Rechenzentrum, das die Datenverarbeitung für eine Anzahl von Ortskrankenkassen durchführt, wollte wissen, wie die **Nutzung eines fremden Datennetzes** rechtlich zu werten sei. Das Rechenzentrum untersuchte die Möglichkeit der Nutzung eines Leitungsnetzes, das von einer privaten Bank verwaltet wird. Über dieses Leitungsnetz sollte der Datenaustausch zwischen dem Rechenzentrum und den an dieses angeschlossenen Ortskrankenkassen erfolgen.

Bei einer eventuellen Nutzung des von der Bank verwalteten Leitungsnetzes durch das Rechenzentrum würde es sich um Datenverarbeitung im Auftrag

durch die Bank handeln. Soweit ein öffentlicher Auftraggeber als Sozialleistungsträger oder als Verband von Sozialleistungsträgern dem Sozialgeheimnis (§ 35 SGB I) unterliegende personenbezogene Daten in Dateien im Auftrag verarbeiten läßt, finden nach § 79 Abs. 1 SGB X anstelle des Datenschutzgesetzes Nordrhein-Westfalen das Bundesdatenschutzgesetz sowie § 80 SGB X Anwendung. Nach § 80 Abs. 1 SGB X gelten neben § 8 Abs. 1 BDSG die bereichspezifischen Vorschriften des § 80 Abs. 2 bis 5 SGB X. Die Verarbeitung personenbezogener Daten im Auftrag durch eine nicht-öffentliche Stelle ist nach § 80 Abs. 5 SGB X nur zulässig, wenn anders Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der automatischen Datenverarbeitung erheblich kostengünstiger besorgt werden können.

Nach § 80 Abs. 2 SGB X ist eine Auftragserteilung nur zulässig, wenn der Datenschutz beim Auftragnehmer nach der Art der zu verarbeitenden Daten den Anforderungen genügt, die für den Auftraggeber gelten (Satz 1). Der Auftraggeber ist verpflichtet, erforderlichenfalls Weisungen zur Ergänzung der beim Auftragnehmer vorhandenen technischen und organisatorischen Maßnahmen (§ 6 Abs. 1 des Bundesdatenschutzgesetzes) zu erteilen (Satz 2). Wird der Auftrag an eine nicht-öffentliche Stelle erteilt, so hat sich der Auftragnehmer vorher schriftlich bestimmten Kontrollen durch den Auftraggeber zu unterwerfen; der Auftraggeber muß jederzeit berechtigt sein, mit Mitteln des § 30 Abs. 2 und 3 BDSG die Einhaltung der Vorschriften über den Datenschutz sowie seiner ergänzenden Weisungen zu den technischen und organisatorischen Maßnahmen zu überwachen (§ 80 Abs. 2 Satz 3 SGB X). Nach Nr. 8 der Anlage zu § 6 Abs. 1 Satz 1 BDSG hat der Auftraggeber Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle).

Soweit ein öffentlicher Auftraggeber personenbezogene Daten, die nicht dem Sozialgeheimnis unterliegen, im Auftrag verarbeiten läßt, sind die entsprechenden Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen anzuwenden. Hierzu zählen die Bestimmungen des § 11 DSG NW sowie die Auftragskontrolle nach § 10 Abs. 2 Nr. 8 DSG NW. Insbesondere ist nach § 11 Abs. 3 DSG NW, sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, der Auftraggeber verpflichtet sicherzustellen, daß der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt und sich, sofern die Datenverarbeitung im Geltungsbereich dieses Gesetzes durchgeführt wird, der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft (Satz 1). Bei einer Auftragsdurchführung außerhalb des Geltungsbereichs dieses Gesetzes ist die zuständige Datenschutzkontrollbehörde zu unterrichten (Satz 2).

Das Beratungsersuchen einer Datenzentrale gab mir Veranlassung, mich zu der Situation zu äußern, die entsteht, wenn ein zur **Unterstützung der Auftraggeber** zuständiges Programmierdezernat der Datenzentrale die Daten des Auftraggebers inhaltlich oder fachlich bearbeitet. Falls die Datenzentrale für ihren Auftraggeber nicht nur die reine Abwicklung der Datenverarbeitung,

sondern auch eine inhaltliche oder fachliche Bearbeitung von dessen Daten übernehmen würde, läge insoweit keine Datenverarbeitung im Auftrag im Sinne des § 11 DSG NW vor. In diesem Fall wäre die Datenzentrale insoweit gegenüber ihrem Auftraggeber Dritter (§ 3 Abs. 3 DSG NW), die Daten wären durch Weitergabe an die Datenzentrale an diese übermittelt (§ 3 Abs. 2 Nr. 4 DSG NW), und die Datenzentrale wäre u. a. verpflichtet, dem Landesbeauftragten für den Datenschutz die Beschreibung einer solchen Datei, in der personenbezogene Daten gespeichert sind, vorzulegen (§ 23 Abs. 1 DSG NW). Soweit das Datenschutzgesetz Nordrhein-Westfalen anzuwenden ist, richtet sich die Zulässigkeit der Übermittlung nach § 14 DSG NW.

Bei einer solchen inhaltlichen oder fachlichen Bearbeitung der Daten des Auftraggebers wäre das Dezernat der Datenzentrale, das die Arbeiten durchführt, in der Rolle des Anwenders oder Auftraggebers gegenüber Programmierung und Produktion. Die Bezeichnung eines solchen Dezernats, von dem die Datenzentrale sagt, daß bei ihm nicht die Entwicklung und weitere Wartung der DV-Verfahren liege, als Programmierdezernat wäre bedenklich. Die organisatorische Zuordnung des Dezernats zum Bereich der Programmierung würde eine Durchbrechung der für die Datensicherheit wichtigen Funktionstrennung zwischen Anwendung und Programmierung bedeuten.

6.4 Funktionstrennungen als Maßnahmen zur Datensicherung

Funktionstrennungen sind nur bei hinreichender Mitarbeiterzahl durchführbar. Zweck von Funktionstrennungen als Sicherheitsmaßnahmen ist es vor allem sicherzustellen, daß ausschließlich freigegebene Programme in unveränderter Fassung zum Einsatz gelangen und daß diese Programme nur anweisungsgemäß zum Ablauf kommen (oben S. 136 bis 139). Dazu gibt es in großen Rechenzentren eine entsprechende Dienstanweisung. Die genannten Maßnahmen helfen sichern, daß diese Dienstanweisung ohne Ausnahme eingehalten wird.

Auch für kleinere Rechenzentren ist es möglich, die Dienstanweisung so zu gestalten, daß bei deren Einhaltung ausschließlich freigegebene Programme in unveränderter Fassung zum Einsatz gelangen und diese Programme nur anweisungsgemäß zum Ablauf kommen können. Schwierigkeiten für den sicheren Betrieb kleinerer Rechenzentren ergeben sich daher nicht etwa aus neuartigen Anforderungen an den Inhalt der Dienstanweisung. Schwierig ist dagegen bei einem kleineren Rechenzentrum die Kontrolle der Einhaltung der Dienstanweisung. Diese Schwierigkeit resultiert unter anderem daraus, daß die bei großen datenverarbeitenden Stellen selbstverständlichen Funktionstrennungen nur teilweise verwirklicht werden können.

Bei Kontrollbesuchen in kleineren Kommunalverwaltungen habe ich Aufgabenzuordnungen angetroffen, bei denen wichtige Funktionstrennungen, die bei großen datenverarbeitenden Stellen selbstverständlich sind, verletzt werden.

So hat in einer Gemeinde der Gemeindedirektor in einem Schreiben an alle Mitarbeiterinnen und Mitarbeiter im Hause unter anderem mitgeteilt, daß auf die Bestellung eines Systemverwalters augenblicklich verzichtet wird. Für die Betreuung der Datenverarbeitungsanlage und der Programme seien zwei bestimmte Mitarbeiter zuständig. Die beiden Mitarbeiter, denen damit die Zuständigkeit für die Betreuung der Datenverarbeitungsanlage und der Programme übertragen wurde, waren die Dezernenten der Dezernate III und I. Zu dem Dezernat III gehört unter anderem die Kämmerei; der Dezernent ist gleichzeitig zweiter stellvertretender Gemeindedirektor. Zum Dezernat I gehören das Hauptamt und das Ordnungsamt.

Die durch diese Aufgabenzuordnung aufgehobene Funktionstrennung zwischen dem Anwenderbereich und der Durchführung der automatisierten Datenverarbeitung ist für die Datensicherheit bedenklich. Während des Kontrollbesuchs wurde diese Tatsache eingehend erörtert. Die Gemeinde berichtete, es werde in Kürze ein neuer Mitarbeiter eingestellt, der als Systemverwalter eingesetzt werden und dem die Verantwortung für die Durchführung der automatisierten Datenverarbeitung übertragen werden soll. Der neue Mitarbeiter soll dem Hauptamt zugeordnet werden. Ich habe empfohlen, baldmöglichst durch eine geeignete Maßnahme die Funktionstrennung zwischen dem Anwenderbereich und der Durchführung der automatisierten Datenverarbeitung zu verwirklichen.

Bei einer anderen Gemeinde ist der Abteilungsleiter der Haupt- und Personalabteilung auch für die Systemverwaltung zuständig. Diese Zusammenfassung von Aufgaben ist unter dem Gesichtspunkt der Datensicherheit nicht günstig. Daher sollte eine Funktionstrennung erfolgen. Die Gemeinde berichtete, es sei beabsichtigt, die Aufgabe der Systemverwaltung in Kürze einem Mitarbeiter in dieser Abteilung zu übertragen.

In einer Stadt wurden folgende besondere Aufgabenzuordnungen vorgenommen:

- Die Stadt hat Kontrolldatenverwalter mit besonderen Funktionen im Rahmen der Durchführung der automatisierten Datenverarbeitung bestimmt. Zu den Funktionen der Kontrolldatenverwalter gehören die Zuordnung von Befugnissen der Mitarbeiter beim Zugriff über Datenendgeräte, die Zuordnung der Zugriffsmöglichkeit zu Programmen über einzelne Datenendgeräte, das Ermöglichen der Eingabe von Paßworten und die Eingabe von Steuerparametern zur Programmgestaltung bei speziellen Programmen.

  Zu Kontrolldatenverwaltern wurden der Leiter der Stadtkämmerei und ein Mitarbeiter aus der Stadtkämmerei bestellt.

- Die wesentlichen zentralen Aufgaben bei der Durchführung der automatisierten Datenverarbeitung nehmen die Systemverantwortlichen wahr. Zu Systemverantwortlichen wurden der Leiter der Stadtkämmerei, ein Mitarbeiter der Stadtkämmerei, der Leiter der Stadtkasse, der stellvertretende Leiter der Stadtkasse und ein Mitarbeiter des Einwohnermeldeamtes bestellt.

Die bei diesen Aufgabenzuordnungen fehlenden Funktionstrennungen zwischen dem Anwenderbereich und der Durchführung der automatisierten Datenverarbeitung sind für die Datensicherheit bedenklich. Während des Kontrollbesuchs wurde diese Tatsache eingehend erörtert. Die Stadt sieht aber derzeit keine Möglichkeit, die vorhandenen Aufgabenzuordnungen zu ändern. Ich habe empfohlen, langfristig anzustreben, durch geeignete personelle Maßnahmen die Funktionstrennung zwischen dem Anwenderbereich und der Durchführung der automatisierten Datenverarbeitung möglichst weitgehend zu verwirklichen.

6.5 Änderungen an freigegebenen Programmen vor deren Einsatz

Regelungen des Verfahrens für Programmtest und Programmfreigabe sind von erheblicher Bedeutung für die Datensicherheit. Durch derartige Regelungen soll unter anderem gewährleistet werden, daß der Anwender sämtliche Entscheidungen, die die Logik eines Programms betreffen, selbst trifft und daß er auch jederzeit weiß, mit welcher Logik ein Programm zum Ablauf kommt. Darüber hinaus sollen diese Regelungen gewährleisten, daß die zum Ablauf kommende Programmversion dokumentiert wird.

Zu den wesentlichen Anforderungen der Datensicherheit gehört es daher auch zu gewährleisten, daß freigegebene Programme ohne jede Änderung zum Einsatz kommen (oben S. 138/139). Maßnahmen, die diesem Ziel dienen, werden als unverzichtbar angesehen. Dennoch stellte ich in Einzelfällen bei Kontrollbesuchen fest, daß Regelungen getroffen wurden, die ein Ändern von freigegebenen Programmen vor deren Einsatz ohne Wissen der zur Freigabe befugten Stelle gestatten.

So habe ich bei einem Kontrollbesuch festgestellt, daß die Programmierrichtlinien einer öffentlichen Stelle Änderungen von Programmen gestatten, die sich im Freigabetest oder sogar schon im Einsatz befinden, ohne Zustimmung und sogar ohne Kenntnis des Anwenders.

Die Datensicherheit ist durch diese Möglichkeit der Programmänderung beeinträchtigt.

Die öffentliche Stelle berichtete, derartige Programmänderungen würden nur in außerordentlich seltenen Fällen durchgeführt. Es handele sich dann jeweils um eine Notmaßnahme, für die ein anderes Vorgehen nicht praktikabel sei. Während des Kontrollbesuchs wurde besprochen, daß derartige Notmaßnahmen nur unter folgenden Voraussetzungen zulässig sein sollten:

- Die Geschäftsführung der öffentlichen Stelle legt durch eine schriftliche Anweisung fest, unter welchen Umständen von dieser Möglichkeit Gebrauch gemacht werden darf.
- Der Abteilungsleiter der zuständigen Fachabteilung oder sein Vertreter im Amt ist zum nächstmöglichen Zeitpunkt über die getroffene Notmaßnahme zu unterrichten.

- Die Notmaßnahme bedarf der vorherigen Zustimmung des Leiters der Abteilung Organisation und Datenverarbeitung oder seines Vertreters im Amt.
- Die Anweisung, eine derartige Notmaßnahme durchzuführen, ist in jedem Einzelfall schriftlich zu erteilen.

Von einer Gemeinde erhielt ich die Auskunft, daß bei Programmen geringerer Bedeutung bisher in Einzelfällen Direktänderungen dieser Programme im Arbeitsspeicher erfolgt sind. Bei einer Direktänderung wird ein im echten Betrieb eingesetztes Programm unmittelbar vor seinem Ablauf oder während seines Ablaufs im Arbeitsspeicher geändert.

Die Direktänderung eines Programms muß dann als sehr bedenklich angesehen werden, wenn es sich um ein Programm mit verbindlicher Verarbeitungslogik handelt. Ein derartiges Programm muß vor seinem ersten Einsatz und nach jeder Änderung von dem Anwender freigegeben werden.

Direktänderung eines Programms mit verbindlicher Verarbeitungslogik im Arbeitsspeicher bedeutet daher die nachträgliche Änderung eines freigegebenen Programms. Die Sicherheit der Verarbeitung wird dabei aufgehoben. Es muß außerdem befürchtet werden, daß die zum Ablauf kommende Programmversion nicht dokumentiert wird. Daher sollten durch den Gemeindedirektor Direktänderungen freigegebener Programme im Arbeitsspeicher ohne jede Ausnahme untersagt werden. Ich habe empfohlen, in der Dienstanweisung festzulegen, daß bei Programmen mit verbindlicher Verarbeitungslogik Direktänderungen im Arbeitsspeicher ausnahmslos untersagt sind.

6.6 Konventionelle Datenverarbeitung

6.6.1 Entscheidungskriterien für Maßnahmen zur Datensicherung

In zahlreichen Fällen traten öffentliche Stellen wegen konkreter Fragen zur Datensicherung bei konventioneller Datenverarbeitung mit der Bitte um Beratung an mich heran. Gefragt wurde ich z. B. bezüglich baulicher Maßnahmen, bezüglich der Zulässigkeit organisatorischer Regelungen, bezüglich der Eignung anzuschaffender Möbel oder auch nach der unter Gesichtspunkten des Datenschutzes zweckmäßigen Raumaufteilung und Anordnung der Arbeitsplätze.

Selbstverständlich bin ich im Rahmen meiner Möglichkeiten gerne bereit, auch in Einzelfragen der Datensicherung Rat zu erteilen. Rat und Empfehlungen, die ich auf derartige Fragen ausspreche, beruhen allerdings nur selten auf Detailkenntnissen über die spezielle Situation. Diese zu erwerben, fehlen mir die zeitlichen und personellen Möglichkeiten. Meine Antwort auf eine derartige Anfrage hat daher im allgemeinen auch nicht primär die Empfehlung einer bestimmten Maßnahme oder Regelung zum Gegenstand. In der Antwort versuche ich vielmehr, Wege und Kriterien aufzuzeigen, die es dem Fragesteller ermöglichen, selbst herauszufinden, welche Maßnahme angemessen ist. Damit bin ich dem Fragesteller behilflich, die Verantwortung selbst wahrzunehmen, die nach §§ 7 und 10 Abs. 1 DSG NW von ihm wahrzunehmen ist.

Hilfreich bei dieser mehr grundsätzlichen und unspezifischen Art der Beantwortung von Beratungsersuchen zur Datensicherheit sind einige von mir herausgegebene Ausarbeitungen. Erwähnen möchte ich in diesem Zusammenhang vor allem die Organisationshilfen zur Datensicherung (unten S. 166/167). Sehr nützlich sind aber auch die in einem Heft zusammengefaßten und mit einem Stichwortverzeichnis versehenen Auszüge der Teile des 1. bis 8. Tätigkeitsberichts, die Fragen der Datensicherheit betreffen.

Als Beispiel mag die Anfrage einer Stadt dienen. In ihrem Schreiben teilte die Stadt mit, daß sie zur Zeit ein neues Stadthaus errichten läßt. Ihr gehe es bei der an mich gerichteten Anfrage um die Unterbringung von Akten mit personenbezogenen Daten. Die Stadt stehe vor der Entscheidung, ob verschließbare Holzschränke generell ausreichend sind oder ob die derzeit geltenden Datenschutzvorschriften eine qualifiziertere Unterbringung in Blech- oder Stahlschränken vorschreiben. Im Hinblick auf die Bedeutsamkeit der jetzt für die nächsten Jahrzehnte zu treffenden Entscheidungen, die auch mit erheblichen finanziellen Aufwendungen verbunden seien, bitte sie hierzu um meine Stellungnahme.

In meiner Stellungnahme wies ich die Stadt darauf hin, daß sie nach § 10 Abs. 1 DSG NW die technischen und organisatorischen Maßnahmen zu treffen hat, die erforderlich sind, um eine den Vorschriften dieses Gesetzes entsprechende Verarbeitung der Daten sicherzustellen (Satz 1). Werden personenbezogene Daten in nicht-automatisierten Dateien oder in Akten verarbeitet, sind nach § 10 Abs. 3 DSG NW Maßnahmen zu treffen, um insbesondere den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (§ 10 Abs. 1 Satz 2 DSG NW).

Die Stadt hat nach pflichtgemäßem Ermessen zu entscheiden, ob der Aufwand für jeweilige Maßnahmen, die zur Datensicherung in Frage kommen, in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Wenn die Angemessenheit hiernach im Einzelfall gegeben ist, sind die Maßnahmen erforderlich.

Wesentlich für die Beurteilung der Angemessenheit des Aufwandes sind nicht nur die Eigenschaften der jeweiligen Maßnahme – im vorliegenden Fall also die Eigenschaften von Holz- und Blech- oder Stahlschränken. Bei der Beurteilung muß vielmehr das gesamte Umfeld, in das eine Maßnahme eingebettet werden soll, berücksichtigt werden. Für die bei der Stadt anstehende Entscheidung gehören zu dem Umfeld unter anderem folgende Aspekte:

a) Außensicherung des Gebäudes

   Dem Schreiben der Stadt ist zu entnehmen, daß bereits Maßnahmen zur technischen Außensicherung des Gebäudes vorgesehen wurden. Es sollte überprüft werden, ob hierdurch eine lückenlose Sicherheit erreicht wird oder ob Schwachstellen zu berücksichtigen sind.

b) Situation außerhalb der Dienstzeit

Für die Bewertung der Situation außerhalb der Dienstzeit ist unter anderem erheblich,

- ob ein Pförtnerdienst außerhalb der Dienstzeit eingerichtet ist,
- ob eine Bewachung des Gebäudes durchgeführt wird,
- ob und gegebenenfalls wo Alarmmelder installiert sind und wo der Alarm gegebenenfalls aufläuft,
- mit welcher Sicherheit gewährleistet ist, daß Fenster und Türen außerhalb der Dienstzeit verschlossen sind und ob entsprechende Kontrollen durchgeführt werden.

c) Situation während der Dienstzeit

Für die Bewertung der Situation während der Dienstzeit ist unter anderem erheblich,

- ob Diensträume ausnahmslos verschlossen sind, wenn sich kein Mitarbeiter darin aufhält,
- ob die Möglichkeit besteht, daß sich Besucher unbeobachtet – eventuell über längere Zeit – allein in einem Dienstraum aufhalten und
- wie sicher Türen und Schlösser technisch ausgestattet sind.

d) Situation bei der Reinigung der Diensträume

Für die Bewertung der Situation bei der Reinigung der Diensträume ist unter anderem erheblich,

- ob die Reinigung während der Dienstzeit und ausnahmslos in Anwesenheit eines zutrittsberechtigten Mitarbeiters erfolgt oder
- ob die Reinigung außerhalb der Dienstzeit erfolgt.

e) Besondere Gefährdungen

Von erheblicher Bedeutung bei der Beurteilung des Umfeldes könnten bereits vorliegende Erkenntnisse über besondere Gefährdungen der Datensicherheit sein.

f) Schriftliche Dienstanweisung

Es sollte geprüft werden, ob alle für die Datensicherheit wichtigen Anweisungen in einer schriftlichen Dienstanweisung geregelt sind.

g) Einhaltung der Dienstanweisung

Ein wichtiger Aspekt des Umfeldes, in das die zu treffenden Maßnahmen eingebettet werden sollen, ist die Frage, ob und wie die Einhaltung der Dienstanweisung gewährleistet wird. Erfahrungsgemäß werden Anweisungen zur Datensicherheit nur befolgt, wenn deren Einhaltung kontrolliert wird. Hinweise zu der erforderlichen Selbstkontrolle bei personeller

Datenverarbeitung und zu deren Institutionalisierung enthält mein 9. Tätigkeitsbericht (S. 128/129).

h) Erfahrungen bei der Kontrolle der Einhaltung der Dienstanweisung

Ein Bild über das zu erwartende Verhalten der Mitarbeiter kann aus den Berichten einer institutionalisierten Kontrollinstanz (oben g)) gewonnen werden.

Die Stadt hat unter Berücksichtigung aller Aspekte des Umfeldes in eigener Verantwortung zu entscheiden, welche Maßnahmen zur Sicherung personenbezogener Daten, die in Akten verarbeitet werden, erforderlich sind.

6.6.2 Vernichten von Unterlagen

Erheblich gestiegen ist in den letzten Jahren das Sicherheitsbewußtsein bezüglich der Vernichtung von Unterlagen. Die öffentlichen Stellen sind für die Sicherheit ihrer Unterlagen verantwortlich, bis deren Vernichtung abgeschlossen ist. Bei auftretenden Fragen dreht es sich vor allem um die Art der zur Vernichtung einzusetzenden Geräte und darum, wie die öffentliche Stelle der Verantwortung für ihre Unterlagen bis zum Abschluß von deren Vernichtung nachkommen kann.

Als Stellungnahme auf eine Anfrage, die die Vernichtung von Akten eines Studentenwerks betraf, habe ich betont, daß die speichernde Stelle so lange für die Sicherung von Unterlagen mit personenbezogenen Daten verantwortlich ist, 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. In dieser Norm werden grundlegende Anforderungen an Maschinen und Einrichtungen, z. B. Aktenvernichter, festgelegt, deren bestimmungsgemäßer Gebrauch darin besteht, Informationsträger, auf denen schutzbedürftige Informationen dargestellt sind, so zu vernichten, daß die Reproduktion der auf ihnen wiedergegebenen Informationen entweder unmöglich ist oder weitgehend erschwert wird. Hierbei wird berücksichtigt, daß der Grad der Schutzbedürftigkeit von Informationen, die physikalischen Eigenschaften von Informationsträgern und die zur Anwendung kommenden technischen Verfahren unterschiedlich sind.

Die speichernde Stelle sollte je nach Art der zu schützenden personenbezogenen Daten in Anlehnung an die Festlegungen der Norm DIN 32 757 entscheiden, welche Anforderungen an den Aktenvernichter zu stellen sind. Ich habe angeregt, bei dem Studentenwerk einen Aktenvernichter einzusetzen, der die Informationsträger so vernichtet, daß die Reproduktion der auf ihnen wiedergegebenen Informationen nur unter Verwendung gewerbeunüblicher Einrichtungen bzw. Sonderkonstruktionen, die im Falle kleiner Auflagen sehr aufwendig sind, möglich ist (vgl. DIN 32 757, Sicherheitsstufe 4).

Eine andere öffentliche Stelle teilte mir mit, daß bisher in jedem Dienstzimmer zwei Behältnisse aufgestellt sind, damit die Bediensteten eine Trennung

des Papierabfalls von dem übrigen Müll (Essensreste, Flaschen, Dosen pp.) vornehmen können. Eine Trennung des Papierabfalls von dem übrigen Müll sei allerdings bei vielen Bediensteten trotz Kontrollen nicht durchsetzbar. Daher sei angeregt worden, eine neue Abfallvernichtungsmaschine anzuschaffen, die für alle Abfallsorten tauglich ist und damit die mit einer Mülltrennung verbundene Verwechslungsgefahr ausschließt.

Nach diesen Aussagen muß ich annehmen, daß nach Installation der neuen Abfallvernichtungsmaschine auf die Trennung von Papierabfall und Müll verzichtet werden soll und daher beabsichtigt ist, alle zur Vernichtung anfallenden Unterlagen einschließlich der Unterlagen mit personenbezogenen Daten bereits in den Büros mit dem dort anfallenden übrigen Müll (Essensreste, Flaschen, Dosen pp.) zusammenzuführen. Die Vernichtung dieses zusammengeführten Abfalls soll dann in der neu zu installierenden Abfallvernichtungsmaschine erfolgen. Ich habe darauf hingewiesen, daß es mir zweifelhaft erscheint, ob der Abfallvernichter auch dann den Anforderungen von DIN 32 757 entsprechend arbeiten kann, wenn er in dieser Weise eingesetzt wird.

6.6.3 Mithören von Gesprächen

In Bürgereingaben werde ich immer wieder auf einen unbefriedigenden Datenschutz öffentlicher Stellen bei persönlichen Vorsprachen der Bürger hingewiesen. Bei Kontrollbesuchen gehe ich dieser Frage daher mit besonderer Aufmerksamkeit nach. Im allgemeinen zeigt sich, daß es möglich ist, bereits mit sehr einfachen Maßnahmen eine deutliche Verbesserung der Situation zu erreichen. Ein Beispiel soll diese Aussage verdeutlichen.

Im Einwohnermeldeamt einer kontrollierten Stadt wird der Bereich der Sachbearbeiter von dem für die Bürger vorgesehenen Bereich durch eine Theke getrennt. An dieser Theke gibt es zwei Arbeitsplätze für den Bürgerkontakt. Im Hinblick auf die aus Artikel 4 Abs. 2 der Landesverfassung folgende Verpflichtung, personenbezogene Daten gegen unbefugte Kenntnisnahme durch Dritte zu schützen, muß besondere Sorgfalt darauf verwandt werden zu verhindern, daß Gespräche am Arbeitsplatz eines Sachbearbeiters von Unbefugten mitgehört werden können. Insbesondere ist sicherzustellen, daß wartende Bürger keines der an einem der Arbeitsplätze geführten Gespräche verfolgen können.

Bei einer Begehung des Einwohnermeldeamts zeigte es sich, daß ein Mithören von Gesprächen, die an Arbeitsplätzen der Sachbearbeiter geführt werden, durch die im gleichen Raum wartenden Bürger möglich ist. Die wartenden Bürger stehen oder sitzen unmittelbar hinter den Bürgern, deren Anliegen bearbeitet werden.

Diese Situation ist sehr unbefriedigend. Während des Kontrollbesuchs wurde besprochen, daß es möglich ist sicherzustellen, daß nur diejenigen Bürger im Raum des Einwohnermeldeamts anwesend sind, deren Anliegen bearbeitet werden. Für die übrigen Bürger sollte unmittelbar vor dem Einwohnermeldeamt eine Wartezone vorgesehen werden. Die Bearbeitung der Bürgeranliegen würde dadurch nicht verzögert.

6.7 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.

Erschienen sind inzwischen vier Organisationshilfen. Alle Organisationshilfen wurden mit einem großen Verteiler an öffentliche Stellen des Landesbereichs in Nordrhein-Westfalen verteilt.

Die Organisationshilfe – Allgemeiner Teil ist bereits in einer Reihe von Auflagen erschienen. Auch im Berichtszeitraum wurde eine aktualisierte Ausgabe herausgegeben.

Im Berichtszeitraum neu erschienen ist die Organisationshilfe zur Datensicherung bei einem persönlichen Computer (Organisationshilfe-PC). Sie soll helfen, die Datensicherung bei Einsatz eines PCs zu gestalten. Gerade bei Einsatz eines PCs sind Art und Umfang der zur Datensicherung erforderlichen Maßnahmen von den Bedingungen des Einzelfalls abhängig.

Bei der modernen Datenverarbeitung gewinnt die Vernetzung von Anlagen und Geräten zunehmend an Bedeutung. In vielen Fällen werden Netze als eigenständige Einheiten angesehen und als solche geplant und installiert.

Aus der Sicht des Datenschutzes ist neben dieser technischen Entwicklung eine besondere Einsatzform der automatisierten Datenverarbeitung – die individuelle Datenverarbeitung (IDV; oben S. 150/151) – bedeutsam, die in den letzten Jahren eine weite Verbreitung fand. IDV ist sowohl auf einem PC als auch auf einer zentralen Datenverarbeitungsanlage möglich.

Mit erheblichen Gefahren für die Datensicherheit sind beide Entwicklungen, die zunehmende Vernetzung und die zunehmende Verbreitung von IDV, verbunden.

Die Gefahren der Vernetzung sind bekannt und unmittelbar verständlich. Unbefugte können möglicherweise über Daten ohne Rücksicht auf den Ort von deren Speicherung verfügen. Weniger offensichtlich und daher häufig auch weniger bewußt sind die Gefahren der IDV. IDV birgt die Gefahr in sich, daß Verantwortlichkeiten verwischt oder ignoriert werden. Diese Gefahr besteht insbesondere dann, wenn die Logik der Verarbeitung der Daten der öffentlichen Stelle verbindlich vorgeschrieben oder von ihr verbindlich zugesagt ist. Den aus einer solchen verbindlichen Verarbeitungslogik resultierenden Anforderungen kann eine öffentliche Stelle bei Einsatz von IDV im allgemeinen nur mit erheblichen Schwierigkeiten entsprechen.

Zur Unterstützung beim Beurteilen und Gestalten der Datensicherheit von Netzen und beim Einsatz von IDV habe ich zwei weitere Organisationshilfen entwickelt.

- Organisationshilfe zur Datensicherung bei Netzen (Organisationshilfe-Netze).

  Die Organisationshilfe-Netze wurde in ihrem Konzept weit ausgelegt. Einige der Fragen sind vor allem für spezielle Netztechniken wie ISDN oder LAN von Bedeutung. Am Schluß der Organisationshilfe-Netze sind Fragen angefügt, die sich nicht mehr direkt auf das Netz beziehen, sondern auf Dienstleistungen, die möglicherweise als zum Netz gehörig angeboten werden.

- Organisationshilfe zur Datensicherung bei individueller Datenverarbeitung (Organisationshilfe-IDV).

Beide Organisationshilfen sind im Berichtszeitraum neu erschienen.

Das Interesse an allen von mir herausgegebenen Organisationshilfen ist sehr groß. Anfragen und Bitten um Übersendung von Organisationshilfen erreichen mich laufend. Derartige Anfragen kommen sowohl von öffentlichen Stellen des Landesbereichs in Nordrhein-Westfalen als auch aus dem privaten Bereich und von öffentlichen Stellen, die nicht meiner Kontrolle unterliegen – auch von solchen aus dem Gebiet der neuen Bundesländer. Bisher war es mir möglich, allen Bitten um Übersendung von Organisationshilfen zu entsprechen.

Auf entsprechende Fragen aus dem Bereich einer Hochschule und einer Fachhochschule habe ich mitgeteilt, daß von meiner Seite keine Bedenken dagegen bestehen, daß die Organisationshilfen auch im Rahmen der Lehre verwandt werden. Die dadurch zu erwartende Verbreitung meiner Vorstellungen über die Anforderungen an eine sichere Datenverarbeitung wird von mir sogar ausdrücklich begrüßt.

Düsseldorf, den 14. Februar 1991

Maier-Bode

Anlagen

Anlage 1 (zu 3.2.1)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juni 1990

zum Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität

Die Konferenz der Datenschutzbeauftragten hat schwerwiegende datenschutzrechtliche Bedenken gegen die Ausweitung der polizeilichen Ermittlungsbefugnisse in der Strafprozeßordnung, wie sie mit dem vom Bundesrat vorgelegten Gesetzentwurf zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG) beabsichtigt ist.

Erstmals werden in die Strafprozeßordnung Regelungen zur Rasterfahndung, zum Einsatz verdeckter Ermittler sowie von Wanzen und Richtmikrofonen und heimlichen Film- und Fotoaufnahmen eingefügt. Die Konferenz der Datenschutzbeauftragten verkennt nicht, daß bestimmte Erscheinungsformen von Kriminalität im Interesse des Schutzes der Bürger besondere Ermittlungsmethoden erforderlich machen können. Der vorgelegte Entwurf regelt jedoch nicht nur neue Eingriffsbefugnisse zur Bekämpfung des illegalen Rauschgifthandels und sonstiger organisierter Kriminalität, – die im übrigen nicht definiert wird – sondern soll tief in die Privatsphäre der Bürger eingreifende Fahndungs- und Ermittlungsmethoden in das Strafverfahrensrecht allgemein einführen.

Gegen den vorliegenden Entwurf bestehen insbesondere folgende datenschutzrechtliche Bedenken:

- Die vorgesehenen Eingriffsbefugnisse der Strafverfolgungsbehörden werden an den konturenlosen Begriff „Straftaten von erheblicher Bedeutung" geknüpft. Damit dürfte nach der Begründung des Gesetzentwurfs in der Praxis allenfalls die Kleinkriminalität ausscheiden. So soll z.B. auch die **Rasterfahndung** für eine Vielzahl von Delikten außerhalb organisierter Kriminalität zugelassen werden. Dies erscheint besonders bedenklich, weil gerade diese Form der Fahndung unbescholtene Bürger in großer Zahl unvermeidlich mit einbezieht und sie in der Folge Ziel weiterer Ermittlungen werden können.
- Tief in die Privatsphäre eindringende Ermittlungsmethoden werden nicht hinreichend präzisiert und sind großenteils unverhältnismäßig: So dürfen ohne Wissen des Betroffenen zur Aufklärung **jeder Straftat**– sogar in Wohnungen hinein – „Lichtbilder und Bildaufzeichnungen" aufgenommen sowie „besondere Sichthilfen" eingesetzt werden.
- Maßnahmen, wie Einsatz von Peilsendern, Richtmikrofonen, Wanzen und sonstiger Überwachungstechniken können sich auch gegen dritte **unverdächtige Personen** richten, wenn „aufgrund bestimmter Tatsa-

chen" anzunehmen ist, „daß sie mit dem Täter in Verbindung stehen oder eine solche Verbindung hergestellt wird". Es bleibt völlig offen, wie das Tatbestandsmerkmal der „Verbindung" eingegrenzt werden soll. Foto- und Filmaufnahmen von Unbeteiligten sind bereits zulässig, wenn sie für Ermittlungen „geeignet" sind. Damit kann kein Bürger vorhersehen, ob und wann er hiervon betroffen sein kann. Ohne Kenntnis der gegen ihn gerichteten Eingriffe kann er im Regelfall nicht einmal Rechtsschutz erlangen.

- Die Möglichkeiten der Telefonüberwachung werden über das vertretbare Maß hinaus ausgeweitet.
- Bedenken richten sich ferner dagegen, bei besonderen Ermittlungsmaßnahmen auf die vorherige **richterliche Kontrolle** zu verzichten und durch Eilkompetenzen die Entscheidung der diese Maßnahmen selbst durchführenden Polizei zu übertragen. Nicht einmal die nachträgliche richterliche Kontrolle ist in jedem Fall zwingend vorgesehen.

Im Gegensatz zu den erweiterten Befugnissen der Strafverfolgungsbehörden sind Regelungen zum Schutz oder im Interesse der Betroffenen nur unzureichend vorgesehen. Die mit besonderen Ermittlungsmethoden für besondere Strafverfolgungszwecke erhobenen Daten dürfen für zu weitgehende andere Zwecke verwendet werden. So sind z. B. die Begriffe „Zwecke der staatsanwaltschaftlichen Vorgangsverwaltung" und „Zwecke der Rechtspflege" zu unbestimmt. Es fehlen weiterhin ausreichende Bestimmungen zum Auskunftsrecht des Betroffenen und zur Löschung.

Zusammenfassend ist festzustellen, daß dieser Entwurf selbst hinter den datenschutzrechtlichen Ansätzen, wie sie etwa noch im Entwurf des Strafverfahrensänderungsgesetzes 1989 enthalten waren, zurückbleibt.

Die Konferenz der Datenschutzbeauftragten fordert den Deutschen Bundestag auf, diese Vorschläge des Gesetzentwurfs abzulehnen und die unterbrochenen Arbeiten an der umfassenden datenschutzrechtlichen Novellierung der Strafprozeßordnung, die dringend geboten ist, wieder aufzunehmen. Hierzu haben die Datenschutzbeauftragten wiederholt konkrete Vorschläge vorgelegt.

Anlage 2 (zu 3.2.8)

Beschluß der Internationalen Konferenz der Datenschutzbeauftragten vom 30. August 1989

zu ISDN

Die nationale und internationale Entwicklung der Telekommunikation ist derzeit gekennzeichnet durch die Einführung diensteintegrierender, digitalisierter Netze. Diese sind die Träger vielfältiger Dienste.

Die Entwicklung führt sowohl für die Netzträger als auch für die Diensteanbieter zur Verarbeitung von erheblich mehr personenbezogenen Daten als

dies bei bisherigen Netzen der Fall war. Diese Situation erfordert nationale und internationale Vorkehrungen zum Schutz personenbezogener Daten.

Die Internationale Konferenz der Datenschutzbeauftragten stellt fest, daß hierzu erhebliche Anstrengungen erforderlich sind. Insbesondere darf der Datenschutz nicht als Hindernis für die Entwicklung des Internationalen Informationsmarktes gesehen werden, sondern er stellt vielmehr eine notwendige Ergänzung der technischen Entwicklung dar, die für die Akzeptanz der neuen Telekommunikationstechnologien unerläßlich ist, er stellt vielleicht sogar ein beschleunigendes Element dieser Entwicklung dar.

Sie geht bei offenen Netzen von folgenden Grundsätzen aus:

- Abrechnungsdaten dürfen nur und nur so lange gespeichert werden, wie dies erforderlich ist, um Rechnungen zu erstellen oder auf eventuelle Anfechtungen zu reagieren; ferner zur Erstellung detaillierter Rechnungen, die ausschließlich für diejenigen Teilnehmer bestimmt sind, die sie angefordert haben. Die Vereinfachung der Tarifsysteme kommt dem Datenschutz entgegen.
- Für bestimmte Telekommunikationsdienste (Telefon, Kabelfernsehen mit Rückkanal, Datenübermittlungsdienste, Autobahngebühreneinzug usw.) müssen anonyme Zahleinrichtungen geschaffen werden. Ungeachtet der Abrechnungsprobleme macht es die Mehrwertigkeit der Netze erforderlich, diese mit den technischen Möglichkeiten eines anonymen Zugangs auszustatten.
- Daten, die für die Vermittlung erforderlich sind, sind unverzüglich zu löschen; Inhaltsdaten dürfen nur gespeichert werden, wenn sie für die Abwicklung des Dienstes erforderlich sind.
- Vorkehrungen sollten getroffen werden, die jenen Teilnehmern, die wünschen, in Teilnehmerverzeichnisse aufgenommen zu werden, garantieren, daß sie nicht Objekt unerwünschter kommerzieller Werbung werden. Das Recht, daß unentgeltlich in den Teilnehmerverzeichnissen kein Eintrag erscheint, sollte angestrebt werden. Daten, die die Erreichbarkeit von Teilnehmern sicherstellen sollen, dürfen nicht zur Erstellung von Personenprofilen führen, die eine Verhaltenskontrolle erlauben.
- Maßnahmen zur Datensicherung insbesondere gegen den Zugang nicht autorisierter Personen, die Manipulation, das Mithören oder zur Gewährleistung der Authentizität des Senders müssen auf höchstem technischen Niveau und zu akzeptablen Preisen angeboten werden.
- Angemessene Kontrollinstitutionen sind sowohl national als auch international einzurichten.
- In lokalen Netzen und bei Telekommunikationsendgeräten ist bereits bei der Normierung und Genehmigung auf den Datenschutz Rücksicht zu nehmen.

Insbesondere erfordern folgende Dienstemerkmale besondere Aufmerksamkeit:

- Die Anzeige des anrufenden Teilnehmers muß sowohl vom Anrufer als auch vom Angerufenen unterdrückt werden können; Mißbrauch muß durch Maßnahmen im Netz verhindert werden.
- Freisprecheinrichtungen müssen so gestaltet werden, daß nur mit Kenntnis der Gesprächsteilnehmer mitgehört oder aufgezeichnet werden kann.
- Beim Zugang zu Anrufbeantwortern, Voice- und Mailboxsystemen sowie Datenübermittlungsdiensten sind hinreichende Zugangssicherungen einzuführen.

Anlage 3 (zu 4.2.2)

Beschluß der Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder vom 29. Januar 1991

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

I.
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in der Vergangenheit zu wiederholten Malen die Untätigkeit der Europäischen Gemeinschaft im Bereich des Datenschutzes kritisiert. Kernpunkt dieser Kritik war die Befürchtung, daß die Dynamik der wirtschaftlichen Entwicklung in Richtung auf den vollendeten Binnenmarkt zu einem „informationellen Großraum" mit einem engen Netzwerk grenzüberschreitender Datenflüsse führt, ohne daß gleichzeitig der Grundrechtsschutz in der Gemeinschaft bei der Verarbeitung und dem Austausch persönlicher Daten gewährleistet wird.

II.
Daher begrüßt die Konferenz, daß die EG-Kommission im Juli 1990 den „Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" vorgelegt hat. Der Kommissionsvorschlag geht in einer Reihe von Punkten über die Konvention des Europarats zum Datenschutz von 1980 hinaus und berücksichtigt insoweit die technische und rechtliche Entwicklung des vergangenen Jahrzehnts. Positiv bewertet die Konferenz vor allem die Intention des Entwurfs, den Datenschutz in der EG nicht auf dem kleinsten gemeinsamen Nenner, sondern auf einem möglichst hohen Niveau zu harmonisieren. Sie legt allerdings entscheidenden Wert darauf, daß die Mitgliedstaaten die Möglichkeit behalten, den Datenschutz in der nationalen Gesetzgebung weiterzuentwickeln.

III.
Zahlreiche bewährte Vorschriften und Instrumente aus dem deutschen Datenschutzrecht sind in den Richtlinientext aufgenommen worden. Die Bewertung der einzelnen Bestimmungen des Richtlinienentwurfs kann jedoch nicht isoliert aus dem Blickwinkel des deutschen Datenschutzrechts erfolgen. Jeder nationale Gesetzgeber muß bei Rechtsharmonisierung auf europäischer Ebene bereit sein, einzelne seiner Regelungen auf dem Hintergrund der Erfahrungen und Vorstellungen anderer Mitgliedstaaten in Frage

zu stellen. Zur Abstimmung der Auffassungen auf EG-Ebene besteht ein intensiver Meinungsaustausch zwischen der Konferenz und den Datenschutzinstitutionen der Partnerländer.

IV.

Die Konferenz hält, abgesehen von der Bereinigung von redaktionellen Unstimmigkeiten, einige Änderungen im Richtlinienvorschlag für notwendig, um die Gleichwertigkeit des Schutzes auf dem Niveau, das die Mitgliedsländer mit bestehender Datenschutzgesetzgebung bereits erreicht haben, sicherzustellen. Folgende Korrekturen sind dabei vorrangig:

1. Datenschutz muß, jedenfalls im Bereich der öffentlichen Verwaltung, für alle Unterlagen mit personenbezogenen Daten gelten. Die in der Richtlinie vorgesehene Beschränkung des Anwendungsbereichs auf die Verarbeitung personenbezogener Daten in „Dateien" ist ebenso technisch überholt wie Anlaß zu einer Fülle von Interpretationsproblemen.

2. Für die Verwendung und Weitergabe persönlicher Daten muß das Prinzip strikter Zweckbindung gelten und ausdrücklich statuiert werden. Wenn der Entwurf die bloße Vereinbarkeit der Zwecke von Erhebung, Speicherung und Übermittlung genügen läßt, werden inakzeptable Verarbeitungsfreiräume eröffnet; die Transparenz des Datenumgangs geht für den einzelnen verloren.

3. Der Anspruch auf Auskunft über die gespeicherten Daten ist das elementarste Individualrecht der Betroffenen. Nur gravierende Interessen der Allgemeinheit oder Dritter dürfen im Ausnahmefall diesen Auskunftsanspruch einschränken. Der im Entwurf vorgesehene Katalog von Fällen der Auskunftsverweigerung muß daher deutlich vermindert werden.

4. Der Forderung des Entwurfs, daß die Erhebung von Daten nur „nach Treu und Glauben" erfolgen darf, kann uneingeschränkt zugestimmt werden. Doch muß dieses Prinzip im Interesse des einzelnen konkretisiert werden. Es gilt klarzustellen, daß persönliche Angaben vorrangig beim Betroffenen selbst zu erheben sind. Die Ausnahmefälle, in denen Informationen ohne Kenntnis des Betroffenen beschafft werden dürfen, sollten soweit wie möglich in der Richtlinie konkret benannt werden.

5. Der Datenschutz der EG-Bürger darf nicht an den Gemeinschaftsgrenzen haltmachen. Ziel der Richtlinie muß neben der EG-internen Harmonisierung auch sein, den Schutz des Betroffenen beim Datenexport in Drittländer zu gewährleisten. Dies setzt voraus, daß im Empfängerland ein dem EG-Standard gleichwertiges Datenschutzniveau besteht. Daß der Richtlinienentwurf sich mit einem „angemessenen" Schutz im Zielland zufriedengibt, genügt nicht. Notwendig ist schließlich, das Verfahren zur Feststellung des Datenschutzstandards in Drittländern übersichtlich und praktikabel auszugestalten.

6. Auf der EG-Ebene bedarf es einer unabhängigen Datenschutzinstanz, die alle EG-Organe in Datenschutzfragen berät und für die Überwachung der Einhaltung sowie die einheitliche Anwendung der Richtlinie sorgt. Die

im Richtlinienvorschlag vorgesehene „Gruppe für den Schutz personenbezogener Daten" erfüllt – betrachtet man ihre Struktur, Aufgaben und Kompetenzen – diese Anforderungen nicht. Die Unabhängigkeit der Datenschutzkontrolle auf EG-Ebene wird in Zweifel gezogen, wenn den Vorsitz nicht ein gewähltes Mitglied dieser – aus den nationalen Datenschutzorganen zusammengesetzten – „Gruppe", sondern ein Vertreter der EG-Kommission führt. Klargestellt werden muß weiter, daß das Votum der „Gruppe" im vorhinein bei allen den Datenschutz betreffenden Initiativen und Entwürfen der Kommission einzuholen ist. Ansprechpartner der „Gruppe" darf nicht ausschließlich die EG-Kommission, sondern muß auch das Europäische Parlament sein.

7. Da die Kommission die entsprechende Anwendung der Richtlinie auf die personenbezogene Datenverarbeitung ihrer eigenen Dienststellen beschlossen hat, muß sie auch umgehend für eine unabhängige Kontrolle dieses Bereichs Sorge tragen.

V.
Die Konferenz weist darauf hin, daß die vorliegende Richtlinie durch Regelungen für besondere Anwendungsbereiche ergänzt werden muß. Sie sind insbesondere für den Arbeitnehmer- und Sozialdatenschutz vordringlich. Die Kommission sollte schon jetzt ihre Bereitschaft erklären, entsprechende Regelungen zu treffen, und möglichst bald erste Vorschläge vorlegen.

VI.
Die Konferenz begrüßt die Gesprächsbereitschaft der Kommission und geht davon aus, daß der bereits begonnene Dialog zu einer substantiellen Verbesserung des Richtlinienvorschlags führen wird. Die Konferenz wird diese Entschließung der EG-Kommission, dem Europäischen Parlament sowie der Bundesregierung zuleiten. Informiert werden ebenfalls die Datenschutzkontrollinstitutionen der Partnerländer in der Gemeinschaft.

Anlage 4 (zu 5.11.6)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 26./27. Oktober 1989

über Genomanalyse und informationelle Selbstbestimmung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz hat den Abschlußbericht der Enquete-Kommission des Deutschen Bundestages „Chancen und Risiken der Gentechnologie" (Drucksache 10/6775) zum Anlaß genommen, die Risiken für die informationelle Selbstbestimmung jedes Betroffenen abzuwägen gegenüber den Chancen, die die Genomanalyse bringt. Durch die Offenlegung genetischer Daten eines Menschen kann dieser in seinem Persönlichkeitsrecht und sonstigen schutzwürdigen Belangen nachhaltig beeinträchtigt werden. Informationen aus dem Kernbereich der Privatsphäre, die dem Betroffenen selbst bisher unbekannt waren, können ihn zu einem an

sich ungewollten Verhalten in seiner Lebens- oder Berufsgestaltung veranlassen; ihre Kenntnis kann zu einer psychischen und sozialen Zwangslage für den Betroffenen führen. Wegen der genetischen Bedingtheit solcher Informationen können sich daher auch entsprechende Auswirkungen auf dritte Personen, insbesondere die Familie, ergeben. Das Bekanntwerden solcher Informationen kann den Betroffenen in seinem sozialen Umfeld diskriminieren mit der möglichen Folge gesellschaftlicher Abgrenzung.

Um den besonderen Risiken bei der Anwendung der Genomanalyse zu begegnen, bedarf es der gesetzlichen Absicherung folgender Grundsätze:

1. Die Genomanalyse darf grundsätzlich nur auf freiwilliger Basis nach umfassender Aufklärung der Betroffenen vorgenommen werden; ausgenommen sind Straf- und Abstammungsverfahren.

2. Die jederzeit widerrufliche Einwilligung muß sich auch auf die weitere Verwendung der genetischen Informationen erstrecken. Im Falle eines Widerrufs sind die gewonnenen Informationen zu löschen oder an den Betroffenen herauszugeben.

3. Jede Genomanalyse muß zweckorientiert vorgenommen werden. Es ist diejenige genomanalytische Methode zu wählen, die keine oder die geringste Menge an Überschußinformationen bringt. Überschußinformationen sind unverzüglich zu vernichten.

4. Es ist zu prüfen, inwieweit genomanalytische Untersuchungsmethoden einer staatlichen Zulassung bedürfen. Für DNA-Sonden ist dies jedenfalls zu bejahen.

5. Die Genomanalyse im gerichtlichen Verfahren muß auf die reine Identitätsfeststellung beschränkt werden; es dürfen keine genomanalytischen Methoden angewandt werden, die Überschußinformationen zur Person liefern. Die Nutzung der Genomanalyse im Strafverfahren setzt eine normenklare gesetzliche Ermächtigung voraus. Präzise Regelungen müssen u.a. sicherstellen, daß genomanalytische Befunde einer strengen Zweckbindung unterworfen werden.

6. Im Arbeitsverhältnis sind die Anordnung von Genomanalysen oder die Verwendung ihrer Ergebnisse grundsätzlich zu verbieten. Ausnahmen bedürfen der gesetzlichen Regelung. Eine bloße Einwilligung des Arbeitnehmers ist wegen der faktischen Zwangssituation, der er im Arbeitsleben häufig unterliegt, nicht ausreichend.

7. Genomanalysen im Versicherungswesen sind grundsätzlich nicht erforderlich und mit dem Prinzip der Versicherungen, Risiken abzudecken und nicht auszuschließen, unvereinbar. Dies sollte durch eine Klarstellung im Versicherungsvertragsgesetz deutlich gemacht werden.

8. Im Rahmen der pränatalen Diagnostik dürfen nur Informationen über das Vorhandensein oder Fehlen von Erbanlagen erhoben werden, bei denen eine Schädigung heilbar ist oder die zu einer so schwerwiegenden Ge-

sundheitsschädigung des Kindes führen würden, daß ein Schwangerschaftsabbruch straffrei bliebe.

Reihenuntersuchungen an Neugeborenen dürfen sich nur auf solche Erbkrankheiten erstrecken, die bei frühzeitiger Erkennung eines genetischen Defekts geheilt oder zumindest spürbar therapeutisch begleitet werden können.

Die Eltern müssen nach umfassender fachkundiger Beratung in voller Freiheit über die Anwendung genomanalytischer Methoden entscheiden können. Jegliche Beeinflussung, insbesondere jeder individuelle und gesellschaftliche Druck muß vermieden werden.

Die informationelle Selbstbestimmung Dritter, zu der auch das Recht auf Nichtwissen gehört, muß berücksichtigt werden.

Die Konferenz versteht ihre Stellungnahme als Beitrag zur Diskussion mit allen Institutionen, die an den Fragen der Genomanalyse arbeiten. Sie legt Wert darauf, den Dialog mit der Wissenschaft fortzusetzen und dabei neue wissenschaftliche Erkenntnisse einzubeziehen.

Stichwortverzeichnis