Der Landesbeauftragte für den Datenschutz Nordrhein-Westfalen

1. Tätigkeitsbericht

Erster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Nordrhein-Westfalen

für die Zeit vom 5. September 1979
bis zum 31. März 1980

Herausgeber: Der Landesbeauftragte
für den Datenschutz Nordrhein-Westfalen
Elisabethstraße 12, 4000 Düsseldorf 1

Druck: Klose & Krechel GmbH
Suitbertusstraße 18, 4000 Düsseldorf 1

Gliederung

A. Aufgaben des Landesbeauftragten für den Datenschutz

1. Notwendigkeit einer externen Kontrolle

Im Gegensatz zu dem Regierungsentwurf eines Bundesdatenschutzgesetzes sah bereits der Entwurf der Landesregierung für ein Datenschutzgesetz Nordrhein-Westfalen (Drucksache 8/2241) eine externe Kontrolle des Datenschutzes durch einen unabhängigen und weisungsfreien Landesbeauftragten vor. Der Gedanke, den Rechtsschutz des Einzelnen bei der Datenverarbeitung durch eine besondere staatliche Kontrollinstanz zu verstärken, geht von folgender Erwägung aus.

Der Einsatz der ADV wird geprägt von der Zielvorstellung der Rationalisierung, der Wirtschaftlichkeit, einer gegenüber herkömmlichen Verfahren größeren Schnelligkeit und Effektivität unter gemeinsamer Nutzung und Verknüpfung der Datenbestände. Dieser Zielvorstellung stehen die Erfordernisse des Datenschutzes oft diametral entgegen. Angesichts dieses Interessenkonfliktes bietet die Selbstkontrolle der Verwaltung keine ausreichende Gewähr dafür, daß der Datenschutz stets in dem erforderlichen Umfange berücksichtigt wird.

Die besonderen Gefahrenquellen der ADV lassen demnach eine besondere Kontrolleinrichtung, die weisungsfrei und unabhängig ist, als unverzichtbar erscheinen. Bereits die ersten Monate der Tätigkeit des Landesbeauftragten haben jedoch gezeigt, daß im Bereich der herkömmlichen, nicht automatisierten Datenverarbeitung eine solche Kontrollinstanz im Interesse der Bürger ebenso notwendig ist. Dies gilt auch für den Umgang der Verwaltung mit Daten der Bürger in Akten und sonstigen Unterlagen. Wie aus zahlreichen Eingaben an den Landesbeauftragten hervorgeht, ist hier die Persönlichkeitssphäre des Bürgers in gleichem Maße bedroht, wie im Bereich der ADV.

Diese Kontrolle dient der Gewährleistung der Rechte des Bürgers gegenüber der öffentlichen Gewalt. Sie umfaßt deshalb alle Bereiche öffentlichen Handelns, in denen nicht im Hinblick auf höherrangige Rechtsgüter (wie etwa die Unabhängigkeit der Gerichte) besondere gesetzliche Vorschriften einer derartigen Kontrolle entgegenstehen.

2. Organisatorische Voraussetzungen

a) Rechtsstellung des Landesbeauftragten

Nach Verfassung und Gesetz ist der Landesbeauftragte für den Datenschutz in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen (Artikel 77a Abs. 2 Satz 1 der Landesverfassung — LV —; § 24 Abs. 2 Satz 2 DSG NW). Insoweit hat er die gleiche Unabhängigkeit wie ein Richter (Artikel 97 Abs. 1 GG; § 25 DRiG). Damit wird das in der Verwaltung geltende Weisungsprinzip durchbrochen und die Landesregierung insoweit von einer parlamentarischen Verantwortung gegenüber dem Landtag entbunden.

Die Unabhängigkeit des Landesbeauftragten kommt auch darin zum Ausdruck, daß er sich jederzeit an den Landtag wenden kann (Artikel 77a Abs. 2 Satz 2 LV; § 31 Abs. 3 DSG NW). Sie wird dadurch unterstrichen, daß jedermann das Recht hat, sich unmittelbar an den Landesbeauftragten zu wenden, wenn er sich bei der Verarbeitung seiner personenbezogenen Daten durch die öffentliche Verwaltung in seinen schutzwürdigen Belangen verletzt glaubt.

Voraussetzung für eine unabhängige und nur dem Gesetz unterworfene Ausübung des Amtes sind eine ausreich[illegible]ede Personal- und Sachausstattung, das Personalvorschlagsrecht des Landesbeauftragten und sein alleiniges Weisungsrecht gegenüber den Bediensteten. Die Unabhängigkeit des Landesbeauftragten wiederum ist Vorbedingung für das Vertrauen, das er bei seiner Kontrolltätigkeit im Interesse der Bürger braucht.

Bei der Berufung des Landesbeauftragten wirken Landesregierung und Landtag zusammen. Dieser wählt auf Vorschlag der Landesregierung den Landesbeauftragten mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder (Artikel 77a Abs. 1 LV; § 24 Abs. 1 Satz 1 DSG NW). Eine Besonderheit liegt in der Ausgestaltung des Dienstverhältnisses. Nach § 24 Abs. 3 DSG NW wird der Landesbeauftragte jeweils auf die Dauer von acht Jahren in ein Beamtenverhältnis auf Zeit berufen. In Nordrhein-Westfalen ist er damit der einzige Landesbeamte auf Zeit.

Auf Vorschlag der Landesregierung hat mich der Landtag am 5. September 1979 mit der erforderlichen Mehrheit gewählt. Mit Aushändigung der Ernennungsurkunde am gleichen Tage durch den Innenminister Dr. Burkhard Hirsch bin ich zum ersten Landesbeauftragten für den Datenschutz ernannt worden.

b) Angliederung an das Innenministerium

Nach § 24 Abs. 2 Satz 1 DSG NW ist der Landesbeauftragte dem Innenministerium „angegliedert". Er untersteht der Dienstaufsicht des Innenministers (§ 24 Abs. 2 Satz 3 DSG NW). Seine Personal- und Sachmittel sind im Einzelplan des Innenministers, aber in einem eigenen Kapitel ausgewiesen (§ 25 Abs. 1 DSG NW). Das Landesorganisationsgesetz findet auf den Landesbeauftragten wie auf den Landesrechnungshof und die Organe der Rechtspflege keine Anwendung (§ 1 Abs. 2 Buchstabe b LOG).

Mit dieser organisationsrechtlichen Sonderstellung hat der Gesetzgeber neue Wege beschritten. Wie die bisherigen Erfahrungen zeigen, wird die sachliche Unabhängigkeit des Landesbeauftragten weder durch die Angliederung an das Innenministerium noch durch die Dienstaufsicht des Innenministers beeinträchtigt. Die Angliederung an das Innenministerium läßt auch orga[illegible]anisatorische Eigenständigkeit in gewissem Umfang zu. So hat mir der Innenminister de[illegible]en größten Te[illegible] der Ausgabemittel für sächliche Verwaltungsaufgaben sowie für Invest[illegible]itionen zur Bewirtschaftung zugewiesen.

Die Erfahrungen werden zeigen, ob sich die gewählte rechtliche Konstruktion bewährt. Sicherlich wird es nicht immer leicht sein, eine klare Abgrenzung im Rahmen der vorgegebenen Zuordnung zu finden.

Daß sich Probleme ergeben können, zeigt ein Verfahren vor dem Verwaltungsgericht Düsseldorf wegen Feststellung der Notwendigkeit, beim Landesbeauftragten für den Datenschutz einen Personalrat zu bilden. Entsprechende Anträge des Hauptpersonalrats beim Innenminister und einer Gewerkschaft sind allerdings (als unzulässig) abgewiesen worden (Beschluß vom 11. Dezember 1979, PVL 26/79). Die Interessen meiner Mitarbeiter werden weiterhin durch den Personalrat des Innenministeriums wahrgenommen.

c) Personal

Nach § 25 Abs. 1 DSG NW ist dem Landesbeauftragten für den Datenschutz die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen. Die hierfür erforderlichen Haushaltsmittel sind im Einzelplan des Innenministers in einem eigenen Kapitel auszuweisen.

Auf Grund der Ermächtigung in § 40 DSG NW hat der Finanzminister im Einvernehmen mit dem Innenminister für das Haushaltsjahr 1979 außerplanmäßig das Kapitel 0363 — Landesbeauftragter für den Datenschutz — eingerichtet und 32 Planstellen und Stellen zur Verfügung gestellt. Der Haushaltsplan 1980 sieht keine Änderung des Stellenplans vor.

Die Aufteilung auf die einzelnen Laufbahnen und Beschäftigungsarten sowie die Stellenbesetzung am 31. März 1980 ergeben sich aus folgender Übersicht:

	Soll	Ist
Höherer Dienst	7	7
Gehobener Dienst	12	4
Mittlerer Dienst	2	1
Sachbearbeiter (BAT)	3	—
Büro-, Vorzimmer- und Schreibdienst (BAT)	6	4,5
Arbeiter (MTL)	2	2
	32	18,5

Im Hinblick auf das Vorschlagsrecht, das der Landesbeauftragte nach § 25 Abs. 2 Satz 1 DSG NW in Personalangelegenheiten hat, konnte mit der Auswahl des Personals erst nach meiner Wahl durch den Landtag im September 1979 begonnen werden. Sie erfolgte in enger Zusammenarbeit zwischen mir und dem Innenminister, der mir jede gewünschte Unterstützung zuteil werden ließ. Meinen Vorschlägen wurde voll entsprochen.

Die Stellenbesetzung im höheren Dienst war, wenn auch teilweise noch im Wege der Abordnung, bis zum Januar 1980 abgeschlossen. Außer der Stelle des Leiters des für organisatorisch-technische Fragen des Datenschutzes zuständigen Referats wurden die Stellen mit Juristen besetzt. Bei meinen entsprechenden Vorschlägen habe ich mich davon leiten lassen, daß die Tätigkeit beim Landesbeauftragten für den Datenschutz wesentlich die Anwendung von Rechtsvorschriften auf Sachverhalte zum Gegenstand hat, also quasi-richterlicher Art ist. Auch die Mitwirkung bei der Fortentwicklung dieser Rechtsvorschriften verlangt eine entsprechende Befähigung. Von den 6 Mitarbeitern im höheren Dienst stammen zwei aus dem Innenministerium, einer aus einem anderen Ministerium, zwei aus Landesmittelbehörden und einer von einer Körperschaft des öffentlichen Rechts.

Vier Planstellen des gehobenen Dienstes konnten ebenfalls bis Januar 1980 besetzt werden. Für weitere Beamte aus diesem Bereich habe ich dem Innenminister Vorschläge unterbreitet. Erfahrungsgemäß lassen sich zeitliche Verzögerungen häufig dann nicht vermeiden, wenn die Bewerber bei anderen Stellen als den obersten Landesbehörden beschäftigt sind. Gleichwohl habe ich Wert darauf gelegt, auch Bewerber aus dem Kreis der Landesmittelbehörden und der Kommunen auszuwählen.

Bisher nicht gelungen ist es, die zur Verfügung stehenden drei Angestelltenstellen für Sachbearbeiter in dem Referat für organisatorisch-technische Fragen zu besetzen. Benötigt werden ADV-Fachkräfte mit Verwaltungserfahrung, die im Rahmen der organisatorisch-technischen Aufgaben der Datenschutzkontrolle eingesetzt werden sollen und deshalb insbesondere unter dem Gesichtspunkt einer weitgehend selbständigen Prüftätigkeit auszuwählen sind. Hier machen sich Schwierigkeiten bemerkbar, die mit den Leistungsanforderungen einerseits und der vorgesehenen Eingruppierung andererseits in Zusammenhang stehen.

Hiervon abgesehen hoffe ich, daß der personelle Aufbau in absehbarer Zeit abgeschlossen ist. Dankenswerterweise wurde schon bisher von Personalvertretungen und Verwaltungen Verständnis auch bei kurzfristigen Arbeitsplatzwechseln, Abordnungen und Versetzungen von Mitarbeitern zum Landesbeauftragten für den Datenschutz gezeigt. Besonders in der ersten Aufbauphase war es von großer Bedeutung, einzelne Personalvorschläge in kürzester Zeit verwirklichen zu können. Auch weiterhin werde ich auf verständnisvolle Mitwirkung und Entgegenkommen beteiligter Stellen angewiesen sein.

d) Organisation

Der Organisationsplan nach dem jetzigen Stand sieht fünf Referate vor. In einem Grundsatzreferat, das von meinem ständigen Vertreter geleitet wird, werden neben den allgemeinen Fragen des Datenschutzes der Bereich der Medien, die Auswirkung der ADV auf Gewaltenteilung und Zuständigkeitsabgrenzungen, die Zusammenarbeit mit den Datenschutzbeauftragten des Bundes und der Länder sowie der Verkehr mit dem Landtag bearbeitet. Darüber hinaus obliegen diesem Referat die Öffentlichkeitsarbeit, die Registerführung, die Büroleitung und die Mittelbewirtschaftung, soweit sie dem Landesbeauftragten zugewiesen ist.

Drei Fachreferate bearbeiten die Datenschutzkontrolle jeweils für folgende Bereiche:

- Einwohnerwesen, Polizei, Verfassungsschutz, Liegenschafts- und Vermessungswesen, Bau- und Wohnungswesen, Rechtswesen;
- Sozialwesen, Gesundheitswesen, Personalwesen, Statistik, raumbezogene Planung;
- Wissenschaft und Forschung, Bildung und Kultur, Finanzwesen, Wirtschaft, Verkehr, Land- und Forstwirtschaft, Eigenbetriebe und öffentliche Unternehmen, nicht-öffentlicher Bereich.

Einem weiteren Referat ist als Querschnittsaufgabe die Bearbeitung aller organisatorischen und technischen Fragen des Datenschutzes zugewiesen. Sie erstreckt sich auf die Bereiche Organisation, konventionelle Technik, ADV-Technik (Hardware, Software einschließlich Betriebssysteme, Datenfernverarbeitung, Datenerfassung) und baulicher Datenschutz. Wesentliches Ziel ist hier auch das Erarbeiten und Durchsetzen neuer Verfahren in der Datensicherung. Einzelfallprüfungen und Kontrollen „vor Ort" führt das Referat sowohl in eigener Zuständigkeit als auch in Zusammenarbeit mit den übrigen Referaten durch, soweit diese in einer Angelegenheit federführend sind.

Die Aufgabenverteilung auf die einzelnen Referate kann angesichts der erst kurzen Erprobungszeit nur vorläufigen Charakter haben. Die weiteren Erfahrungen werden zeigen, ob und welche Veränderungen — auch mit Auswirkungen auf die Personalstruktur — notwendig werden.

e) Diensträume

Die Diensträume für den Landesbeauftragten wurden in einem angemieteten Gebäude in Düsseldorf, Ulenbergstraße 1, zur Verfügung gestellt. Von vornherein war dies nicht als langfristige Lösung gedacht. Schon bald wurde deutlich, daß diese Räumlichkeiten den Anforderungen nicht voll gerecht werden und eine anderweitige Lösung geboten ist. Innenminister und Finanzminister prüfen deshalb die Möglichkeit der Unterbringung in einem anderen Dienstgebäude, das dem Raumbedarf einschließlich der notwendigen Sonderräume (etwa für das Dateienregister) entspricht, den Sicherheitserfordernissen voll genügt und einen weiteren Ausbau der Diensstelle nicht ausschließt. Die räumliche Trennung von dem Innenministerium, die die sachliche Unabhängigkeit betont, sollte auf jeden Fall erhalten bleiben.

3. Aufgaben

a) Kontrolle der Einhaltung der Datenschutzvorschriften

Im Mittelpunkt der Tätigkeit des Landesbeauftragten steht seine Überwachungsaufgabe. Sie ist in der Bestimmung des Gesetzes über die Aufgaben des Landesbeauftragten (§ 26) an den Anfang gestellt. Nach § 26 Abs. 1 Satz 1 DSG NW hat der Landesbeauftragte die Einhaltung der Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen sowie

anderer Vorschriften über den Datenschutz zu kontrollieren, und zwar bei

- den Behörden, Einrichtungen und sonstigen öffentlichen Stellen des Landes (bei Gerichten nur, soweit sie Verwaltungsaufgaben wahrnehmen),
- den Gemeinden und Gemeindeverbänden,
- den sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts (mit Ausnahme des Westdeutschen Rundfunks Köln) sowie deren Vereinigungen.

Die Kontrolle beschränkt sich nicht auf die Einhaltung der Bestimmungen des Datenschutzgesetzes Nordrhein-Westfalen, sondern erstreckt sich auch auf andere Datenschutzbestimmungen. Dazu gehören etwa die Vorschriften über das Steuergeheimnis, das Sozialgeheimnis und das Statistikgeheimnis, aber auch der neue Artikel 4 Abs. 2 der Landesverfassung mit dem Grundrecht auf Datenschutz, in das nur im überwiegenden Interesse der Allgemeinheit auf Grund eines Gesetzes eingegriffen werden darf.

Die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen finden nur Anwendung, wenn personenbezogene Daten in einer Datei verarbeitet oder aus einer Datei übermittelt werden (§ 1 Abs. 2 Satz 1 DSG NW). Folglich kann sich die Kontrolle insoweit nur auf die Datenverarbeitung in einer Datei oder die Übermittlung aus einer solchen beziehen.

Hinsichtlich der Kontrolle der Einhaltung sonstiger Datenschutzbestimmungen vertreten einige Kommentare zu der entsprechenden Regelung im Bundesdatenschutzgesetz (§ 19 Abs.1 Satz 1) die gleiche Auffassung. Danach wäre es dem Datenschutzbeauftragten z. B. verwehrt, sich mit einer Verletzung des Sozialgeheimnisses zu befassen, wenn die unbefugte Übermittlung von Daten an Dritte nicht aus einer Datei, sondern aus einer Akte oder sonstigen Unterlage erfolgt. Entsprechendes würde für Verletzungen des Grundrechts auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung gelten.

Der Justizminister geht noch weiter und ist der Ansicht, daß die Kontrollbefugnis auf die Einhaltung derjenigen Vorschriften beschränkt ist, die (allein) den Schutz von in Dateien verarbeiteten Daten betreffen, also im wesentlichen nur der Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen. Damit bestreitet er dem Landesbeauftragten die Kontrollbefugnis für die Einhaltung aller Vorschriften, die zugleich auch Daten schützen, die nicht in Dateien verarbeitet werden, wie Artikel 4 Abs. 2 der Landesverfassung.

Beiden Auffassungen muß mit Nachdruck widersprochen werden. Es ist kein vernünftiger Grund erkennbar, die Kontrolle bei diesen sonstigen Vorschriften, für die der Dateibegriff keine Bedeutung hat, an der Relevanzschwelle der Datei enden zu lassen. Für den Schutzzweck dieser Vorschriften wie auch für die durch sie geschützten Belange des Betroffenen ist es unerheblich, ob die Daten in einer Datei oder in einer Akte oder sonstigen Unterlage verarbeitet werden. Erst recht ist es mit dem Sinn und Zweck einer externen Kontrolle des Datenschutzes nicht vereinbar, eine Kontrollbefugnis für die Einhaltung dieser Vorschriften schlechthin auszuschließen. Ich gehe deshalb auch Beschwerden nach, die die Verletzung solcher Datenschutzbestimmungen rügen, und zwar auch dann, wenn die Daten nicht in einer Datei gespeichert sind, und werde gegebenenfalls solche Verstöße beanstanden.

Die Kontrolle durch den Landesbeauftragten kann vorbeugender oder nachgehender Art sein. Zwar ist anzustreben, Verstöße gegen den Datenschutz möglichst von vornherein zu verhindern. Dies wird jedoch wegen der Größe der zu kontrollierenden Verwaltung und der geringen Zahl der Mitarbeiter des Landesbeauftragten nur begrenzt möglich sein. Umso wichtiger ist die nachgehende Kontrolle, gerade auch wegen ihrer Signalwirkung über den Einzelfall hinaus.

Bei der Kontrolle hat der Landesbeauftragte in erster Linie die Belange des Bürgers zu vertreten. Er ist eine Art Ombudsmann, „Bürgeranwalt" in Datenschutzfragen. Daneben soll er das Datenschutzgewissen der Verwaltung sein und die öffentlichen Stellen in Datenschutzfragen beraten.

b) Vertretung der Belange des Bürgers

Nach § 29 DSG NW hat jedermann das Recht, sich unmittelbar an den Landesbeauftragten zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch eine öffentliche Stelle in seinen schutzwürdigen Belangen verletzt zu sein. Er hat einen Anspruch darauf, daß seine Eingabe zügig bearbeitet wird. Andere Aufgaben des Landesbeauftragten müssen demgegenüber grundsätzlich zurückstehen.

Bei derartigen Eingaben bin ich stets um sorgfältige Sachverhaltsklärung bemüht. Bestätigt das Ergebnis meiner Ermittlungen, daß schutzwürdige Belange des Betroffenen verletzt sind, so dringe ich nachdrücklich auf Abhilfe. Fällt die Angelegenheit in die Zuständigkeit anderer Kontrollinstitutionen, sorge ich für unverzügliche Information der Beteiligten und klärende Hinweise, soweit mir dies mit den mir zur Verfügung stehenden Mitteln möglich ist.

Besonders wichtig ist es, dem Bürger dort zu helfen, wo er sich selbst nicht die notwendigen Informationen verschaffen kann, die er braucht, um seine Rechte gezielt geltend zu machen. Dies gilt insbesondere für die Behörden für Verfassungsschutz, die Staatsanwaltschaft und die Polizei, die weder zur Veröffentlichung ihrer Dateien noch zur Auskunft gegenüber dem Betroffenen über die über ihn gespeicherten Daten verpflichtet sind. In diesem Bereich hat der Bürger keine Möglichkeit festzustellen, bei welchen Stellen welche Daten über ihn gespeichert sind. Dagegen ist der Landesbeauftragte berechtigt, auch bei diesen Behörden die Beachtung der Datenschutzvorschriften ohne Einschränkung zu kontrollieren. Soweit ich Verstöße feststelle, werde ich auch hier auf schnelle Abhilfe dringen. Allerdings ist es mir nach dem Gesetz verwehrt, hierbei gewonnene Erkenntnisse ohne Zustimmung der Behörde dem Betroffenen oder der Öffentlichkeit mitzuteilen. Umso mehr bin ich darauf angewiesen, daß der betroffene Bürger mir für meine Kontrolltätigkeit Vertrauen entgegenbringt.

Das Anrufungsrecht nach § 29 DSG NW wird allerdings häufig mißverstanden. Bei zahlreichen Eingaben mußte ich darauf hinweisen, daß es nicht Aufgabe des Landesbeauftragten für den Datenschutz sein kann, bei der Beschaffung personenbezogener Daten anderer behilflich zu sein, und sei es auch nur durch eine Bestätigung der datenschutzrechtlichen Unbedenklichkeit. § 29 DSG NW gibt jedermann nur dann das Recht, sich unmittelbar an den Landesbeauftragten zu wenden, wenn er glaubt, daß er bei der Verarbeitung **seiner** personenbezogenen Daten in seinen schutzwürdigen Belangen verletzt ist.

Auch wenn der Landesbeauftragte nicht auf eine Eingabe nach § 29 DSG NW, sondern von Amts wegen tätig wird, hat er die Datenschutzbelange des Bürgers zu vertreten. Andere Belange müssen von den jeweils Zuständigen oder von dem Bürger selbst vertreten werden.

c) Beratung der Verwaltung

Nach § 26 Abs. 2 DSG NW kann der Landesbeauftragte die Landesregierung, einzelne Minister, die Gemeinden und Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen in Fragen des Datenschutzes beraten.

Die Häufigkeit, mit der schon bisher aus dem Bereich der öffentlichen Verwaltung Datenschutzfragen an mich herangetragen wurden, ist angesichts der kurzen Zeit seit der Übernahme meines Amtes erfreulich groß. Vor allem von den Gemeinden und Gemeindeverbänden wurde von dieser Möglichkeit reger Gebrauch gemacht. Die Anfragen betrafen insbesondere die Datenübermittlung, die Verpflichtung auf das Datengeheimnis und die Veröffentlichung von Dateien. Sie waren wertvolle Hinweise auch für meine weitere Tätigkeit. Bei Fragen von grundsätzlicher Bedeutung gaben sie mir mehrfach Veranlassung, mit obersten Landesbehörden in Verbindung zu treten. Meine Anregungen wurden überwiegend positiv aufgenommen.

Die Beratung der Verwaltung in Datenschutzfragen kann wesentlich dazu beitragen, daß es gar nicht zu begründeten Beschwerden kommt. Hierzu ist notwendig, daß sie möglichst frühzeitig einsetzt. Sie kann also nicht auf den Vollzug geltender Datenschutzvorschriften beschränkt bleiben, sondern muß sich auch auf die Vorbereitung datenschutzrelevanter Regelungen erstrecken. Beratung setzt allerdings voraus, daß sie gewünscht wird. Der Landesbeauftragte kann sie zwar anbieten, aber niemandem aufdrängen.

d) Beobachtung der Auswirkungen der ADV auf Gewaltenteilung und Zuständigkeitsabgrenzungen

Nach § 26 Abs. 4 DSG NW hat der Landesbeauftragte die Auswirkungen der ADV auf Arbeitsweise und Entscheidungsbefugnisse der öffentlichen Stellen zu beobachten. Er hat insbesondere darauf zu achten, ob sie zu einer Verschiebung in der Gewaltenteilung zwischen den Verfassungsorganen und in der Zuständigkeitsabgrenzung zwischen den Organen der kommunalen Selbstverwaltung sowie zwischen der staatlichen Verwaltung und der kommunalen Selbstverwaltung führen. Diese Aufgabe dient nicht dem Schutz des Bürgers, sondern der Bewahrung des verfassungsmäßigen Gefüges sowie der Zuständigkeitsabgrenzungen im kommunalen Bereich vor einer Veränderung durch die ADV.

Da meine Dienststelle erst seit September 1979 eingerichtet und noch im Aufbau begriffen ist, kann ich noch nicht über spezifische Erkenntnisse zu diesem Bereich berichten. Gleichwohl wende ich ihm die seiner Bedeutung entsprechende Aufmerksamkeit zu. Dies gilt insbesondere für den Bereich der raumbezogenen Planung.

Der Einsatz modernster Hilfsmittel der ADV kann Entscheidungsspielräume einengen und die Entscheidungsfindung beeinflussen. Dies gilt gleichermaßen für die Legislative wie für die Exekutive. Dem Ausschluß solcher Gefahren dienen auch die Regelungen in den §§ 2 und 3 des Gesetzes über die Organisation der automatisierten Datenverarbeitung in Nordrhein-Westfalen. So wird jeweils sorgfältig zu verfolgen sein, ob durch den Einsatz der ADV das Informationsgleichgewicht zwischen den Organen der gesetzgebenden und der vollziehenden Gewalt beeinträchtigt wird.

Entsprechendes gilt für die Zuständigkeitsabgrenzung unter den Organen der kommunalen Selbstverwaltung. Zuständigkeiten dürfen weder nach Inhalt und Gewicht verschoben noch durch Veränderung des Informationsgleichgewichts im Ergebnis eingeschränkt werden. In diesem Zusammenhang müssen auch Überlegungen, die im Rahmen der Diskussion über die „Weiterentwicklung der gemeinsamen kommunalen Datenverarbeitung" angestellt werden, in die Beobachtung einbezogen werden. Auch Pläne für ein „Infrastruktur-Kataster" können sich auf das reale Machtgefüge auswirken.

Der mir vom Gesetz auferlegten Pflicht zur Beobachtung von Auswirkungen der automatisierten Datenverarbeitung werde ich umso gezielter nachkommen können, je größer der Informationsfluß ist, der von den betroffenen Organen ausgeht. Unterrichtung und Einschaltung in einem frühen Stadium erleichtern die Prüfung, ob und gegebenenfalls welche Maßnahmen angeregt werden können, um Gefahren für die verfassungsgemäße Struktur entgegenzuwirken.

4. Informationsrechte

a) Auskunfts-, Einsichts- und Zutrittsrecht

Der Landesbeauftragte kann seine Aufgaben nur dann erfüllen, wenn er die Möglichkeit zur umfassenden Information hat.

Alle seiner Kontrolle unterworfenen öffentlichen Stellen sind verpflichtet, den Landesbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen (§ 26 Abs. 1 Satz 2 DSG NW).

Soweit es zur Erfüllung seiner Aufgaben erforderlich ist, kann er von diesen Stellen insbesondere Auskunft zu den Fragen sowie Einsicht in die Unterlagen verlangen, die im Zusammenhang mit der Datenverarbeitung stehen (§ 26 Abs. 3 Nr. 1 DSG NW). Als einziges Bundesland und im Gegensatz zum Bund hat Nordrhein-Westfalen auf eine Staatswohlklausel verzichtet, auf Grund deren die Einsichtnahme verweigert werden kann, wenn die zuständige oberste Bundes- oder Landesbehörde feststellt, daß hierdurch die Sicherheit des Bundes oder eines Landes gefährdet wird (vgl. § 19 Abs. 3 Satz 4 BDSG). Ferner kann der Landesbeauftragte alle öffentlichen Stellen jederzeit unangemeldet aufsuchen und ihre Diensträume betreten (§ 26 Abs. 3 Nr. 2 DSG NW). Die Landesregierung und alle öffentlichen Stellen haben ihm bei der Durchführung seiner Aufgaben Amtshilfe zu leisten (§ 26 Abs. 6 DSG NW).

Von meinem Auskunftsrecht habe ich in zahlreichen Fällen Gebrauch gemacht. Nennenswerte Schwierigkeiten, die erforderlichen Informationen zu erlangen, haben sich nicht ergeben. Wenn auch Auskünfte in einigen Fällen nur mit zeitlicher Verzögerung gegeben wurden, so wurde doch allgemein meine Absicht verstanden, dem hilfesuchenden Bürger möglichst schnell eine Antwort zu erteilen. Hier war zu berücksichtigen, daß bei Antritt meines Amtes bereits zahlreiche Eingaben vorlagen, die zum Teil älter als ein halbes Jahr waren.

Schon deswegen mußte ich in meinen Auskunftsersuchen kurze Fristen setzen. Nicht immer wurde mir hierfür das rechte Verständnis entgegengebracht. Dennoch werde ich grundsätzlich daran festhalten, dem Interesse des Bürgers auch auf diese Weise Rechnung zu tragen. Für den Berichtszeitraum ist dies, so glaube ich, im wesentlichen gelungen. Obwohl der Aufbau der Dienststelle noch andauert, konnten die Beschwerden Betroffener größtenteils abschließend bearbeitet werden.

Soweit Einsicht in Akten und sonstige Unterlagen notwendig war, ist meinen Wünschen im Ergebnis gefolgt worden. Auch wenn dies mehr Zeit erfordert, hat sich gezeigt, daß durch Akteneinsicht Auskünfte mitunter sinnvoll ergänzt oder auch korrigiert und Stellungnahmen entbehrlich werden können.

Neben Auskunfts- und Einsichtrecht hat sich auch mein Recht auf jederzeitigen (auch unangemeldeten) Zutritt bei den meiner Kontrolle unterliegenden Stellen als hilfreich erwiesen. Dieses vermittelt Erkenntnisse „vor Ort", die für eine effektive Arbeitsweise unentbehrlich sind.

Unmittelbare Einblicke in den Verwaltungsablauf machen Zusammenhänge deutlich, die sonst kaum feststellbar sind. Von besonderer Bedeutung ist dies nach meinen bisherigen Erfahrungen für den Bereich der Datenverarbeitung im Auftrag (§ 7 Abs. 1 DSG NW). Insbesondere bei Maßnahmen der Datensicherung sehe ich hier Gefahren für die Einwirkungsmöglichkeit des Auftraggebers, die stets uneingeschränkt gewährleistet sein muß. Aus gegebenem Anlaß dränge ich stets auf eindeutige vertragliche Absicherung.

b) Dateienregister

Eine weitere Erkenntnisquelle wird das Dateienregister sein, das nach § 27 DSG NW von dem Landesbeauftragten geführt werden soll. Es erschließt diesem den Gesamtbestand der seiner Kontrolle unterliegenden Dateien und wird damit auch die Prüftätigkeit im Einzelfall erheblich erleichtern.

Das Register besteht derzeit noch nicht. Es kann erst eingerichtet werden, wenn die Landesregierung die zur Regelung der Einzelheiten erforderliche Rechtsverordnung — im Einvernehmen mit dem zuständigen Landtagsausschuß — erlassen hat (§ 27 Abs. 6 DSG NW). Ein entsprechender Verordnungsentwurf ist in Vorbereitung. Unter anderem geht er auf Vorstellungen zurück, die der Landesbeauftragte entwickelt hat und bei denen einschlägige Erfahrungen des Bundes und anderer Länder berücksichtigt worden sind.

Die Abstimmung mit den Ressorts und den kommunalen Spitzenverbänden ist noch nicht abgeschlossen. Zusammen mit dem federführenden Innenminister habe ich mich

für größtmögliche Beschleunigung eingesetzt. So soll alles versucht werden, noch vor der Neuwahl des Landtags das erforderliche Einvernehmen mit dem zuständigen Landtagsausschuß herzustellen und die Dateienregisterverordnung noch in dieser Wahlperiode in Kraft treten zu lassen. Im Interesse des Datenschutzes bleibt zu hoffen, daß dies gelingt und dem Aufbau des Registers damit nichts mehr im Wege steht.

Nicht nur mir wird damit ein wichtiges Hilfsmittel in die Hand gegeben; auch der Bürger erhält die Möglichkeit, über mehr Transparenz zu mehr Information zu gelangen. Durch Einsichtnahme in das Register kann er feststellen, welche öffentlichen Stellen vermutlich welche Daten über ihn zu welchem Zweck speichern. Neben den Veröffentlichungen nach § 15 DSG NW ermöglicht ihm das Register, die ihm durch das Datenschutzgesetz Nordrhein-Westfalen eingeräumten Rechte, insbesondere sein Auskunftsrecht nach § 16 DSG NW, gezielt auszuüben.

5. Durchsetzungsmöglichkeiten

a) Empfehlungen

Zur Durchsetzung seiner Vorstellungen stehen dem Landesbeauftragten eine Reihe sehr unterschiedlicher Möglichkeiten zur Verfügung. An erster Stelle nennt das Gesetz die Empfehlung.

Nach § 26 Abs. 2 DSG NW kann der Landesbeauftragte Empfehlungen „zur Verbesserung des Datenschutzes" geben; dies schließt Empfehlungen zur Vermeidung von Verstößen gegen Vorschriften über den Datenschutz ein. Von dieser Möglichkeit habe ich in zahlreichen Fällen Gebrauch gemacht. Von wenigen Ausnahmefällen abgesehen ist meinen Empfehlungen gefolgt worden.

b) Beanstandungen

Nach § 30 DSG NW hat der Landesbeauftragte ferner die Möglichkeit der Beanstandung von Verstößen gegen die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen oder anderer Datenschutzbestimmungen oder von sonstigen Mängeln bei der personenbezogenen Datenverarbeitung. In diesem Falle teilt er die Verstöße oder Mängel der im Gesetz bezeichneten Stelle zur Stellungnahme innerhalb einer von ihm bestimmten Frist mit.

Von der förmlichen Beanstandung habe ich bisher nur in zwei Fällen Gebrauch gemacht. Hierbei lasse ich mich davon leiten, daß in der ersten Zeit der Anwendung eines neuen Gesetzes in der Regel das Mittel der Empfehlung ausreicht, um Verstöße künftig zu vermeiden und sonstige Mängel zu beseitigen. Nur wenn die Bedeutung der Angelegenheit, die Schwere des Verstoßes oder die mangelnde Einsicht der verantwortlichen Stelle dies verlangt, ist bereits jetzt eine Beanstandung geboten. Ich werde dieses „gestufte Verfahren" jedoch nach einiger Zeit überprüfen.

c) Befassung des Landtags

Nach § 31 Abs. 3 DSG NW kann sich der Landesbeauftragte darüberhinaus jederzeit an den Landtag wenden. Dieses Recht ist insbesondere dann von Bedeutung, wenn eine Empfehlung oder eine Beanstandung nicht beachtet wird. Ich habe von dieser Möglichkeit bisher in zwei Fällen Gebrauch gemacht.

In dem einen Fall habe ich empfohlen, die Landeswahlordnung und die Kommunalwahlordnung dahin zu ändern, daß die Geburtsdaten im auszulegenden Wählerverzeichnis unkenntlich zu machen sind oder für die Auslegung ein gesondertes Wählerverzeichnis ohne Angabe der Geburtsdaten zu verwenden ist. Der Innenminister ist dieser Empfeh-

lung in der Verordnung zur Änderung der Landeswahlordnung nicht gefolgt. Ich habe den Ausschuß für Innere Verwaltung des Landtags hierüber unterrichtet (Vorlage 8/2150). Dieser hat sich in seiner Sitzung am 20. März 1980 mit der Angelegenheit befaßt.

Ferner habe ich in der öffentlichen Anhörung über Bildschirmtext am 31. Januar 1980 im Hauptausschuß des Landtags zu den notwendigen Vorkehrungen für den Datenschutz Stellung genommen und Vorschläge zur Änderung des Entwurfs eines Bildschirmtextversuchsgesetzes unterbreitet (Zuschrift 8/2985). Im Hinblick auf die Stellungnahme des Chefs der Staatskanzlei habe ich meine Empfehlungen hinsichtlich der Regelungen für die Anbieter ergänzt (Vorlage 8/2274). Der Hauptausschuß ist diesen ergänzenden Empfehlungen in seiner Sitzung am 6. März 1980 einstimmig gefolgt. Hinsichtlich meiner Empfehlung für Regelungen für die Bildschirmtext-Zentrale hat der Ausschuß festgestellt, er interpretiere eine von der Deutschen Bundespost gegebene schriftliche Zusage so, daß meinem Anliegen voll Rechnung getragen werde (vgl. Vorlage 8/2299).

d) Unterrichtung der Öffentlichkeit

Bürger und Öffentlichkeit haben auch und gerade im Bereich des Datenschutzes Anspruch auf umfassende Information. Dieser Anspruch ist zwar im Gesetz nicht ausdrücklich festgelegt, ergibt sich aber aus der Natur des Datenschutzes. Dieser ist keine Geheimwissenschaft, sondern eine Angelegenheit der Öffentlichkeit. Neben den im Gesetz geregelten Befugnissen des Landesbeauftragten ist die Unterrichtung der Öffentlichkeit ein Mittel zur Durchsetzung von mehr Datenschutz.

In Presseerklärungen, Zeitungs- und Rundfunkinterviews sowie Vorträgen und Referaten habe ich zu verschiedenen Themen, insbesondere aus den Bereichen Meldewesen und Polizei, Stellung genommen. Im Interesse des Datenschutzes werde ich auch weiterhin für Transparenz meiner Tätigkeit sorgen.

Grenzen, die mir in einzelnen Sachgebieten gezogen sind, müssen hierbei respektiert werden. Diese mußte ich auf einen Pressebericht zur Rasterfahndung klarstellen: Nach dem Datenschutzgesetz haben Polizei und Verfassungsschutz ein Auskunftsverweigerungsrecht gegenüber dem Bürger. Dieses Recht darf der Datenschutzbeauftragte nicht durch Mitteilungen über die ihm bei seiner Prüfung zugänglich gemachten Erkenntnisse umgehen. Er ist insoweit gesetzlich zur Verschwiegenheit verpflichtet. Die Verschwiegenheitspflicht hindert ihn jedoch nicht daran, die Öffentlichkeit über Verstöße gegen Vorschriften über den Datenschutz zu unterrichten. Soweit ich solche Verstöße feststelle, werde ich nicht schweigen. Ein „geheimes Zusammenspiel zwischen Kontrolleuren und Kontrollierten" gibt es nicht.

e) Förderung des Datenschutzbewußtseins

Der Arbeit des Landesbeauftragten kann nur dann Erfolg beschieden sein, wenn seine Vorstellungen auf die entsprechende Resonanz bei Bürger und Verwaltung treffen. Entscheidend hierfür wird das Bewußtsein sein, das unsere Gesellschaft zum Datenschutz entwickelt. Fehlt dieses in ausreichendem Maße, muß alles Bemühen vergeblich sein, der Zielsetzung des Gesetzes gerecht zu werden.

Ich sehe deshalb meine Aufgabe auch darin, das Datenschutzbewußtsein zu fördern. So habe ich jede Gelegenheit genutzt, auch bei der Beantwortung von Eingaben und Anfragen den Gedanken des Datenschutzes zu vertiefen und insbesondere auf seine verfassungsrechtliche Grundlage hinzuweisen.

Dazu gehörte auch, der bei vielen Bürgern vorhandenen Vorstellung entgegenzutreten, daß der Landesbeauftragte eine Zentralstelle mit dem Gesamtbestand aller gespeicherten personenbezogenen Daten sei. Die Bürger müssen darauf hingewiesen werden, daß eine zentrale Speicherung und die damit ermöglichte Erfassung des Menschen in seiner ganzen Persönlichkeit mit den Grundsätzen des Datenschutzes unvereinbar wäre.

Erfreulicherweise zeigt die bisherige Erfahrung, daß der Datenschutz in der Bevölkerung erhebliches Interesse findet. Zahlreiche Wünsche nach Informationsmaterial machen dies deutlich. Hierbei war für mich von großem Nutzen, daß ich von Beginn an auf eine Informationsschrift des Innenministers zum Datenschutzgesetz Nordrhein-Westfalen mit dem Gesetzestext zurückgreifen konnte.

Seit Anfang des Jahres steht mir zudem die Informationsschrift „Der Bürger und seine Daten" zur Verfügung. Die Schrift ist von dem Bundesbeauftragten für den Datenschutz in Zusammenarbeit mit den Landesbeauftragten für den Datenschutz, der Datenschutzkommission Rheinland-Pfalz und den obersten Aufsichtsbehörden der Länder für den Datenschutz herausgegeben worden. Sie soll es dem Bürger erleichtern, sich einen Überblick über die Stellen zu verschaffen, die vermutlich Daten über ihn speichern und bei denen er sein Recht auf Datenschutz geltend machen kann.

Diese Informationsschrift stößt auf zunehmendes Interesse sowohl bei der Bevölkerung als auch bei den Stellen der öffentlichen Verwaltung. Das Interesse zeigt, daß sich immer mehr Bürger ihres Rechts auf Schutz ihrer personenbezogenen Daten bewußt werden.

f) Bewertung der Durchsetzungsmöglichkeiten

Den umfassenden Informationsrechten des Landesbeauftragten stehen keine entsprechenden rechtlichen Möglichkeiten gegenüber, die Einhaltung der Datenschutzbestimmungen bei den seiner Kontrolle unterliegenden Stellen im Konfliktfall durchzusetzen. Aus verfassungsrechtlichen Gründen konnte dem Landesbeauftragten kein Weisungsrecht gegenüber den öffentlichen Stellen eingeräumt werden. Das Gesetz sieht auch kein Klagerecht des Landesbeauftragten zur Durchsetzung seiner Rechtsauffassung vor. Unter den gegebenen Umständen hängt die Effektivität seiner Tätigkeit von seiner Überzeugungskraft gegenüber der Verwaltung ab, noch mehr aber von der Unterstützung durch den Landtag und die Öffentlichkeit.

6. Zusammenarbeit mit den anderen Datenschutzbeauftragten

Nach § 26 Abs. 5 DSG NW arbeitet der Landesbeauftragte mit den Behörden und sonstigen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz im Bund und in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach §§ 30, 40 des Bundesdatenschutzgesetzes zusammen. Ziel der Zusammenarbeit ist es, der Gefahr zu begegnen, daß vergleichbare Sachverhalte datenschutzrechtlich unterschiedlich beurteilt und allgemein bestehende Probleme angesichts der Vielzahl von Zuständigkeiten unterschiedlich gelöst werden.

Die seit 1978 bestehende **Konferenz der Datenschutzbeauftragten der Länder und des Bundes** ist im Berichtszeitraum zweimal zusammengetreten. In den Sitzungen im November 1979 und im Februar 1980 wurden u. a. folgende Themen behandelt:

- Datenschutz in der Steuerverwaltung (Kontrollbefugnisse, Veröffentlichung, Auskunft an die Betroffenen);
- Datenschutz bei den Sicherheitsbehörden (Neukonzeption des INPOL-Systems, Rasterfahndung, polizeiliche Beobachtung);
- Änderung des Personalausweisgesetzes (Verwendungsbeschränkung des maschinenlesbaren Personalausweises);
- Entwurf eines Melderechtsrahmengesetzes;
- Erhebung von Kosten für das Geltendmachen von Rechten nach den Datenschutzgesetzen.

Soweit nach dem Verfahrensstand geboten, habe ich die zuständigen Ressorts über die Sitzungsergebnisse unterrichtet und um Unterstützung der gemeinsam erarbeiteten und einstimmig beschlossenen Empfehlungen der Datenschutzbeauftragten gebeten.

Zur Vorbereitung der Sitzungen der Konferenz und zur Vertiefung des Gedankenaustausches sind mehrere Arbeitsgruppen gebildet worden, an deren Sitzungen die zuständigen Referenten meiner Dienststelle teilnehmen.

Eine weitere Möglichkeit der Zusammenarbeit besteht in den sogenannten **Kooperationssitzungen,** zu denen der Bundesbeauftragte für den Datenschutz regelmäßig einlädt. Teilnehmer sind jeweils die Landesbeauftragten für den Datenschutz und die obersten Aufsichtsbehörden für den Datenschutz der Länder. Mit der Durchführung dieser Sitzungen folgt der Bundesbeauftragte einem gesetzlichen Auftrag aus § 19 Abs. 5 BDSG, der ihn verpflichtet, auf die Zusammenarbeit mit Behörden und sonstigen öffentlichen Stellen hinzuwirken, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern und nach § 30 BDSG zuständig sind.

Im übrigen verfolge ich die Sitzungsergebnisse des sogenannten **Düsseldorfer Kreises,** in dem die Datenschutzreferenten der obersten Landesbehörden aus den einzelnen Bundesländern zusammenkommen. Er dient einer möglichst einheitlichen Handhabung der Vorschriften des Bundesdatenschutzgesetzes im nicht-öffentlichen Bereich. Konferenzteilnehmer sind auch die Landesbeauftragten für den Datenschutz in Bremen, Saarland und Schleswig-Holstein, und zwar in ihrer gleichzeitigen Eigenschaft als oberste Aufsichtsbehörde dieser Länder, sowie der Bundesbeauftragte für den Datenschutz. Auf diese Weise ist zugleich der ständige gegenseitige Erfahrungsaustausch mit den Gremien der Datenschutzbeauftragten sichergestellt.

B. Das Grundrecht auf Datenschutz

Mit dem neuen Artikel 4 Abs. 2 der Landesverfassung ist erstmals der Schutz personenbezogener Daten als ausdrücklich formuliertes Grundrecht in einer deutschen Verfassung verankert worden. Zwar räumt das Grundgesetz in den Grundrechten auf Schutz der Menschenwürde und freie Entfaltung der Persönlichkeit in Verbindung mit dem Rechtsstaats- und dem Sozialstaatsprinzip nach der Rechtssprechung des Bundesverfassungsgerichts dem Einzelnen ähnliche Rechte ein. Das Grundrecht auf Datenschutz stärkt jedoch den Rechtsschutz des Einzelnen, der den Schutz seiner personenbezogenen Daten nicht mehr aus den allgemeinen Grundrechten und Prinzipien des Grundgesetzes und der Rechtssprechung des Bundesverfassungsgerichts herleiten muß, sondern sich auf ein ausdrückliches Abwehrrecht berufen kann. Darüberhinaus wird in dem Grundrecht der hohe Rang des Datenschutzes unterstrichen.

Nach Artikel 4 Abs. 2 der Landesverfassung hat jeder Anspruch auf Schutz seiner personenbezogenen Daten (Satz 1). In dieses Grundrecht darf nur im überwiegenden Interesse der Allgemeinheit auf Grund eines (Landes-) Gesetzes (Satz 2) oder auf Grund Bundesrechts eingegriffen werden, das nach Artikel 31 GG Vorrang auch gegenüber der Landesverfassung hat.

Danach bedarf jeder behördliche Umgang mit personenbezogenen Daten, also jedes Erheben, Sammeln, Festhalten, Nutzen und Weitergeben solcher Daten einer gesetzlichen Grundlage. Dies gilt unabhängig davon, ob die Daten in einer Datei gespeichert oder in Akten, Listen oder sonstigen Unterlagen festgehalten werden (vgl. Hunsche in Ruckriegel/ v. d. Groeben/Hunsche, Datenschutz und Datenverarbeitung in Nordrhein-Westfalen, Art. 4 Anm. 8). Fehlt eine solche gesetzliche Grundlage und liegt auch keine Einwilligung des Betroffenen vor, so ist der Umgang mit seinen Daten unzulässig.

Werden personenbezogene Daten in Dateien verarbeitet, so sind gesetzliche Grundlage die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen, soweit nicht besondere Rechtsvorschriften des Landes nach § 37 DSG NW oder Rechtsvorschriften des Bundes nach Artikel 31 GG vorgehen. Nach § 3 Satz 1 DSG NW ist die Verarbeitung personenbezogener Daten in jeder ihrer Phasen nur zulässig, wenn entweder dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt (Nr. 1) oder der Betroffene eingewilligt hat (Nr. 2).

Gesetzliche Grundlage für das Erheben von Daten kann das Datenschutzgesetz Nordrhein-Westfalen allerdings nicht sein. Zwar läßt § 10 Abs. 1 DSG NW das Speichern in einer Datei zu, wenn es zur rechtmäßigen Erfüllung der Aufgaben der speichernden Stelle erforderlich ist. Diese Vorschrift ermächtigt jedoch nicht zur Datenerhebung, sondern setzt eine rechtmäßige, also eine ihrerseits durch Gesetz zugelassene oder mit Einwilligung des Betroffenen vorgenommene Datenerhebung voraus.

Werden personenbezogene Daten nicht in Dateien verarbeitet, so kommen als gesetzliche Grundlage für einen Eingriff in das Grundrecht auf Datenschutz nicht die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen, sondern nur andere Rechtsvorschriften in Betracht. In diesem Bericht wird ausgeführt, daß in einigen Bereichen die gesetzliche Grundlage für den Umgang mit personenbezogenen Daten fehlt oder zweifelhaft ist. Das Grundrecht auf Datenschutz zwingt deshalb zu einer durchgehenden Verrechtlichung der personenbezogenen Informationsverarbeitung.

Soweit Eingriffe in dieses Grundrecht auf Vorschriften des Landesrechts gestützt werden, muß ein überwiegendes Interesse der Allgemeinheit vorliegen. Darüber hinaus muß — wie auch bei Eingriffen auf Grund Bundesrechts — der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit beachtet werden, der nach der Rechtssprechung des Bundesverfassungsgerichts übergreifende Leitregel allen staatlichen Handelns ist und seinerseits aus dem Rechtsstaatsprinzip (Artikel 20 Abs. 3 GG) hergeleitet wird.

Das Erfordernis des überwiegenden Interesses der Allgemeinheit und der Verhältnismäßigkeitsgrundsatz binden nicht nur den Gesetzgeber, wenn er einen Eingriff in das Grundrecht zuläßt. Sie sind auch bei der Auslegung und Anwendung der den Eingriff zulassenden Rechtsvorschrift zu beachten.

Ausgehend von der Rechtssprechung des Bundesverfassungsgerichts zu dem Schutz der Menschenwürde, dem Recht auf freie Entfaltung der Persönlichkeit, dem Rechtsstaat- und dem Sozialstaatprinzip sowie in Anlehnung an die von dem Gesetzgeber in dem Datenschutzgesetz Nordrhein-Westfalen vorgenommene Interpretation des Grundrechts auf Datenschutz lasse ich mich bei der Kontrolle der Einhaltung von Artikel 4 Abs. 2 der Landesverfassung von folgenden Grundsätzen leiten:

1. Nach dem Verhältnismäßigkeitsgrundsatz muß der Eingriff, hier also jeder Umgang mit personenbezogenen Daten, nicht nur notwendig sein, um den angestrebten Zweck der Verwaltung zu erreichen. Die mit dem Eingriff verbundene Belastung muß auch in einem angemessenen Verhältnis zu den daraus erwachsenden Vorteilen stehen.
2. Personenbezogene Daten dürfen nur erhoben, gesammelt, festgehalten, genutzt oder weitergegeben werden, soweit die Kenntnis der Daten zur rechtmäßigen Erfüllung der Aufgaben einer öffentlichen Stelle erforderlich ist.
3. Personenbezogene Daten dürfen darüber hinaus an eine nicht-öffentliche Stelle weitergegeben werden, soweit ein berechtigtes Interesse des Empfängers an der Kenntnis der Daten gegenüber dem Interesse des Betroffenen an dem Schutz dieser Daten überwiegt. Hierzu ist in der Regel mindestens erforderlich, daß das Interesse des Empfängers ein rechtliches oder zugleich ein öffentliches ist.
4. In den Kernbereich der Persönlichkeitssphäre darf überhaupt nicht eingegriffen werden. Ein Eingriff in diesen Bereich liegt in der Regel vor, wenn die Daten die Intimsphäre oder diejenigen Beziehungen des Einzelnen betreffen, die von Natur aus Geheimnischarakter haben. Er liegt in der Regel nicht vor, wenn die Erhebung nur an das Verhalten in der Außenwelt anknüpft.
5. Daten, deren Erheben, Sammeln, Festhalten oder Nutzen unzulässig war, sind zu löschen.
6. Unrichtige Daten sind zu berichtigen. Daten, deren Richtigkeit von dem Betroffenen bestritten wird, sind zu löschen oder zu sperren, wenn sich weder ihre Richtigkeit noch ihre Unrichtigkeit feststellen läßt.
7. Daten, deren Kenntnis zur rechtmäßigen Erfüllung der Aufgaben nicht mehr erforderlich ist, sind zu löschen oder zu sperren.
8. Auch bei Personen, die auf Grund persönlicher Schwäche oder Schuld gegen die Ordnung der Gesellschaft verstoßen haben, dürfen im Interesse der Wiedereingliederung in die Gesellschaft belastende Daten nach einer bestimmten Zeit nicht mehr genutzt oder weitergegeben werden.
9. Öffentliche Stellen, die mit personenbezogenen Daten umgehen, haben die technischen und organisatorischen Maßnahmen zu treffen, die zum Schutz der Daten gegen unbefugtes Nutzen oder Weitergeben erforderlich sind.

Ich gehe demnach entsprechend dem Wortlaut des Artikels 4 Abs. 2 der Landesverfassung von einer weiten Auslegung des Anspruchs auf Schutz der personenbezogenen Daten aus. Der Einwand von Bull (Zur verfassungsrechtlichen Verankerung des Datenschutzes, in ÖVD 1979, Heft 2, Seite 3,5), daß danach die nordrhein-westfälische Verwaltung zur Durchsetzung privater Interessen keine personenbezogenen Daten mehr verarbeiten darf, wenn sie nicht dem Begriff des überwiegenden Allgemeininteresses Zwang antun will, überzeugt mich nicht. Die Durchsetzung von Forderungen Privater dient der Erhaltung oder Wiederherstellung des Rechtsfriedens, die im überwiegenden Interesse

der Allgemeinheit liegt. Es wäre für die Allgemeinheit unerträglich, wenn die Rechtsordnung zwar Rechtsansprüche schafft oder anerkennt, aber nicht die zu ihrer Durchsetzung erforderlichen Mittel zur Verfügung stellt. Die in § 36 Abs. 2 und in der 2. Alternative von § 13 Abs. 1 Satz 1 DSG NW zugelassenen Eingriffe in das Grundrecht auf Datenschutz sind deshalb bei verfassungskonformer Auslegung mit Artikel 4 Abs. 2 der Landesverfassung vereinbar.

C. Datenschutz in den Bereichen der Verwaltung

1. Meldewesen

a) Datenübermittlung an nicht-öffentliche Stellen

Im Bereich des Meldewesens war bei einigen Behörden eine gewisse Unsicherheit in der Handhabung der neuen Datenschutzbestimmungen festzustellen. Das führte manchmal dazu, daß Meldebehörden unter Berufung auf das Datenschutzgesetz generell keine Auskünfte an private Stellen gaben. Andererseits mußten sowohl öffentliche Stellen als auch Bürger und private Institutionen von mir darüber aufgeklärt werden, daß der „reibungslose" Datenfluß früherer Jahre („das war schon immer so") nach dem Inkrafttreten des Datenschutzgesetzes nicht mehr zulässig ist.

Rechtsgrundlage für die Datenübermittlung durch Meldebehörden an nicht-öffentliche Stellen sind die §§ 36 Abs. 2 und 13 Abs. 1 Satz 1 DSG NW. Nach § 36 Abs. 2 dürfen Meldebehörden Namen, akademische Grade und Anschriften eines oder mehrerer vom Empfänger bezeichneter Betroffener an Personen oder andere nicht-öffentliche Stellen übermitteln (Satz 1); Namen, akademische Grade und Anschriften einer Vielzahl Betroffener dürfen nur übermittelt werden, wenn dies im öffentlichen Interesse liegt (Satz 2). § 13 Abs. 1 Satz 1 DSG NW läßt die Übermittlung anderer Daten zu, wenn sie entweder zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgabe erforderlich ist (1. Alternative) oder soweit der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden (2. Alternative).

Zwar vertritt das Oberverwaltungsgericht Münster in seinem Beschluß vom 4. April 1979 (NJW 1979, S. 2221) die Auffassung, daß neben § 36 Abs. 2 DSG NW für Auskünfte aus dem Melderegister an Stellen außerhalb des öffentlichen Bereichs § 13 Abs. 1 Satz 1 DSG NW nicht anzuwenden sei. Dieser Auffassung kann jedoch, wie Hunsche (in Ruckriegel/v. d. Groeben/Hunsche, Datenschutz und Datenverarbeitung in Nordrhein-Westfalen, § 36 Anm. 4) überzeugend ausführt, nicht gefolgt werden.

§ 13 Abs. 1 Satz 1 DSG NW wird nur insoweit durch § 36 Abs. 2 Satz 1 DSG NW verdrängt, als der Anwendungsbereich dieser Spezialvorschrift reicht. Sie stellt die Meldebehörden von der in § 13 Abs. 1 Satz 1 DSG NW geforderten Prüfung des berechtigten Interesses des Empfängers und schutzwürdiger Belange des Betroffenen sowie von einer Abwägung der Interessen der Beteiligten frei, soweit sich die Übermittlung auf Namen, akademische Grade und Anschriften beschränkt.

Ein Verbot, andere Daten zu übermitteln, folgt aus § 36 Abs. 2 Satz 1 DSG NW nicht. Es ist kein Grund erkennbar, den Meldebehörden die Übermittlung von Daten zu untersagen, die andere Behörden unter den Voraussetzungen des § 13 Abs. 1 Satz 1 DSG NW übermitteln dürfen. Auch aus der Entstehungsgeschichte der Vorschrift läßt sich ein solches Verbot nicht herleiten. Der Gesetzgeber wollte die Übermittlung bestimmter Daten erleichtern, nicht aber die Übermittlung aller anderen Daten ausschließen.

Entgegen der Auffassung des Oberverwaltungsgerichts Münster halte ich deshalb Auskünfte aus dem Melderegister über andere Daten als Namen, akademische Grade und Anschriften für zulässig, wenn die Voraussetzungen des § 13 Abs. 1 Satz 1 DSG NW vorliegen und der Übermittlung nicht andere Rechtsvorschriften entgegenstehen. Allerdings können über die Zulässigkeit von Auskünften wie auch über alle anderen Datenschutzfragen nur die zuständigen Gerichte im Einzelfall verbindlich entscheiden. Es ist zu hoffen,

daß das Oberverwaltungsgericht Münster an der in seiner Entscheidung vertretenen Auffassung zu § 36 Abs. 2 und § 13 Abs. 1 Satz 1 DSG NW nicht festhält.

Mehrere Beratungsersuchen und Eingaben betrafen die Übermittlung von **Jubiläumsdaten.** Bisher war es üblich, Ehe- und Altersjubiläen, aber auch Geburts- und Sterbedaten an Stellen außerhalb des öffentlichen Bereichs weiterzugeben, so etwa an Bundestags- und Landtagsabgeordnete und an die Presse.

Da § 36 Abs. 2 Satz 1 DSG NW eine Übermittlung nur zuläßt, wenn sie sich auf Namen, akademische Grade und Anschriften beschränkt, kommt diese Vorschrift als Rechtsgrundlage für die Übermittlung von Geburts-, Heirats- und Sterbedaten nicht in Betracht. Auch die 1. Alternative des § 13 Abs. 1 Satz 1 DSG NW scheidet als Rechtsgrundlage aus. Es kann dahingestellt bleiben, ob es zu den in der Zuständigkeit einer Gemeinde liegenden Aufgabe gehört, die Öffentlichkeit über Jubiläumsdaten ihrer Bürger zu unterrichten oder die Unterrichtung durch die Presse zu ermöglichen. Die Unterrichtung von Abgeordneten gehört sicher nicht zu ihren Aufgaben.

Auf jeden Fall wäre die Erfüllung einer solchen Aufgabe ohne Einwilligung des Betroffenen nicht rechtmäßig, weil damit in sein Grundrecht auf Schutz seiner personenbezogenen Daten (Artikel 4 Abs. 2 Satz 1 LV) eingegriffen würde, ohne daß ein überwiegendes Interesse der Allgemeinheit hierfür vorläge (Artikel 4 Abs. 2 Satz 2 LV).

Das in der 2. Alternative des § 13 Abs. 1 Satz 1 DSG NW geforderte berechtigte Interesse dürfte zwar sowohl bei Abgeordneten als auch bei der Presse in der Regel vorliegen. Durch die Weitergabe dieser Daten können jedoch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Zwar wünschen viele Bürger, daß von ihren Jubiläen Notiz genommen wird; andere hingegen empfinden dies als Belästigung. Bei einer Abwägung der Interessen überwiegt hier das Interesse des Betroffenen oder (bei Angaben über Geburten und Sterbefälle) das Interesse der Angehörigen an dem Schutz der Privatsphäre gegenüber dem Interesse des Abgeordneten an der Übermittlung von Glückwünschen oder dem Informationsinteresse der Öffentlichkeit.

Da eine Verletzung schutzwürdiger Belange jedenfalls nicht auszuschließen ist, bedarf die Übermittlung solcher Daten an die Presse der Einwilligung des Betroffenen (§ 3 Satz 1 Nr. 2 DSG NW). Bei der Beantwortung einer Mündlichen Anfrage in der Sitzung des Landtags am 12. März 1980 hat der Innenminister den gleichen Standpunkt vertreten. Die Möglichkeit, einer Weitergabe oder Veröffentlichung widersprechen zu können, würde zum Schutz des Betroffenen vor Eingriffen in seine Privatsphäre nicht ausreichen.

Ob eine Gemeinde die erforderliche Einwilligung einholen oder auf die Mitteilung solcher Daten an Abgeordnete oder an die Presse verzichten will, steht in ihrem Ermessen. Eine rechtliche Verpflichtung, sich um die Einwilligung zu bemühen, besteht nicht. Die Gemeinde hat in eigener Verantwortung zu entscheiden, ob sie diese Aufgabe im Interesse der an einer Gratulation interessierten Bürger unter Inkaufnahme des für die Einholung der Einwilligung erforderlichen Verwaltungsaufwandes übernehmen will.

Die Einwilligung ist grundsätzlich schriftlich zu erklären, nachdem der Betroffene über ihre Bedeutung aufgeklärt worden ist (§ 3 Satz 2 und 3 DSG NW). Dazu muß dem Betroffenen vor seiner Erklärung mitgeteilt werden, welche Daten an welche Stellen übermittelt werden sollen.

Ebenso ist bei dem Wunsch von Vereinen zu verfahren, zur **Pflege des Brauchtums** Namen und Anschriften unverheirateter Mädchen bestimmter Altersgruppen zu erhalten. § 36 Abs. 2 Satz 2 DSG NW, der die Übermittlung personenbezogener Daten einer Vielzahl Betroffener zuläßt, wenn dies im öffentlichen Interesse liegt, findet hier keine Anwendung. Er erlaubt nur die Übermittlung von Namen, akademischen Graden und Anschriften, nicht aber von Angaben über den Familienstand oder über die Zugehörigkeit zu einer bestimmten Altersgruppe (§ 36 Abs. 2 Satz 1 DSG NW).

Zwar hält Hunsche (in Ruckriegel/v. d. Groeben/Hunsche, Datenschutz und Datenverarbeitung in Nordrhein-Westfalen, § 36 Anm. 5) die Übermittlung von Angaben über die Zu-

gehörigkeit zu einer Gruppe in Anwendung des Selektionsprinzips für zulässig. Er übersieht dabei aber, daß das Gebot der Selektion dazu bestimmt ist, den Umfang der zu übermittelnden Daten zu beschränken, nicht ihn zu erweitern. Der Umstand, daß durch die Beschränkung der Übermittlung auf Angehörige einer Gruppe der Kreis der Betroffenen begrenzt wird, rechtfertigt nicht, in das Recht der Betroffenen auf Schutz ihrer personenbezogenen Daten über die in § 36 Abs. 2 Satz 1 DSG NW ausdrücklich zugelassene Übermittlung von Namen, akademischen Graden und Anschriften hinaus einzugreifen.

Eine Übermittlung von Angaben über den Familienstand oder über die Zugehörigkeit zu einer bestimmten Altersgruppe wäre nur unter den Voraussetzungen der 2. Alternative des § 13 Abs. 1 Satz 1 DSG NW zulässig. Ein berechtigtes Interesse der Vereine, die das Brauchtum pflegen, an der Kenntnis der genannten Daten dürfte zwar vorliegen. Durch die Weitergabe dieser Daten an einen solchen Verein können jedoch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Zwar werden es viele der unverheirateten Mädchen begrüßen, wenn ihre Namen ausgerufen oder sie auf Maifesten „versteigert" werden; andere hingegen empfinden dies als Belästigung. Bei einer Abwägung der Interessen überwiegt in diesen Fällen das Interesse des betroffenen Mädchens an dem Schutz seiner Privatsphäre gegenüber dem Interesse des Vereins an der Durchführung des Brauches.

Eine Übermittlung der gewünschten Daten ist somit nur mit Einwilligung des Betroffenen zulässig, da die Beeinträchtigung schutzwürdiger Belange auch hier nicht auszuschließen ist. Die Gemeinde hat in eigener Verantwortung zu entscheiden, ob sie die Pflege des Brauchtums auch dadurch fördern will, daß sie den für die Einholung der Einwilligung erforderlichen Verwaltungsaufwand übernimmt.

Entsprechendes gilt für die Übermittlung personenbezogener Daten an **wirtschaftliche Unternehmen.** Zwar dürfte ein berechtigtes Interesse etwa der in einer Gemeinde ansässigen Kreditinstitute an der Kenntnis der Namen und Anschriften der zugezogenen und neugeborenen Einwohner vorliegen. Durch die Weitergabe dieser Daten an solche Unternehmen können jedoch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Gerade die gezielte Werbung empfinden viele Bürger als Belästigung. Bei einer Abwägung der Interessen überwiegt das Interesse des Betroffenen an dem Schutz seiner Privatsphäre gegenüber dem rein kommerziellen Interesse der Unternehmen, so daß eine Übermittlung auch in diesen Fällen der Einwilligung des Betroffenen bedarf.

Keine Bedenken habe ich gegen die Übermittlung von Namen, akademischen Graden und Anschriften einer Vielzahl Betroffener zum Zweck der Herausgabe von **Adreßbüchern,** da dies im öffentlichen Interesse liegt (§ 36 Abs. 2 DSG NW). Wenn sich die Übermittlung auf diese Daten beschränkt, ist eine Einwilligung des Betroffenen nicht erforderlich.

Eine Übermittlung weiterer Daten, etwa des Berufes oder der Hauseigentümerschaft, an Adreßbuchverlage wäre dagegen nur unter den Voraussetzungen der 2. Alternative des § 13 Abs. 1 Satz 1 DSG NW zulässig. Ein berechtigtes Interesse der Adreßbuchverlage an der Kenntnis der gewünschten Daten dürfte zwar vorliegen. Durch die Weitergabe solcher Daten können jedoch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Bei der Abwägung der Interessen überwiegt auch hier das Interesse des Betroffenen an dem Schutz seiner Privatsphäre gegenüber dem kommerziellen Interesse des Verlages. Da die Verletzung schutzwürdiger Belange des Betroffenen jedenfalls nicht auszuschließen ist, bedarf die Übermittlung solcher Daten durch die Meldebehörde an den Verlag der Einwilligung des Betroffenen.

An mich ist auch die Frage herangetragen worden, ob (über die Regelungen in den Wahlordnungen hinaus) Anschriften von Bürgern an die **Parteien** übermittelt werden dürfen.

Die Parteien wirken nach Artikel 21 Abs. 1 GG bei der politischen Willensbildung des Volkes mit. Um diese Aufgabe wirksam erfüllen zu können, müssen sie auch die Möglichkeit haben, sich an namentlich bezeichnete Bürger zu wenden. Deshalb liegt nach meiner

Auffassung die Übermittlung von Namen, akademischen Graden und Anschriften an die Parteien im öffentlichen Interesse (§ 36 Abs. 2 Satz 2 DSG NW).

Soweit die Parteien darüber hinaus bestimmte Gruppen von Bürgern (Jungwähler, Senioren oder Neubürger) gezielt ansprechen wollen, bin ich der Ansicht, daß bei einer Abwägung der Interessen das Interesse des Bürgers an dem Schutz vor einer Mitteilung seiner Zugehörigkeit zu der Gruppe gegenüber dem Interesse der Parteien an einer Verbesserung der Kommunikation mit dem Bürger, das zugleich ein öffentliches ist, zurücktreten muß (§ 13 Abs. 1 Satz 1 DSG NW; vgl. Dammann in Simitis/Dammann/Mallmann/Reh, BDSG, § 11 Rdnr. 22).

Unzulässig wäre die Übermittlung nur, wenn sich aus den Umständen ergibt, daß die Daten für einen anderen Zweck als für die Mitwirkung bei der politischen Willensbildung des Volkes verwendet werden sollen.

Etwaige Befürchtungen, daß aus einer mangelnden Reaktion eines Bürgers auf eine persönliche Zuschrift Schlüsse über sein politisches Interesse oder seine politische Meinung gezogen werden könnten, halte ich für unbegründet. Derartige Schlußfolgerungen müßten sonst auch aus der Nichtteilnahme an Veranstaltungen gezogen werden, zu denen öffentlich eingeladen worden ist. Gegenüber totalitär regierten Staaten zeichnet sich unsere freiheitliche Demokratie durch einen freien und offenen Prozeß der Meinungs-und Willensbildung des Volkes aus. Es steht jedem Bürger frei, ob und inwieweit er an diesem teilnehmen will, ohne daß ihm aus einer Nichtteilnahme Nachteile erwachsen würden.

b) Datenübermittlung an die Polizei

Der Vorsitzende einer Ratsfraktion der Stadt Bochum hat mir mitgeteilt, daß nach einer von der Verwaltung im Hauptausschuß des Rates gegebenen Auskunft die Stadt sämtliche Bestandsdaten aus dem Melderegister monatlich auf Mikrofiches an die Polizei weitergebe.

Meine Ermittlungen haben ergeben, daß folgende Daten auf Mikrofiches an die Polizei übermittelt wurden:

- Familienname
- frühere Namen
- Vornamen
- akademischer Grad
- Tag und Ort der Geburt
- Geschlecht
- Familienstand
- Beginn des jeweiligen Familienstandes (verheiratet, verwitwet, geschieden)
- Religion
- gegenwärtige Anschriften (Haupt- und Nebenwohnung)
- vorhergehende Anschrift
- Wegzug
- Ausstellungsbehörde, Ausstellungsdatum, Gültigkeitsdauer, Seriennummer des Personalausweises/Passes
- Staatsangehörigkeit(en)
- Beruf
- Sterbedatum
- Übermittlungssperren

Ich habe mich gegen diese Handhabung gewandt. Zwar dürfen nach § 36 Abs. 1 DSG NW in Verbindung mit § 1 der Verordnung vom 21. Dezember 1979 Meldebehörden bis 31. Dezember 1980 personenbezogene Daten an andere Behörden durch Weitergabe der Meldescheine übermitteln, soweit dies auch schon vor Inkrafttreten des Datenschutzgesetzes Nordrhein-Westfalen geschah. Jede weitergehende Übermittlung solcher Daten, insbesondere eine Übermittlung auf andere Weise als durch Weitergabe der Meldescheine oder eine Übermittlung anderer als der in den Meldescheinen enthaltenen Daten, ist aber bereits jetzt nur unter den Voraussetzungen des § 11 Abs. 1 Satz 1 DSG NW zulässig.

Nach der hier allein in Betracht kommenden 2. Alternative des § 11 Abs. 1 Satz 1 DSG NW dürfen personenbezogene Daten anderen Behörden nur übermittelt werden, wenn die Übermittlung zur rechtmäßigen Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist. Bei der Prüfung der Erforderlichkeit der Übermittlung ist der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit zu beachten. Danach muß der Eingriff, hier also die Übermittlung personenbezogener Daten von der Meldebehörde an die Polizei, nicht nur notwendig sein, um den angestrebten Zweck der Verwaltung zu erreichen; die mit dem Eingriff verbundene Belastung muß auch in einem angemessenen Verhältnis zu dem mit dem Eingriff verbundenen Vorteil stehen.

An die Erforderlichkeit sind danach sowohl hinsichtlich des Umfangs der zu übermittelnden Daten als auch in zeitlicher Hinsicht strenge Anforderungen zu stellen. Eine Übermittlung „auf Vorrat" für den Fall, daß die Daten später einmal zur Erfüllung einer Aufgabe gebraucht werden, ist — von hier nicht in Betracht kommenden Sonderfällen abgesehen — nicht zulässig. Vielmehr muß in jedem einzelnen Fall geprüft werden, ob die angeforderten Daten (diese Daten, bezogen auf diese Person, zu diesem Zeitpunkt) zur Erfüllung der Aufgaben des Empfängers gebraucht werden (vgl. Ruckriegel in Ruckriegel/v. d. Groeben/Hunsche, Datenschutz und Datenverarbeitung in Nordrhein-Westfalen, § 11 Anm. 3 und § 10 Anm. 5).

Bei einigen der von der Meldebehörde an die Polizei übermittelten Daten (wie etwa bei der Religionszugehörigkeit) ist nicht erkennbar, inwiefern sie überhaupt für die Erfüllung der Aufgaben der Polizei von Bedeutung sein können. Auch fehlt es bei dem in Bochum praktizierten Verfahren an der Prüfung der Erforderlichkeit im Einzelfall. Auf jeden Fall steht der mit der regelmäßigen Übermittlung der genannten Bestandsdaten an die Polizei verbundene Eingriff in die Rechtssphäre aller Bürger in keinem angemessenen Verhältnis zu dem Nutzen dieser Maßnahme für die Arbeit der Polizei.

Nach meiner Auffassung fehlt für eine derart umfassende Übermittlung personenbezogener Daten eine gesetzliche Grundlage. Ich habe deshalb dem Oberstadtdirektor und dem Polizeipräsidenten meine Rechtsauffassung mitgeteilt und auf die daraus sich ergebenden Rechtsfolgen hingewiesen.

Inzwischen hat der Innenminister durch Erlaß Weisungen für den Datenaustausch zwischen dem Amt für Einwohnerwesen und der Polizei in Bochum erteilt. Danach können bis zur Verwirklichung neuer technischer Möglichkeiten die bereits bisher übermittelten personenbezogenen Daten mit Ausnahme des akademischen Grades, des Beginns des jeweiligen Familienstandes, der Religion, des Wegzugs und des Sterbedatums auf Mikrofiches übermittelt werden.

Zusätzlich zu den bisher schon weitergegebenen Daten hat der Innenminister noch die Übermittlung des Familiennamens, des Vornamens und der Anschrift des gesetzlichen Vertreters sowie des Familiennamens, des Vornamens und der Anschrift des Ehegatten zugelassen.

Wenngleich diese Regelung eine gewisse Verbesserung gegenüber der bisherigen Handhabung darstellt, da einige nicht erforderliche personenbezogene Daten nicht mehr übermittelt werden, so halte ich auch die nunmehr praktizierte Handhabung für rechtlich bedenklich. Auch für die regelmäßige Übermittlung des zwar leicht reduzierten, aber

immer noch umfangreichen Datenbestandes über jeden Einwohner ohne Prüfung der Erforderlichkeit im Einzelfall vermag ich eine Rechtsgrundlage nicht zu erkennen. § 11 Abs. 1 Satz 1 DSG NW kommt hierfür jedenfalls nicht in Betracht.

Ich werde mich daher mit den mir zur Verfügung stehenden Mitteln dafür einsetzen, daß durch eine landeseinheitliche Regelung der Zugang der Polizei zu diesen Daten auf ein nach § 11 Abs. 1 Satz 1 DSG NW zulässiges Maß begrenzt wird, sofern nicht eine Rechtsgrundlage für die bisherige Handhabung geschaffen wird.

c) Datenübermittlung an die Kirchen

Die öffentlich-rechtlichen Religionsgesellschaften unterliegen wegen ihrer verfassungsrechtlich garantierten Autonomie (Artikel 140 GG in Verbindung mit Artikel 137 Abs. 3 WRV) nicht den staatlichen Datenschutzvorschriften. Die Übermittlung personenbezogener Daten aus dem öffentlichen Bereich an Stellen der öffentlich-rechtlichen Religionsgesellschaften ist aber nach § 11 Abs. 2 DSG NW in entsprechender Anwendung der Vorschriften über die Datenübermittlung an Behörden und sonstige öffentliche Stellen nur zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist und wenn außerdem sichergestellt ist, daß bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen werden.

Ihre Aufgaben und Ziele legen die Religionsgesellschaften im Rahmen ihrer Autonomie selbst fest. Es kann unterstellt werden, daß die Übermittlung der Grunddaten der Kirchenmitglieder (Namen, akademische Grade, Anschrift, Geburtsdatum, Geburtsort, Beruf, Familienstand, Zahl der Kinder) und deren Änderungen zur rechtmäßigen Erfüllung der Aufgaben der öffentlich-rechtlichen Religionsgesellschaften erforderlich ist. Bei weitergehenden Übermittlungswünschen müßten die Kirchen die Erforderlichkeit schlüssig darlegen.

Unzulässig ist aber die Übermittlung personenbezogener Daten von Familienangehörigen eines Kirchenmitgliedes, die nicht selbst Mitglieder der jeweiligen Kirche sind. Zwar haben die Kirchen ein Interesse daran, für Zwecke der Seelsorge auch Daten familienangehöriger Nichtmitglieder zu erhalten. Eine solche Übermittlung würde jedoch in den Kernbereich des Grundrechts des Nichtmitglieds auf Schutz seiner personenbezogenen Daten (Artikel 4 Abs. 2 der Landesverfassung) eingreifen und ist deshalb nicht gerechtfertigt. Ebenso würde die Übermittlung von Daten eines Nichtmitglieds dessen Recht verletzen, seine religiöse Überzeugung zu verschweigen (Artikel 140 GG in Verbindung mit Artikel 136 Abs. 3 Satz 1 WRV).

Danach dürfen den Kirchen hinsichtlich der zur Familie gehörenden Nichtmitglieder auch nicht bestimmte „Rumpfdaten" (Name und Geburtsdatum) zur Verfügung gestellt werden. Angaben über familienangehörige Nichtmitglieder dürfen die Kirchen nur im Rahmen der ihnen zu übermittelnden Grunddaten des familienangehörigen Kirchenmitglieds (Familienstand, Zahl der Kinder) erhalten. Ihnen wird damit die Möglichkeit eröffnet, aus diesen Angaben den Familienverband in seinen Umrissen zu erkennen und daraus zu entnehmen, daß der Familie auch Nichtmitglieder der jeweiligen Kirche angehören. Falls erforderlich, können die Kirchen Daten dieser Nichtmitglieder bei den Betroffenen auf der Grundlage der Freiwilligkeit selbst erheben.

Die Datenschutzmaßnahmen, die nach § 11 Abs. 2 DSG NW von den Religionsgemeinschaften getroffen werden müssen, können in rechtlichen Regelungen, personellen Maßnahmen und organisatorisch-technischen Vorkehrungen bestehen. Für die Frage, ob die Maßnahmen ausreichen, ist die Summe aller Vorkehrungen entscheidend. Zwar müssen die Maßnahmen nicht in allen Einzelheiten denen der öffentlichen Verwaltung entsprechen; ein vergleichbarer Standard ist aber zu fordern (Ruckriegel in Ruckriegel/v. d. Groeben/Hunsche, Datenschutz und Datenverarbeitung in Nordrhein-Westfalen, § 11 Anm. 6).

Die Kirchen haben derartige Datenschutzmaßnahmen getroffen. Als Beispiele sei auf das Kirchengesetz über den Datenschutz der Evangelischen Kirche im Rheinland und die

Anordnung über den kirchlichen Datenschutz (KDO) für das Erzbistum Köln hingewiesen. Beauftragte für den Datenschutz sind bestellt, organisatorisch-technische Maßnahmen getroffen. Mit einer Ausnahme sind mir Verstöße nicht bekannt geworden.

Der Verlust eines — später wieder aufgefundenen — Magnetbandes mit Einwohnerdaten durch Bedienstete eines kirchlichen Rechenzentrums, das diese Daten im Auftrag einer kirchlichen Körperschaft verarbeitet, gab mir Veranlassung, auf Vorkehrungen zur Vermeidung ähnlicher Vorkommnisse hinzuwirken. Wenn eine kirchliche Stelle Daten durch eine andere Stelle verarbeiten läßt, muß sie mit dem Auftragnehmer eine Regelung treffen, die der nach § 7 Abs. 1 Satz 2 DSG NW mit Auftragnehmern der öffentlichen Verwaltung zu treffenden vergleichbar ist. Dies bedeutet, daß der Auftragnehmer sich nicht nur dem Datenschutzgesetz Nordrhein-Westfalen gleichwertigen Datenschutzvorschriften, sondern auch der Kontrolle des für den Auftraggeber zuständigen Datenschutzbeauftragten unterwerfen muß.

Von dem Vorliegen ausreichender Datenschutzmaßnahmen hat sich die übermittelnde Stelle, hier also die Meldebehörde, vor der Übermittlung zu überzeugen; dies gilt auch für die besonderen Vorkehrungen, die bei der Datenverarbeitung durch andere Stellen im Auftrag des Empfängers erforderlich sind. Eine bloße Zusicherung des Empfängers, daß die Forderungen des Datenschutzes beachtet werden, genügt nicht.

d) Datenübermittlung zwischen Meldebehörden

Nach den bestehenden Melderechtsvorschriften ist beim Zuzug von Personen von der Zuzugsgemeinde eine Rückmeldung an die Fortzugsgemeinde und die Gemeinde eines weiteren Wohnsitzes zu übersenden. In dieser Rückmeldung sind personenbezogene Daten enthalten (Name, Vorname, Geburtsdatum, Staatsangehörigkeit, Familienstand und Daten über die neue und die bisherige Wohnung).

Im Kreis der Datenschutzbeauftragten ist die Frage aufgeworfen worden, ob die Rückmeldung wegen des Dateninhalts in verschlossenem Briefumschlag erfolgen muß. Ich neige dazu, diese Frage zu bejahen, da mir das Postgeheimnis allein kein ausreichender Schutz für die Belange der Betroffenen zu sein scheint. Wie ich festgestellt habe, erfolgt in Nordrhein-Westfalen die Rückmeldung im Regelfall noch durch Postkarte. Im Gegensatz dazu bestehen in Berlin, Niedersachsen, Rheinland-Pfalz und im Saarland bereits Regelungen, nach denen nur ein Versand der Rückmeldungen in verschlossenem Umschlag zulässig ist.

Ich habe dem Innenminister meine Auffassung mitgeteilt und ihn um Stellungnahme zur Frage der Versendungsform der Rückmeldung gebeten. Dieser hat mir inzwischen mitgeteilt, daß er eine Regelung zur Versendung der Rückmeldungen in verschlossenem Umschlag anstrebt. Eine derartige Regelung wird jedoch nur dann den gewünschten Erfolg haben, wenn in allen Ländern entsprechend verfahren wird.

e) Zustellung der Lohnsteuerkarten

Datenschutzrechtliche Probleme ergaben sich auch bei der Zustellung von Lohnsteuerkarten durch die Gemeinden. Durch Eingaben von Bürgern wurde ich auf die in einigen Städten übliche Praxis aufmerksam gemacht, die Lohnsteuerkarten ohne Briefumschlag zuzustellen, so daß neben dem Namen und der Anschrift auch die Steuermerkmale und die Geburtsdaten den Postbediensteten oder den mit der Zustellung beauftragten Bediensteten der Gemeinde zugänglich werden konnten. In mehreren Fällen wurde sogar die Lohnsteuerkarte offenliegend im Hausflur vorgefunden.

Ich habe mich dafür eingesetzt, daß in Zukunft bei der Zustellung der Lohnsteuerkarten eine Form gewählt wird, die gewährleistet, daß die personenbezogenen Daten weder von dem Zusteller noch von anderen Personen eingesehen werden können (etwa durch Zustellung in einem verschlossenen Umschlag).

f) Änderung des Personalausweisgesetzes

Das vom Bundesgesetzgeber verabschiedete Gesetz zur Änderung des Gesetzes über Personalausweise sieht einen neuen fälschungssicheren und maschinenlesbaren Personalausweis vor. Selbstverständlich sind Maßnahmen der Kontrolle zu Zwecken der Gefahrenabwehr und Strafverfolgung im Rahmen des Polizei- und Strafprozeßrechts zulässig. Die Intensivierung dieser Art von Kontrolle ist, solange der Verhältnismäßigkeitsgrundsatz beachtet wird, rechtlich nicht zu beanstanden.

Die Einführung eines maschinenlesbaren Personalausweises hat jedoch erhebliche Konsequenzen für den Datenschutz der Ausweisinhaber. Die vorgesehene Ausweiskarte ist mehr als ein fälschungssicherer Ersatz des bisherigen Ausweisbuches. Sie kann auch zum Instrument für eine weitaus effektivere Kontrolle über den Bürger werden (hierzu 2.1.3 des Zweiten Tätigkeitsberichts des Bundesbeauftragten für den Datenschutz).

Es ist nicht zu verkennen, daß es gerade auch dem Rechtsschutz des Bürgers dienen kann, wenn durch Verwendung eindeutiger Identifikationsmerkmale eine Verwechslung ausgeschlossen wird, etwa bei Fahndungsmaßnahmen der Polizei. Doch ist es keineswegs immer notwendig, daß die eindeutige Identifizierung bereits maschinell erfolgt. Die Gefahr eines maschinenlesbaren Ausweises besteht vor allem darin, daß mit seiner Hilfe vorhandene, zu unterschiedlichen Zwecken angelegte Datensammlungen mit geringem Aufwand maschinell miteinander verknüpft oder neue Datenbestände maschinell aufgebaut werden können. Der damit verbundenen Gefahr für das Recht des Bürgers auf Schutz seiner personenbezogenen Daten kann nur dadurch begegnet werden, daß die Verwendungszwecke des Ausweises beschränkt werden. Dies ist in der Novelle in mehrfacher Weise geschehen.

Hervorzuheben ist, daß die Angaben zur Person des Ausweisinhabers nur bei den örtlich zuständigen Personalausweisbehörden gespeichert werden dürfen. Diese dürfen auch die maschinelle Lesbarkeit nutzen, um auf ihre Dateien zurückzugreifen.

Auf andere Dateien darf mittels der Maschinenlesbarkeit des Ausweises grundsätzlich nicht zugegriffen werden. Ausgenommen von diesem Verbot sind lediglich Dateien, die für Zwecke der Grenzkontrolle und der Fahndung aus Gründen der Strafverfolgung oder der Gefahrenabwehr durch die hierfür zuständigen Behörden betrieben werden.

Mit diesen Verwendungsbeschränkungen wird sowohl den Belangen des Datenschutzes als auch dem Sicherheitsinteresse Rechnung getragen. Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb gegen die neue Regelung keine Einwendungen erhoben. Sie haben jedoch betont, daß ein maschinenlesbarer Personalausweis nur in Verbindung mit einem datenschutzgerechten Melderecht und bereichsspezifischen Datenschutzregelungen für den Sicherheitsbereich hinnehmbar ist.

Der Deutsche Bundestag hat diese Forderung aufgegriffen; er hat bei der Verabschiedung der Novelle in einer Entschließung einstimmig die Auffassung vertreten, daß „weitere Maßnahmen erforderlich sind, um einen ausreichenden Schutz der Persönlichkeitsrechte der Bürger gegen mißbräuchliche Verwendung ihrer persönlichen Daten zu gewährleisten". Er hat deshalb die Bundesregierung ersucht,

„1. den Entwurf eines datenschutzgerechten Melderechtsrahmengesetzes einzubringen und

2. die Arbeiten zur Entwicklung bereichsspezifischer Datenschutzregelungen für die Sicherheitsbehörden nachdrücklich fortzusetzen."

g) Melderechtsrahmengesetz

Der von der Bundesregierung vorgelegte Entwurf eines Melderechtsrahmengesetzes trägt den Forderungen des Datenschutzes weitgehend Rechnung. Hervorzuheben ist, daß der Katalog der Daten, die die Meldebehörden erheben dürfen, gegenüber den früheren Entwürfen wesentlich reduziert werden soll. So soll z. B. auf die Angabe des Berufs, die

ohnehin bei vielen Bürgern wenig aussagekräftig ist, verzichtet werden. Ferner soll die Datenübermittlung an andere Behörden auf bestimmte Grunddaten beschränkt werden.

Ein besonderes Problem bestand darin, die Belange der Sicherheitsbehörden bei ihren Datenanforderungen gegenüber den Meldebehörden in einer Weise zu berücksichtigen, die den Betroffenen nicht übermäßig belastet. Der Entwurf sieht dazu vor, daß den Sicherheitsbehörden nicht nur bestimmte Grunddaten, sondern alle Meldedaten zur Verfügung stehen, die nicht ausdrücklich zweckgebunden sind. Er sieht ferner vor, daß die Sicherheitsbehörden im Gegensatz zu allen anderen Behörden ihren Datenbedarf nicht im Einzelfall gegenüber der Meldebehörde begründen müssen, daß sie aber selbst eine Niederschrift erstellen müssen, in der die betroffenen Personen und der Grund der Datenübermittlung aufgeführt sind. Damit soll eine nachträgliche Kontrolle der Rechtmäßigkeit der Übermittlung ermöglicht werden.

Diese Lösung erscheint unter den gegebenen Umständen und bei Abwägung der beiderseitigen Interessen vertretbar. Mit geeigneten Formularen oder (bei Automatisierung des Meldewesens) mit einer automatisierten Protokollierung kann auch der Verwaltungsaufwand niedriger gehalten werden, als wenn der Datenbedarf gegenüber der Meldebehörde in jedem einzelnen Fall begründet werden müßte.

Leider hat der Bundesrat in seiner Stellungnahme im ersten Durchgang Änderungen vorgeschlagen, die den Datenschutz in entscheidenden Punkten in Frage stellen. Der Datenkatalog soll wieder erweitert werden. Alle Behörden sollen wieder zu allen nicht ausdrücklich zweckgebundenen Meldedaten Zugang haben, und bei den Sicherheitsbehörden soll die Protokollierungspflicht entfallen.

Die Datenschutzbeauftragten des Bundes und der Länder betrachten diese Änderungswünsche, die im Bundesrat von einer großen Mehrheit aller Länder beschlossen wurden, mit Sorge. Die Forderung des Bundestags nach einem datenschutzgerechten Melderechtsrahmengesetz kann nach ihrer Auffassung dann nicht mehr erfüllt werden, wenn der Datenkatalog über den Regierungsentwurf hinaus erweitert wird und es an klaren eingrenzenden Regelungen über die Datenübermittlung insbesondere an die Sicherheitsbehörden fehlt. Die Entscheidung liegt jetzt beim Deutschen Bundestag.

2. Wahlen

Eingaben, in denen die Übermittlung des **Geburtsdatums der Wahlberechtigten** an Dritte durch Auslegung des Wählerverzeichnisses oder Weitergabe des Wählerverzeichnisses an Parteien und Wählergruppen gerügt wurde, habe ich zum Anlaß genommen, mich an den Innenminister zu wenden.

Nach § 13 Abs. 1 der Landeswahlordnung (LWahlO) und § 9 Abs. 1 der Kommunalwahlordnung (KWahlO) ist in das Wählerverzeichnis außer dem Familiennamen, dem Vornamen und der Wohnung des Wahlberechtigten auch dessen Geburtsdatum aufzunehmen. Nach § 17 Abs. 1 LWahlO und § 13 Abs. 1 KWahlO ist das Wählerverzeichnis vor der Wahl zur Einsichtnahme öffentlich auszulegen. Damit wird jedermann die Möglichkeit eröffnet, sich über den Geburtstag seiner Nachbarn und anderer Mitbürger zu informieren. Gegen einen solchen freien Zugang zu personenbezogenen Daten bestehen unter dem Gesichtspunkt des Datenschutzes Bedenken.

Da § 17 Abs. 1 LWahlO und § 13 Abs. 1 KWahlO nach § 37 DSG NW den Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen vorgehen, finden die Vorschriften dieses Gesetzes über die Übermittlung von Daten an Stellen außerhalb des öffentlichen Bereichs (§ 13 DSG NW) keine Anwendung. Die Regelung über die Auslegung des Wählerverzeichnisses ist jedoch an der Landesverfassung, insbesondere an dem Grundrecht auf Datenschutz (Artikel 4 Abs. 2) zu messen.

Nach Artikel 4 Abs. 2 LV darf in das Grundrecht auf Schutz der personenbezogenen Daten nur im überwiegenden Interesse der Allgemeinheit eingegriffen werden. Ein Interesse der Allgemeinheit daran, daß jedermann Kenntnis von den Geburtsdaten anderer Wahlberechtigter erhalten kann, vermag ich nicht zu erkennen. Zur Identifizierung eines Wahlberechtigten reichen fast immer Familienname, Vorname und Wohnanschrift aus. In den wenigen Fällen, in denen Träger des gleichen Vornamens die gleiche Wohnanschrift haben, können bei der Einsichtnahme entstandene Zweifel an der Identität eines im Wählerverzeichnis eingetragenen Wahlberechtigten an Ort und Stelle durch Rückfrage bei der Gemeindebehörde geklärt werden. In diesen Fällen ist eine Klärung durch sofortige Rückfrage sowohl dem das Wählerverzeichnis einsehenden Bürger als auch der Gemeindebehörde zumutbar.

Selbst wenn ein Interesse der Allgemeinheit unterstellt wird, überwiegt dieses nicht gegenüber dem Interesse des Bürgers an dem Schutz vor Übermittlung seines Geburtsdatums an Dritte. Der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit läßt einen Eingriff in das Grundrecht nur zu, wenn die Belastung des Einzelnen noch in einem vernünftigen Verhältnis zu den der Allgemeinheit erwachsenden Vorteilen steht. Bei Beachtung dieses Grundsatzes rechtfertigen es die Fälle von Namensgleichheit bei gleicher Wohnanschrift — mögen es im ganzen Land auch einige Tausend sein — nicht, die Geburtsdaten von über zwölf Millionen Wahlberechtigten jedermann zugänglich zu machen.

Da somit kein überwiegendes Interesse der Allgemeinheit an der Bekanntgabe der Geburtsdaten besteht, sind § 17 Abs. 1 LWahlO und § 13 Abs. 1 KWahlO insoweit mit Artikel 4 Abs. 2 LV nicht vereinbar.

Entsprechende Bedenken bestanden gegen die Regelung in § 17 Abs. 4 LWahlO und § 13 Abs. 5 KWahlO, wonach der Gemeindedirektor unter bestimmten Voraussetzungen die Anfertigung von Auszügen oder Abschriften des Wählerverzeichnisses durch an der Wahl teilnehmende Parteien und Wählergruppen zulassen oder selbst Auszüge oder Abschriften erteilen kann.

Ich habe deshalb empfohlen, § 17 LWahlO und § 13 KWahlO dahin zu ändern, daß

- die Geburtsdaten im auszulegenden Wählerverzeichnis unkenntlich zu machen sind oder für die Auslegung ein gesondertes Wählerverzeichnis ohne Angabe der Geburtsdaten zu verwenden ist und
- bei der Anfertigung oder Erteilung von Auszügen oder Abschriften des Wählerverzeichnisses die Kenntnisnahme von den Geburtsdaten der Wahlberechtigten ausgeschlossen wird.

Ferner habe ich empfohlen, das in der Kommunalwahlordnung enthaltene Verbot der Übermittlung durch Herausgabe von maschinell lesbaren Datenträgern oder mittels Datenübertragung sowie das Verbot der Zweckentfremdung der Auszüge und Abschriften des Wählerverzeichnisses auch in die Landeswahlordnung aufzunehmen.

Der Innenminister hat in der Verordnung zur Änderung der Landeswahlordnung vom 3. November 1979 einen Teil meiner Empfehlungen berücksichtigt. Dies gilt insbesondere für die neue Regelung, nach der in den Abdrucken des Wählerverzeichnisses, die den Parteien und Wählergruppen für Zwecke der Wahl überlassen werden, die Geburtsdaten der Wahlberechtigten wegzulassen sind. Damit wird künftig ausgeschlossen, daß die Parteien Kenntnis von den Geburtsdaten der einzelnen Wahlberechtigten erhalten, die sie für die Erfüllung ihrer Aufgabe der Mitwirkung bei der politischen Willensbildung des Volkes nicht benötigen.

Ich bedaure jedoch, daß der Innenminister meine Empfehlung, im auszulegenden Wählerverzeichnis die Geburtsdaten unkenntlich zu machen oder für die Auslegung ein gesondertes Wählerverzeichnis ohne Angabe der Geburtsdaten zu verwenden, nicht gefolgt ist. Der neue § 17 Abs. 4 LWahlO sieht lediglich vor, daß **auf Verlangen des Wahl-**

berechtigten in dem Wählerverzeichnis während der Auslegungsfrist das Geburtsdatum unkenntlich zu machen ist.

Der Innenminister begründet seine Entscheidung damit, daß die öffentliche Kontrolle der Wahl („Publizität des Wahlgeschehens") eine indispensable Komponente der Freiheit der Wahl sei, die dem Individualrecht auf Datenschutz vorgehe.

Ich verkenne nicht den hohen verfassungsrechtlichen Rang der öffentlichen Kontrolle der Wahl. Für diese Kontrolle ist es aber nicht notwendig, die Geburtsdaten der Wahlberechtigten jedermann zugänglich zu machen. Es genügt, ein Wählerverzeichnis auszulegen, das lediglich Familienname, Vorname und Wohnanschrift enthält. In den wenigen Fällen, in denen bei der Einsichtnahme zur Feststellung der Identität eines Wahlberechtigten auf das Geburtsdatum zurückgegriffen werden muß, kann dies auf zumutbare Weise durch Rückfrage bei der Gemeindebehörde geschehen.

Die dem Wahlberechtigten in dem neuen § 17 Abs. 4 LWahlO eingeräumte Möglichkeit, zu verlangen, daß in dem Wählerverzeichnis während der Auslegungsfrist das Geburtsdatum unkenntlich gemacht wird, reicht zum Schutz vor einer Verletzung seines Grundrechts aus Artikel 4 Abs. 2 LV nicht aus. Dieses Grundrecht schützt den Bürger unmittelbar. Seine Schutzwirkung darf nicht davon abhängig gemacht werden, daß der Bürger selbst tätig wird. Der Staat hat das Grundrecht von Amts wegen zu beachten, sofern nicht die Voraussetzungen für einen Eingriff vorliegen.

Im übrigen bestätigt gerade die Regelung in § 17 Abs. 4 LWahlO, daß die Angabe der Geburtsdaten bei der Auslegung des Wählerverzeichnisses nicht erforderlich ist. Wenn auf die Angabe des Geburtsdatums derjenigen Wahlberechtigten verzichtet werden kann, die dies verlangen, so ist sie auch bei den anderen Wahlberechtigten entbehrlich.

Nach § 31 Abs. 3 DSG NW habe ich den Ausschuß für Innere Verwaltung des Landtags über die Angelegenheit unterrichtet.

Vorkommnisse bei den letzten Kommunalwahlen nahmen Bürger zum Anlaß, sich an mich zu wenden. In einem Falle wurden bei der Stimmabgabe im Wahlraum von den Mitgliedern des Wahlvorstandes die Geburtsdaten der Wähler laut vorgelesen. Als Begründung für diese Handhabung gab die zuständige Verwaltung an, die Nennung der Geburtsdaten diene der eindeutigen Identifizierung der Wähler

Ich habe dieser Auffassung widersprochen. Zwar hat der Wahlvorstand nach § 38 Abs. 1 Satz 6 KWahlO die Wahlberechtigung festzustellen; dazu gehört die eindeutige Identifizierung des Wahlberechtigten. Für diesen Zweck reichen jedoch fast immer Familienname, Vorname und Wohnanschrift aus. Lediglich in den wenigen Fällen, in denen Träger des gleichen Familien- und Vornamens die gleiche Wohnanschrift haben oder sonstige Zweifel an der Identität bestehen, ist es notwendig, zur Identifizierung zusätzlich auf das Geburtsdatum zurückzugreifen. Nur in diesen Fällen muß der Wahlberechtigte hinnehmen, daß sein Geburtsdatum im Wahlraum genannt wird. Zur Vermeidung von Verstößen gegen das Datenschutzgesetz Nordrhein-Westfalen habe ich dem zuständigen Oberstadtdirektor empfohlen, bei künftigen Wahlen die Wahlvorstände auf diese Rechtslage hinzuweisen. Der Oberstadtdirektor hat zugesagt, meiner Empfehlung zu folgen.

Im Zusammenhang mit den bevorstehenden Landtagswahlen hatte ich auf Grund mehrerer Anfragen zu prüfen, inwieweit die Übermittlung personenbezogener Daten an den Gemeindedirektor zwecks Gewinnung von Wahlvorstandsmitgliedern zulässig ist.

Nach den geltenden Wahlgesetzen und den dazu erlassenen Wahlordnungen beruft der Gemeindedirektor die Mitglieder des Wahlvorstandes. Hierzu muß er unter anderem auf die Mitarbeiter der am Ort befindlichen Behörden, Körperschaften und sonstigen öffentlichen Stellen zurückgreifen.

Eine Körperschaft des öffentlichen Rechts hatte datenschutzrechtliche Bedenken, einer Bitte des zuständigen Oberstadtdirektors um Übermittlung von Namen, Anschrift, Ge-

burtsdatum und Amtsbezeichnung bzw. Vergütungs- oder Lohngruppe der Mitarbeiter im Alter von 18 bis 60 Jahren nachzukommen. Ich teile diese Bedenken. Mir erscheint zweifelhaft, ob alle erbetenen Daten erforderlich sind, um dem Oberstadtdirektor die Besetzung der Wahlvorstände mit geeigneten Personen zu ermöglichen (2. Alternative des § 11 Abs. 1 Satz 1 DSG NW).

Es ist zwar einzusehen, daß hinsichtlich der Eignung für das Ehrenamt des Wahlvorstandsmitglieds gewisse Auswahlkriterien erforderlich sind. Auch sollte eine altersmäßige Streuung erreicht werden. Ich habe aber Zweifel, ob dazu auch das Geburtsdatum und die Angabe der Amtsbezeichnung oder der Vergütungs- oder Lohngruppe nötig sind. Es genügt nach meiner Auffassung, wenn das Alter und die Laufbahngruppe, bei Angestellten und Arbeitern entsprechende Angaben mitgeteilt werden. Der zuständige Oberstadtdirektor hat dies auf Anfrage bestätigt.

Dementsprechend hat ihm die öffentlich-rechtliche Körperschaft inzwischen die Namen, Anschriften und Altersangaben der Mitarbeiter, jeweils zusammengefaßt nach Laufbahngruppen unter Einbeziehung der Mitarbeiter in den vergleichbaren Vergütungs- oder Lohngruppen, übermittelt.

Ein Bürger hat mir die Frage vorgelegt, ob es mit dem Datenschutzgesetz vereinbar sei, wenn ein öffentlich-rechtliches Unternehmen, das am Wettbewerb teilnimmt, eine Liste seiner Bediensteten mit Namen, Anschrift und Gehaltsgruppe zwecks Bestellung von Wahlhelfern an die Gemeindeverwaltung übermittelt.

Auch in diesem Fall habe ich dem Einsender mitgeteilt, daß zur Bestellung von Wahlhelfern die Übermittlung der Gehalts-, Vergütungs- oder Lohngruppe des einzelnen Mitarbeiters an den Gemeindedirektor nicht erforderlich ist.

Ich werde mich gegenüber dem Innenminister dafür einsetzen, daß landeseinheitlich im Sinne meiner Rechtsauffassung verfahren wird.

3. Personenstandswesen

Eine Eingabe betraf die Zulässigkeit einer Auskunft aus Personenstandsbüchern für Zwecke der **zeitgeschichtlichen Forschung.** Im Zusammenhang mit seiner Dissertation über die Anfänge der Sozialdemokratie in einer nordrhein-westfälischen Großstadt benötigte ein Bürger das Todesdatum eines verstorbenen SPD-Politikers. Unter Hinweis auf das Datenschutzgesetz hat ihm das zuständige Standesamt die Auskunft verweigert. Die Verweigerung ist im Ergebnis nicht zu beanstanden.

Der Anspruch auf Schutz der personenbezogenen Daten besteht nach Artikel 4 Abs. 2 Satz 1 LV grundsätzlich auch nach dem Tode des Betroffenen. Eingriffe bedürfen einer gesetzlichen Grundlage.

Gesetzliche Grundlage für die Übermittlung aus Personenstandsbüchern ist § 61 Abs. 1 des Personenstandsgesetzes (PStG). Diese Vorschrift geht als Bundesrecht nach Artikel 31 GG den Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen vor. Da sie eine abschließende Regelung der Einsicht in und damit der Auskunft aus Personenstandsbüchern enthält, sind die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen für die Übermittlung von Daten an Personen und Stellen außerhalb des öffentlichen Bereichs (§ 13) auch nicht ergänzend anzuwenden.

Nach § 61 Abs. 1 PStG kann Einsicht in die Personenstandsbücher, Durchsicht dieser Bücher und Erteilung von Personenstandsurkunden nur von Personen verlangt werden, auf die sich der Eintrag bezieht, sowie von deren Ehegatten, Vorfahren und Abkömmlingen (Satz 1). Andere Personen haben nur dann ein Recht auf Einsicht, Durchsicht oder

Erteilung von Personenstandsurkunden, wenn sie ein rechtliches Interesse glaubhaft machen (Satz 3).

Danach bestand für den Doktoranden kein Anspruch auf Einsicht, da sein wissenschaftliches Interesse zwar ein berechtigtes (im Einklang mit der Rechtsordnung stehendes), aber kein rechtliches (in unmittelbarem Zusammenhang mit seinen Rechtsverhältnissen stehendes) war. Insoweit ist eine Auskunft mangels einer gesetzlichen Grundlage nur mit Einwilligung des Betroffenen zulässig, also derjenigen Person, auf die sich die Eintragung bezieht. Ist diese Person verstorben, so reicht es aus, wenn die Einwilligung einer der Personen vorliegt, die nach § 61 Abs. 1 Satz 1 PStG selbst Einsicht in die Personenstandsbücher nehmen können.

Eine Auskunft aus Personenstandsbüchern zu Forschungszwecken ohne Einwilligung einer der genannten Personen setzt eine entsprechende Änderung des Personenstandsgesetzes voraus, für die der Bundesgesetzgeber zuständig ist.

Ein **Familienforscher** führte Klage darüber, daß er etwa seit Herbst letzten Jahres „erheblichen Widerstand" bei Auskunftsersuchen aus den Personenstandsbüchern erfahre. Ich habe auch ihn darauf hingewiesen, daß ein Anspruch auf Einsicht in die Personenstandsbücher nur besteht, wenn sich die Eintragungen auf den Ehegatten, die Abkömmlinge oder die Vorfahren des Auskunftssuchenden beziehen. Soweit Auskunft über andere Familienmitglieder gewünscht wird, besteht kein Anspruch auf Einsicht, da das Interesse an genealogischen Forschungen zwar ein berechtigtes, aber kein rechtliches ist.

Das Vorliegen eines rechtlichen Interesses habe ich auch im Falle eines Journalisten verneint, der zu **publizistischen Zwecken** Auskunft über Datum, Uhrzeit und Ort der Geburt eines Bürgers wünschte. Eine Auskunft ist auch in solchen Fällen mangels einer gesetzlichen Grundlage nur mit Einwilligung des Betroffenen oder, wenn dieser verstorben ist, mit Einwilligung einer der Personen zulässig, die nach § 61 Abs. 1 Satz 1 PStG selbst Einsicht in die Personenstandsbücher nehmen können.

4. Kommunalwesen

Im kommunalen Bereich bin ich um datenschutzrechtliche Prüfung der **Ehrenordnung** des Rates einer Stadt gebeten worden. Der Entwurf sah vor, daß Ratsmitglieder dem Bürgermeister bestimmte Daten über ihre persönlichen und wirtschaftlichen Verhältnisse mitzuteilen haben. Er war datenschutzrechtlich nicht zu beanstanden.

Da § 30 Abs. 2 Satz 2 bis 4 der Gemeindeordnung für das Land Nordrhein-Westfalen (GO NW) nach § 37 DSG NW den Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen vorgeht, finden die Vorschriften dieses Gesetzes über die Erhebung und Speicherung personenbezogener Daten in diesem Falle keine Anwendung. Die Regelung in § 30 Abs. 2 Satz 2 bis 4 GO NW und in den auf Grund dieser Vorschriften zu erlassenden Ehrenordnungen sind jedoch an der Landesverfassung, insbesondere an dem Grundrecht auf Datenschutz (Artikel 4 Abs. 2) zu messen.

Nach Artikel 4 Abs. 2 LV darf in das Grundrecht auf Schutz der personenbezogenen Daten nur im überwiegenden Interesse der Allgemeinheit eingegriffen werden. Die Allgemeinheit hat ein Interesse daran, daß bei der Tätigkeit der Rats- und Ausschußmitglieder Interessenkollisionen vermieden werden. Um ihnen vorzubeugen, ist erforderlich, daß zumindest der Bürgermeister und der jeweilige Ausschutzvorsitzende Kenntnis von den personenbezogenen Daten der Rats- oder Ausschußmitglieder hat, die auf mögliche Interessenkollisionen hindeuten können. Dies gilt insbesondere für Daten, die ein Mitwirkungsverbot nach §§ 23 und 30 Abs. 2 Satz 1 GO NW begründen können. Dieses Interesse der Allgemeinheit überwiegt gegenüber dem Interesse des Rats- oder Ausschuß-

mitglieds an dem Schutz seiner personenbezogenen Daten. § 30 Abs. 2 Satz 2 bis 4 GO NW ist daher mit Artikel 4 Abs. 2 LV vereinbar.

Der mir vorgelegte Entwurf einer Ehrenordnung sah ausschließlich eine Auskunft über solche Daten vor, die ein Mitwirkungsverbot begründen können. Er sah ferner vor, daß die erteilten Auskünfte nur im Rahmen der Geschäftsführung des Rates oder der Ausschüsse verwendet werden dürfen. Die in dem Entwurf enthaltene Verpflichtung, die Auskünfte vertraulich zu behandeln, ergibt sich bereits aus dem Gesetz (§ 30 Abs. 2 Satz 4 GO NW). Eine unbefugte Offenbarung solcher Auskünfte ist als Verletzung der Verschwiegenheitspflicht (§ 22 Abs. 2 GO NW) mit Strafe oder Ordnungsgeld bedroht (§ 22 Abs. 6 in Verbindung mit § 21 Abs. 3 GO NW). Dabei ist eine Weitergabe der Daten durch den Bürgermeister an den jeweiligen Ausschußvorsitzenden nicht als unbefugt anzusehen.

Mehrere Beratungsersuchen betrafen die Weitergabe von **Jubiläumsdaten** durch die Verwaltung an Bürgermeister, Ratsmitglieder und sachkundige Bürger. Hierbei handelt es sich nicht um eine Übermittlung im Sinne des Datenschutzgesetzes Nordrhein-Westfalen, weil der Bürgermeister kein Dritter ist (§ 2 Abs. 2 Nr. 2, Abs. 3 Nr. 2 DSG NW). Die Gemeinden haben jedoch für die Beachtung der Grundsätze über die Zulässigkeit der Übermittlung (§ 11 Abs. 1 DSG NW) auch dann zu sorgen, wenn Daten innerhalb der Gemeinde von einer Stelle an eine andere weitergegeben werden (§ 8 Satz 1 DSG NW). Danach muß die Weitergabe zur rechtmäßigen Erfüllung einer in der Zuständigkeit des Bürgermeisters liegenden Aufgabe erforderlich sein.

Diese Voraussetzung dürfte vorliegen. Es kann davon ausgegangenen werden, daß es zu den Aufgaben einer Gemeinde gehört, ihren Bürgern zu bestimmten Jubiläen zu gratulieren. Hierzu ist in erster Linie der Rat als die gewählte Vertretung der Bürgerschaft berufen, der hierbei grundsätzlich durch den Bürgermeister vertreten wird (§ 27 Abs. 2 Satz 3 GO NW). Soweit der Bürgermeister daran gehindert ist, die Glückwünsche selbst zu übermitteln, ist es unbedenklich, wenn er sich hierbei durch ein anderes Ratsmitglied oder auch durch einen sachkundigen Bürger vertreten läßt. Die Gratulation muß jedoch im Namen der Gemeinde, nicht etwa im Namen der Fraktion oder der Partei ausgesprochen werden. Da die Weitergabe der Daten an Bürgermeister, Ratsmitglieder und sachkundige Bürger nur zulässig ist, wenn die Aufgabenerfüllung rechtmäßig ist, sollten im Hinblick auf eine unparteiische Amtsführung des Bürgermeisters bei solchen Gratulationsaufträgen alle im Rat vertretenen Parteien angemessen berücksichtigt werden.

Eine Weitergabe von Jubiläumsdaten an Fraktionen auf deren Anforderung ist meines Erachtens nicht zulässig. Es kann jedoch hingenommen werden, daß die jeweilige Fraktion von solchen Daten Kenntnis erhält, wenn der Bürgermeister ein Ratsmitglied beauftragt, für die Gemeinde zu gratulieren.

Entsprechendes gilt für das Überreichen von **Weihnachtspräsenten an Senioren.**

Es wurde im übrigen festgestellt, daß bei einzelnen Städten und Gemeinden **Repräsentationsdateien** mit personenbezogenen Daten von Bürgern für Glückwünsche zu Ehe- und Altersjubiläen geführt werden. Diese Dateien enthalten oftmals weitaus mehr Daten, als für den gewünschten Zweck erforderlich ist. Ich habe darauf hingewirkt, daß eine Überprüfung dieser Dateien auf ihren erforderlichen Inhalt erfolgt. Soweit die Daten zur Erfüllung der Aufgabe nicht benötigt werden, sind sie zu löschen.

Zwei Bürger haben mich gebeten, die Weitergabe der Anschriften von Schülereltern durch die Verwaltung an den Bürgermeister und den Vorsitzenden des Schulausschusses zum Zweck der **Unterrichtung der Eltern** über Angelegenheiten der Schule datenschutzrechtlich zu prüfen. Eine Verletzung von Datenschutzvorschriften habe ich hierbei nicht feststellen können.

Nach § 8 Satz 1 in Verbindung mit § 11 Abs. 1 DSG NW muß die Weitergabe zur rechtmäßigen Erfüllung einer in der Zuständigkeit des Bürgermeisters liegenden Aufgabe erforderlich sein. Diese Voraussetzung lag in dem von den beiden Bürgern dargelegten Fall vor. Nach § 6b Abs. 1 Satz 1 GO NW hat der Rat die Aufgabe, die Einwohner über

alle allgemein bedeutsamen Angelegenheiten der Gemeinde zu unterrichten. Nach § 27 Abs. 2 Satz 3 GO NW wird der Rat nach außen durch den Bürgermeister vertreten. Dieser kann bei der Unterrichtung der Bürger den Vorsitzenden des zuständigen Ratsausschusses hinzuziehen. Gegen eine gezielte Unterrichtung der von einer Angelegenheit betroffenen Bürger bestehen keine Bedenken. Hierzu ist, wenn die Versendung nicht von einer anderen Stelle der Gemeindeverwaltung übernommen wird, die Weitergabe der Anschriften an den Bürgermeister erforderlich. Dies gilt allerdings nur, soweit der Rat für die Unterrichtung der Einwohner keine andere Regelung getroffen hat.

5. Polizei

a) Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen (KpS)

Der Arbeitskreis II der Innenministerkonferenz hat Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen (KpS) erarbeitet. In Nordrhein-Westfalen sind diese Richtlinien durch Runderlaß des Innenministers vom 4. Mai 1979 (MBl. NW. S. 876/SMBl. 20531) in Kraft gesetzt worden. Sie gelten für alle personenbezogenen kriminalpolizeilichen Unterlagen, die in Form von Akten, Karteien, Dateien oder einer anderen systematischen Form unterhalten werden. Sie regeln Zweck und Inhalt der Sammlungen, die Datenübermittlung, die Auskunft an den Betroffenen, die Datensicherung, die Aufbewahrungsdauer und die Aussonderung.

Die Richtlinien, in denen ausdrücklich auf die Beachtung des Datenschutzgesetzes Nordrhein-Westfalen bei der Verarbeitung personenbezogener Daten hingewiesen wird, sind als erster Schritt auf dem Wege zur Verbesserung des Datenschutzes im Polizeibereich zu begrüßen. Insbesondere ist die nunmehr vorgesehene regelmäßige Zehnjahresfrist für die Aussonderung von Akten ein erheblicher Fortschritt gegenüber der bisherigen Praxis.

Im Januar dieses Jahres hat der Bundesminister des Inneren über einen Beschluß der AG Kripo unterrichtet, der umfangreiche Änderungsvorschläge zu den erst in einem Teil der Bundesländer in Kraft gesetzten Richtlinien enthält. Diese Vorschläge werden im Arbeitskreis Sicherheit der Datenschutzbeauftragten des Bundes und der Länder erörtert. Ich bin allerdings mit dem Bundesbeauftragten für den Datenschutz der Auffassung, daß zur Zeit eine uneingeschränkte Anwendung der KpS-Richtlinien in der jetzigen Fassung in allen Bundesländern Vorrang vor einer kurzfristigen Überarbeitung haben sollte.

Kritisch stehen die Datenschutzbeauftragten Plänen des Bundeskriminalamts gegenüber, die Speicherung — verformelter — daktyloskopischer Unterlagen abweichend von den Regelfristen der KpS-Richtlinien über die Aussonderung zu behandeln. Begründet wird die — verlängerte — Aussonderungsfrist mit der weiteren Erforderlichkeit der Daten für die Ermittlungsarbeit, insbesondere für die Identifizierung von Straftätern, unbekannten Toten und hilflosen Personen. Auf ihrer letzten Konferenz im Februar dieses Jahres in München haben die Datenschutzbeauftragten der Länder den Bundesbeauftragten gebeten, den Bundesminister des Innern um nähere Begründung für die Rechtfertigung und Notwendigkeit der abweichenden Behandlung zu bitten.

b) Neukonzeption des INPOL-Systems

Das Bundeskriminalamt ist Zentralstelle des gemeinsamen elektronischen Informations- und Auskunftssystems für die Polizei des Bundes und der Länder (INPOL). Teilnehmer auf Landesebene sind das Landeskriminalamt und die anderen Polizeibehörden. Da die erfassenden Landesdienststellen für die von ihnen eingegebenen Daten verantwortlich bleiben, richtet sich die datenschutzrechtliche Prüfung dieser Daten nach dem Datenschutzgesetz Nordrhein-Westfalen.

Im Rahmen einer Neukonzeption des INPOL-Systems wird die zentrale Speicherung aller, auch lediglich regional in Erscheinung getretener Straftäter erwogen. Die Datenschutzbeauftragten haben hiergegen rechtliche Bedenken erhoben. Nach ihrer Meinung wäre eine solche Maßnahme mit dem Gesetz über die Einrichtung eines Bundeskriminalpolizeiamtes (Bundeskriminalamtes) nicht vereinbar; auf jeden Fall würde sie gegen den Grundsatz der Verhältnismäßigkeit verstoßen. Ich habe deshalb den Innenminister gebeten, bei den Beratungen über die Neukonzeption dafür einzutreten, daß im INPOL-System nur Daten zu überregional bedeutsamen Straftaten und Straftätern gespeichert werden.

c) Polizeiliche Beobachtung

Umstritten sind die gesetzlichen Grundlagen für die Polizeiliche Beobachtung, auch „beobachtende Fahndung" genannt. Es kann nicht zweifelhaft sein, daß die heimliche Beobachtung von Personen einen Eingriff in die Rechtssphäre der Betroffenen darstellt, der einer Rechtsgrundlage bedarf. Dabei kann die Frage, ob die Polizeiliche Beobachtung überwiegend als Maßnahme der Gefahrenabwehr oder im Rahmen der Strafverfolgung eingesetzt wird, offen bleiben. Auf jeden Fall findet sie in beiden Bereichen Anwendung.

Als Rechtsgrundlage im Rahmen der Gefahrenabwehr kommen die Polizeigesetze in Betracht. Die polizeiliche Generalklausel ermächtigt zu Eingriffen nur im Fall einer konkreten Gefahr. Da bei der Polizeilichen Beobachtung meist keine konkrete Gefahr bejaht werden kann, reicht die Generalklausel nicht aus. Auch die Vorschrift der Datenschutzgesetze, die die Datenspeicherung zuläßt, wenn sie zur rechtmäßigen Aufgabenerfüllung erforderlich ist, ist keine Rechtsgrundlage, die zur Datenerhebung ermächtigt. Sie setzt vielmehr eine rechtmäßige, also durch Gesetz zugelassene Datenerhebung voraus.

Als Rechtsgrundlage für die Polizeiliche Beobachtung zur Strafverfolgung werden die §§ 161, 163 StPO genannt. Nach § 161 Satz 1 StPO kann die Staatsanwaltschaft zur Erforschung von Straftaten Ermittlungen jeder Art durch die Behörden und Beamten des Polizeidienstes vornehmen lassen. Nach § 163 Abs. 1 StPO haben die Behörden und Beamten des Polizeidienstes auch ohne Auftrag der Staatsanwaltschaft Straftaten zu erforschen.

Ob diese Vorschriften als Rechtsgrundlage für die Polizeiliche Beobachtung ausreichen, ist zumindest zweifelhaft. Bundesminister Dr. Vogel hat in einem Beitrag in NJW 1978, S. 1217, 1225f. zu Recht ausgeführt, daß den staatsanwaltlichen Aufgabenzuweisungen in den §§ 152, 160 StPO keine entsprechenden Eingriffsermächtigungen korrespondieren und die Strafprozeßordnung anders als das Polizeirecht keine Generalklausel enthält. Das gilt in gleichem Maße für die polizeiliche Aufgabenumschreibung im Rahmen der Strafverfolgung nach den §§ 161, 163 StPO. Die genannten Vorschriften der Strafprozeßordnung ermächtigen nach meiner Auffassung und der des Bundesbeauftragten für den Datenschutz allein zu schlicht-hoheitlichem Handeln, nicht aber zu Handeln, das als Eingriff in die Rechtssphäre der Bürger zu qualifizieren ist.

Aus diesen Überlegungen ergibt sich das verfassungsrechtliche Gebot, zumindest aber die rechtspolitische Forderung, die Voraussetzungen für die Polizeiliche Beobachtung im Gesetz zu regeln. Wenn die Polizeiliche Beobachtung für notwendig gehalten wird, muß sie in beiden Bereichen auf eine einwandfreie gesetzliche Grundlage gestellt werden. Innerdienstliche Vorschriften reichen nicht aus. Der Gesetzgeber ist aufgerufen, die Verantwortung für den rechtlichen Rahmen zu übernehmen.

d) Rasterfahndung

Die Frage nach der gesetzlichen Grundlage polizeilicher Informationsverarbeitung stellt sich auch bei der Rasterfahndung, die vor einigen Wochen im Mittelpunkt der öffentlichen Datenschutzdiskussion stand. Nach geltendem Recht kommen als gesetzliche Grundlage § 24 BDSG sowie die §§ 161, 163 und 94 StPO in Betracht. § 24 Abs. 1 Satz 1 BDSG erlaubt privaten Unternehmen, personenbezogene Daten von Kunden an Dritte, also auch an die Polizei, zu übermitteln, soweit es zur Wahrung berechtigter Interessen der

Allgemeinheit erforderlich ist und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

Es kann nicht zweifelhaft sein, daß die Fahndung nach Personen, die schwerer Verbrechen beschuldigt werden, im Interesse der Allgemeinheit liegt. Ich habe auch keine Zweifel, daß die Polizei die von privaten Unternehmen angeforderten Daten zur Fahndung nach diesen Personen braucht. Andererseits haben Unbeteiligte ein Interesse daran, nicht in derartige Fahndungsmaßnahmen einbezogen zu werden. Bei Abwägung der Interessen überwiegt in diesen Fällen in der Regel das Interesse der Allgemeinheit an einer wirksamen Fahndung gegenüber dem Interesse des einzelnen Bürgers an dem Schutz seiner Persönlichkeitssphäre.

Die Voraussetzungen des § 24 Abs. 1 Satz 1 BDSG dürften also bei den bisherigen Rasterfahndungen vorgelegen haben. Allerdings werden private Unternehmen durch diese Vorschrift zur Datenübermittlung nur ermächtigt, nicht aber verpflichtet. Wenn ein Unternehmen im Interesse seiner Kunden eine Datenübermittlung ablehnt, kann die Polizei sie nicht auf Grund dieser Vorschrift erzwingen.

Die Polizei kann sich ihrerseits für ihr Tätigwerden zunächst nur auf die §§ 161, 163 StPO stützen. Bereits im Zusammenhang mit der polizeilichen Beobachtung habe ich dargelegt, daß zumindest zweifelhaft ist, ob diese Vorschriften als Rechtsgrundlage für Eingriffe in das Recht des Bürgers auf Schutz seiner personenbezogenen Daten ausreichen. Auf jeden Fall genügen sie nicht, um private Unternehmen zur Herausgabe personenbezogener Daten ihrer Kunden zu zwingen.

Deshalb sind bei fast allen in der letzten Zeit durchgeführten Rasterfahndungen Beschlüsse des Ermittlungsrichters beim Bundesgerichtshof nach § 94 StPO ergangen, durch die die entsprechenden Magnetbänder oder Belege beschlagnahmt wurden. Beschlagnahmt werden können nach dieser Vorschrift „Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können". Wenngleich dem Begriff „Beweismittel" in diesem Zusammenhang etwas Gewalt angetan wird (die Bänder und Belege dürften als Beweismittel im Prozeß keine Rolle mehr spielen), so sind doch die Datenschutzbeauftragten des Bundes und der Länder einhellig der Auffassung, daß diese Beschlagnahmebeschlüsse die Rasterfahndungsmaßnahmen der Polizei abdecken.

Die Datenschutzbeauftragten haben zwar übereinstimmend festgestellt, daß sich bei den bisher in ihrer jeweiligen Zuständigkeit geprüften Fällen keine Anlässe zu Beanstandungen ergeben haben. Sie sind jedoch der Meinung, daß die genannten, sehr allgemein gefaßten Bestimmungen den mit der Rasterfahndung verbundenen Problemen nicht gerecht werden. Die große Zahl der einbezogenen Personen, die Menge der verarbeiteten Daten und die dank der veränderten Informationsmethoden gegebenen vielfältigen Nutzungsmöglichkeiten zwingen nach Auffassung der Datenschutzbeauftragten zu präzisen bereichsspezifischen Regelungen, wie sie etwa in § 100a StPO für die Überwachung des Telefonverkehrs und in § 111 StPO für die Einrichtung von Kontrollstellen getroffen worden sind. Das Ziel muß sein, den Verhältnismäßigkeitsgrundsatz stärker zur Geltung zu bringen und insbesondere die Interessen Unverdächtiger zu schützen, soweit diese von den Fahndungsmaßnahmen betroffen werden.

Vor allem wird zu regeln sein,

- zu welchen Zwecken solche Fahndungsmaßnahmen angewendet werden dürfen (zu denken wäre an die gleichen Straftatbestände wie in § 100a StPO für die Überwachung des Telefonverkehrs),
- welche tatsächlichen Voraussetzungen zu fordern sind,
- ob und in welchem Umfang bestimmte Datenarten nicht einbezogen werden dürfen (zu denken wäre an alle amtshilfefesten Geheimnisse wie Sozialgeheimnis, Steuergeheimnis, Statistikgeheimnis),
- ob die Daten auch zu anderen Zwecken als zu der jeweiligen Fahndung verwendet

werden dürfen (nach meiner Auffassung nur für solche Zwecke, die selbst eine Rasterfahndung rechtfertigen würden, auf keinen Fall aber zur Verfolgung von Ordnungswidrigkeiten),

- welche verfahrensmäßigen Sicherungen zu fordern sind (Löschung, Dokumentation, Kontrolle),
- ob und in welchem Umfang dem Datenschutzbeauftragten Gelegenheit zu vorheriger Stellungnahme zu geben ist (eine Unterrichtung wäre nützlich, Beratung falls gewünscht, Schweigen bedeutet kein Einverständnis, die Verantwortung muß bei der Behörde bleiben, die Kontrollaufgabe bleibt unberührt),
- wie die Kontrolle bei länderübergreifender Fahndung sicherzustellen ist.

e) Eingaben von Bürgern

Zahlreiche Eingaben betrafen den Polizeibereich. In mehreren Fällen wollten Bürger wissen, ob und in welchem Umfang bei der Polizei personenbezogene Daten über sie gespeichert sind. Andere baten mich, ihnen bei der Löschung der über sie gespeicherten Daten behilflich zu sein.

In einigen Fällen war meiner Einschaltung eine vergebliche Anfrage bei der Polizei vorausgegangen. Diese hatte die Auskunft unter Berufung auf das im Datenschutzgesetz Nordrhein-Westfalen festgelegte Auskunftsverweigerungsrecht abgelehnt. Nach § 16 Abs. 2 in Verbindung mit § 15 Abs. 2 Nr. 1 DSG NW kann die Polizei dem Betroffenen die Auskunft über die über ihn gespeicherten personenbezogenen Daten verweigern. Dieses Recht darf auch der Landesbeauftragte für den Datenschutz nicht durch Mitteilungen über die ihm bei seiner Prüfung zugänglich gemachten Erkenntnisse umgehen.

Die genannten Vorschriften ermächtigen zwar die Polizei zur Auskunftsverweigerung, verpflichten sie aber nicht dazu. Ich habe Zweifel, ob die bisherige Praxis der Polizeibehörden, fast immer die Auskunft an den Betroffenen zu verweigern, in allen Fällen geboten ist und ob sie im wohlverstandenen Interesse der Polizei liegt. Eine Erweiterung der Auskunftspraxis der Polizei würde vielen Menschen unbegründete Angst nehmen und die Arbeit der Polizei transparenter machen, was wiederum auch ihrer Aufgabenerfüllung zugute käme. Dementsprechend sieht Nr. 6 Satz 1 der Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen vor, daß dem Betroffenen auf Antrag Auskunft darüber erteilt werden kann, ob und gegebenenfalls welche Unterlagen über ihn in diesen Sammlungen vorhanden sind, wenn eine Abwägung ergibt, daß sein Interesse das öffentliche Interesse an der Geheimhaltung überwiegt.

Ich habe daher einige Polizeibehörden, die von ihrem Auskunftsverweigerungsrecht Gebrauch gemacht hatten, gebeten, ihre Entscheidung im Hinblick auf diese Erwägungen noch einmal zu überprüfen. Teilweise gaben daraufhin die Polizeibehörden dem Betroffenen die gewünschte Auskunft, oder sie waren damit einverstanden, daß ich diese Auskunft erteilte. In einigen Fällen mußte ich mich dem Bürger gegenüber auf die Mitteilung beschränken, daß ich keine Verstöße gegen Vorschriften über den Datenschutz festgestellt habe.

Die Frage der Auskunftsverweigerung durch die Polizei bedarf einer grundsätzlichen Erörterung mit dem Innenminister, um eine einheitliche, datenschutzfreundliche Handhabung bei den Polizeibehörden zu erreichen.

In einigen Fällen habe ich unter Hinweis auf § 17 Abs. 3 DSG NW und die Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen (KpS) angefragt, wann mit einer Löschung der gespeicherten oder festgehaltenen Daten zu rechnen sei. In einem Falle konnte ich dem Betroffenen mitteilen, daß auf meine Veranlassung die Unterlagen über seine erkennungsdienstliche Behandlung von der zuständigen Polizeibehörde vernichtet worden sind.

6. Verfassungsschutz

a) Nachrichtendienstliches Informationssystem (NADIS)

Das Bundesamt für Verfassungsschutz unterhält im Datenverbund eine Hinweisdatei für die Verfassungsschutzbehörden des Bundes und der Länder. Dieses Nachrichtendienstliche Informationssystem (NADIS) enthält lediglich Personengrunddaten und Hinweise auf Aktenfundstellen. Einzeldaten, die über die Personengrunddaten hinausgehen, sind — davon habe ich mich durch Einsichtnahme in die Arbeitsweise des Systems überzeugt — in NADIS nicht zu finden. Es handelt sich vielmehr um ein Fundstellenregister, das den anfragenden Verfassungsschutzbehörden Auskunft darüber gibt, ob und bei welcher Behörde Informationen über eine Person vorliegen.

Zu begrüßen sind die neuen Löschungsrichtlinien, nach denen auch im Lande Nordrhein-Westfalen bereits gearbeitet wird. Sie stellen eine erhebliche Verbesserung des Datenschutzes dar. Die Datenschutzbeauftragten des Bundes und der Länder werden allerdings prüfen, ob weitere Verbesserungen möglich sind.

b) Erhebung über Betriebsrätewahlen

In der Presse war berichtet worden, daß der Verfassungsschutz alle neugewählten Betriebsräte, die Mitglieder in radikalen Parteien seien, per Computer erfasse.

Nach § 3 Abs. 1 Nr. 1 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes ist Aufgabe der Verfassungsschutzbehörden die Sammlung und Auswertung von Auskünften, Nachrichten und sonstigen Unterlagen über Bestrebungen, die gegen die freiheitliche demokratische Grundordnung gerichtet sind. Meine Ermittlungen haben ergeben, daß die Verfassungsschutzbehörden der Länder im Rahmen dieser Aufgabe anhand vorhandener Unterlagen feststellen, ob und gegebenenfalls welche Betriebsratsmitglieder Organisationen mit verfassungsfeindlicher Zielsetzung angehören. Das Bundesamt für Verfassungsschutz koordiniert diese Erhebungen und wertet die Erkenntnisse aus.

Für Nordrhein-Westfalen hat der Innenminister als Verfassungsschutzbehörde dem Bundesamt für Verfassungsschutz formularmäßig und ohne Speicherung mitgeteilt, welche Mitglieder extremistischer Organisationen in Betriebsräte gewählt worden sind. Daten anderer gewählter Arbeitnehmervertreter sind weder an Dritte weitergegeben noch intern in irgendeiner Form gesammelt oder verwertet worden. Betriebliche oder gewerkschaftliche Aktivitäten haben bei der Analyse des Wahlergebnisses keine Rolle gespielt; sie wurden daher weder erfaßt noch gespeichert. Beobachtungsgegenstand sind nicht Betriebsräte oder gewerbliche Unternehmen, sondern die Bestrebungen von Organisationen, deren Tätigkeit gegen den Kernbestand der Verfassung gerichtet ist. Die Verfassungsschutzbehörde hat in diesem Zusammenhang keine personenbezogenen Daten von Betriebsratsmitgliedern in einer Datei gespeichert.

c) Eingaben von Bürgern

Mehrere Eingaben von Bürgern betrafen den Verfassungsschutz. Dabei war häufig die Frage zu prüfen, ob und gegebenenfalls wann beim Verfassungsschutz festgehaltene personenbezogene Daten zu löschen sind.

Soweit erforderlich, habe ich Prüfungen in den Diensträumen der Verfassungsschutzabteilung des Innenministeriums durchgeführt. Verstöße gegen Vorschriften über den Datenschutz habe ich nicht festgestellt. Im Hinblick auf das auch den Verfassungsschutzbehörden zustehende Auskunftsverweigerungsrecht konnte ich den Betroffenen lediglich dieses Ergebnis mitteilen. In einem Fall wurde auf meinen Wunsch eine Einzelangabe gesperrt.

Der von einem Bürger vertretenen Ansicht, das Sammeln von Erkenntnissen über die Teilnahme an nicht verbotenen Veranstaltungen sei schlechthin unzulässig, habe ich widersprochen. Auch in der Teilnahme an einer solchen Veranstaltung kann eine Unterstützung gegen die freiheitliche demokratische Grundordnung gerichteter Bestrebungen liegen, deren Beobachtung gesetzliche Aufgabe des Verfassungsschutzes ist. Ob die Teilnahme an einer Veranstaltung als Unterstützung derartiger Bestrebungen zu werten ist, kann nur unter Berücksichtigung der gesamten Umstände des Einzelfalles beurteilt werden.

7. Bauwesen

Es war früher üblich, Angaben über Namen und Anschriften von Bauherren, Lage und Art des Bauvorhabens an nicht-öffentliche Stellen, wie zum Beispiel Baustelleninformationsdienste, weiterzugeben oder diese Angaben in den Bekanntmachungsorganen der Gemeinden oder in der Tagespresse zu veröffentlichen. Ich habe in Übereinstimmung mit dem Innenminister darauf hingewiesen, daß diese Praxis nach dem Inkrafttreten des Datenschutzgesetzes Nordrhein-Westfalen nicht beibehalten werden kann. Das gleiche gilt für die Veröffentlichung dieser Angaben im Rahmen der Bekanntgabe der Tagesordnungspunkte von Ratssitzungen.

Es kann nicht zweifelhaft sein, daß diese Angaben, soweit es sich um Bauvorhaben natürlicher Personen handelt, nach § 1 Abs. 2 Satz 1 DSG NW geschützte personenbezogene Daten sind. Sie sind Einzelangaben über sachliche Verhältnisse bestimmter natürlicher Personen (§ 2 Abs. 1 DSG NW); der Umstand, daß einige Angaben von dem Zeitpunkt des Baubeginns an offenkundig sind, steht dem nicht entgegen.

Die Angaben werden in fast allen Fällen auch in Dateien gespeichert (§ 2 Abs. 3 Nr. 3 DSG NW). Solange sie in einer Datei gespeichert sind, unterliegt ihre Übermittlung nach § 1 Abs. 2 Satz 1 DSG NW den Beschränkungen des Datenschutzgesetzes Nordrhein-Westfalen, ohne daß es im Einzelfall darauf ankommt, ob sie aus der Datei selbst, einer entsprechenden Liste, den Eingabebelegen oder einer inhaltlich mit ihnen übereinstimmenden Akte übermittelt werden (unten D.1.b).

§ 3 Satz 1 DSG NW knüpft die Zulässigkeit der Verarbeitung personenbezogener Daten daran, daß dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat. Nach § 13 Abs. 1 Satz 1 DSG NW ist die Datenübermittlung an nichtöffentliche Stellen zulässig, soweit der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

Von einem berechtigten Interesse an den gewünschten Angaben kann zwar ausgegangen werden; die Datenübermittlung würde jedoch schutzwürdige Belange der Betroffenen beeinträchtigen. Die Bauantragsteller haben einen Anspruch darauf, daß die Tatsache ihrer Antragstellung nicht zu Werbe- oder sonstigen Geschäfts- oder Informationszwecken Dritten mitgeteilt wird. Schon angesichts der weithin mit Unmut aufgenommenen Reklameflut kann nicht angenommen werden, daß allen Bauantragstellern die Weitergabe der Daten gleichgültig ist. Viele von ihnen mögen sogar ausdrücklich daran interessiert sein, daß ihr Bauvorhaben — zumindest im Zeitpunkt der Antragstellung — noch nicht bekannt wird. Bei einer Abwägung der Interessen überwiegt in diesen Fällen das grundrechtlich geschützte Interesse der Bauherren an der Nichtbekanntgabe ihrer Vorhaben gegenüber den Belangen des allgemeinen Informationsbedürfnisses, der Transparenz des Marktes, des unternehmerischen Wettbewerbs oder der Bekämpfung der Schwarzarbeit.

Eine Veröffentlichung der genannten Angaben oder eine Bekanntgabe in sonstiger Weise ist demnach nur mit Einwilligung der Betroffenen zulässig (§ 3 Satz 1 Nr. 2 DSG NW).

Sie setzt voraus, daß die Bauherren schriftlich ihr Einverständnis zu einer Weitergabe der gewünschten Daten erklären, nachdem sie in geeigneter Weise über Inhalt und Tragweite der Einwilligung aufgeklärt worden sind (§ 3 Satz 2 und 3 DSG NW).

Auch bei der Bekanntgabe der Tagesordnungspunkte von Ratssitzungen im Bekanntmachungsorgan der Gemeinde oder in der Tagespresse ist eine Veröffentlichung der genannten Angaben nur mit Einwilligung des Betroffenen zulässig. Die Anregung eines Bürgers, dabei nur die Grundstücksbezeichnung anzugeben, könnte zwar zu einer Verbesserung des Schutzes der Betroffenen führen. Diese Verfahrensweise reicht allerdings nicht aus, den datenschutzrechtlichen Belangen voll zu genügen, zumal gerade in kleineren Gemeinden von der Grundstücksbezeichnung relativ leicht auf den Bauherrn geschlossen werden kann. Die Angabe solcher Daten bei der Bekanntgabe der Tagesordnungspunkte ist auch nicht erforderlich. Es genügt der Hinweis auf die „Behandlung mehrerer Bauanträge". Gegen die Angabe der Zahl der Bauanträge ist nichts einzuwenden.

8. Rechtswesen

a) Staatsanwaltschaft

Nach § 26 Abs. 1 Satz 1 DSG NW habe ich die Einhaltung der Vorschriften des Datenschutgesetzes Nordrhein-Westfalen sowie anderer Vorschriften über den Datenschutz bei allen Behörden, Einrichtungen und sonstigen öffentlichen Stellen des Landes zu kontrollieren. Zu diesen Vorschriften gehört auch Artikel 4 Abs. 2 LV, und zwar ohne Rücksicht darauf, ob der Umgang mit personenbezogenen Daten unter den näheren Voraussetzungen des Datenschutzgesetzes Nordrhein-Westfalen oder anderer Rechtsvorschriften erfolgt.

Von meiner Kontrolle ausgenommen sind nach § 32 Abs. 1 Nr. 1 DSG NW lediglich die Gerichte, soweit sie nicht Verwaltungsaufgaben wahrnehmen. Die Behörden der Staatsanwaltschaft unterliegen meiner Kontrolle ohne Einschränkungen.

Ob die Behörden der Staatsanwaltschaft Verwaltungsaufgaben erledigen oder als Organe der Rechtspflege tätig werden, ist nur für die Frage von Bedeutung, welches materielle Datenschutzrecht anzuwenden ist. Erledigen sie Verwaltungsaufgaben, gelten die materiellen Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen (§ 1 Abs. 2 Satz 2 DSG NW), soweit nicht besondere Rechtsvorschriften des Landes nach § 37 DSG NW oder Rechtsvorschriften des Bundes nach Artikel 31 GG vorgehen. Werden sie als Organe der Rechtspflege tätig, gelten die materiellen Vorschriften des Bundesdatenschutzgesetzes (§ 7 Abs. 2 Satz 1 Nr. 2 BDSG), soweit nicht besondere Rechtsvorschriften des Bundes nach § 45 BDSG vorgehen. Werden personenbezogene Daten nicht in Dateien verarbeitet, so kommen als gesetzliche Grundlage für einen Eingriff in das Grundrecht auf Datenschutz weder das Datenschutzgesetz Nordrhein-Westfalen noch das Bundesdatenschutzgesetz, sondern allenfalls andere Rechtsvorschriften, wie etwa die Strafprozeßordnung, in Betracht.

Der Justizminister bestreitet dem Landesbeauftragten die Kontrollbefugnis für die Einhaltung des Artikels 4 Abs. 2 LV. Er ist der Ansicht, daß die Kontrolle auf die Einhaltung derjenigen Vorschriften beschränkt sei, die den Schutz von in Dateien verarbeiteten Daten betreffen. Diese Auffassung berührt in grundsätzlicher Weise meine Stellung als Datenschutzbeauftragter und kann nicht hingenommen werden (oben A.3.a).

Ein Bürger hat sich mit einer Eingabe dagegen gewandt, daß eine Staatsanwaltschaft einem Versicherungsunternehmen **Einsicht in** die den Freitod seines Sohnes betreffenden **Ermittlungsakten** gewährt hat. Der Bürger hatte weder Ansprüche gegen das Versicherungsunternehmen geltend gemacht noch in die Einsichtnahme eingewilligt. Er

befürchtet, daß das Versicherungsunternehmen dadurch auch Kenntnis von dem Abschiedsbrief seines Sohnes erhalten hat, und sieht darin eine schwerwiegende Verletzung seines Grundrechts auf Datenschutz.

Nach meiner Auffassung ist die Gewährung von Einsicht in die den Freitod des Sohnes betreffenden Ermittlungsakten ohne Einwilligung der Eltern ein Eingriff in das Grundrecht der Eltern und des verstorbenen Sohnes auf Datenschutz. Ich habe deshalb den Justizminister um Auskunft über die gesetzliche Grundlage eines solchen Eingriffs gebeten.

In seiner Stellungnahme vertritt der Justizminister — vorbehaltlich seiner abweichenden Auffassung zu der Kontrollbefugnis des Landesbeauftragten — die Ansicht, das Grundrecht des Sohnes sei mit dessen Tod erloschen; auch habe der Staat mit der Einsichtgewährung in die Akten nicht das Andenken des Toten verletzt. Personenbezogene Daten der Eltern seien dem Versicherungsunternehmen durch die Einsichtnahme nicht bekanntgeworden. Im übrigen sei der kraft bundesrechtlichen Gewohnheitsrechts geltende und Artikel 4 Abs. 2 LV überlagernde Grundsatz angewendet worden, daß Einsicht in die staatsanwaltschaftlichen Ermittlungsakten Dritten gewährt werden kann, wenn diese ein berechtigtes Interesse geltend machen.

Die Ansicht, daß das Grundrecht auf Datenschutz mit dem Tod erlösche, kann ich nicht teilen (unten D.1.a). Auf jeden Fall ist in das Grundrecht der Eltern eingegriffen worden, da wegen der engen familienrechtlichen und psychischen Bindungen zwischen Kind und Eltern Angaben über Gründe des Freitodes in dem Abschiedsbrief des Sohnes zugleich auch personenbezogene Daten der Eltern sind oder Rückschlüsse auf solche Daten zulassen (unten D.2.b). Schließlich ist, sofern überhaupt im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts zum Schutz der Menschenwürde und zum Recht auf freie Entfaltung der Persönlichkeit ein bundesrechtliches Gewohnheitsrecht auf Akteneinsicht Geltung beanspruchen kann, im Fall dieses Bürgers kein berechtigtes Interesse des Versicherungsunternehmens erkennbar, da der Bürger keinen Versicherungsanspruch geltend gemacht hatte. Die Angelegenheit ist noch nicht abgeschlossen.

In einer anderen Eingabe bat ein Bürger um Auskunft darüber, ob er die Löschung des Hinweises auf das gegen ihn geführte, dann aber eingestellte Ermittlungsverfahren in der **Zentralnamenkartei** einer Staatsanwaltschaft verlangen könne. Ich mußte dem Bürger mitteilen, daß ein solcher Anspruch nicht besteht.

Die materiellen Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen finden auf die Behörden der Staatsanwaltschaft nur Anwendung, wenn diese Verwaltungsaufgaben erledigen. Das ist bei einer solchen Zentralnamenkartei nicht der Fall. Sie dient der Wiederauffindung der Ermittlungsakten und damit der Strafrechtspflege. Auch die Vorschriften des Bundesdatenschutzgesetzes über die Löschung auf Verlangen des Betroffenen (§ 14 Abs. 3 Satz 2) finden keine Anwendung, da es sich um ein internes, manuell geführtes Aktenregister handelt; eine Auskunfterteilung an Dritte findet nicht statt (§ 1 Abs. 2 Satz 2 BDSG).

Eine Verletzung anderer Vorschriften über den Datenschutz, wie etwa Artikel 4 Abs. 2 LV, war nicht erkennbar. Nach der Strafprozeßordnung hindert der Einstellungsbescheid die Staatsanwaltschaft nicht daran, das Verfahren bis zum Ablauf der Verfolgungsverjährung wiederaufzunehmen, wenn Anlaß dazu besteht. Aus diesem Grund ist die Aufbewahrung der Akten des Ermittlungsverfahrens (und zu deren Wiederauffindung die Registrierung des Namens des Beschuldigten in der Zentralnamenkartei) erforderlich. Die Regelungen der Strafprozeßordnung gehen als Bundesrecht den Vorschriften der Landesverfassung vor.

b) MiStra und RiStBV

In der Anordnung über **Mitteilungen in Strafsachen** (MiStra) in der Fassung vom 15. November 1977 wird bestimmt, unter welchen Voraussetzungen, in welchem Umfang und zu welchen Zeitpunkten andere Behörden über Strafverfahren zu unterrichten sind.

Da es sich hierbei um die Übermittlung personenbezogener Daten handelt und jede Übermittlung ein Eingriff in das Grundrecht auf Datenschutz ist, bedarf eine derartige Anordnung einer gesetzlichen Grundlage. Eine solche ist nicht erkennbar.

Der Bundesbeauftragte für den Datenschutz hat eine Überarbeitung der MiStra angeregt. In einer Stellungnahme zu dieser Anregung wird ausgeführt, die durch das Strafrecht und das Strafverfahrensrecht garantierte Friedensordnung können nur bestehen, wenn „das Strafrecht und die an die Begehung von Straftaten geknüpften Rechtsfolgen in anderen Bereichen der öffentlichen Verwaltung in einem effektiven Verfahren durchgesetzt werden". Mit dem Bundesbeauftragten bin ich der Auffassung, daß hierüber der Gesetzgeber zu entscheiden hat. Eine solche „Verlängerung" der Wirkungen des Strafrechts bedarf jeweils einer besonderen Begründung, für die der Gesetzgeber die Verantwortung übernehmen muß.

Bei der Überarbeitung der MiStra ist zu prüfen, ob die darin vorgesehenen Mitteilungspflichten zur Erfüllung der Aufgaben der Empfänger in jedem Fall erforderlich sind. Zwei Beispiele mögen die Notwendigkeit einer Einschränkung verdeutlichen:

- Nach Nr. 12a MiStra ist der zuständigen Verwaltungsbehörde (Wahlamt) die Urteilsformel mitzuteilen, wenn sich aus dem Urteil Konsequenzen für die Wahlberechtigung des Betroffenen ergeben. Für die Prüfung der Frage, ob eine Person das aktive oder passive Wahlrecht besitzt, ist aber nur die Information von Bedeutung, ob ein Ausschlußgrund vorliegt. Die Angabe des Grundes der Verurteilung ist nicht erforderlich.
- Nach Nr. 28 MiStra sind in Strafsachen gegen Studierende die Entscheidungen der jeweiligen Ausbildungsstätte mitzuteilen. Das Ordnungsrecht der Universitäten sieht aber nur in wenigen Fällen Sanktionen gegen Studierende vor, die sich strafbar gemacht haben. Die Mitteilungspflicht sollte deshalb entsprechend eingeschränkt werden, sofern sie nicht überhaupt entfallen kann.

Die MiStra beruht auf einer Vereinbarung der Justizminister des Bundes und der Länder. Sie kann deshalb auch nur bundeseinheitlich geändert werden. Die Datenschutzbeauftragten des Bundes und der Länder haben eine Arbeitsgruppe mit dem Ziel gebildet, die nach der MiStra vorgesehenen Datenflüsse daraufhin zu überprüfen, ob sie überhaupt oder in dem vorgesehenen Umfang erforderlich sind.

Das Recht auf **Akteneinsicht** ist, soweit gesetzlich nichts anderes bestimmt ist, in den Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) vom 1. Januar 1977 geregelt. Der Bundesminister der Justiz hat auf Anregung des Bundesbeauftragten für den Datenschutz Vorschläge für eine Verbesserung des Akteneinsichtsrechts erarbeitet. Ich begrüße diese Vorschläge als einen weiteren Schritt in Richtung auf mehr Bürgernähe und Transparenz.

Nr. 187 Abs. 1 RiStBV sieht vor, daß die Akteneinsicht auf einzelne Aktenteile beschränkt werden kann, wenn dadurch die Bloßstellung einer Privatperson vermieden werden kann. Ich begrüße, daß der Bundesminister der Justiz die Anregung des Bundesbeauftragten aufgegriffen hat, diese Kann-Vorschrift durch eine Soll-Vorschrift zu ersetzen. Dadurch wird schutzwürdigen Belangen Dritter stärker als bisher Rechnung getragen. Dabei sollte jedoch die Formulierung „Bloßstellung einer Privatperson" dem heutigen Datenschutzverständnis entsprechend durch den weitergehenden Begriff „Beeinträchtigung schutzwürdiger Belange Dritter" ersetzt werden.

Darüber hinaus habe ich vorgeschlagen, die Akteneinsichtsmöglichkeiten des Angeklagten zu erweitern. Zwar gibt § 147 Abs. 1 StPO nur dem Verteidiger, nicht aber dem Angeklagten ein Recht auf Akteneinsicht. Der enge, ganz auf die Rechte des Verteidigers abgestellte Wortlaut dieser Vorschrift schließt jedoch nach meiner Auffassung eine weitergehende Regelung zugunsten des Betroffenen während der Dauer des Verfahrens genausowenig aus, wie er eine Akteneinsicht nach Abschluß des Verfahrens verbietet. Jedenfalls dem Angeklagten, der keinen Verteidiger hat, sollte Akteneinsicht auch während der Dauer des Verfahrens gewährt werden.

Damit würde dem allgemeinen Rechtsgedanken des Zugangs zu den eigenen Daten Rechnung getragen, der in Artikel 1 Abs. 1 und Artikel 2 Abs. 1 GG sowie in dem Anspruch auf rechtliches Gehör (Artikel 103 Abs. 1 GG) wurzelt und in dem Auskunftsrecht des Betroffenen nach § 13 BDSG/§ 16 DSG NW seinen Ausdruck gefunden hat. Mit diesem Rechtsgedanken ist es nicht vereinbar, den Betroffenen von der Akteneinsicht auszuschließen und ihn auf die Akteneinsichtsmöglichkeit eines Anwalts zu verweisen.

Etwaigen Mißbräuchen bei der Akteneinsicht durch den Angeklagten könnte dadurch begegnet werden, daß ihm die Akten in den Diensträumen der Staatsanwaltschaft oder des Gerichts im Beisein eines Bediensteten vorgelegt werden. Darüber hinaus kann die Akteneinsicht durch den Angeklagten von den gleichen Voraussetzungen abhängig gemacht werden, wie die Akteneinsicht eines Rechtsanwalts oder Rechtsbeistands.

c) Ordnungswidrigkeitenverfahren

Im Kreise der Datenschutzbeauftragten wurde die Frage erörtert, inwieweit sich das neue Datenschutzrecht auf die Sammlung von Daten aus Ordnungswidrigkeitsverfahren bei den Verwaltungsbehörden auswirkt. Insbesondere geht es um die Zulässigkeit der Erhebung und karteimäßigen Erfassung von „Mehrfachtätern". Soweit diese bejaht wird, muß die Sperrung und vor allem die Löschung solcher Daten geregelt und auch regelmäßig durchgeführt werden. Es wird zur Zeit geprüft, ob eine einheitliche Regelung dieser Fragen getroffen werden kann.

d) Schuldnerverzeichnis

Nach § 915 ZPO wird bei den Amtsgerichten ein Schuldnerverzeichnis geführt, in das die Personen eingetragen werden, die die eidesstattliche Versicherung über ihre Vermögenslage (§ 807 ZPO) abgegeben haben oder gegen die Haft zur Abgabe der eidesstattlichen Versicherung angeordnet wurde. Aus diesem Verzeichnis können nach den Allgemeinen Vorschriften über die Erteilung und die Entnahme von Abschriften oder Auszügen aus dem Schuldnerverzeichnis (AV) vom 1. August 1955 Rechtsanwaltskammern, Industrie- und Handelskammern und gleichartige Berufsvertretungen sowie andere vertrauenswürdige Körperschaften, Personen oder Unternehmen vollständige Abschriften erhalten. Die Berufsvertretungen können außerdem ihren Mitgliedern Listen über die in das Schuldnerverzeichnis eingetragenen Personen zur Verfügung stellen. Alle, die eine Abschrift aus dem Schuldnerverzeichnis erhalten haben, sind dazu verpflichtet, die Angaben nach Ablauf bestimmter Fristen zu löschen, da auch die Eintragung im Schuldnerverzeichnis nach Ablauf einer gewissen Zeit gelöscht wird.

Da der Kreis, der eine Abschrift aus dem Verzeichnis erhält, sehr groß ist, findet kaum eine Kontrolle der Einhaltung der Löschungsfristen statt. Dies widerspricht jedoch den Grundsätzen der Datenschutzgesetze. Aus diesem Grunde haben die Datenschutzbeauftragten des Bundes und der Länder einen gemeinsamen Änderungsvorschlag erarbeitet und dem Bundesminister der Justiz unterbreitet. Ich begrüße es, daß der Bundesminister der Justiz diesen Änderungsvorschlag aufgegriffen hat.

In meiner Stellungnahme gegenüber dem Justizminister des Landes Nordrhein-Westfalen habe ich die Ansicht vertreten, daß die Erteilung von Abschriften an die nicht zu den öffentlich-rechtlichen Berufsvertretungen gehörenden vertrauenswürdigen Körperschaften, Personen und Unternehmen (§ 1 Abs. 2 AV) aus datenschutzrechtlicher Sicht nicht zu beanstanden sein dürfte, da sie nur im Einzelfall vertrauliche Auskünfte erteilen dürfen (§ 3 Abs. 1 Satz 1 AV). Allerdings sollte erwogen werden, die Höchstdauer von 5 Jahren auf 3 Jahre zu verkürzen, um eine wirksamere Kontrolle zu gewährleisten.

Gegen die den öffentlich-rechtlichen Berufsvertretungen zuerkannten Befugnisse, die Abschriften aus den Schuldnerverzeichnissen ihren Mitgliedern zugänglich zu machen (§ 4 ff AV), bestehen dagegen erhebliche Bedenken. Ich habe Zweifel, ob diese Bestimmungen mit dem sich aus Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG ergebenden Recht des Bürgers auf Schutz seiner personenbezogenen Daten vereinbar ist, und

zwar insbesondere deshalb, weil bei einem so großen Empfängerkreis nicht gewährleistet ist, daß die Löschungsauflagen erfüllt und die Unterlagen nicht zum Nachteil der Betroffenen über die vorgesehenen Fristen hinaus genutzt werden. Hier stehen das Bedürfnis der Wirtschaft, sich schnell über die wirtschaftlichen Verhältnisse eines Vertragspartners zu informieren, und der Datenschutz nicht in dem erforderlichen ausgewogenen Verhältnis. Eine datenschutzrechtlich vertretbare Lösung kann dadurch erreicht werden, daß die öffentlich-rechtlichen Berufsvertretungen wie die anderen Empfänger von Abschriften des Schuldnerverzeichnisses auf die Erteilung von Einzelauskünften beschränkt werden.

e) Grundbuchwesen

Die Grundbuchordnung enthält in den §§ 12 und 55 Vorschriften über die Übermittlung von personenbezogenen Daten, und zwar über die Einsichtnahme in das Grundbuch, die Erteilung von Auszügen aus dem Grundbuch und die Fertigung von Urkundsabschriften sowie über die Bekanntmachung von Grundbucheintragungen.

Wenn auch diese bereichsspezifischen Datenschutzregelungen den Bestimmungen der Datenschutzgesetze des Bundes und der Länder vorgehen, so bin ich doch mit dem Bundesbeauftragten für den Datenschutz der Meinung, daß vor diesem Bereich die Datenschutzdiskussion nicht haltmachen, sondern kritische Anstöße zu überkommenen Vorschriften und Verfahrensweisen geben sollte. So kann es aus der Sicht des Datenschutzes durchaus nicht gleichgültig sein, in welchem Umfang Auszüge oder Abschriften erteilt werden.

Ich werde diesen Bereich zusammen mit den anderen Datenschutzbeauftragten im Auge behalten.

f) Gesetz über die Prozeßkostenhilfe

In dem Verfahren zur Entscheidung über die Gewährung von Prozeßkostenhilfe nach dem vom Deutschen Bundestag beschlossenen neuen Gesetz über die Prozeßkostenhilfe werden Daten über die persönlichen und wirtschaftlichen Verhältnisse der beantragenden Partei sehr weitgehend offengelegt. Die betroffene Partei kann aber ein erhebliches Interesse daran haben, daß den übrigen Prozeßparteien die von ihr gemachten Angaben nicht bekannt werden.

Mit dem Bundesbeauftragten für den Datenschutz bin ich der Ansicht, daß die in dem Verfahren zur Entscheidung über die Prozeßkostenhilfe anfallenden Daten grundsätzlich nicht in der Prozeßakte, sondern in einer Beiakte, die den Prozeßparteien nicht zugänglich ist, festgehalten werden sollten. Dies ist auch deshalb durchführbar, weil das Verfahren zur Bewilligung der Prozeßkostenhilfe durch eine gewisse Selbständigkeit gekennzeichnet ist (z. B. Bewilligung der Prozeßkostenhilfe in jedem Rechtszug gesondert).

Ich habe dem Justizminister meine Auffassung zur Kenntnis gebracht.

g) Änderung der Verfahrensordnung für Höfesachen

Die Höfeordnung knüpft seit der am 1. Juli 1976 in Kraft getretenen Gesetzesänderung bei der Frage, ob eine land- und forstwirtschaftliche Besitzung Hof ist, werden oder bleiben kann, an den Wirtschaftswert an und macht den Erwerb der Hofeigenschaft von einem Mindestwirtschaftswert von 10.000 DM abhängig. Auf Grund der vorgenannten Gesetzesänderung ist für die Zukunft sicherzustellen, daß die im Grundbuch eingetragenen Hofvermerke den tatsächlichen Rechtszustand wiedergeben. Hierbei handelt es sich um die Fälle, in denen der Wirtschaftswert unter 10.000 DM sinkt oder auf mindestens 20.000 DM ansteigt. In diesen Fällen hat das Landwirtschaftsgericht nach § 3 Abs. 1 Nr. 1 der Verfahrensordnung für Höfesachen (Höfe VfO) von Amts wegen die Löschung oder die Eintragung des Hofvermerks zu veranlassen.

In diesem Zusammenhang hat der Justizminister des Landes Nordrhein-Westfalen an mich die Frage gerichtet, ob datenschutzrechtliche Bedenken dagegen bestünden, gesetzlich eine begrenzte Mitteilungspflicht der Finanzämter gegenüber den Landwirtschaftsgerichten über festgestellte Wirtschaftswerte zu begründen.

Gegen die angestrebte Novellierung der Höfe VfO bestehen aus dem Gesichtspunkt des Datenschutzes keine Bedenken.

Nach den datenschutzrechtlichen Grundsätzen, die der Gesetzgeber in § 10 Abs. 1 Satz 1 BDSG und in § 11 Abs. 1 Satz 1 DSG NW zum Ausdruck gebracht hat, ist eine Datenübermittlung im öffentlichen Bereich dann gerechtfertigt, wenn die Kenntnis der Daten für den Empfänger zur rechtmäßigen Erfüllung seiner Aufgaben erforderlich ist. An die Voraussetzung der Erforderlichkeit sind allerdings im Interesse des Datenschutzes strenge Anforderungen zu stellen. Der Behörde muß es unmöglich sein, ohne die Kenntnis der ihr übermittelten Daten ihre Aufgabe zu erfüllen. Der Erforderlichkeit steht jedoch nicht entgegen, daß die benötigten Angaben auch vom Betroffenen erfragt oder von dritter Seite erlangt werden können. Die mit den Datenschutzgesetzen vom Gesetzgeber bereits getroffenen Regelungen dienen vielmehr gerade dazu, Mehrfacherhebungen zu vermeiden (Dammann in Simitis/Dammann/Mallmann/Reh, BDSG, § 10 Rdnr. 12; Ruckriegel in Ruckriegel/v. d. Groeben/Hunsche, Datenschutz und Datenverarbeitung in Nordrhein-Westfalen, § 11 Anm. 4).

Die vorgeschlagene begrenzte Mitteilungspflicht der Finanzämter steht mit diesen Grundsätzen im Einklang. Denn das Landwirtschaftsgericht ist zur Erfüllung seiner Aufgabe nach § 3 Abs. 1 Nr. 1 Höfe VfO auf die Kenntnis der von den Finanzämtern festgestellten Wirtschaftswerte angewiesen.

Der Grundsatz der Verhältnismäßigkeit ist ebenfalls gewahrt. Wegen der erheblichen Rechtsfolgen, die mit der Hofeigenschaft verbunden sind, überwiegt das öffentliche Interesse an der Rechtsklarheit hinsichtlich der Hofeigenschaft gegenüber dem Interesse des Betroffenen, die Datenübermittlung vom Finanzamt zum Landwirtschaftsgericht zu beschränken.

9. Sozialwesen

a) Sozialhilfe

Im Bereich der Sozialverwaltung werden besonders empfindliche personenbezogene Daten in großer Zahl verarbeitet. Der Einhaltung und Kontrolle datenschutzrechtlicher Bestimmungen in diesem Bereich kommt daher erhebliche Bedeutung zu. Ein konsequenter Datenschutz muß hier nicht nur der unzulässigen Übermittlung, sondern jeder Zweckentfremdung der Daten entgegenwirken.

Dies gilt selbst dann, wenn der Zugriff auf die personenbezogenen Angaben in billigenswerter Absicht erfolgt. Deshalb habe ich den Mitarbeiter einer Sozialbehörde, der die ihm aus dienstlicher Tätigkeit bekannten Anschriften von Sozialhilfeempfängerinnen ohne Zustimmung seiner Dienststelle für die Einladung zur Gründung einer Selbsthilfegruppe verwendet hat, darauf hingewiesen, daß er das Datengeheimnis (§ 5 Abs. 1 DSG NW) verletzt habe.

Da der Mitarbeiter der Sozialbehörde die Anschriften der Sozialhilfeempfängerinnen zu einem Zweck genutzt hat, der nicht zu den ihm übertragenen Aufgaben gehörte, und die Nutzung im übrigen unbefugt war, habe ich ihm empfohlen, sich bei ähnlichen Aktionen zunächst um die Zustimmung seiner Dienststelle zu bemühen, die hierbei allerdings schutzwürdige Belange der Betroffenen zu beachten hat (§ 13 Abs. 1 DSG NW).

Durch eine andere Sozialbehörde habe ich erfahren, daß Überleitungsanzeigen nach § 90 BSHG sowie Mitteilungen nach § 91 Abs. 2 BSHG bislang auch durch Aushängen am Schwarzen Brett öffentlich zugestellt worden sind.

Gegen diese Praxis bestehen datenschutzrechtliche Bedenken. Der Sozialhilfeempfänger und der Unterhaltspflichtige haben nach § 35 Abs. 1 Satz 1 SGB I, der als Bundesrecht dem Datenschutzgesetz Nordrhein-Westfalen vorgeht, einen Anspruch darauf, daß ihre Geheimnisse von den Leistungsträgern nicht unbefugt offenbart werden (Sozialgeheimnis). Eine Offenbarung ist dann nicht unbefugt, wenn der Betroffene zustimmt oder eine gesetzliche Mitteilungspflicht besteht (§ 35 Abs. 1 Satz 2 SGB I).

Da diese Voraussetzungen hier nicht vorliegen, verstößt die öffentliche Zustellung von Überleitungsanzeigen nach § 90 BSHG sowie von Mitteilungen nach § 91 Abs. 2 BSHG durch Aushängen an der von der Behörde hierfür allgemein bestimmten Stelle, zum Beispiel am Schwarzen Brett (§ 15 Abs. 2 Satz 1 VwZG), gegen das Sozialgeheimnis.

Aus datenschutzrechtlicher Sicht unbedenklich ist demgegenüber die in § 15 Abs. 2 Satz 2 VwZG vorgesehene Möglichkeit, eine Benachrichtigung auszuhängen, in der allgemein angegeben ist, daß und wo das Schriftstück eingesehen werden kann. Eine derartige allgemeingehaltene Benachrichtigung hat sich jedoch auf „Elementartatsachen" wie Name und Anschrift des Unterhaltspflichtigen sowie auf neutrale Hinweise zu beschränken, die ihm die Einsichtnahme des Schriftstücks ermöglichen.

Ich habe die Sozialbehörde gebeten, künftig entsprechend zu verfahren und insbesondere darauf zu achten, daß die Benachrichtigung keine Tatsachen enthält, die Rückschlüsse auf die Unterhaltspflicht des Adressaten oder auf die Person des Sozialhilfeempfängers zulassen. Gleichzeitig habe ich den Minister für Arbeit, Gesundheit und Soziales gebeten, durch Runderlaß sicherzustellen, daß die Sozialämter in Nordrhein-Westfalen einheitlich im Sinne meiner Rechtsauffassung verfahren.

b) Sozialversicherung

Der weite Bereich der Sozialversicherung, in dem höchst sensible Daten fast aller Bürger gespeichert und ausgetauscht werden, erfordert die besondere Aufmerksamkeit des Landesbeauftragten. Deshalb habe ich meinen ersten umfassenden **Kontrollbesuch** nach § 26 Abs. 1 Satz 1 DSG NW bei einer Allgemeinen Ortskrankenkasse (AOK) durchgeführt.

Inhaltliche Schwerpunkte meines Kontrollbesuchs waren vor allem die Datenverarbeitung und die Maßnahmen zur Datensicherung. Dabei ergab sich eine Anzahl von Mängeln. Wege zu deren Behebung wurden schon während des Kontrollbesuchs mit dem Geschäftsführer und den Mitarbeitern der AOK, insbesondere mit dem Datenschutzbeauftragten erörtert.

Die Arbeiten des Rechenzentrums werden durch Mitarbeiter der AOK in einem privaten Dienstleistungs-Rechenzentrum abgewickelt. Die dort installierte Datenverarbeitungsanlage wird dabei gemeinsam mit einem anderen Kunden genutzt.

Gleichwohl ist die AOK der Ansicht, sie betreibe ein eigenes Rechenzentrum. Sie beruft sich dabei vor allem darauf, daß die Abwicklung der AOK-Arbeiten durch AOK-Maschinenbediener von einem getrennten Bedienungsblattschreiber erfolgt.

Im Hinblick auf die Sensibilität der verarbeiteten Daten habe ich gegen diese Organisationsform des Rechenzentrumsbetriebes erhebliche Bedenken. Von der AOK wird zwar darauf hingewiesen, sie habe bereits im Dezember 1979 einen neuen Mietvertrag abgeschlossen, nach dem eine eigene Anlage in den Räumen der AOK installiert werden soll. Diese neue Anlage wird aber nicht vor Ende 1980 geliefert werden. Mindestens bis zu diesem Zeitpunkt werden daher die Daten in einem fremden Rechenzentrum verarbeitet.

Der Ansicht der AOK, es werde lediglich in fremden Räumen eine eigene Anlage der AOK betrieben, kann ich nicht folgen. Jedenfalls soweit im Rahmen der Anlagennutzung Arbei-

ten durch das private Dienstleistungs-Rechenzentrum im Auftrag der AOK erledigt werden und soweit die AOK keinen unmittelbaren Einfluß auf die Datensicherung hat, liegt Auftragsdatenverarbeitung nach § 7 Abs. 1 DSG NW vor.

Die rechtliche Situation bedarf dringend der Klärung. Dabei ist jedenfalls festzulegen, daß das private Dienstleistungs-Rechenzentrum, soweit es im Auftrag der AOK bei der Verarbeitung personenbezogener Daten tätig wird, sich zur Beachtung der Bestimmungen des Datenschutzgesetzes Nordrhein-Westfalen verpflichtet und sich der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft (§ 7 Abs. 1 Satz 2 DSG NW).

Bedenken mußte ich auch bezüglich einer Reihe weiterer Sachverhalte geltend machen:

- Die Sicherung des Datenarchivs entsprach nicht ganz den Anforderungen, die bei der Empfindlichkeit der gespeicherten Daten zu stellen sind. Der AOK wurden Maßnahmen empfohlen, um die Sicherheit zu verbessern.
- Ein Verbot der Mitnahme von Mänteln und Taschen in das Rechenzentrum besteht nicht. Ich habe empfohlen, möglichst umgehend Gespräche mit dem privaten Dienstleistungs-Rechenzentrum aufzunehmen mit dem Ziel, hinreichende Verbesserungen einzuführen.
- Das Musterformular, das die AOK für die Übersicht über die bei ihr gespeicherten Daten verwendet, entspricht zwar im wesentlichen den Anforderungen des § 8 Satz 2 Nr. 1 DSG NW. Allerdings werden — vermutlich in Anlehnung an den insoweit engeren § 15 BDSG — nur Stellen erfaßt, an die personenbezogene Daten regelmäßig übermittelt werden. Die AOK wurde darauf hingewiesen, daß nach § 8 Satz 2 Nr. 1 DSG NW die Übersicht sich auf alle Datenempfänger (nicht nur die regelmäßigen) erstreckt. Ich habe der AOK eine entsprechende Erweiterung des Formulars und der Eintragungen empfohlen.
- Die Dateien selbst sind in einigen Fällen zu allgemein beschrieben. Dies gilt insbesondere für die Aufgaben, zu deren Erfüllung die Kenntnis der gespeicherten Daten erforderlich ist. Ich habe der AOK empfohlen, die entsprechenden Aufgabenbeschreibungen zu konkretisieren.
- Es ist dringend erforderlich, daß der Datenschutzbeauftragte der AOK seine Prüftätigkeit wesentlich erweitert und darin insbesondere allgemeine Fragen der Einhaltung von Organisationsanweisungen auf dem Gebiet der ADV einbezieht.
- Die ADV ist einem Fachbereich zugeordnet. Ich habe der AOK empfohlen zu prüfen, ob zur Gewährleistung der erforderlichen Unabhängigkeit eine direkte Zuordnung zum Geschäftsführer möglich ist.
- Programmtests, die bei der AOK selbst durchgeführt werden und nur unter Verwendung von echten Daten erfolgen können, werden ohne Anonymisierung dieser Daten durchgeführt. Durch Dienstanweisung sollte umgehend festgelegt werden, daß Programmtests mit echten Daten nur nach deren Anonymisierung erfolgen dürfen.
- Die Freigabe eines Programmes sollte nicht nur durch den Leiter der zuständigen Fachabteilung erfolgen. Vielmehr sollte auch der Datenschutzbeauftragte die datenschutzmäßige Unbedenklichkeit bestätigen. Hier besteht zur Zeit eine Verantwortungslücke, da eine entsprechende Regelung nicht vorhanden ist. Der AOK wurde empfohlen, durch Dienstanweisung umgehend eine derartige Regelung einzuführen.
- Bei der AOK sind Bildschirme ohne Zugangsbeschränkung frei zugänglich in den Arbeitsräumen aufgestellt. Es gibt lediglich eine interne Anweisung, daß nur Mitarbeiter mit bestimmter Funktion den Bildschirm benutzen dürfen. Damit erscheint jedoch keinesfalls gesichert, daß der Zugang Unbefugter zu den Bildschirmgeräten immer unmöglich ist. Ich habe daher auf die Notwendigkeit hingewiesen, einen allgemeinen Schutz der Bildschirme — etwa über die Programme — zu realisieren.

- Alle Mitarbeiter, die befugt sind, einen Bildschirm zu benutzen, sind insoweit grundsätzlich gleichberechtigt. Eine Ausnahme besteht lediglich für die Versicherungsdaten der Angestellten des eigenen Hauses. Hier gibt es nur einzelne Mitarbeiter, die über ein spezielles Kodewort den Zugriff erhalten. Das Kodewort wurde in seinem Aufbau allerdings unglücklich gewählt, so daß der dadurch erreichte Schutz nur sehr gering ist. Hier muß kurzfristig durch neue Kodeworte der notwendige Schutz gewährleistet werden.

- Nicht in diesen besonderen Schutz sind zur Zeit die Daten der freiwilligen Mitglieder aus dem Hause einbezogen. Deren persönliche Daten können daher von jedem Mitarbeiter abgefragt werden. Eine Änderung dieser Situation ist beabsichtigt. Da das Programm jedoch nicht von der AOK entwickelt wurde, ist es fraglich, ob die Änderung eingeführt wird. Für den Fall, daß die Sicherung programmtechnisch nicht verwirklicht werden kann, habe ich empfohlen, die freiwilligen Mitglieder wieder aus der ADV-Bearbeitung herauszunehmen.

- Im Rahmen der Zugriffsbeschränkungen sollten weitere Abschottungen vorgenommen werden. Insbesondere ist nicht einzusehen, warum Mitarbeiter des Beitragswesens unbeschränkt Zugang zu den Leistungsdaten der ADV-Datei haben. Die AOK erkennt das Problem. Sie sieht aber die Schwierigkeit, daß sie die Entwicklung und Änderung des Programms nicht selbst in der Hand hat. Ich habe dringend empfohlen, bei den entwickelnden Stellen darauf hinzuwirken, daß das Programm entsprechend ergänzt wird.

- Ein Datenaustausch über Magnetband findet mit verschiedenen Stellen statt. So werden DÜVO-Daten ausgetauscht; durch Weitergabe von Magnetbändern an die Kreissparkasse oder das Postscheckamt werden Zahlungen und durch Datenverarbeitung im Auftrag von einer kommunalen Datenverarbeitungszentrale Gehälter angewiesen. Die Datenträger sind beim Austausch durch Koffer gesichert, von denen je ein Schlüssel bei der absendenden und bei der annehmenden Stelle vorhanden ist.

  Nach Erledigung der Arbeit werden die Magnetbänder an den jeweiligen Absender zurückgesandt. Ein Löschen der Magnetbänder vor Rücksendung erfolgt nicht. Auf diese Weise entsteht bei der Rücksendung der Magnetbänder ein durchaus vermeidbares Transportrisiko.

  Die geschilderte Praxis kann nicht hingenommen werden. Ich habe die AOK aufgefordert, ab sofort nur gelöschte Magnetbänder zurückzusenden und auf ihre Partner erneut einzuwirken, ebenso zu verfahren.

- Die verwendeten Magnetbänder enthalten nur teilweise maschinenlesbare Dateietiketten. Insbesondere die Bänder für die Mitgliederbestandsführung und für das Leistungswesen enthalten derartige Etiketten nicht. Dadurch ist die Sicherheit der Verarbeitung deutlich eingeschränkt. Eine Änderung setzt allerdings die Modifikation von Programmen voraus, die nicht von der AOK selbst entwickelt wurden. Ich habe die AOK daher aufgefordert, mit Nachdruck darauf hinzuwirken, daß die Programme entsprechend geändert werden.

- Seit dem 1. Januar 1978 gilt bei der AOK eine Besondere Dienstanweisung für den Einsatz der automatischen Datenverarbeitung. Deren Regelungen sind grundsätzlich zu begrüßen. Ich habe jedoch insbesondere folgende Änderungen vorgeschlagen:

  Es sollte eindeutig zum Ausdruck gebracht werden, daß die zuständige Fachabteilung als „Herr der Daten" die volle Verantwortung für ihre Dateien trägt. Für die Maschinenbedienung sollten wegen der Sensibilität der verarbeiteten Daten keine Ausnahme von dem Vier-Augen-Prinzip zugelassen werden. Ferner sollten für die Maschinenbedienung aus Gründen der Sicherheit der Verarbeitung mündliche Bedienungsanweisungen nicht zugelassen werden.

Besonders begrüßt habe ich die Tatsache, daß bereits eine erste Ausbildung von Mitarbeitern des Datenschutzbeauftragten auf dem ADV-Sektor erfolgt ist. Eine Erweiterung des ADV-Wissens wäre sehr wünschenswert und wird von der AOK angestrebt. Darüber hinaus befürworte ich Überlegungen der AOK, Mitarbeiter des Datenschutzbeauftragten zeitweise in der ADV-Abteilung und hier insbesondere im Bereich des Rechenzentrums mitarbeiten zu lassen.

Der Kontrollbesuch bei der AOK hat mir insgesamt den Eindruck vermittelt, daß der Datenschutz im Bereich der Sozialversicherung verbesserungsbedürftig ist.

Auch mehrere **Eingaben von Bürgern** deuten auf ein wachsendes Bewußtsein der Notwendigkeit des Datenschutzes auf diesem immer stärker von der Automatisierung durchdrungenen Gebiet hin.

Einige Bürger haben ihren Unmut darüber geäußert, daß eine AOK, bei der sie nicht versichert sind, ihnen unter Verwendung ihrer Sozialversicherungsdaten Werbeschreiben übersandt hat.

Der Zugriff auf die Sozialversicherungsdaten von Nichtmitgliedern war der Krankenkasse möglich, weil nach dem durch die Datenerfassungsverordnung (DEVO) vom 24. November 1972 (BGBl. I 2159) und durch die Datenübermittlungsverordnung (DÜVO) vom 18. Dezember 1972 (BGBl. I 2482) bundeseinheitlich geregelten Meldeverfahren zur gesetzlichen Sozialversicherung die Krankenkassen Empfänger der vom Arbeitgeber zu erstattenden Meldungen über die Beitragspflicht des Arbeitnehmers zur Sozialversicherung sind.

Gleichwohl ist die Nutzung dieser Daten zur Mitgliederwerbung datenschutzrechtlich unzulässig. Sie widerspricht dem Grundsatz der Zweckbindung und stellt überdies eine unbefugte Offenbarung von Geheimnissen Sozialversicherter dar.

§ 35 Abs. 1 SGB I schützt die Geheimnisse der Versicherten auch innerhalb der öffentlichen Stelle, die der Geheimnispflicht unterliegt. Da in den genannten Fällen weder eine Zustimmung der Betroffenen noch eine gesetzliche Mitteilungspflicht vorlag (§ 35 Abs. 1 Satz 2 SGB I), hat die Ortskrankenkasse durch die Verwendung der im Zuge des DEVO-DÜVO-Datenflusses bei ihr gespeicherten Sozialversicherungsdaten für eine gezielte Mitgliederwerbung gegen das Sozialgeheimnis verstoßen. Von einer förmlichen Beanstandung habe ich indessen abgesehen, nachdem die Krankenkasse schon vor meiner Einschaltung von sich aus die Versendung von Werbeschreiben an Nichtmitglieder eingestellt hatte.

Ein anderer Bürger, dem von einer Privatfirma Werbematerial und eine Bestellkarte für einen Pulsmeßcomputer übersandt worden war, hat mir mitgeteilt, er habe den Verdacht, daß seine Anschrift von Ärzten oder von seiner Sozialversicherung an die Firma weitergegeben worden sei. Da der Einsender jedoch nicht in der Lage war, Hinweise auf die Informanten der Versandfirma zu geben und Tatsachen zu benennen, die seinen Verdacht stützen, habe ich keine Möglichkeit gesehen, der Sache nachzugehen. Ich konnte den Betroffenen nur auf folgendes hinweisen.

Ärzte, sofern sie nicht Amtsärzte sind, gehören nicht zu den öffentlichen Stellen, die nach § 26 Abs. 1 Satz 1 DSG NW meiner Kontrolle unterliegen. Sie sind natürliche Personen, deren Datenverarbeitung nach § 30 BDSG durch die für den Ort ihrer Niederlassung zuständige Aufsichtsbehörde überwacht wird.

Sollte die Anschrift des Bürgers von einem der Aufsicht des Landes Nordrhein-Westfalen unterliegenden Sozialversicherungsträger an die Versandfirma gelangt sein, so wäre diese Übermittlung von Name, Anschrift und Versichertenstatus ein Verstoß gegen das Sozialgeheimnis, da weder seine Zustimmung vorlag noch eine gesetzliche Mitteilungspflicht bestanden hat (§ 35 Abs. 1 SGB I).

c) Jugendwesen

Auf dem Gebiet des Jugendwesens war ich insbesondere mit der datenschutzrechtlichen Überprüfung der Jahreserhebung der Erziehungsberatungsstellen befaßt.

Die Jahreserhebung soll die im Jahre 1977 in Nordrhein-Westfalen eingeführte „Basisdokumentation" ersetzen, die wegen datenschutzrechtlicher Bedenken inzwischen wieder aufgegeben worden ist. Das vom Minister für Arbeit, Gesundheit und Soziales erarbeitete neue Erhebungsmuster gliedert sich in das Deckblatt und das eigentliche Erhebungsformular. Nur in dem Deckblatt werden personenbezogene Daten festgehalten; sie werden unmittelbar von dem in der Beratungsstelle erschienenen Jugendlichen oder von den ihn begleitenden Erziehungsberechtigten erfragt. Eine Übermittlung dieser Daten an Dritte findet nicht statt. Das Deckblatt verbleibt in der Beratungsstelle und wird dort in Akten unter Verschluß aufbewahrt.

Das Erhebungsformular selbst wird zur Aufbereitung an die Landschaftsverbände weitergeleitet. Es enthält keine Individualdaten, sondern lediglich typisierte Erhebungsmerkmale, deren Zuordnung zu einer bestimmten Person faktisch ausgeschlossen ist.

Ich habe unter diesen Voraussetzungen derzeit keine datenschutzrechtlichen Bedenken gegen die vorgesehene Jahreserhebung.

Weiterhin hat im Bereich des Jugendwesens ein Bürger, der sich nach erfolgreicher Anfechtung der Ehelichkeit eines Kindes vergeblich bemüht hatte, vom Jugendamt zwecks Geltendmachung zivilrechtlicher Ersatzansprüche gegen den Erzeuger dessen Namen und Anschrift zu erfahren, meinen Beistand erbeten.

Ich konnte ihn zur Sache nur darauf hinweisen, daß es sich bei den von ihm gewünschten Angaben aus den Unterlagen des Jugendamtes um personenbezogene Daten des Erzeugers handelt, die nach Artikel 4 Abs. 2 LV geschützt sind. Eine gesetzliche Grundlage, nach der das Jugendamt die Angaben übermitteln dürfte, ist nicht ersichtlich. Insbesondere kann eine Datenübermittlung hier nicht auf § 13 Abs. 1 Satz 1 DSG NW gestützt werden. Die Anwendung des Datenschutzgesetzes Nordrhein-Westfalen setzt voraus, daß Angaben aus einer Datei übermittelt werden sollen (§ 1 Abs. 2 Satz 1 DSG NW). Nach meinen Informationen werden bei den Jugendämtern in Nordrhein-Westfalen keine „Erzeuger"-Dateien geführt. Soweit Mündel-Dateien geführt werden, ist darin nicht der Name des Erzeugers verzeichnet. Ich bin deshalb davon ausgegangen, daß der Name des Erzeugers beim Jugendamt nicht in einer Datei gespeichert ist, sondern lediglich in einer Akte festgehalten wird.

Darüber hinaus würde § 13 Abs. 1 Satz 1 DSG NW hier auch deswegen keine Anwendung finden, weil § 35 SGB I als Bundesrecht vorgeht. Diese Vorschrift schützt den Erzeuger des Kindes gegen die unbefugte Offenbarung seiner Geheimnisse. Da weder die Zustimmung des Betroffenen noch eine gesetzliche Mitteilungspflicht vorlag und sich eine Befugnis zur Auskunftserteilung auch nicht aus dem Schutz höherrangiger Rechtsgüter herleiten läßt, hat das Jugendamt dem Einsender die gewünschte Auskunft zu Recht verweigert.

10. Gesundheitswesen

a) Blindendatei

Durch einen Hinweis des Niedersächsischen Datenschutzbeauftragten habe ich erfahren, daß die Firma Infratest-Gesundheitsforschung GmbH und Co, München, im Auftrag des Bundesministers für Forschung und Technologie eine Studie zur Darstellung und Analyse des Blindenwesens in der Bundesrepublik Deutschland durchführt. Die Untersuchung soll insbesondere Aufschluß über die derzeitige Versorgung der Blinden und Sehbehinderten mit Blindenhilfsmitteln geben. Die Firma Infratest-Gesundheitsforschung wird im Rahmen des ihr erteilten Auftrages eine repräsentative Umfrage bei Blinden und Sehbehinderten durchführen und will dabei auf die den Versorgungsstellen der Länder eingerichteten zentralen Blindendateien zurückgreifen.

In Nordrhein-Westfalen werden die zentralen Blindendateien bei den Landschaftsverbänden geführt, die nach § 7 des Landesblindengeldgesetzes für die Gewährung des Blindengeldes zuständig sind.

Nach dem Erhebungsplan der Firma Infratest-Gesundheitsforschung soll die Ziehung der Stichprobe in zwei Schritten erfolgen. Zunächst wird eine der eigentlichen Ziehung vorgeschaltete Strukturerhebung durchgeführt. Sie dient dazu, die Gesamtzahl, die Geschlechtsverteilung und die Altersverteilung der Sehgeschädigten in der Bundesrepublik Deutschland festzustellen. Auf einzelne Personen beziehbare Daten werden dabei nicht erhoben. An diese Vorabanalyse schließt sich die Ziehung der Stichprobe durch Zugriff auf die zentralen Blindendateien an. Aus dem Erhebungsplan geht nicht hervor, daß die Namen und Anschriften der dabei gezogenen Personen nur mit deren Zustimmung an die Firma Infratest-Gesundheitsforschung übermittelt werden sollen. Die zu befragenden Personen werden lediglich darauf hingewiesen, daß die Beteiligung an der Umfrage freiwillig ist.

Ich halte die Übermittlung der Namen und Anschriften von Blinden und Sehbehinderten an die Firma Infratest-Gesundheitsforschung ohne Zustimmung der Betroffenen für unzulässig. § 35 Abs. 1 SGB I schützt Geheimnisse, insbesondere die zum persönlichen Lebensbereich gehörenden Geheimnisse sowie die Betriebs- und Geschäftsgeheimnisse. Die unbefugte Offenbarung dieser Geheimnisse ist nach § 203 StGB strafbar.

Zwar sind in der Regel Name und Anschrift allein keine Geheimnisse im Sinne des § 35 SGB I. Unstreitig ist aber die Tatsache, daß eine bestimmte Person blind oder sehbehindert ist, ein solches Geheimnis. Dessen Offenbarung ist, da eine gesetzliche Mitteilungspflicht nicht besteht, unbefugt.

Da sich die Firma Infratest-Gesundheitsforschung gleichwohl auf die datenschutzrechtliche Unbedenklichkeit der Adressenübermittlung und eine diesbezügliche Abstimmung mit dem Bundesminister für Forschung und Technologie beruft, habe ich mich im Rahmen meiner Kontrollbefugnis nach § 26 Abs. 1 DSG NW unmittelbar bei den für die Führung der zentralen Blindendateien zuständigen Landschaftsverbänden nach dem Sachstand erkundigt, um einer drohenden Verletzung des Sozialgeheimnisses zu begegnen. Dabei hat sich herausgestellt, daß die zweite Phase der Studie, die eigentliche Ziehung der Stichprobe, noch aussteht. Sie soll, wie mir die zuständigen Referenten der Landschaftsverbände versichert haben, unter Wahrung datenschutzrechtlicher Belange wie folgt ablaufen.

Die gezogenen Personen werden zunächst mit einem Informationsschreiben über Sinn und Zweck der Studie unterrichtet. Dem Informationsschreiben wird eine vorbereitete Einverständniserklärung beigefügt mit der Bitte, diese, falls die Betroffenen das geplante Verfahren fördern und sich zu einem Interview zur Verfügung stellen wollen, unmittelbar an Infratest zurückzuschicken. Auf diese Weise wird sichergestellt, daß nicht die Landschaftsverbände Geheimnisse unbefugt offenbaren, sondern daß die Betroffenen selbst, nachdem sie über den Sinn und Zweck des Vorhabens und die Tragweite ihrer Einverständniserklärung unterrichtet worden sind, sich freiwillig zu einem Interview zur Verfügung stellen.

Den Minister für Arbeit, Gesundheit und Soziales habe ich in seiner Eigenschaft als Aufsichtsbehörde über den Vorgang und meine Rechtsauffassung hierzu unterrichtet mit der Bitte, in vergleichbaren Fällen die Wahrung des Sozialgeheimnisses (§ 35 Abs. 1 SGB I) sicherzustellen.

b) Krebsregister

Der Minister für Arbeit, Gesundheit und Soziales ist an mich mit der Frage herangetreten, ob das mit seiner finanziellen Unterstützung von der Gesellschaft zur Bekämpfung der Krebskrankheiten Nordrhein-Westfalen e. V. (GBK) eingerichtete Register für onkologische Nachsorge den Vorschriften über den Datenschutz entspricht.

Bei der GBK handelt es sich zwar um eine juristische Person des privaten Rechts und damit nicht um eine meiner Kontrolle nach § 26 Abs. 1 Satz 1 DSG NW unterliegende Stelle. Dieser Umstand verwehrt es dem Minister für Arbeit, Gesundheit und Soziales jedoch nicht, sich auch insoweit durch den Landesbeauftragten in Fragen des Datenschutzes beraten zu lassen (§ 26 Abs. 2 DSG NW).

Eine erste Prüfung hat ergeben, daß auf den Erhebungsbögen für die Erfassung der Erkrankungs-, Behandlungs- und Nachsorgedaten eine Erklärung eingedruckt ist, die der behandelnde Arzt mit seiner Unterschrift bestätigen muß. Die Erklärung lautet: „Der Patient ist mit der Aufnahme seiner Daten in das Register für onkologische Nachsorge einverstanden".

Ich habe darauf hingewiesen, daß eine solche Erklärung des Arztes die Einwilligung des Patienten in die Aufnahme seiner medizinischen Daten in das Krebsregister nicht ersetzen kann. Erforderlich ist eine schriftliche Einwilligungserklärung des Patienten selbst.

Der Minister für Arbeit, Gesundheit und Soziales hat daraufhin gegenüber der GBK verlangt, daß die Erhebungsbögen entsprechend geändert werden.

Im übrigen wirft die Führung des Registers für onkologische Nachsorge schwierige datenschutzrechtliche Fragen auf, deren Prüfung noch andauert.

c) Chemikaliengesetz

Die Bundesregierung hat den Entwurf eines Gesetzes zum Schutz vor gefährlichen Stoffen (Chemikaliengesetz) im Deutschen Bundestag eingebracht (Drucksache 8/3319). In § 19 Abs. 2 des Entwurfs ist vorgesehen, daß die zuständigen Landesbehörden vierteljährlich an das Bundesgesundheitsamt alle Krebserkrankungen melden. Nach der Begründung zu dieser Vorschrift soll dem Bundesgesundheitsamt statistisches Material zugeleitet werden, das insbesondere der Aufstellung eines Krebsregisters dient, um z. B. mögliche Zusammenhänge zwischen der Häufigkeit von Krebserkrankungen und dem Umgang mit gefährlichen Stoffen feststellen zu können.

Ich halte die vorgesehene Regelung aus der Sicht des Datenschutzes für bedenklich.

Der Entwurf geht, wie sich aus der Begründung ergibt, davon aus, daß die Aufzählung der Meldeangaben in § 19 Abs. 2 Satz 2 — anders als die Aufzählung in § 19 Abs. 1 Satz 2 — nicht abschließend ist, die Mitteilung des Namens und der Anschrift des Patienten also nicht ausgeschlossen wird.

Diese Regelung birgt die Gefahr eines umfangreichen Austausches besonders sensibler Daten, die grundsätzlich dem Geheimnisschutz des § 203 StGB unterliegen. Daher sollte vor der Einführung der in § 19 Abs. 2 des Entwurfs vorgesehenen Meldepflicht zunächst eine sorgfältige Prüfung stattfinden, ob und in welchem Umfang personenbezogene Daten zur Führung eines Krebsregisters erforderlich sind oder ob anonymisierte Daten ausreichen. Dabei ist im Interesse eines effektiven Datenschutzes ein strenger Maßstab anzulegen. Personenbezogene Daten, deren Kenntnis nur „zur Abrundung des Bildes" oder „als Hintergrundinformation" von Nutzen sind, dürfen nicht gespeichert werden (vgl. Ruckriegel in Ruckriegel/v. d. Groeben/Hunsche, Datenschutz und Datenverarbeitung in Nordrhein-Westfalen, § 10 Anm. 5).

Aus der Sicht des Datenschutzes ist zu begrüßen, daß der Bundesrat im ersten Durchgang die Regelung in § 19 des Entwurfs insgesamt abgelehnt hat, wenn auch vorwiegend aus anderen Gründen. Sollte gleichwohl eine personenbezogene Meldepflicht vorgesehen werden, so müßten durch bereichspezifische Regelung im Gesetz der Datenfluß auf ein Mindestmaß beschränkt und eine weitere Übermittlung ausgeschlossen werden.

d) Verzeichnis der Kammermitglieder

Im Kreise der Landesbeauftragten für den Datenschutz ist die Frage erörtert worden, ob gegen die Veröffentlichung eines Verzeichnisses der Mitglieder einer Tierärztekammer Bedenken bestehen.

Ich habe Zweifel, ob jeder Empfänger des veröffentlichten Verzeichnisses der Tierärzte, also grundsätzlich jedermann, ein berechtigtes Interesse an der Kenntnis der Daten hat. Auf jeden Fall neige ich zu der Ansicht, daß durch die Veröffentlichung schutzwürdige Belange der Betroffenen beeinträchtigt werden können, und diese Belange etwaige berechtigte Interessen der Empfänger überwiegen.

Da eine Beeinträchtigung schutzwürdiger Belange der Bertoffenen auch bei einer Beschränkung der Angaben auf Name, Vorname, akademischer Grad, Anschrift und Fachrichtung jedenfalls nicht auszuschließen ist, würde ich nach § 3 Satz 1, § 13 Abs. 1 Satz 1 DSG NW in vergleichbaren Fällen die Einwilligung des Betroffenen für erforderlich halten. Die Möglichkeit, einer Veröffentlichung widersprechen zu können, reicht nach der von mir ständig vertretenen Auffassung nicht aus.

e) Eingaben von Bürgern

Die Apothekerkammern in Nordrhein-Westfalen erheben umsatzbezogene Beiträge. Für die Höhe des Umsatzes ist die Selbsteinschätzung der Kammermitglieder maßgebend. In einem Rundschreiben an ihre Mitglieder hat die Apothekerkammer Nordrhein die Befürchtung geäußert, daß nicht alle Apotheker den ihrem tatsächlichen Jahresumsatz entsprechenden Beitrag entrichten. Deshalb habe sich die Kammerversammlung dazu entschlossen, von jedem Mitglied den Nachweis des Umsatzes durch Vorlage des Umsatzsteuerbescheides zu verlangen.

Gegen dieses Verfahren hat sich ein Apotheker bei mir beschwert. Er sieht darin eine Verletzung des Steuergeheimnisses.

Durch Rückfrage beim Minister für Arbeit, Gesundheit und Soziales habe ich erfahren, daß nach neuen Überlegungen im Kammervorstand den Mitgliedern auferlegt werden soll, ihren Umsatz künftig durch Beifügung einer Durchschrift der Umsatzsteuererklärung nachzuweisen.

Ich habe gegen eine derartige Regelung in der Beitragsordnung keine datenschutzrechtlichen Bedenken. Das Steuergeheimnis wird dadurch nicht berührt. § 30 der Abgabenordnung, der als Bundesrecht dem Datenschutzgesetz Nordrhein-Westfalen vorgeht, gilt nur für die Offenbarung von Daten durch Amtsträger, nicht aber für die Erhebung von Daten eines Steuerpflichtigen bei diesem selbst.

Bei der Erhebung der Umsatzzahlen (einschließlich der Verpflichtung zur Vorlage der Umsatzsteuererklärung) zum Zwecke der Beitragsbemessung müssen die Kammermitglieder allerdings auf die entsprechende Vorschrift der Beitragsordnung hingewiesen werden (§ 10 Abs. 2 Satz 1 DSG NW). Gegen eine etwaige Speicherung der Umsatzzahlen der Kammermitglieder in einer Datei bestehen keine Bedenken, soweit sie zu Zwecken der Beitragserhebung erforderlich ist (§ 10 Abs. 1 DSG NW). Diese Daten müssen allerdings nach § 17 Abs. 2 Satz 2 DSG NW gesperrt werden, sobald sie für die Beitragserhebung nicht mehr benötigt werden. In diesem Fall können die Kammermitglieder nach § 17 Abs. 3 Satz 2 DSG NW auch die Löschung der Daten verlangen.

Inzwischen hat die Kammerversammlung der Apothekerkammer Nordrhein eine Änderung der Beitragsordnung beschlossen (MBl. NW. 1980 S. 224). Danach hat der Beitragspflichtige durch eine Erklärung über die Höhe des Umsatzes nachzuweisen, daß die von ihm getroffene Einstufung richtig ist. Der Erklärung ist entweder eine Durchschrift der Umsatzsteuererklärung oder die schriftliche Bestätigung eines Steuerberaters beizufügen.

Durch den Anruf eines Bürgers erhielt ich Kenntnis von folgendem Vorfall:

In Lengerich hatten spielende Kinder einen auf einer Gartenmauer an einer öffentlichen Straße abgestellten Karton mit ausgefüllten medizinischen Fragebögen gefunden. Der Karton war weder mit einer Adresse noch mit einem Absender versehen. Er enthielt personenbezogene medizinische Daten von 175 Frauen, die in den letzten zwei Jahren entbunden hatten. Die Daten waren im Auftrag des Ministers für Arbeit, Gesundheit und Soziales von dem Institut für Lufthygiene und Silikoseforschung an der Universität Düsseldorf e.V. (MILS) im Rahmen einer medizinisch-epidemiologischen Untersuchung etwaiger Auswirkungen der Thallium-Emission eines Lengericher Zementwerkes erhoben worden. Die Untersuchung hatte in der Außenstelle Lengerich des Gesundheitsamtes Steinfurt stattgefunden. Die dabei genommenen Urin- und Haarproben sowie die Fragebögen sollten mit einem Kraftfahrzeug des MILS zu dessen Institutsgebäude in Düsseldorf befördert werden. Beim Verladen des Untersuchungsmaterials hat der Fahrer des Instituts den Karton mit den Fragebögen versehentlich auf dem Parkplatz stehen gelassen.

Ich habe mich nach der Aufklärung des Sachverhalts davon überzeugt, daß ein Fall der Datenverarbeitung im Auftrag (§ 7 DSG NW) nicht vorliegt. Der vom Minister für Arbeit, Gesundheit und Soziales dem MILS erteilte Auftrag ist nicht auf die Verarbeitung personenbezogener Daten, sondern auf die Durchführung einer medizinischen Untersuchung nach einem vom MILS ausgearbeiteten Untersuchungsplan durch Erhebung und Auswertung von Befunden und anamnestischen Angaben gerichtet. Eine Verletzung von Vorschriften über den Datenschutz durch eine meiner Kontrolle unterliegende öffentliche Stelle habe ich nicht feststellen können. Zur Klärung der Frage, ob das MILS gegen Datenschutzvorschriften verstoßen hat, habe ich den Vorgang an die für die Überwachung des Datenschutzes im privaten Bereich zuständige Aufsichtsbehörde abgegeben.

11. Personalwesen

a) Bearbeitung von Personalangelegenheiten

Ein Landesbeamter hat sich bei mir darüber beschwert, daß eine Mitarbeiterin seiner Dienststelle Einsicht in seine Personalakte genommen hat, obwohl sie seiner Ansicht nach nicht mit der Bearbeitung von Personalangelegenheiten beauftragt war.

Gesetzliche Grundlage für den Umgang mit Personalakten ist § 102 LBG in Verbindung mit den für die Bearbeitung von Personalangelegenheiten geltenden Rechtsvorschriften. Das Datenschutzgesetz Nordrhein-Westfalen kommt als gesetzliche Grundlage nicht in Betracht, da es nur in Dateien gespeicherte personenbezogene Daten schützt und Personalakten keine Dateien sind (§ 1 Abs. 2 Satz 1 in Verbindung mit § 2 Abs. 3 Nr. 3 DSG NW).

§ 102 LBG, der die Einsicht des Beamten in seine Personalakten regelt, setzt voraus, daß alle Vorgänge über die dienstlichen oder persönlichen Verhältnisse des Beamten in Personalakten gesammelt werden. Die für die Bearbeitung von Personalangelegenheiten geltenden Rechtsvorschriften setzen voraus, daß die mit der Bearbeitung beauftragten Bediensteten Zugang zu den Personalakten haben, soweit die Kenntnis der in diesen gesammelten Vorgänge für die Bearbeitung erforderlich ist. Ist die Beauftragung auf bestimmte Personalangelegenheiten beschränkt, so erstreckt sich der Zugang nur auf den Teil der Personalakten, in dem sich Vorgänge befinden, deren Kenntnis zur Bearbeitung erforderlich ist. In diesem Umfang ist der Zugang zu den Personalakten durch Bedienstete zulässig.

Meine Prüfung ergab, daß die Mitarbeiterin mit der Bearbeitung bestimmter Personalangelegenheiten beauftragt war und im Rahmen ihre Zuständigkeit nur den Unterordner der

Personalakte eingesehen hatte, in dem sich die zur Bearbeitung erforderlichen Vorgänge befanden. Dagegen bestehen keine datenschutzrechtlichen Bedenken.

Gleichwohl habe ich dem Innenminister empfohlen, in das Landesbeamtengesetz eine ausdrückliche gesetzliche Regelung für das Sammeln personenbezogener Daten in Personalakten und für den Zugang zu diesen Daten aufzunehmen.

b) Weitergabe von Daten an den Personalrat

An mich ist auch die Frage herangetragen worden, ob die Weitergabe von Privatanschriften und Geburtsdaten der Mitarbeiter an den Personalrat zulässig ist.

Gesetzliche Grundlage für die Weitergabe personenbezogener Daten von Mitarbeitern an den Personalrat sind die Vorschriften des Landespersonalvertretungsgesetzes (LPVG). Das Datenschutzgesetz Nordrhein-Westfalen kommt als gesetzliche Grundlage schon deshalb nicht in Betracht, weil es nach § 37 DSG NW durch die besonderen Rechtsvorschriften des Landespersonalvertretungsgesetzes verdrängt wird. Aufgaben und Befugnisse des Personalrates, insbesondere der Informationsaustausch zwischen Dienststelle und Personalrat einschließlich des Informationsrechts des Personalrats (§ 65 LPVG) und der Schweigepflicht seiner Mitglieder (§ 9 LPVG) sind damit bereichspezifisch und abschließend geregelt.

Nach § 65 Abs. 1 LPVG ist der Personalrat zur Durchführung seiner Aufgaben rechtzeitig und umfassend zu unterrichten. Ihm sind die dafür erforderlichen Unterlagen vorzulegen.

Es ist nicht erkennbar, inwiefern die Kenntnis von Privatanschriften oder Geburtsdaten der Mitarbeiter zur Durchführung der Aufgaben des Personalrats erforderlich sein können. Deshalb kann auch nicht beurteilt werden, ob für die Bekanntgabe dieser Daten ein Interesse der Allgemeinheit besteht und dieses gegenüber dem Anspruch der Mitarbeiter auf Schutz ihrer personenbezogenen Daten überwiegt (Artikel 4 Abs. 2 Satz 2 LV). Ohne ein solches überwiegendes Interesse der Allgemeinheit ist die Bekanntgabe der genannten Daten an den Personalrat unzulässig.

c) Datenübermittlung an nicht-öffentliche Stellen

Mehrere Eingaben von Angehörigen des öffentlichen Dienstes waren für mich Anlaß zur Prüfung, inwieweit die Übermittlung von Personaldaten an Personen oder andere Stellen außerhalb des öffentlichen Bereichs zulässig ist.

In einem Fall hatte ich zu prüfen, ob im Zusammenhang mit Personalratswahlen den in der Dienststelle vertretenen **Gewerkschaften** außer dem Namen auch dienstbezogene Personalangaben der Bediensteten (z. B. Amtsbezeichnung) für Zwecke der Wahlwerbung mitgeteilt werden dürfen. Solange sich die Datenübermittlung auf die genannten personenbezogenen Angaben beschränkt und nicht auch die Privatanschrift der Bediensteten mitgeteilt wird, habe ich keine datenschutzrechtlichen Bedenken.

Nach § 3 Satz 1 Nr. 1 DSG NW ist die Übermittlung zulässig, wenn das Datenschutzgesetz Nordrhein-Westfalen oder eine andere Rechtsvorschrift sie erlaubt. Eine solche andere Rechtsvorschrift ist § 2 Abs. 1 in Verbindung mit § 16 Abs. 4 des Landespersonalvertretungsgesetzes (LPVG).

Nach § 2 Abs. 1 LPVG wirken Dienststelle und Personalvertretung zur Erfüllung der dienstlichen Aufgaben und zum Wohle der Beschäftigten mit den in der Dienststelle vertretenen Gewerkschaften zusammen. Nach § 16 Abs. 4 LPVG sind die in der Dienststelle vertretenen Gewerkschaften berechtigt, für die Personalratswahl Wahlvorschläge zu machen. Aus dem Gebot des Zusammenwirkens mit den Gewerkschaften sowie aus deren Wahlvorschlagsrecht folgt die Berechtigung der Dienststelle wie auch des Personalrats, den Gewerkschaften außer den Namen auch dienstbezogene Personalangaben wie die Amtsbezeichnung für Zwecke der Wahlwerbung mitzuteilen. Auf diese Weise wird dem berechtigten Interesse der in der Dienststelle vertretenen Gewerkschaften Rechnung ge-

tragen, den einzelnen Beschäftigten gezielt als Angehörigen einer bestimmten Gruppe (Beamter, Angestellter, Arbeiter) ansprechen zu können.

In einem anderen Fall hatte ich zu prüfen, ob den in der Dienststelle vertretenen Gewerkschaften Namen und Privatanschriften der Mitarbeiter zum Zwecke der Mitgliederwerbung mitgeteilt werden dürfen. Dies halte ich für unzulässig.

Als Rechtsgrundlage käme nur § 13 Abs. 1 Satz 1 DSG NW in Betracht. Nach dieser Vorschrift ist das berechtigte Interesse des Empfängers an der Kenntnis der zu übermittelnden Daten gegen die schutzwürdigen Belange des Betroffenen abzuwägen.

Ein berechtigtes Interesse einer in der Dienststelle vertretenen Gewerkschaft an der Kenntnis von Namen und Privatanschriften der Mitarbeiter zum Zwecke der Mitgliederwerbung dürfte zwar regelmäßig vorliegen. Durch die Bekanntgabe der Privatanschriften von Bediensteten können jedoch deren schutzwürdige Belange beeinträchtigt werden. Jedenfalls ist nicht auszuschließen, daß Mitarbeiter die gezielt an ihre Privatanschrift gerichtete Werbung, der Gewerkschaft beizutreten, als Belästigung oder sogar als mittelbaren Druck empfinden. Bei der Abwägung der Interessen überwiegt in diesem Fall das Interesse der Mitarbeiter am Schutz ihrer Privatsphäre gegenüber dem Interesse der Gewerkschaft an der Mitgliederwerbung, die im übrigen auch ohne Eindringen in den privaten Bereich der Mitarbeiter möglich ist.

Diesem Ergebnis steht nicht entgegen, daß das Grundrecht der Koalitionsfreiheit (Artikel 9 Abs. 3 GG) mit dem Bestand der Koalitionen auch deren freie Betätigung, also auch die Werbung neuer Mitglieder gewährleistet. Denn die Freiheit der Betätigung findet ihre Grenze an dem aus Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG folgenden Recht des Einzelnen auf Schutz seiner Privatsphäre. Die aus der Koalitionsfreiheit hergeleitete Betätigungsfreiheit der Koalition rechtfertigt nicht, in Grundrechte anderer einzugreifen.

Ein anderer Bürger hat mich darauf aufmerksam gemacht, daß die Gymnasien und Gesamtschulen in Nordrhein-Westfalen dem Verlag des **Philologen-Jahrbuches** personenbezogene Daten von Lehrern ohne deren Einwilligung mitteilen. Zu den Daten, die übermittelt werden, gehören Familienname, Vorname, Datum der Ernennung, Mitgliedschaft im Philologenverband, Fächerkombination, Konfession, Geburtsdatum, Funktion als Fachleiter am Bezirksseminar. Gegen eine derartige Praxis habe ich datenschutzrechtliche Bedenken.

Als Rechtsgrundlage käme auch hier nur § 13 Abs. 1 Satz 1 DSG NW in Betracht. Es erscheint bereits zweifelhaft, ob der Verlag des Philologen-Jahrbuchs ein berechtigtes Interesse an der Kenntnis aller Datenarten hat, die bislang in dem Jahrbuch veröffentlicht wurden. Auf jeden Fall können durch die Bekanntgabe dieser Daten schutzwürdige Belange des Betroffenen beeinträchtigt werden. Bei der Interessenabwägung überwiegt das Interesse des Betroffenen an dem Schutz seiner Persönlichkeitssphäre gegenüber dem Veröffentlichungsinteresse des Verlages und dem Informationsinteresse der Benutzer des Jahrbuches.

Zur Vermeidung von Verstößen gegen das Datenschutzgesetz Nordrhein-Westfalen habe ich dem Kultusminister empfohlen, eine landeseinheitliche Regelung herbeizuführen, die sicherstellt, daß entweder vor jeder Weitergabe der genannten Daten die erforderliche Einwilligung des Betroffenen eingeholt oder auf die Weitergabe überhaupt verzichtet wird.

Einige Bürger haben sich bei mir darüber beschwert, daß der vom Landesamt für Besoldung und Versorgung für die Auszahlung ihrer Bezüge verwendete **Überweisungsträger** neben den zur Vornahme der Gutschrift notwendigen Daten eine detaillierte Aufschlüsselung der Bezüge in Bruttogehalt, Zulagen, Lohn- und Kirchensteuer und weitere Abzüge enthält. Auf diese Weise werden zahlreiche personenbezogene Daten den Bankinstituten und ihren Mitarbeitern zugänglich gemacht, ohne daß eine Rechtsvorschrift es erlaubt.

Ich habe das berechtigte Anliegen der Bürger gegenüber dem Innenminister aufgegriffen und dabei auf das den Erfordernissen des Datenschutzes entsprechende Überweisungsverfahren in Niedersachsen und im Saarland hingewiesen.

12. Statistik

a) Mikrozensus

Auf Grund des Gesetzes über die Durchführung einer Repräsentativstatistik der Bevölkerung und des Erwerbslebens (Mikrozensus) vom 15. Juli 1975 (BGBl. I S. 1909) wird in den Jahren 1975 bis 1982 eine Bundesstatistik auf repräsentativer Grundlage (Mikrozensus) durchgeführt. Nach § 2 Abs. 1 dieses Gesetzes wird die Statistik einmal jährlich mit einem Auswahlsatz von 1 v. H. der Bevölkerung erhoben. Dabei haben die zur Auskunft herangezogenen Bürger auf einem umfangreichen Fragebogen zahlreiche Fragen zu beantworten, die teilweise erheblich in den persönlichen Bereich eindringen. Dies gilt insbesondere für die Fragen nach der Höhe des Nettoeinkommens, nach der Erkrankung in den letzten vier Wochen und nach Rauchgewohnheiten.

Insoweit halte ich die Erhebung für bedenklich. Zwar hat das Bundesverfassungsgericht in seinem Beschluß vom 16. Juli 1969 (BVerfGE 27, 1 ff) entschieden, daß die Erfassung der Tatbestände Urlaubs- und Erholungsreisen für Zwecke des Mikrozensus mit dem Grundgesetz vereinbar ist. In den Gründen hat das Gericht aber ausgeführt, daß dem Staat ein Eindringen in den Persönlichkeitsbereich durch eine umfassende Einsichtnahme in die persönlichen Verhältnisse seiner Bürger versagt ist, weil dem Einzelnen um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein „Innenraum" verbleiben muß, in dem er „sich selbst besitzt" und „in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt". Eine statistische Befragung zur Person kann deshalb dort als entwürdigend und als Bedrohung des Selbstbestimmungsrechts empfunden werden, wo sie den Bereich menschlichen Eigenlebens erfaßt, der von Natur aus Geheimnischarakter hat.

Ich bezweifele, ob einige Fragen des Mikrozensus — gemessen an diesen Maßstäben des Bundesverfassungsgerichts — einer verfassungsrechtlichen Prüfung standhalten. Die seit dem Beschluß des Bundesverfassungsgerichts ergangene Rechtssprechung der Verwaltungsgerichte hat allerdings die Verfassungsmäßigkeit des Mikrozensus ausdrücklich bejaht (so VG Minden, Beschluß vom 15. 10. 1979 — 3 L 380/79 — und Beschluß vom 31. 10. 1979 — 3 L 371/79 —), sofern sie sie nicht offengelassen hat (so VG Köln, Urteil vom 30. 8. 1979 — 1 K 4728/78 —).

Das Verwaltungsgericht Köln ist zu einer verfassungsrechtlichen Prüfung des Mikrozensus deshalb nicht vorgedrungen, weil es die Auffassung vertreten hat, das Landesamt für Datenverarbeitung und Statistik (LDS) sei mangels entsprechender Rechtsgrundlage für die Durchführung der Statistik nicht zuständig. Nachdem das LDS gegen dieses Urteil Berufung eingelegt und die Landesregierung inzwischen durch Verordnung vom 11. Februar 1980 die Zuständigkeit des LDS zur Durchführung von Bundesstatistiken ausdrücklich festgelegt hat, wird das Oberverwaltungsgericht Münster demnächst in zweiter Instanz über die Verfassungsmäßigkeit des Mikrozensus zu entscheiden haben.

Ungeachtet dieser Entscheidung, der ich nicht vorgreifen will, halte ich es im Interesse eines effektiven Persönlichkeitsschutzes der Bürger für erforderlich, beim Mikrozensus künftig auf die den Kernbereich der Persönlichkeitssphäre berührenden Fragen entweder zu verzichten oder die Antwort dem Bürger freizustellen. Insofern begrüße ich es, daß der Innenminister im Bundesrat eine Gesetzesänderung unterstützt hat, nach der die Erteilung von Auskünften zur Gesundheit nunmehr wieder freiwillig ist.

b) Wanderungsstatistik

Auf Grund des Gesetzes über die Statistik der Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes vom 4. Juli 1957 in der Fassung vom 14. März 1980 (BGBl. I S. 309) wird eine Wanderungsstatistik durchgeführt. Nach § 4 dieses Gesetzes werden hierfür verschiedene Merkmale nach den Meldescheinen der Meldeämter laufend erfaßt. § 6 Abs. 1 Satz 1 des Gesetzes sieht vor, daß eine Ausfertigung der Meldescheine mindestens monatlich an das Statistische Landesamt weiterzuleiten ist.

Diese Vorschriften haben nach Artikel 31 GG Vorrang vor landesrechtlichen Vorschriften. Deshalb sind die Übergangsvorschriften für die Weitergabe von Meldescheinen in den Datenschutzgesetzen der Länder (§ 36 Abs. 1 DSG NW) hier nicht von Bedeutung.

Ich habe allerdings Zweifel, ob § 6 Abs. 1 Satz 1 des genannten Gesetzes mit dem aus Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG sich ergebenden Recht des Bürgers auf Schutz seiner personenbezogenen Daten vereinbar ist. Denn mit der in § 6 Abs.1 Satz 1 vorgeschriebenen Übersendung der Meldescheine fließen dem LDS mehr personenbezogene Daten zu, als es für die Durchführung der Wanderungsstatistik nach § 4 des Gesetzes benötigt. Insoweit verstößt § 6 Abs. 1 gegen den aus Artikel 20 Abs. 3 GG hergeleiteten Grundsatz der Verhältnismäßigkeit. Eine verfassungskonforme Auslegung dahingehend, daß nur die für die Wanderungsstatistik erforderlichen Angaben übermittelt werden dürfen, ist nicht möglich, weil die Vorschrift insoweit eindeutig und daher keiner Auslegung fähig ist. Ich habe deshalb beim Bundesbeauftragten für den Datenschutz angeregt, auf eine Änderung des § 6 Abs. 1 Satz 1 dergestalt hinzuwirken, daß den Statistischen Landesämtern nur die für die Wanderungsstatistik benötigten Daten (§ 4) zu übermitteln sind.

c) Sozialhilfestatistik

Auf Grund des Gesetzes über die Durchführung von Statistiken auf dem Gebiet der Sozialhilfe, der Kriegsopferfürsorge und der Jugendhilfe vom 15. Januar 1963 (BGBl. I S. 49) wird eine Jahresstatistik der Sozialhilfe durchgeführt. Im Rahmen dieser Erhebung wird bei den Trägern der Sozialhilfe die **Zahl** der Hilfeempfänger, gegliedert nach Empfängergruppen und nach Hilfearten, erfragt (§§ 2, 5 Abs. 1 Nr. 1 des Gesetzes).

Mit dem vom LDS versandten Zählblatt werden die Sozialhilfeträger aufgefordert, außer den im Gesetz vorgesehenen Merkmalen auch personenbezogene Daten wie Name und Anschrift des Hilfeempfängers mitzuteilen. Insoweit entbehrt die Erhebung der nach Artikel 4 Abs. 2 LV erforderlichen gesetzlichen Grundlage.

Sofern die Sozialhilfestatistik, wie das LDS geltend macht, ohne Kenntnis des Namens und der Anschrift des Hilfeempfängers nicht durchführbar ist, kann nur der Gesetzgeber Abhilfe schaffen. Ich habe inzwischen den Bundesbeauftragten für den Datenschutz gebeten, gegenüber den zuständigen Bundesressorts auf das Fehlen einer Rechtsgrundlage für die Erhebung personenbezogener Daten der Hilfeempfänger hinzuweisen.

d) Eingaben von Bürgern

Zum Bereich der amtlichen Statistik haben sich auch einige Bürger an mich gewandt.

Ein Bürger hat sich bei mir darüber beschwert, daß die Handwerkszählung 1977, zu der er auskunftspflichtig war, unter Verwendung personenbezogener Daten durchgeführt worden ist, die bei der Handwerkskammer gespeichert sind und von dieser an das LDS übermittelt werden. Nach § 3 Satz 1 Nr. 1 DSG NW ist die Übermittlung personenbezogener Daten zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt. Eine solche Rechtsvorschrift ist § 3 des Gesetzes über die Handwerkszählung 1977 (Handwerkszählungsgesetz 1977) vom 10. August 1976 (BGBl. I S. 2125). Danach sind die Handwerkskammern verpflichtet, dem LDS die Anschriften der Auskunftspflichtigen zur

Verfügung zu stellen. Der Datenfluß von der Handwerkskammer zum LDS ist somit nicht zu beanstanden.

Ich habe den Bürger jedoch darauf hingewiesen, daß das LDS zur strikten Geheimhaltung der ihm übermittelten personenbezogenen Daten verpflichtet ist.

Ein anderer Bürger hat mich gefragt, ob es erforderlich ist, daß Studenten bei der Stammdatenerfassung durch die Hochschule auch Auskunft über Ausbildung und soziale Stellung ihrer Eltern geben müssen.

Rechtsgrundlage für dieses Auskunftsbegehren der Universität ist das Gesetz über eine Bundesstatistik für das Hochschulwesen (Hochschulstatistikgesetz) vom 31. August 1971 (BGBl. I S. 1473). Dieses Gesetz dient dem Zweck, Ländern und Hochschulen ausgewählte Daten als Planungs- und Entscheidungshilfen für die Hochschulentwicklung bereitzustellen (§ 1). Welche Daten hiernach erforderlich sind, hat der Gesetzgeber u. a. in § 4 Nr. 2 des Hochschulstatistikgesetzes festgelegt. Nach dieser Vorschrift sind insbesondere bei den Studenten der Hochschulen zum Zwecke der Durchführung einer Bestands- und Verlaufsstatistik auch Daten über „Ausbildung der Eltern und deren Stellung im Beruf" zu erheben.

Die dementsprechend von der Universität bei der Stammdatenerfassung gestellte Frage hält sich im Rahmen des gesetzlichen Auftrages zur Durchführung der Hochschulstatistik. Es kann auch nicht davon ausgegangen werden, daß der Grundsatz der Verhältnismäßigkeit verletzt ist.

In einer weiteren Eingabe war ein Student der Auffassung, daß der Erhebungsbogen für Prüfungskandidaten gegen Datenschutzvorschriften verstoße. Insbesondere hielt er die Erhebung des Namens für nicht erforderlich.

Ich habe den Einsender darauf hingewiesen, daß das Hochschulstatistikgesetz die Erhebung, Aufbereitung und Speicherung von Daten ermöglichen soll, die für die Hochschulplanung bedeutsam sind. Dazu gehören auch aktuelle Daten über Kandidaten, die sich zu Abschlußprüfungen oder Promotionen vor den staatlichen und kirchlichen Prüfungsämtern sowie vor den in § 2 Nr. 1 und 2 des Hochschulstatistikgesetzes genannten Einrichtungen gemeldet haben. Deshalb sieht § 13 Abs. 1 des Hochschulstatistikgesetzes vor, daß bei den Prüfungskandidaten folgende Tatbestände erhoben werden: Angaben zur Person, Staatsangehörigkeit, Wohnsitze, Studienverlauf, Art und Fachrichtung der abzulegenden Prüfung.

Soweit dabei der Familienname und der Vorname erfragt werden, sind dies „Angaben zur Person". Die Erhebung des Namens verletzt auch nicht den Grundsatz der Verhältnismäßigkeit. Der Name ist erforderlich, weil zur Feststellung von Erfolgsquoten die Statistik der Prüfungskandidaten mit der Studentenverlaufsstatistik verknüpft werden muß. Dies ist nur über den Namen als konstantes Identifikationsmerkmal möglich.

13. Hochschulen

a) Auskünfte über Studenten

An Hochschulen ist in jüngster Zeit lebhaft erörtert worden, inwieweit Daten über Studenten durch die Hochschulverwaltungen an Dritte übermittelt werden. Anlaß dieser Diskussion war ein Artikel des Studentenmagazins „Rote Blätter" des Marxistischen Studentenbundes Spartakus, Ausgabe 1/80. In dem Artikel wird behauptet, ein Informant des Magazins habe sich in Telefonaten mit verschiedenen Hochschulverwaltungen als Kriminalrat Bunte vom 14. Kommissariat in Bonn ausgegeben und fernmündlich Auskünfte über persönliche Daten von Studenten erhalten; außerdem wurde der Verdacht geäußert, daß an

einigen Hochschulen die Mitgliedschaft in Studentengruppen in der Matrikel gespeichert werde.

Auf Grund meiner Ermittlungen habe ich gemäß § 30 Abs. 1 Satz 1 Nr. 3 DSG NW folgende Verstöße gegen Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen festgestellt:

1. Ein Mitarbeiter der Universität zu Köln sowie ein Mitarbeiter der Fachhochschule Niederrhein haben die Verpflichtung zur Wahrung des Datengeheimnisses nach § 5 Abs. 1 in Verbindung mit §§ 11 Abs. 1 Satz 1, 13 Abs. 1 Satz 1 DSG NW verletzt, indem sie einer nicht identifizierten Person, die sich als Kriminalrat ausgab, Auskünfte über personenbezogene Daten eines Studenten erteilt haben.

   Die fernmündliche Übermittlung personenbezogener Daten an nicht identifizierte Auskunftssuchende stellt eine erhebliche Verletzung der zur Wahrung des Datengeheimnisses erforderlichen Sorgfaltspflicht dar. Um eine Verletzung des Datengeheimnisses auszuschließen, dürfen grundsätzlich keine fernmündlichen Auskünfte über personenbezogene Daten erteilt werden. Wenn ausnahmsweise aus zwingenden Gründen auf eine fernmündliche Anfrage eine fernmündliche Auskunft gegeben wird, muß nach sorgfältiger Überprüfung der Telefonnummer aufgrund amtlicher Unterlagen durch Rückruf bei der ersuchenden Stelle deren Identität eindeutig festgestellt sein. Der Rückruf der beiden Mitarbeiter unter der von der nicht identifizierten Person angegebenen Telefonnummer war untauglich, die Identität der ersuchenden Stelle festzustellen.

2. Die Universität zu Köln und die Fachhochschule Niederrhein haben es unterlassen, die organisatorischen Maßnahmen zu treffen, die nach § 6 Abs. 1 DSG NW erforderlich sind, um die Ausführung des Datenschutzgesetzes Nordrhein-Westfalen hinsichtlich der Studentenmatrikel zu gewährleisten.

   Es ist nicht darauf hingewiesen worden, daß Auskunftsersuchen nach § 11 Abs. 1 Satz 1 DSG NW nur ausnahmsweise aus zwingenden Gründen und nur dann fernmündlich beantwortet werden dürfen, wenn die Identität der ersuchenden Stelle durch Rückruf unter der überprüften Telefonnummer eindeutig festgestellt ist. Wie der vorliegende Fall zeigt, hätten zum Schutz des Datengeheimnisses den Mitarbeitern der Hochschulverwaltungen entsprechende Hinweise gegeben werden müssen.

Die betroffenen Hochschulen haben die Ansicht vertreten, daß die Anwendbarkeit der §§ 5, 11, 13 DSG NW im vorliegenden Fall zweifelhaft sei, weil es sich bei der Studentenmatrikel um eine „interne Datei" im Sinne des § 1 Abs. 2 Satz 3 DSG NW handele. Dieser Ansicht bin ich entgegengetreten.

Schon die Übermittlung der studentischen Daten an das Landesamt für Datenverarbeitung und Statistik schließt die Anwendung des § 1 Abs. 2 Satz 3 DSG NW aus. Die Verpflichtung zur Datenübermittlung an das Landesamt für Datenverarbeitung und Statistik ergibt sich insbesondere aus §§ 12 Nr. 2, 17 Abs. 3 Satz 3 des Hochschulstatistikgesetzes (HStatG). Nach § 17 Abs. 1 Nr. 9 HStatG ist die Hochschulverwaltung in den Fällen des § 12 Nr. 2 HStatG selbst auskunftspflichtig. Soweit nach § 17 Abs. 1 Nr. 1 HStatG die Studenten auskunftspflichtig sind, haben die Hochschulen nach § 17 Abs. 3 Satz 3 HStatG als Erhebungsstellen vor Weiterleitung der Erhebungsbogen an die Statistischen Landesämter die Pflicht zur Überprüfung der Richtigkeit der Angaben. Da mit der Weiterleitung der Erhebungsbogen zumindest die Übereinstimmung mit der Studentenmatrikel bestätigt wird, ist die Weiterleitung ebenfalls als eine Datenübermittlung aus der Studentenmatrikel anzusehen.

Darüber hinaus findet eine regelmäßige Datenübermittlung aus der Studentenmatrikel nach § 23 Abs. 1 Satz 1 der Vergabeverordnung an die Zentralstelle für die Vergabe von Studienplätzen statt. Ferner wird nach Maßgabe des § 7 der Meldeverordnung für die Krankenversicherung der Studenten aus der Studentenmatrikel regelmäßig die Immatrikulation der einzelnen versicherungspflichtigen Studenten bestätigt. Hinzu kommt, daß

aus der Studentenmatrikel der Bundesversicherungsanstalt für Angestellte unmittelbar Auskünfte erteilt werden.

Zur Vermeidung von Verstößen gegen Vorschriften über den Datenschutz habe ich den betroffenen Hochschulen nach § 30 Abs. 3 DSG NW vorgeschlagen, die Mitarbeiter, die Zugang zu personenbezogenen Daten haben, darauf hinzuweisen, daß

a) das Datenschutzgesetz Nordrhein-Westfalen auf die Studentenmatrikel nach § 1 Abs. 2 Satz 1 DSG NW uneingeschränkt Anwendung findet,

b) Auskunftsersuchen von Behörden und sonstigen öffentlichen Stellen über personenbezogene Daten zum Schutz des Datengeheimnisses grundsätzlich nur schriftlich zu beantworten sind,

c) eine fernmündliche Beantwortung nur ausnahmsweise aus zwingenden Gründen und nur dann zulässig ist, wenn nach sorgfältiger Überprüfung der Telefonnummer aufgrund amtlicher Unterlagen durch Rückruf bei der ersuchenden Stelle deren Identität eindeutig festgestellt ist.

Die Fachhochschule Niederrhein beabsichtigt nunmehr, über die von mir gegebenen Vorschläge hinaus Inhalt, Grenzen, Form und Zuständigkeiten für die Erteilung von Auskünften an Dritte durch eine allgemeine Dienstanweisung umfassend zu regeln. Diese Bemühungen der Fachhochschule zur besseren Durchsetzung der Datenschutzbestimmungen sind zu begrüßen.

Der Rektor der Universität zu Köln hat meiner Feststellung, sein Mitarbeiter habe einer nicht identifizierten Person telefonisch Auskunft über personenbezogene Daten eines Studenten gegeben, widersprochen. In seiner Stellungnahme hat er abschließend aber mitgeteilt, daß er meinen Vorschlägen unter b) und c) folgen und überdies die Studentenmatrikel nicht als interne Datei im Sinne von § 1 Abs. 2 Satz 3 DSG NW behandeln lassen werde.

Bei meinen Ermittlungen hinsichtlich der im Studentenmagazin „Rote Blätter" gegebenen Darstellung hat sich im übrigen nicht bestätigt, daß die Zugehörigkeit zu Studentengruppen in der Studentenmatrikel gespeichert wird. Bei der Universität zu Köln werden lediglich die an der Universität zugelassenen Studentengruppen auf eigenen Antrag in eine Hochschulgruppen-Matrikel aufgenommen und dabei auch die Namen ihrer Vertreter festgehalten. Bei der Fachhochschule Niederrhein kann die Gruppenzugehörigkeit einiger Studenten sowohl den Angaben über die Studentenschaft als auch den Angaben über die politischen Hochschulgruppen im Personal- und Vorlesungsverzeichnis der Fachhochschule entnommen werden. Die Veröffentlichung der Gruppenzugehörigkeit erfolgt nach Auskunft der Fachhochschule mit Einwilligung der betroffenen Studenten. Damit ist ihre Gruppenzugehörigkeit offenkundig. Soweit aber über eine offenkundige Gruppenzugehörigkeit eines Studenten Auskunft erteilt wird, ist eine Verletzung des Datengeheimnisses nach § 5 Abs. 1 DSG NW nicht festzustellen.

Im Zusammenhang mit diesem Vorfall hat der Rektor der Universität zu Köln in einem Schreiben an die Studentenschaft die Auffassung vertreten, die Amtshilfe durch Auskunft an andere Behörden sei durch § 11 Abs. 1 Satz 1 DSG NW für zulässig erklärt. Auf die Bitte der Studentenschaft um Stellungnahme habe ich darauf hingewiesen, daß diese Feststellung mißverständlich ist. Der Amtshilfegrundsatz als formelles Prinzip kann die Übermittlung personenbezogener Daten nicht legitimieren. Materiell-rechtliche Grundlage für die Übermittlung ist vielmehr § 11 Abs. 1 Satz 1 DSG NW.

Diese Vorschrift läßt Amtshilfe durch Übermittlung personenbezogener Daten nur zu, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist. Bei Auskünften an die Polizei kommen Aufgaben der Strafverfolgung (§§ 161, 163 StPO) oder der Gefahrenabwehr (§ 15 Abs. 1 Satz 1, § 20 Abs. 1 Satz 1 PolG) in Betracht. Danach ist Amtshilfe durch Datenübermittlung an die Polizei nur zulässig, wenn sie entweder zu Ermittlungen zur Erforschung von Straftaten oder zur

Abwehr einer im Einzelfall bestehenden Gefahr für die öffentliche Sicherheit oder Ordnung erforderlich ist.

Zwar hat die ersuchende Behörde die Rechtmäßigkeit des Ersuchens zu verantworten und dafür einzustehen, daß sie die angeforderten Daten für die Erfüllung ihrer Aufgaben braucht. Die ersuchte Behörde ist jedoch von einer eigenen Prüfpflicht nicht völlig entbunden; sie muß in einer Art „Plausibilitätskontrolle" feststellen, ob die Datenanforderung unter Berücksichtigung der Aufgaben und Befugnisse der ersuchenden Behörde schlüssig erscheint (vgl. Ruckriegel in Ruckriegel/v. d. Groeben/Hunsche, Datenschutz und Datenverarbeitung in Nordrhein-Westfalen, § 11 Anm. 3). Dieser Prüfpflicht kann sich die Universität bei der Anforderung personenbezogener Daten durch die Polizei nicht mit dem Hinweis auf ihre Verpflichtung zur Amtshilfe entziehen.

In einem weiteren Fall, der eine andere Hochschule betrifft, habe ich ebenfalls Ermittlungen darüber geführt, ob im Bereich der Hochschule personenbezogene Daten über Studenten unbefugt Dritten — hier einer politischen Vereinigung — zu Zwecken der Mitgliederwerbung zugänglich gemacht wurden. Die Hochschule hat mir versichert, daß weder die Studentenschaft noch politische Hochschulgruppen Zugang zu den Daten erhielten. Da der betroffene Student, der ein solches Werbeschreiben erhalten hat, nicht genannt sein will, ist eine gezielte Ermittlung schwierig.

b) Meldepflicht der Studentenwerke

Ein Bürger hat sich darüber beschwert, daß ein Studentenwerk als Wohnungsgeber die Meldebehörden über Einzüge und Auszüge in den Studentenwohnheimen laufend ohne Einwilligung der Betroffenen unterrichtet. Ich habe darin keinen Verstoß gegen Vorschriften über den Datenschutz feststellen können.

Nach § 3 Satz 1 Nr. 1 DSG NW ist die Übermittlung zulässig, wenn das Datenschutzgesetz Nordrhein-Westfalen oder eine andere Rechtsvorschrift sie erlaubt. Diese Voraussetzung liegt hier vor. Nach § 3 Abs. 2 Satz 1 des Meldegesetzes für das Land Nordrhein-Westfalen (MG NW) ist der Wohnungsgeber neben dem Ein- oder Ausziehenden (Hauptmeldepflichtigen) zur An- oder Abmeldung verpflichtet. Der Wohnungsgeber hat sich davon zu überzeugen, daß der Hauptmeldepflichtige die Meldung tatsächlich erstattet hat; dies kann durch Rückfrage bei der Meldebehörde geschehen (§ 5 Abs. 1 MG NW). Unterläßt der Hauptmeldepflichtige die Meldung innerhalb der Meldefrist, so hat der Wohnungsgeber den meldepflichtigen Vorgang der Meldebehörde unverzüglich anzuzeigen (§ 5 Abs. 3 MG NW). Diese Verpflichtungen kann der Wohnungsgeber nur erfüllen, wenn bzw. indem er der Meldebehörde den Namen des Hauptmeldepflichtigen mitteilt.

Da somit die Vorschriften des Meldegesetzes eine Unterrichtung der Meldebehörde über Ein- und Auszüge nicht nur erlauben (§ 3 Satz 1 Nr. 1 DSG NW), sondern sogar vorschreiben, ist die Einwilligung des Betroffenen (§ 3 Satz 1 Nr. 2 DSG NW) nicht erforderlich.

c) Wissenschaftliche Bibliotheken

Ein Bürger hat sich dagegen gewandt, daß von den Institutsbibliotheken der Universitäten des Landes Nordrhein-Westfalen die Namen der gegenwärtigen Entleiher ohne deren Einwilligung anderen Buchinteressenten auf Wunsch mitgeteilt werden. Es handelt sich hierbei um Bibliotheken, deren Datenverarbeitung nicht automatisiert ist.

Dem Minister für Wissenschaft und Forschung habe ich meine auf §§ 3 Satz 1, 13 Abs. 1 Satz 1 DSG NW gestützten Bedenken gegen eine derartige Praxis der Institutsbibliotheken mitgeteilt.

Ein Bibliotheksbenutzer, der ein ausgeliehenes Buch sucht, dürfte zwar ein berechtigtes Interesse an der Kenntnis des Namens des Ausleihers haben; diese Kenntnis kann ihm einen schnelleren Zugriff auf das entliehene Buch ermöglichen. Die Bekanntgabe des Namens des Ausleihers beeinträchtigt jedoch dessen schutzwürdige Belange, da sie Schlüsse über sein Leseverhalten zuläßt; damit wird in sein Persönlichkeitsrecht einge-

griffen. Bei einer Abwägung der Interessen überwiegt das Interesse des Ausleihers an dem Schutz seines Persönlichkeitsrechts gegenüber dem Interesse des Dritten an einem schnelleren Zugriff auf das ausgeliehene Buch. Dies gilt sowohl für Bibliotheken, die ihre Bücher regelmäßig ausleihen, als auch für Präsenzbibliotheken. Der Umstand, daß auch bei Präsenzbibliotheken gelegentlich Bücher kurzfristig ausgeliehen werden, ändert nichts daran, daß auch in diesen Fällen die Ausleiher Schutz vor der Übermittlung ihres Namens an Dritte beanspruchen können.

Die Bekanntgabe des Namens eines Ausleihers an einen Dritten ist demnach nur mit Einwilligung des Betroffenen zulässig. Um die Funktionsfähigkeit einer Präsenzbibliothek sicherzustellen und dem Interesse ihrer Benutzer an der ständigen Verfügbarkeit aller Bücher Rechnung zu tragen, bietet es sich an, entweder auf die kurzfristige Ausleihe zu verzichten oder sie davon abhängig zu machen, daß der Ausleiher einwilligt, daß sein Name anderen Benutzern mitgeteilt wird.

Auf meine Empfehlung, insoweit eine landeseinheitliche Regelung herbeizuführen, hat mir der Minister für Wissenschaft und Forschung mitgeteilt, daß er meine Bedenken teile. Die Hochschulen und Einrichtungen seines Geschäftsbereichs habe er auf diese Problematik aufmerksam gemacht und um künftige Beachtung der entsprechenden Bestimmungen des Datenschutzgesetzes Nordrhein-Westfalen gebeten.

14. Schulen

- Im Schulbereich betraf eine Eingabe die Datenübermittlung zwischen Grundschule und weiterführender Schule. Der Bürger wandte sich dagegen, daß die weiterführende Schule, zu der ein Schüler nach dem Besuch der Grundschule von den Erziehungsberechtigten angemeldet wurde, das Gutachten der Grundschule über die Eignung des Schülers unmittelbar erhalte. Nach seiner Auffassung sollten zunächst die Erziehungsberechtigten unterrichtet werden, damit diese Gelegenheit erhielten, ein als „nicht geeignet" beurteiltes Kind bei der weiterführenden Schule wieder abzumelden. So könne sich die Weiterleitung einer negativen Beurteilung an die weiterführende Schule erübrigen.

  Ich habe das Anliegen gegenüber dem Kultusminister aufgegriffen. Er hat mitgeteilt, daß er der Anregung bei der nächsten Überarbeitung der einschlägigen Verwaltungsvorschriften in der Weise entsprechen werde, daß das Beratungsgespräch mit den Erziehungsberechtigten vor Übersendung des Gutachtens an die weiterführende Schule zu führen sei. Vorab werde in Dienstbesprechungen mit den Schulaufsichtsbeamten darauf hingewirkt, daß an allen Schulen so verfahren werde.

15. Steuerverwaltung

a) Kontrollbefugnis des Landesbeauftragten

Die für die Abgabenordnung (AO) zuständigen Referenten des Bundes und der Länder haben in einer gemeinsamen Besprechung die Ansicht vertreten, das Steuergeheimnis nach § 30 AO setze der Kontrollbefugnis der Datenschutzbeauftragten des Bundes und der Länder Grenzen. Ohne Zustimmung der Betroffenen dürfe den Datenschutzbeauftragten nach § 30 Abs. 4 Nr. 2 AO keine Einsicht in die dem Steuergeheimnis unterliegenden Einzelvorgänge gewährt werden, da die Datenschutzgesetze des Bundes und der Länder die Offenlegung nicht ausdrücklich zuließen.

Die Datenschutzbeauftragten des Bundes und der Länder vertreten demgegenüber einhellig die Auffassung, daß die Kontrolle der öffentlichen Verwaltung durch die Daten-

schutzbeauftragten uneingeschränkt auch die dem Steuergeheimnis unterliegenden Einzelvorgänge umfaßt.

Der Finanzminister hat mir mitgeteilt, er sehe davon ab, dazu eine Entscheidung zu treffen, „bevor nicht die unter Federführung des Bundesfinanzministers durchgeführte Abstimmung unter den Ländern abgeschlossen und eine einheitliche mit den Datenschutzbeauftragten des Bundes und der Länder abgestimmte Linie gefunden worden" sei.

Meiner Kontrollbefugnis unterliegen nach § 26 Abs. 1 Satz 1 DSG NW alle Finanzbehörden des Landes. Gegenstand der Kontrollbefugnis ist die Einhaltung der Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen sowie anderer Vorschriften über den Datenschutz.

Zu diesen anderen Vorschriften gehören auch die in § 45 Satz 2 BDSG aufgezählten besonderen bundesrechtlichen Datenschutzvorschriften, die als Bundesrecht dem materiellen Datenschutzrecht des Landes vorgehen. Zu diesen anderen Datenschutzvorschriften sind insbesondere die Vorschriften über das Steuergeheimnis nach § 30 AO zu rechnen (§ 45 Satz 2 Nr. 1 BDSG). Da § 26 Abs. 1 Satz 1 DSG NW ausdrücklich die Einhaltung dieser anderen Vorschriften über den Datenschutz meiner Kontrolle unterwirft, liegt eine ausdrückliche Regelung im Sinne des § 30 Abs. 4 Nr. 2 AO vor, die mich nicht nur berechtigt, sondern auch verpflichtet, uneingeschränkt die Rechtmäßigkeit des Handelns der Steuerverwaltung im Bereich des durch das Steuergeheimnis konkretisierten Datenschutzes zu überwachen.

Die Verweigerung der Einsichtnahme in personenbezogene Einzelvorgänge würde dem gesetzlichen Auftrag des Landesbeauftragten widersprechen, die schutzwürdigen Belange des Bürgers zu wahren. Mit den Grundsätzen des Datenschutzes wäre es unvereinbar, die vom Gesetzgeber eigens eingesetzte unabhängige Kontrollinstanz an einer wirksamen Datenschutzkontrolle dadurch zu hindern, daß ihr generell die Einsichtnahme in Einzelvorgänge verweigert wird. Die anfänglichen Versuche der Steuerverwaltung, sich einer wirksamen Datenschutzkontrolle zu entziehen, dürfen in ihrer Bedeutung nicht unterschätzt werden. Es gilt, den Anfängen zu wehren und einer Entwicklung entgegenzutreten, die im offenen Widerspruch zu dem in der Datenschutzgesetzgebung verbürgten Schutz des Bürgers steht.

b) Auskunftspflicht der Presse

Im Bereich der Steuerverwaltung findet aus der Sicht des Datenschutzes nicht nur das Steuergeheimnis, sondern auch das Presse- und Bankgeheimnis besonderes Interesse.

Der Verlag einer Tageszeitung hat sich in einer an mich gerichteten Eingabe dagegen gewandt, daß ein Finanzamt unter Bezugnahme auf §§ 93, 102 Abs. 1 Nr. 4 AO bei Chiffre-Anzeigen wie „Übernehme Schreibarbeiten" den Verlag aufgefordert hat, Name und Anschrift der Inserenten bekanntzugeben. Der Verlag befürchtet, daß die Finanzverwaltung derartige Auskünfte auch künftig gezielt bei Kleinanzeigen mit Chiffre-Angaben fordern wird. Dazu vertritt der Verlag die Ansicht, daß es bei solchen Bagatellfällen nicht gerechtfertigt sei, den Verlag zum Bruch des mit dem Inserenten vereinbarten Chiffre-Geheimnisses zu zwingen.

Ich bin der Auffassung, daß an die Presse gerichtete Auskunftsersuchen der Finanzverwaltung bei Chiffre-Anzeigen in Bagatellfällen weder mit dem sich aus Artikel 5 Abs. 1 Satz 2 GG ergebenden Schutz des Vertrauensverhältnisses zwischen Presse und Inserenten noch mit dem sich aus Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG ergebenden Recht des Bürgers auf Schutz seiner personenbezogenen Daten vereinbar sind.

Allerdings gilt das Auskunftsverweigerungsrecht der Presse nach § 102 Abs. 1 Nr. 4 der am 1. Januar 1977 in Kraft getretenen Abgabenordnung nur für den redaktionellen Teil.

Ein gesetzliches Auskunftsverweigerungsrecht für den Anzeigenteil besteht dagegen nicht. Damit hat der Gesetzgeber — wie von der Rechtsprechung (BFH — Urteil vom 25. Oktober 1973, BStBl. II 1974, 172 ff (175)) gefordert — den Konflikt, der sich bei der Güterabwägung aus der Sicherstellung der Steuereinnahmen und dem Grundsatz der Gleichmäßigkeit der Besteuerung einerseits und dem Grundrecht der Pressefreiheit andererseits ergibt, grundsätzlich gelöst. Diese grundsätzliche Entscheidung des Gesetzgebers schließt jedoch meines Erachtens im Einzelfall die Auskunftsverweigerung der Presse hinsichtlich des Anzeigenteils nicht aus. Die Abgabenordnung ist ein allgemeines Gesetz im Sinne des Artikel 5 Abs. 2 GG, das zwar der Pressefreiheit Schranken setzt, jedoch in seiner begrenzenden Wirkung angesichts der besonderen Bedeutung dieses Grundrechts selbst der Einschränkung bedarf. Inwieweit hiernach ein Auskunftsverweigerungsrecht der Presse hinsichtlich des Anzeigenteils anzunehmen ist, muß im Einzelfall unter Abwägung der im einzelnen gegebenen Besonderheiten und unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit entschieden werden.

Der Grundsatz der Verhältnismäßigkeit dürfte hier in gleicher Weise anzuwenden sein wie beim Bankgeheimnis. Auch beim Bankgeheimnis ist das Auskunftsverweigerungsrecht gesetzlich nicht verankert. Gleichwohl steht außer Frage, daß sich aus der Natur des Bankgeschäfts im Anwendungsbereich der Abgabenordnung die Gefahr einer unangemessenen Belastung des zwischen der Geldanstalt und ihren Kunden bestehenden Vertrauensverhältnisses ergeben kann. Dem wird in dem sog. Bankenerlaß Rechnung getragen.

Ich habe mich deshalb gegenüber dem Finanzminister dafür eingesetzt, daß das Chiffregeheimnis der Presse in Bagatellfällen von den Finanzämtern gewahrt wird. Dazu habe ich vorgeschlagen, daß auch im Interesse der Gleichbehandlung der einzelnen Presseverlage allgemeine Kriterien entwickelt werden sollten, wann im Einzelfall ein Bagatellfall von den Finanzämtern anzunehmen ist.

Der Finanzminister hat zu der von mir gegebenen Anregung auf zwei Urteile des Finanzgerichts Münster vom 20. September 1979 (III 376/79 und III 592/79) hingewiesen. Auch nach Auffassung des Gerichts kann der Zeitungsverlag wegen der durch das Grundrecht der Pressefreiheit eingeschränkten Auskunftspflicht der Presse die Auskunft unter den Aspekten der Güterabwägung im Anzeigenbereich ablehnen, wenn das Finanzamt in Bagatellsachen gegen den Inserenten ermittelt. Wegen der grundsätzlichen Bedeutung der Streitsachen hat das Finanzgericht in beiden Urteilen die Revison zugelassen.

Zu meiner Anregung, im Erlaßwege das presserechtliche Chiffregeheimnis in Bagatellfällen sicherzustellen, hat der Finanzminister mitgeteilt, daß er zunächst in den genannten Revisionsverfahren die Entscheidung des Bundesfinanzhofes abwarten und sich wegen der Notwendigkeit und des Inhalts einer eventuellen Regelung zuvor mit dem Bundesminister der Finanzen und den Finanzministern der Länder abstimmen wolle. Dazu vertrete ich die Auffassung, daß bis zu einer abschließenden bundeseinheitlichen Regelung für Nordrhein-Westfalen sichergestellt werden sollte, daß die Finanzämter, soweit das Chiffregeheimnis berührt ist, in Bagatellfällen keine Auskünfte bei der Presse über den Inserenten einholen.

c) Auskunftsrecht des Betroffenen

Das Auskunftsrecht des Betroffenen nach § 16 Abs. 1 DSG NW über die zu seiner Person gespeicherten Daten und über die Stellen, denen Daten regelmäßig übermittelt werden, ist gegenüber den Finanzbehörden nach § 16 Abs. 2 in Verbindung mit § 15 Abs. 2 Nr. 1 DSG NW beschränkt. Das Auskunftsrecht gilt nicht gegenüber Landesfinanzbehörden, soweit diese personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung in Dateien speichern.

Die Meinung der für die Abgabenordnung zuständigen Referenten des Bundes und der Länder, daß „sämtliche im Bereich der Steuerverwaltung in Dateien gespeicherten perso-

nenbezogenen Daten im Anwendungsbereich der AO der steuerlichen Überwachung und Prüfung dienen" und somit nicht der Auskunftspflicht unterliegen, kann nicht gefolgt werden. Allerdings trifft dies für die Dateien der Aufgabenbereiche Außenprüfung (§ 193 AO), Steuerfahndung (§ 208 AO), Steueraufsicht (§ 209 AO) und der Steuerstrafverfahren und Bußgeldverfahren (§§ 369 ff AO) zu. Die Datenschutzbeauftragten des Bundes und der Länder sind jedoch einhellig der Auffassung, daß für Dateien der Feststellungs-, Festsetzungs- und Erhebungsverfahren im allgemeinen eine volle Auskunftspflicht besteht, da diese Dateien nicht der Überwachung und Prüfung dienen.

Der Finanzminister strebt auch hinsichtlich dieser strittigen Auslegungsfrage eine mit den Finanzressorts und den Datenschutzbeauftragten des Bundes und der Länder abgestimmte Klärung an. Er hat mir mitgeteilt, daß der Bundesfinanzminister eine Arbeitsgruppe damit beauftragt habe, ein Verzeichnis der steuerlichen Dateien zu erarbeiten, das Auskunft gibt über Namen und Zweck jeder einzelnen Datei und eine Stellungnahme enthält zu der Frage, ob und aus welchem Grund die einzelne Datei der „Überwachung" oder „Prüfung" dient.

16. Wirtschaft

Eine Werbefirma hat sich darüber beschwert, daß eine Stadtverwaltung einem Konkurrenzunternehmen die Anschriften aller Gewerbetreibenden ihres Gebietes zu Werbezwecken weitergegeben hat. Ich habe dazu wie folgt Stellung genommen.

Nach § 3 Satz 1 DSG NW darf eine Gemeinde Anschriften von Gewerbetreibenden nur dann an Dritte übermitteln, wenn das Datenschutzgesetz Nordrhein-Westfalen oder eine andere Rechtsvorschrift es erlaubt oder der Betroffene eingewilligt hat.

Die allein in Betracht kommende Vorschrift des § 13 Abs. 1 Satz 1 DSG NW läßt eine Übermittlung aller Anschriften der Gewerbetreibenden an Personen oder Unternehmen außerhalb des öffentlichen Bereichs zu Werbezwecken nicht zu.

Ein berechtigtes Interesse an den Anschriften aller Gewerbetreibenden einer Stadt kann bei einer Werbefirma zwar unterstellt werden. Bei einer Abwägung der Interessen überwiegt aber das Interesse der Betroffenen, daß ihre Anschriften nicht zu rein kommerziellen Zwecken Dritten mitgeteilt werden. Da die Verletzung schutzwürdiger Belange der Betroffenen jedenfalls nicht ausgeschlossen werden kann, ist ihre Einwilligung für die Datenübermittlung erforderlich.

Dieser Fall ist im Zusammenhang mit Bestrebungen zu sehen, für Auskünfte aus dem Gewerberegister in den Ländern möglichst einheitliche Regelungen zu treffen. Ein entsprechender Entwurf ist unter Federführung des Bayerischen Staatsministers für Wirtschaft und Verkehr unter Beteiligung der übrigen Länder erarbeitet worden. Bayern und Niedersachsen haben inzwischen entsprechende Allgemeine Verwaltungsvorschriften erlassen.

Nach dem Entwurf für eine möglichst ländereinheitliche Regelung werden für Auskünfte aus dem Gewerberegister an Stellen außerhalb des öffentlichen Bereichs sogenannte einfache Einzelauskünfte und erweiterte Einzelauskünfte unterschieden.

Die einfachen Einzelauskünfte betreffen Namen, betriebliche Anschrift und angemeldete Tätigkeit eines Gewerbetreibenden. Bei diesen einfachen Einzelauskünften sollen nach dem Entwurf in der Regel — falls der Behörde keine gegenteiligen Umstände bekannt sind — Beeinträchtigungen schutzwürdiger Belange des Gewerbetreibenden „nicht zu befürchten" sein. Dieser Vermutungstatbestand der Nichtbeeinträchtigung schutzwürdiger Belange des Bürgers soll auch für Einzelauskünfte an Auskunfteien oder Detekteien, ferner für die Erteilung von Einzelauskünften an Berufsverbände zum Zwecke der Mitgliederwerbung gelten.

Eine solche Regelung wäre mit dem nordrhein-westfälischen Datenschutzrecht unvereinbar. Soweit der Betroffene nicht eingewilligt hat, ist nach § 3 Satz 1 in Verbindung mit § 13 Abs. 1 Satz 1 DSG NW eine Datenübermittlung an nicht-öffentliche Stellen nur zulässig, wenn im Einzelfall feststeht, daß schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

Nach dem auch im Datenschutzrecht anzuwendenden Untersuchungsgrundsatz (§ 24 des Verwaltungsverfahrensgesetzes Nordrhein-Westfalen) braucht die Behörde über die Richtigkeit ihrer Entscheidungsgrundlage zwar keine absolute Gewißheit erlangt zu haben. Es genügt, daß ein so hoher Grad der Wahrscheinlichkeit vorliegt, daß eine andere Auffassung bei vernünftiger Überlegung nicht denkbar ist. Bei den sogenannten einfachen Einzelauskünften ist jedoch in jedem Einzelfall durchaus denkbar, daß der Betroffene durch die Aktivitäten, die bei Einholung der Einzelauskunft beabsichtigt sind, in seinen Belangen beeinträchtigt wird. Dies gilt nicht nur für Recherchen, die durch Auskunfteien und Detekteien, in zahlreichen Fällen auch durch Anwaltsbüros angestellt werden. Da die Meldepflicht zum Gewerberegister einen sehr großen Personenkreis umfaßt, ist nicht auszuschließen, daß sich auch Gewerbetreibende in nicht unerheblicher Zahl entschieden dagegen wenden, gegen ihren Willen Gegenstand der Werbung zu werden.

Ohne genauere Kenntnis über die Einstellung des betroffenen Gewerbetreibenden zu den Maßnahmen, die mit Hilfe der Auskunft gegen ihn gerichtet werden sollen, fehlt für die Entscheidung, ob die Auskunft erteilt werden darf oder nicht, eine hinreichend gesicherte Grundlage. Diese Ungewißheit über die Entscheidungsgrundlage hat zur Folge, daß die Auskunft nicht erteilt werden darf, solange die Ungewißheit nicht durch sorgfältige Einzelfallprüfung ausgeräumt ist. Ob die Voraussetzungen für die Auskunftserteilung gegeben sind, ist daher nicht nur, wie in dem Entwurf vorgesehen, bei den sogenannten erweiterten Einzelauskünften zu prüfen, sondern nach den nordrhein-westfälischen Vorschriften über den Datenschutz und das Verwaltungsverfahren in jedem Einzelfall auch bereits bei den sogenannten einfachen Einzelauskünften.

17. Verkehrswesen

Die an mich gerichteten Eingaben zeigen, daß die Durchsetzung des Datenschutzes im Bereich des **Kraftfahrzeugzulassungswesens** noch einer erheblichen Verbesserung bedarf.

Für die **Datenerhebung** in Zulassungsverfahren gilt § 23 der Straßenverkehrs-Zulassungs-Ordnung (StVZO). Danach muß der Antrag insbesondere Name, Geburtstag, Beruf und Anschrift des Antragstellers enthalten. Der Antragsvordruck für die Fahrzeugzulassung dient zugleich als Vordruck für die Kraftfahrzeugsteuererklärung. Wegen der Einbeziehung der Kraftfahrzeugsteuererklärung werden mit dem Antragsvordruck mehr Daten erhoben, als für den Zulassungsantrag nach § 23 StVZO und demgemäß für die Speicherung in der nach § 26 Abs. 1 StVZO zu führenden Kartei erforderlich ist.

In keinem der mir bekannt gewordenen Fälle haben die Zulassungsstellen der ihnen bei der Datenerhebung nach § 10 Abs. 2 Satz 1 DSG NW obliegenden Hinweispflicht genügt. Nach dieser Vorschrift ist der Betroffene auf die Rechtsgrundlage der Datenerhebung oder sonst auf die Freiwilligkeit seiner Angaben hinzuweisen.

Dabei hat sich gezeigt, daß über den begrifflichen Unterschied zwischen Datenerhebung und Datenerfassung in der Verwaltungspraxis noch Unklarheiten bestehen. Ich habe mich deshalb veranlaßt gesehen, ausdrücklich darauf hinzuweisen, daß die in dem Vordruck des Zulassungsantrages vorgesehenen Fragen unter den Begriff der Datenerhebung und damit unter die Hinweispflicht des § 10 Abs. 2 Satz 1 DSG NW fallen.

Einige Eingaben richteten sich gegen die **Übermittlung** von Kraftfahrzeughalterdaten an Dritte zu Werbezwecken.

Hierzu ist von einem Straßenverkehrsamt die Ansicht vertreten worden, daß die Zulassungsstellen die mit dem Zulassungsantrag erhobenen Daten an andere als öffentliche Stellen „bei Darlegung eines berechtigten Interesses" nach § 26 Abs. 5 StVZO übermitteln dürfen. Dies entspricht jedoch nicht dem geltenden Recht.

Abgesehen davon, daß § 25 Abs. 5 StVZO nur Auskünfte über Fahrzeuge, Halter und Versicherungen zuläßt, wird vor allem übersehen, daß diese Vorschrift über die Auskunfterteilung an Dritte durch die Vorschriften der §§ 3 Satz 1, 13 Abs. 1 Satz 1 DSG NW ergänzt wird. Diese datenschutzrechtlichen Vorschriften werden durch die bundesrechtliche Regelung des § 26 Abs. 5 StVZO nach Artikel 31 GG aus folgenden Gründen nicht verdrängt.

Eine Regelung, die wie im Falle des § 26 Abs. 5 StVZO für die Auskunfterteilung **allein** auf das berechtigte Interesse des Auskunftsuchenden abstellt, zielt darauf ab, einer mißbräuchlichen Inanspruchnahme der Auskunftsstellen zu begegnen. Hierbei geht es lediglich um den Schutz der Behörde, nicht aber um die schutzwürdigen Belange des Bürgers, über den die Auskunft erteilt werden soll. Eine solche Regelung ist im Sinne der Kollisionsnorm des Artikels 31 GG nicht deckungsgleich mit der Datenschutzregelung des § 13 Abs. 1 Satz 1 DSG NW. Denn eine Regelung, die lediglich die Behörden vor mißbräuchlicher Inanspruchnahme schützen soll, enthält keine Entscheidung darüber, inwieweit dem Datenschutz in Bezug auf den betroffenen Bürger Rechnung zu tragen ist. Die Regelung des § 26 Abs. 5 StVZO geht hinsichtlich der Auskunfterteilung an Dritte nicht auf die Konfliktlage ein, die der Regelung im Datenschutzgesetz Nordrhein-Westfalen, insbesondere den Vorschriften des § 3 Satz 1 in Verbindung mit § 13 Abs. 1 Satz 1 DSG NW, zugrunde liegt.

Dem entspricht es, daß der Bundesminister für Verkehr in seiner Verlautbarung vom 10. Oktober 1978 (VkBl. S. 435) gerade im Hinblick auf die Datenübermittlung an Dritte darauf hingewiesen hat, daß seit Inkrafttreten des Bundesdatenschutzgesetzes die Weitergabe von Daten für Zwecke der Werbung nur noch mit der Einwilligung des Betroffenen zulässig ist. Auch der Bundesminister für Verkehr geht also davon aus, daß die Weitergabe der Daten an Dritte nur unter den Voraussetzungen des § 11 Satz 1 BDSG (der dem § 13 Abs. 1 Satz 1 DSG NW entspricht) zulässig ist.

Dies bedeutet, daß auch Auskünfte, die zu anderen als zu Zwecken der Werbung und Meinungsforschung von Privaten erbeten werden, ohne Einwilligung des Betroffenen nur erteilt werden dürfen, wenn die Voraussetzung des berechtigten Interesses des Auskunftsuchenden erfüllt ist und darüber hinaus gewährleistet ist, daß schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Ob die Belange des Betroffenen schutzwürdig sind, kann nur aufgrund einer Abwägung mit den Interessen des Auskunftsuchenden im Einzelfall beantwortet werden.

Die nach Maßgabe der Verlautbarung des Bundesministers für Verkehr vom 10. Oktober 1978 in den Vordrucken der Zulassungsanträge vorgesehene **Einwilligung** in die Weitergabe von Daten zu Werbezwecken gilt ausdrücklich nur für die Datenübermittlung durch das Kraftfahrt-Bundesamt. Für eine Datenübermittlung durch die Zulassungsstellen reicht die vorgedruckte Einwilligungserklärung also nicht aus.

Für die Einwilligung ist nach der Verlautbarung des Bundesministers für Verkehr erforderlich, daß eine entsprechende ausdrückliche Erklärung vom Fahrzeughalter eigenhändig unterschrieben wird. Soll die Zulassung durch einen Bevollmächtigten beantragt werden, muß nach der Verlautbarung die vom Fahrzeughalter eigenhändig zu unterschreibende Vollmacht für die Einwilligung ebenfalls eine entsprechende ausdrückliche Erklärung enthalten. Wenn der Fahrzeughalter in dem durch die Verlautbarung vorgeschriebenen Text des Antrages oder der Vollmacht weder das Ja-Kästchen noch das Nein-Kästchen ankreuzt, gilt die Einwilligung als nicht erteilt.

In drei Eingaben haben sich Bürger darüber beschwert, daß trotz fehlender Erklärung über die Einwilligung eine Übermittlung zu Werbezwecken stattgefunden hat. Die Übermittlung erfolgte jeweils durch das Kraftfahrt-Bundesamt. Dieses Amt geht auf Grund der ihm nach § 25 Abs. 1 Satz 3 StVZO von der Zulassungsstelle zu übersendenden Durchschrift der Karteikarte über die Fahrzeugzulassung generell von der Einwilligung in die Datenübermittlung zu Werbezwecken aus, es sei denn, daß auf der Karteikarte gemäß Vordruck ausdrücklich vermerkt wird: „Nicht veröffentlichen". Diese Unterstellung der Einwilligung des Betroffenen in die Datenübermittlung in den Fällen, in denen sich die Zulassungsstelle gegenüber dem Kraftfahrt-Bundesamt nicht ausdrücklich über die Einwilligung erklärt, birgt, wie die vorliegenden Fälle erkennen lassen, ein vermeidbares Risiko der Verletzung des Datengeheimnisses in sich.

Ich halte es daher für geboten, darauf hinzuwirken, daß der Vordruck der Karteikarte in der Weise abgeändert wird, daß das Kraftfahrt-Bundesamt von einer Einwilligung des Betroffenen in die Datenübermittlung nur ausgehen darf, wenn die Zulassungsstelle ausdrücklich bestätigt hat, die Einwilligung des Betroffenen sei ihr gegenüber erklärt worden.

Bei der Bearbeitung einer dieser Eingaben wurde mir bekannt, daß die Zulassungsstelle einer Großstadt auch dann von einer wirksamen Einwilligung des Halters ausgeht, wenn dessen Bevollmächtigter bei der Erklärung der Einwilligung keine schriftliche, den Anforderungen der Verlautbarung vom 10. Oktober 1978 entsprechende Vollmacht des Halters vorlegt. Eine wirksame Einwilligung liegt in diesen Fällen jedoch nicht vor, so daß die Übermittlung an Dritte nach § 3 Satz 1 DSG NW unzulässig ist. Die Praxis dieser Zulassungsstelle gibt Veranlassung, in Nordrhein-Westfalen die Durchsetzung der Datenschutzvorschriften im Kraftfahrzeugzulassungswesen generell zu überprüfen.

18. Öffentliche Unternehmen

a) Personalwesen

Für öffentlich-rechtliche Unternehmen, die der Aufsicht des Landes unterstehen, gelten nach § 18 Nr. 2 DSG NW besondere Regelungen (§§ 19 bis 23 DSG NW). Soweit solche Unternehmen personenbezogene Daten ihrer Beschäftigten im Zusammenhang mit deren dienst- oder arbeitsrechtlichen Rechtsverhältnissen verarbeiten, sind nicht diese besonderen Vorschriften, sondern die §§ 10 bis 17 DSG NW anzuwenden, da die Unternehmen insoweit personenbezogene Daten nicht als Hilfsmittel für die Erfüllung ihrer Geschäftszwecke oder Ziele verarbeiten (§ 18 Nr. 2 DSG NW).

Die Weitergabe von Personallisten an eine Gewerkschaft zum Zweck der Mitgliederwerbung dient geschäftsfremden Zielen. Ihre Zulässigkeit richtet sich daher nicht nach den §§ 19 bis 23 DSG NW, sondern nach den §§ 10 bis 17 DSG NW.

b) Datenträgeraustausch

Im Bereich des Sparkassenwesens ist ein Fall an mich herangetragen worden, der Anlaß gibt, die Datenübermittlung durch Datenträgeraustausch künftig allgemein zu überprüfen.

Das Rechenzentrum einer Stadtsparkasse hatte unter Verletzung der Grundsätze des Datenschutzes (§ 5 Abs. 1, § 6 Abs. 1, § 3 Satz 1 in Verbindung mit § 20 DSG NW) personenbezogene Daten zu einem anderen als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck Dritten zugänglich gemacht.

Das Rechenzentrum verwandte im Datenträgeraustausch mit anderen Kreditinstituten und Wirtschaftsunternehmen Magnetbänder, auf denen sich nicht nur die jeweils für den

Datenträgeraustausch benötigten Daten befanden, sondern auch Daten, die aus der früheren Verwendung der Datenträger herrührten. Die Daten aus der früheren Verwendung der Magnetbänder wurden nur insoweit gelöscht, als das Magnetband für den Datenträgeraustausch beansprucht wurde. Der nicht gelöschte Teil der Datenträger gab Auskunft über Anschriften, Geburtsdaten, Geschäftsbereiche und Vermögensverhältnisse von Sparkassenkunden.

Bei der Sparkasse wird inzwischen ein Datenlöschgerät eingesetzt, das es ermöglicht, alle Daten aus vorheriger Verwendung des Bandes zu löschen.

c) Kontonummern auf Briefumschlägen

Auch die Beurteilung eines weiteren Falles aus dem Sparkassenbereich erlangt grundsätzliche Bedeutung.

Ein Sparkassenkunde hat sich darüber beschwert, daß seine Sparkasse bei Versendung von Geschäftsberichten, Dividendengutschriften und sonstigen Mitteilungen für Inhaber von Wertpapierkonten bei den Anschriften auch die jeweilige Nummer des Wertpapierkontos ausdrucke.

Die Nummer eines Wertpapierkontos gehört zu den geschützten personenbezogenen Daten im Sinne des § 2 Abs. 1 DSG NW. Diese Daten darf die Sparkasse nach § 3 Satz 1 DSG NW nur übermitteln, wenn das Datenschutzgesetz oder eine andere Rechtsvorschrift es erlaubt oder der Betroffene eingewilligt hat.

Nach § 20 Abs. 1 Satz 1 DSG NW, der die Übermittlung solcher Daten im Rahmen der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen zuläßt, darf die Sparkasse nur solche Daten ihrer Kunden der Post zugänglich machen, die für die Postbeförderung erforderlich sind. Dazu gehört nicht die Kontonummer.

§ 5 Abs. 1 DSG NW verbietet, geschützte personenbezogene Daten unbefugt einem Dritten zugänglich zu machen. Diese Verpflichtung wird auch dann verletzt, wenn die Vorkehrungen außer acht gelassen werden, die nach § 6 Abs. 1 DSG NW erforderlich sind, um einer unbefugten Kenntnisnahme von personenbezogenen Daten durch Dritte bis zum Eingang der Sendung bei dem Betroffenen oder dem befugten Empfänger vorzubeugen.

Dies gilt insbesondere für die Übersendung von Geschäftsberichten als Drucksache unter Angabe des Wertpapierkontos. Nach der Postordnung sind die Postbediensteten bei Drucksachensendungen berechtigt, die Sendungen zu öffnen und daraufhin zu überprüfen, ob die einschlägigen Bestimmungen für die Übersendung als Drucksache eingehalten sind. Bei dieser formalen Prüfung läßt es sich nicht vermeiden, daß den Postbediensteten Informationen über das Wertpapierkonto offenbart werden. Die Übersendung der Geschäftsberichte unter Angabe des Wertpapierkontos läßt Rückschlüsse auf die Wertpapiere zu, die unter diesem Konto geführt werden. Dies halte ich für ein vermeidbares Mißbrauchsrisiko.

Außerdem ist zu berücksichtigen, daß auch Dritte nach Zustellung der Sendung diese unbemerkt öffnen und aus dem Inhalt in Verbindung mit der Wertpapierkonto-Nummer Rückschlüsse auf den Wertpapierbesitz des Betroffenen ziehen können. Auch insoweit wird hier den Anforderungen an die Datensicherung nicht hinreichend Rechnung getragen.

Danach halte ich es nicht für zulässig, bei Übersendung von Mitteilungen an Wertpapierkontoinhaber die jeweilige Kontonummer so anzubringen, daß sie auf dem Briefumschlag erkennbar ist, es sei denn, daß der Kontoinhaber in die Angabe der Kontonummer auf dem Briefumschlag eingewilligt hat. Ohne Einwilligung des Betroffenen muß nach meiner Auffassung darüber hinaus bei unverschlossenen Sendungen jede Angabe vermieden werden, die Rückschlüsse auf den Wertpapierbesitz des Kontoinhabers zuläßt.

19. Bildschirmtext

Der Landtag hat am 12. März 1980 das Gesetz über die Durchführung eines Feldversuchs mit Bildschirmtext (Bildschirmtextversuchsgesetz NW) einstimmig verabschiedet. Mit dem Beginn des Versuchs kann noch in diesem Jahr gerechnet werden.

Nach § 2 des Gesetzes ist Bildschirmtext ein Informations- und Kommunikationssystem, bei dem die Teilnehmer elektronisch gespeicherte, textorientierte Informationen und andere Dienste bestimmter Anbieter abrufen sowie Einzelmitteilungen an von ihnen bestimmte Teilnehmer übermitteln können; hierbei werden Fernmeldenetze zur Übermittlung und typischerweise Fernsehbildschirme unter Verwendung bestimmter Einrichtungen (Decoder) zur Wiedergabe verwendet.

Die in das Gesetz aufgenommenen datenschutzrechtlichen Regelungen für den Bereich der Anbieter von Informationen und anderen Diensten gehen auf Vorschläge zurück, die ich während der parlamentarischen Beratung gemacht habe. Entsprechendes gilt für die rechtsverbindliche schriftliche Zusage des Bundesministers für das Post- und Fernmeldewesen, mit der auch für den Bereich der Bildschirmtext-Zentrale meinem sachlichen Anliegen in vollem Umfang Rechnung getragen werden soll.

Damit ist es gelungen, die Teilnehmer des Feldversuchs vor einem Mißbrauch ihrer Daten zu schützen, die an die Bildschirmtext-Zentrale und an die Anbieter übermittelt und dort zumindest vorübergehend festgehalten werden. Mit den genannten Regelungen und Zusagen ist nach dem derzeitigen Erkenntnisstand sichergestellt, daß der Datenfluß auf ein Mindestmaß beschränkt, die Daten soweit als möglich anonymisiert und sie sobald als möglich wieder gelöscht werden. Es wird verhindert, daß durch Sammlung von Daten über Art, Inhalt und Häufigkeit der von einzelnen Teilnehmern abgerufenen Informationen oder Diensten Persönlichkeitsprofile der Teilnehmer erstellt werden können. Bereits eine automatisierte Erstellung und Speicherung von Interessenprofilen wird ausgeschlossen.

Ich betrachte es als meine Aufgabe, während des Verlaufs und nach Abschluß des Feldversuchs zu prüfen, ob die tatsächlichen Verhältnisse weitere Forderungen für einen ausreichenden Datenschutz notwendig machen.

D. Allgemeine Fragen des Datenschutzes

1. Anwendungsbereich des Gesetzes

a) Personenbezogene Daten

Eine große Zahl von Eingaben und Beratungsersuchen betraf allgemeine Fragen des Datenschutzes. Häufig hatten sie den Anwendungsbereich des Datenschutzgesetzes Nordrhein-Westfalen zum Gegenstand.

Das Gesetz schützt personenbezogene Daten (§ 1 Abs. 2 Satz 1 DSG NW). Nach § 2 Abs. 1 DSG NW sind dies Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

Im Hinblick auf die Veröffentlichung von Sterbedaten war zu entscheiden, ob Verstorbene Betroffene im Sinne des § 2 Abs. 1 DSG NW sein können und so von dem Schutz des Gesetzes mit erfaßt werden. Ich habe hierzu die Auffassung vertreten, daß das Datenschutzgesetz Nordrhein-Westfalen dazu beitragen soll, daß die Menschenwürde geachtet (Artikel 1 Abs. 1 GG) und die freie Entfaltung der Persönlichkeit für jedermann gesichert wird (Artikel 2 Abs. 1 GG). Wie das Bundesverfassungsgericht anerkannt hat, reicht insbesondere das Recht auf Menschenwürde über den Tod hinaus.

Der Schutzzweck des Gesetzes besteht somit nach dem Tode eines Bürgers fort. Diesem Zweck würde es widersprechen, wenn personenbezogene Daten eines Bürgers bei seinem Tode zu freien Daten würden, mit denen Dritte nach ihrem Belieben umgehen könnten. Demzufolge ist davon auszugehen, daß das Gesetz grundsätzlich auch die Daten Verstorbener schützt. Einzelangaben über persönliche oder sachliche Verhältnisse eines Verstorbenen, zu denen auch das Sterbedatum gehört, sind danach personenbezogene Daten im Sinne von § 2 Abs. 1 DSG NW, die nach § 1 Abs. 2 Satz 1 DSG NW dem Schutz durch das Gesetz unterliegen.

Eine Einschränkung ergibt sich daraus, daß der verstorbene Betroffene Rechte nicht mehr selbst ausüben kann. Rechte nach dem Datenschutzgesetz Nordrhein-Westfalen können deshalb, obwohl höchstpersönlich, unübertragbar und unvererblich, von den jeweils nächsten Angehörigen wahrgenommen werden, wie dies die Rechtsordnung auch in anderen Bereichen vorsieht. Die Einwilligung des Betroffenen nach § 3 Satz 1 Nr. 2 DSG NW kann daher nach seinem Tode von seinen nächsten Angehörigen erteilt werden. Der Kernbereich der Persönlichkeitssphäre des Verstorbenen darf allerdings nicht angetastet werden.

Im Zusammenhang mit der Bekanntgabe von Bauvorhaben natürlicher Personen habe ich die Auffassung vertreten, daß Angaben über Namen und Anschrift des Bauherrn sowie Lage und Art des Bauvorhabens nach § 1 Abs. 2 Satz 1 DSG NW geschützte personenbezogene Daten sind. Es handelt sich um Einzelangaben über sachliche Verhältnisse bestimmter natürlicher Personen (§ 2 Abs. 1 DSG NW).

Der Umstand, daß einige Angaben vom Zeitpunkt des Baubeginns an offenkundig sind, steht dem nicht entgegen. Das Datenschutzgesetz Nordrhein-Westfalen unterscheidet für den Bereich der öffentlichen Verwaltung grundsätzlich nicht zwischen mehr oder weniger sensiblen Daten. Ebensowenig kennt es freie Daten, die vom Anwendungsbereich des Gesetzes ausgenommen sind.

b) Datei

Das Gesetz schützt personenbezogene Daten nur, wenn sie in einer Datei gespeichert sind (§ 1 Abs. 2 Satz 1 DSG NW). Nach § 2 Abs. 3 Nr. 3 DSG NW ist eine Datei eine gleich-

artig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen geordnet und nach anderen bestimmten Merkmalen umgeordnet werden kann; Akten und Aktensammlungen sind keine Datei, sofern sie nicht durch automatisierte Verfahren umgeordnet werden können.

Unstreitig ist jede Datensammlung, die in automatisierten Verfahren verarbeitet wird, eine Datei. Anerkannt ist auch, daß Datensammlungen auf Karteikarten als Dateien anzusehen sind. Das gleiche muß für Datensammlungen auf sonstigen Vordrucken gelten.

Auf Anfragen von Gemeinden und Eingaben von Bürgern habe ich klargestellt, daß Bücher und Listen als solche keine Dateien sind, da die in ihnen gesammelten Daten nicht umgeordnet werden können, ohne das Buch oder die Liste zu zerstören. Dem steht nicht entgegen, daß darin enthaltende Daten zwecks Übermittlung an Dritte oder zur Verarbeitung in einer Datei in einem automatisierten oder nicht-automatisierten Verfahren auf Datenträger aufgenommen werden können.

Werden die Daten in einer Datei gespeichert, so unterliegt ihre Übermittlung nach § 1 Abs. 2 Satz 1 DSG NW den Beschränkungen des Datenschutzgesetzes Nordrhein-Westfalen, ohne daß es im Einzelfall darauf ankommt, ob sie aus der Datei selbst, einer entsprechenden Liste, den Eingabebelegen oder einer inhaltlich mit ihnen übereinstimmenden Akte übermittelt werden (so auch 4.1.2 des Ersten Tätigkeitsberichts des Bundesbeauftragten für den Datenschutz).

Personalakten sind keine Dateien. Personalkarteien sind Dateien. Werden Daten, die den Personalakten entnommen sind, in einer Personalkartei gespeichert, so unterliegt ihre Übermittlung nach § 1 Abs. 2 Satz 1 DSG NW den Beschränkungen des Datenschutzgesetzes Nordrhein-Westfalen, soweit nicht wegen ihrer Herkunft aus den Personalakten nach anderen Rechtsvorschriften ein weitergehender Schutz besteht.

Während die Frage, ob eine Datensammlung als Datei anzusehen ist, in der Praxis kaum noch Schwierigkeiten bereitet, ist die damit vorgenommene Beschränkung des Anwendungsbereichs des Gesetzes umstritten. Es gibt Aktensammlungen, die durch automatisierte Fundstellennachweise inhaltlich erschlossen werden. Dadurch werden die in den Akten festgehaltenen Daten in ähnlicher Weise verfügbar, wie bei einer Speicherung in einer Datei. In diesen Fällen sind zwar die in den Fundstellennachweisen enthaltenen personenbezogenen Daten durch das Gesetz geschützt, die wesentlich genaueren Einzelangaben in den Akten dagegen nicht. Die Auffassung des Hessischen Datenschutzbeauftragten, daß bei solchen Informationssystemen Akten und Fundstellennachweis eine Einheit bilden und deshalb der gesamte Datenbestand einschließlich der allein in den Akten festgehaltenen Daten unter den Schutz des Gesetzes falle (5.1.1 des Siebenten Tätigkeitsberichts), hat sich noch nicht durchgesetzt.

c) Interne Datei

Nach § 1 Abs. 2 Satz 3 DSG NW gilt für personenbezogene Daten, die nicht zur Übermittlung an Dritte bestimmt sind und in nicht automatisierten Verfahren verarbeitet werden, nur § 6 DSG NW, soweit er die Verpflichtung enthält, technische und organisatorische Maßnahmen zum Schutz dieser Daten gegenüber Dritten zu treffen.

Zu den Voraussetzungen dieser Ausnahmeregelung für interne Dateien mußte ich auf Anfrage einer Stadt klarstellen, daß Daten in Karteien, die lediglich als Arbeitshilfe für das schnellere Auffinden von Fallakten geführt werden, nicht zur Übermittlung an Dritte bestimmt sind. Das gleiche gilt für Daten in Karteien, die lediglich für das Schreiben von Gebührenbescheiden verwendet werden, sofern der Gebührenbescheid nicht an eine andere Person oder Stelle außerhalb der speichernden Stelle, ausgenommen den Betroffenen (§ 2 Abs. 3 Nr. 2 DSG NW), weitergegeben wird. Eine Stadtkasse ist für andere städtische Ämter kein Dritter, da speichernde Stelle die Gemeinde in ihrer Gesamtheit ist (§ 2 Abs. 3 Nr. 1 in Verbindung mit § 1 Abs. 2 Satz 1 DSG NW).

Die Ausnahmeregelung für interne Dateien enthält eine wesentliche Einschränkung der Anwendbarkeit des Gesetzes. Beim Bürger stößt es immer wieder auf Unverständnis, daß

der Schutz seiner Daten, insbesondere der Schutz vor unbefugter Nutzung, davon abhängig gemacht wird, daß diese Daten befugterweise auch Dritten übermittelt werden.

d) Datenerhebung

Regelungen für die Datenerhebung enthält das Datenschutzgesetz Nordrhein-Westfalen allein in § 10 Abs. 2. Danach ist der Betroffene auf die der Erhebung zugrunde liegende Rechtsvorschrift oder, falls eine solche nicht besteht, auf die Freiwilligkeit seiner Angaben hinzuweisen. Dem Betroffenen dürfen aus der Verweigerung der Einwilligung keine Nachteile entstehen.

An mich ist die Frage herangetragen worden, ob die Hinweispflicht voraussetzt, daß die zu erhebenden Daten anschließend in einer Datei gespeichert werden. In Übereinstimmung mit dem Bundesbeauftragten für den Datenschutz habe ich dies aus den nachfolgenden Gründen verneint.

§ 1 Abs. 2 Satz 1 DSG NW, der den Anwendungsbereich des Gesetzes auf Datenverarbeitung in Dateien beschränkt, nennt als Phase der Datenverarbeitung nicht die Datenerhebung, die kein Bestandteil der Speicherung, sondern dieser vorgelagert ist. § 10 Abs. 2 DSG NW ist ein Ausfluß eines allgemeinen Rechtsprinzips, das die Aufklärung des Bürgers über seine Rechtspflichten verlangt. Die Vorschrift dient dem Schutz des Betroffenen. Dieser Schutz wäre unvollkommen und die Rechtssicherheit nicht gewährleistet, wenn die in der Vorschrift vorgesehene Hinweispflicht von einem künftigen ungewissen Ereignis abhängig gemacht würde. Denn nicht immer wird die Stelle, die die Daten erheben will, zu diesem Zeitpunkt schon wissen, ob eine Speicherung in einer Datei erfolgen wird. Auch ließe sich die Hinweispflicht dadurch umgehen, daß die Entscheidung darüber, ob eine Speicherung in einer Datei erfolgen soll, bewußt zurückgestellt wird.

Da die Hinweispflicht somit nicht von einer anschließenden Speicherung in einer Datei abhängig gemacht werden kann, gilt auch die Einschränkung der Anwendbarkeit des Gesetzes für interne Dateien (§ 1 Abs. 2 Satz 3 DSG NW) nicht für die Vorschrift über die Hinweispflicht.

Mit der Praxis der Datenerhebung hat sich die Konferenz der Datenschutzbeauftragten der Länder und des Bundes befaßt. In einer einvernehmlichen Stellungnahme, über die ich den Innenminister unterrichtet habe, hat sie die Auffassung vertreten, daß die Behörden in Anwendung des neuen Datenschutzrechts vor allem die jeweilige Notwendigkeit einer Datenerhebung prüfen müssen.

Alle Fragebögen, Antragsformulare und sonstige Datenerhebungsfälle sind nach den Datenschutzgesetzen daraufhin zu überprüfen, ob auch tatsächlich alle verlangten Daten für die Aufgabe der Behörde konkret erforderlich sind. Keine Angabe darf erhoben oder gespeichert werden, die nicht erforderlich ist. Außerdem ist auf den Fragebögen und Formularen die Rechtsgrundlage für die Erhebung klar und in einer allgemein verständlichen Form anzugeben oder auf die Freiwilligkeit der Angaben unmißverständlich hinzuweisen.

2. Bereichübergreifende Fragen

a) Speichernde Stelle

Nach § 2 Abs. 3 Nr. 1 in Verbindung mit § 1 Abs. 2 Satz 1 DSG NW sind speichernde Stellen die Behörden, Einrichtungen und sonstigen öffentlichen Stellen des Landes, die Gemeinden und Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen, die Daten für sich selbst speichern oder durch andere speichern lassen.

Verantwortlich für den Datenschutz ist danach diejenige Stelle, die die Verarbeitung der Daten veranlaßt, also der „Herr der Daten", unabhängig davon, ob er die Datenverarbeitung selbst technisch durchführt oder eine andere Stelle damit beauftragt.

Abweichend von dem Bundesdatenschutzgesetz und anderen Landesdatenschutzgesetzen behandelt das Datenschutzgesetz Nordrhein-Westfalen die Gemeinden und Gemeindeverbände als Einheit. Für den Bürger hat dies den Vorteil, daß er seine Rechte nach dem Gesetz gegenüber der Gemeinde oder dem Gemeindeverband als Ganzes geltend machen kann und nicht die jeweils zuständige Untereinheit ausfindig machen muß.

b) Betroffener

Nach § 2 Abs. 1 DSG NW ist Betroffener diejenige bestimmte oder bestimmbare natürliche Person, über deren persönliche oder sachliche Verhältnisse Einzelangaben verarbeitet werden. Ein Betroffener kann Rechte nach dem Gesetz geltend machen (§ 4 DSG NW). Seine Einwilligung ist erforderlich, soweit nicht das Gesetz oder eine andere Rechtsvorschrift die Verarbeitung seiner personenbezogenen Daten erlaubt (§ 3 Satz 1 Nr. 2 DSG NW). Bei Erhebung von Daten bei ihm selbst ist er auf die Rechtsgrundlage oder auf die Freiwilligkeit seiner Angaben hinzuweisen (§ 10 Abs. 2 Satz 1 DSG NW).

Oft sind Daten Einzelangaben über die Verhältnisse mehrerer Betroffener, etwa bei Angaben über Eltern, Ehegatten und Kinder. Die Frage der Behandlung solcher Daten ist auch im Kreise der Datenschutzbeauftragten des Bundes und der Länder erörtert worden. Ich bin der Auffassung, daß die Rechte nach § 4 DSG NW von jedem der Betroffenen geltend gemacht werden können. Grundsätzlich ist nach § 3 Satz 1 Nr. 2 DSG NW die Einwilligung jedes der Betroffenen erforderlich. Nur so kann eine Verletzung des Grundrechts jedes Einzelnen auf Schutz seiner personenbezogenen Daten ausgeschlossen werden. Ob unter bestimmten Voraussetzungen die Einwilligung eines oder eines Teils der Betroffenen als ausreichend angesehen werden kann, bedarf noch eingehender Prüfung. Die Hinweispflicht nach § 10 Abs. 2 Satz 1 DSG NW besteht nach dem Zweck der Vorschrift nur gegenüber dem Betroffenen, bei dem die Daten erhoben werden.

c) Datengeheimnis

Nach § 5 Abs. 1 DSG NW ist den bei der Datenverarbeitung beschäftigten Personen untersagt, geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekanntzugeben, zugänglich zu machen oder sonst zu nutzen. Der Bruch des Datengeheimnisses kann straf-, disziplinar- und haftungsrechtliche Folgen für den Bediensteten haben. Dem Betroffenen kann es zudem nach § 4 Abs. 2 DSG NW einen Schadensersatzanspruch gegen die Stelle geben, die die Datenverarbeitung betreibt.

Auf Anfrage eines Bürgers habe ich darauf hingewiesen, daß das Verbot der unbefugten Nutzung unabhängig davon gilt, ob im Einzelfall auch eine Verpflichtung auf das Datengeheimnis nach § 5 Abs. 2 DSG NW vorgenommen worden ist. Eine solche Verpflichtung hat keine konstitutive Wirkung, sondern soll den Beschäftigten auf seine gesetzliche Pflicht hinweisen und einen Verbotsirrtum ausschließen.

Mehrere Anfragen von öffentlichen Stellen und Bürgern betrafen den Umfang des nach § 5 Abs. 2 DSG NW auf das Datengeheimnis zu verpflichtenden Personenkreises. Der Begriff der „bei der Datenverarbeitung beschäftigten Personen" führt zu Abgrenzungsschwierigkeiten. Im Interesse des Datenschutzes ist der Personenkreis weit zu fassen. „Bei der Datenverarbeitung beschäftigt" ist eine Person dann, wenn der ihr übertragene oder von ihr wahrgenommene Tätigkeitskreis sie mit geschützten Daten in der Weise in Verbindung bringt, daß sie diese zur Kenntnis nehmen, verarbeiten oder sonst nutzen kann. Entscheidend ist allein die faktische Möglichkeit solcher Aktivitäten.

Ob sie zur Aufgabenerfüllung gehören, ist unerheblich, ebenso ob sie nach den Anweisungen der speichernden Stelle erlaubt oder verboten sind. Auch auf den Schwerpunkt der Tätigkeit kommt es nicht an. Es genügen auch typische Begleit- und Hilfsfunktionen (so Dammann in Simitis/Dammann/Mallmann/Reh, BDSG, 2. Aufl., § 5 Rdnr. 6).

Die Entscheidung, welche Bediensteten einer datenverarbeitenden Stelle auf das Datengeheimnis zu verpflichten sind, muß diese in ihrer Verantwortung nach § 6 Abs. 1 DSG NW selbst treffen.

Das Datengeheimnis nach § 5 Abs. 1 DSG NW hat eigenständigen Charakter. Pflichten aus anderen Lebensbereichen, die Ausfluß bestimmter Vertrauensstellungen sind, bleiben zwar unberührt, können andererseits aber auch das Datengeheimnis in seinen Auswirkungen nicht verdrängen. Die Pflicht zur Amtsverschwiegenheit steht einer — zusätzlichen — Verpflichtung auf das Datengeheimnis weder entgegen, noch macht sie sie entbehrlich.

Probleme in Grenzbereichen sind allerdings nicht vermeidbar. So bleibt die wiederholt von Gemeinden an mich herangetragene Frage zu entscheiden, ob auch Ratsmitglieder, Mitglieder von Bezirksvertretungen, sachkundige Bürger und andere ehrenamtlich Tätige, die Zugang zu in Dateien verarbeiteten personenbezogenen Daten haben, auf das Datengeheimnis zu verpflichten sind. Hierzu besteht offenbar eine unterschiedliche Praxis. Im Interesse einer einheitlichen Regelung im Lande Nordrhein-Westfalen habe ich zunächst den Innenminister unterrichtet und um Stellungnahme gebeten.

d) Technische und organisatorische Maßnahmen

— Bestellung eines internen Datenschutzbeauftragten

Die Bestellung eines internen Datenschutzbeauftragten für eine Behörde oder sonstige öffentliche Stelle ist im Datenschutzgesetz Nordrhein-Westfalen nicht vorgesehen. In welcher Form die datenschutzrechtliche Selbstkontrolle der Verwaltung durchgeführt wird, ist im Rahmen der §§ 6 und 8 DSG NW von der Verwaltung nach pflichtgemäßem Ermessen zu entscheiden. Ein Verbot, mit dieser Selbstkontrolle den Vorgesetzten der EDV-Abteilung zu beauftragen, enthält das Datenschutzgesetz Nordrhein-Westfalen nicht.

Die Bestellung des Vorgesetzten der EDV-Abteilung zum Datenschutzbeauftragten hätte allerdings zur Folge, daß damit der Kontrolleur sich selbst kontrolliert; dadurch könnte der Zweck der Kontrolle beeinträchtigt werden. Die Verantwortung für die Durchführung des Datenschutzes obliegt auf jeden Fall dem Leiter der jeweiligen datenverarbeitenden Behörde oder Stelle.

— Kontrolle durch den internen Datenschutzbeauftragten

Auch ohne eine ausdrückliche Verpflichtung durch das Datenschutzgesetz Nordrhein-Westfalen haben die Behörden und Körperschaften im allgemeinen einen internen Datenschutzbeauftragten bestellt. Diesem obliegt dann die Kontrolle der Einhaltung der Vorschriften über den Datenschutz.

In diesem Zusammenhang scheint mir ein Hinweis auf den zweckmäßigen Umfang dieser Kontrolle angebracht zu sein, soweit sie sich auf Fragen der Datensicherheit — insbesondere beim Einsatz von ADV — erstreckt.

Hier geht es vor allem um die Kontrolle der Einhaltung von Dienstanweisungen, die einer detaillierten Regelung organisatorischer Abläufe dienen. Geregelt sind dort zum Beispiel Fragen wie die Sicherung von Systemdaten, die Programmsicherung, die Archivierung oder auch allgemeine Sicherheitsvorkehrungen für das Rechenzentrum.

Der interne Datenschutzbeauftragte sollte seine Aufgabe so begreifen, und diese sollte auch entsprechend von der Behördenleitung formuliert sein, daß durch ihn im Rahmen einzelner Prüfungen die Einhaltung der bestehenden Dienstanweisungen

bis ins letzte Detail zu kontrollieren ist. Globale Überprüfungen sind nicht ausreichend. Im konkreten Fall muß auch die Archivierung des einzelnen Bandes oder der spezielle Verarbeitungslauf der einzelnen Datei kontrolliert werden. Erst dadurch lassen die Kontrollen erkennen, ob bestehende Dienstanweisungen auch wirklich eingehalten werden. Für die Dienstanweisungen selbst ergibt sich der günstige Nebeneffekt, daß sie in allen Detailregelungen präzise formuliert sein müssen, um die Durchführung der gewünschten Kontrollen überhaupt erst zu ermöglichen.

— Programmfreigabe

Es sollte selbstverständlich sein, ein neu entwickeltes Programm erst dann in den routinemäßigen Einsatz zu nehmen, wenn es von der zuständigen Fachabteilung — dem „Herrn der Daten" — freigegeben worden ist. Auch jede Programmänderung, die sich auf den sachlichen Inhalt des Programms auswirkt, bedarf einer Freigabe durch die Fachabteilung.

Vergessen wird aber leider in Einzelfällen, in die Freigabeprozedur auch den internen Datenschutzbeauftragten einzubeziehen. Dieser hätte, wäre er eingeschaltet, noch eine letzte Möglichkeit, eventuelle Bedenken des Datenschutzes zu äußern und deren Berücksichtigung zu verlangen. Es sollten daher nur solche Programme für den echten Betrieb zugelassen sein, die nicht nur von der Fachabteilung, sondern auch vom Datenschutzbeauftragten offiziell und in schriftlicher Form freigegeben sind.

— Zugang zu personenbezogenen Daten

Welche Mitarbeiter einer Dienststelle zur Erfüllung ihrer Aufgaben Kenntnis von personenbezogenen Daten erhalten müssen, hat die Dienststelle im Rahmen der §§ 6 und 8 DSG NW nach pflichtgemäßem Ermessen zu entscheiden. Aus Gründen der Datensicherung empfiehlt es sich, den Kreis dieser Mitarbeiter möglichst klein zu halten.

— Transport von Magnetbändern

Zur Einsparung der Kosten einer erneuten Datenerfassung und um die dabei zu erwartenden Erfassungsfehler zu vermeiden, ist es heute weitgehend üblich, Dateien durch Versenden entsprechender Magnetbänder zu übermitteln. Je nach der Art der Daten, nach der zur Verfügung stehenden Zeit und nach den örtlichen und personellen Möglichkeiten werden für den Transport unterschiedliche Methoden wie etwa der Versand als Wertpaket oder die Abholung durch Boten praktiziert.

Durch den Empfänger wird das übermittelte Band nach der Verarbeitung im allgemeinen noch für eine gewisse Zeit archiviert und dann an den Absender zurückgesandt. Bei dieser Rücksendung ist leider immer wieder zu beobachten, daß das Magnetband noch seinen gesamten ursprünglichen Datenbestand enthält und nicht etwa — was von der Sache her ohne weiteres möglich wäre — vorher gelöscht wurde. Es gibt keinen sachlichen Grund, warum dem Absender die von ihm stammenden Daten auf dem Magnetband wieder zurückgesandt werden. Das in jedem Magnetbandtransport liegende Transportrisiko wird bei fehlender Löschung auf dem Rückweg völlig unnötig in Kauf genommen.

Eine derartige Praxis werde ich keinesfalls tolerieren. Ich halte es für unvertretbar, wenn ein zum Transport vorgesehenes Magnetband eine Datei mit personenbezogenen Daten enthält, ohne daß der Transport dieser Datei sachlich erforderlich ist. Deshalb müssen Magnetbänder mit personenbezogenen Daten vor ihrer Rücksendung gelöscht werden.

— Vermeidung von Personenverwechslungen

Ein Bürger hat sich darüber beschwert, daß ihm auf Grund einer Verwechslung im Einwohnermeldeamt mit einem wegen Diebstahl Verurteilten gleichen Namens Mitteilungen zweier Amtsgerichte zugegangen sind.

Um Verwechslungen in Fällen von Namensgleichheit auszuschließen, sollten für derartige Fälle die Mitarbeiter angewiesen werden, vor der Auskunftserteilung an Dritte die Identität der gesuchten Person anhand eines Geburtsdatums oder anderer von dem Auskunftssuchenden beizubringender Daten festzustellen.

- **Telefonische Auskünfte**

  Um eine Verletzung des Datengeheimnisses auszuschließen, dürfen grundsätzlich keine fernmündlichen Auskünfte über personenbezogene Daten erteilt werden. Wenn ausnahmsweise aus zwingenden Gründen auf eine fernmündliche Anfrage eine fernmündliche Auskunft gegeben wird, muß nach sorgfältiger Überprüfung der Telefonnummer auf Grund amtlicher Unterlagen durch Rückruf bei der anfragenden Stelle deren Identität eindeutig festgestellt sein. Ein Rückruf unter der von dem Anrufer angegebenen Telefonnummer ist untauglich, die Identität der anfragenden Stelle festzustellen.

e) Auftragsdatenverarbeitung

Die Verarbeitung personenbezogener Daten im Auftrag, in Nordrhein-Westfalen nach dem Gesetz über die Organisation der automatisierten Datenverarbeitung in Nordrhein-Westfalen (ADV-Organisationsgesetz) der Regelfall, ist in § 7 DSG NW geregelt. Der Gesetzgeber stellt hier ausdrücklich klar, daß der Auftraggeber den Vorschriften des Datenschutzgesetzes voll unterworfen bleibt (§ 7 Abs. 1 Satz 1 DSG NW). Sofern diese Vorschriften auf den Auftragnehmer keine Anwendung finden, ist er verpflichtet, sicherzustellen, daß der Auftragnehmer die Bestimmungen des Gesetzes beachtet und sich der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft (§ 7 Abs. 1 Satz 2 DSG NW).

Unklare Vertragsgestaltung oder unzutreffende datenschutzrechtliche Wertung des Vertragsverhältnisses werden sich fast immer zu Lasten des Datenschutzes auswirken. So habe ich bei einem Kontrollbesuch auf Grund der tatsächlichen Umstände durchweg Merkmale einer Datenverarbeitung im Auftrag festgestellt, während der Auftraggeber die Auffassung vertrat, er betreibe ein eigenes Rechenzentrum. Die Folge war, daß sich der Auftragnehmer, ein privates Dienstleistungs-Rechenzentrum, weder zur Beachtung der Bestimmungen des Datenschutzgesetzes Nordrhein-Westfalen verpflichtet noch sich der Kontrolle des Landesbeauftragten für den Datenschutz unterworfen hatte.

Die Gefahr einer falschen Wertung des Vertragsverhältnisses liegt nahe, wenn Vertragsgegenstand die Vernichtung von Altpapier ist. Sofern auch Datenträger aus Dateien vernichtet werden, handelt es sich um eine Löschung als Phase der Datenverarbeitung. Damit ist Vertragsgegenstand eine Datenverarbeitung im Auftrag mit den sich für den Auftraggeber ergebenden Verpflichtungen aus § 7 Abs. 1 Satz 2 DSG NW.

Von der Datenverarbeitung im Auftrag zu unterscheiden sind allerdings Werkverträge, bei denen der Unternehmer sich verpflichtet, ein bestimmtes Werk herzustellen, für das er selbst in eigener Verantwortung personenbezogene Daten verarbeiten muß.

f) Übersicht nach § 8 DSG NW

Nach § 8 Satz 2 Nr. 1 DSG NW haben die datenverarbeitenden Stellen eine Übersicht zu führen, die mindestens folgende Angaben enthält:

- die Art der gespeicherten personenbezogenen Daten,
- die Aufgaben, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist,
- die Empfänger oder Empfängergruppen,
- die Voraussetzungen für die Übermittlung der Daten.

Die Übersicht dient als Grundlage bei der Erfüllung der Veröffentlichungspflicht (§ 15 Abs. 1 DSG NW), der Auskunftspflicht (§ 16 Abs. 1 DSG NW) und der Meldepflicht zum

Dateienregister (§ 27 Abs. 3 DSG NW). In Verbindung mit den Vorschriften über die Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitung (§ 8 Satz 2 Nr. 2 DSG NW) und über die technischen und organisatorischen Sicherungsmaßnahmen (§ 6 DSG NW und die darin genannte Anlage) ist sie zugleich Voraussetzung für eine Vielzahl von Datenschutzmaßnahmen. Deshalb empfiehlt es sich, die Übersicht nicht auf die dem Datenschutzgesetz Nordrhein-Westfalen unterliegenden Dateien zu beschränken, sondern sie auf alle Sammlungen personenbezogener Daten zu erstrecken und darüber hinaus auch die zur Veröffentlichung und die zur Meldung zum Dateienregister erforderlichen Angaben sowie Angaben über den Grad der Sensibilität der Daten, die Art der Datenverarbeitungsanlage und das eingesetzte Speichermedium aufzunehmen.

g) Veröffentlichung nach § 15 DSG NW

Nach § 15 Abs. 1 Satz 1 DSG NW haben die datenverarbeitenden Stellen ihre Dateien zu veröffentlichen. Auf Anfrage einer Gemeinde habe ich dazu Stellung genommen, ob der aus einer Stammdatei kurzfristig zwecks Datenträgeraustausch auf Magnetbänder als Zwischenträger gespeicherte Datenbestand als Datei zu veröffentlichen ist.

Die Veröffentlichung nach § 15 DSG NW soll den Bürger darüber informieren, wo Daten über ihn gespeichert sein können, damit er in die Lage versetzt wird, von seinem Auskunftsrecht nach § 16 DSG NW gezielt Gebrauch zu machen. Diesem Zweck würde es widersprechen, wenn Magnetbänder, auf denen lediglich für den Datenträgeraustausch personenbezogene Daten vorübergehend gespeichert sind, als gesonderte Dateien nach der Anlage zu § 3 der Datenschutzveröffentlichungsverordnung Nordrhein-Westfalen bekanntgegeben werden. Eine Bekanntgabe dieser Zwischenträger würde dem Bürger über die Angaben für die Stammdatei hinaus keine zusätzlichen Informationen vermitteln, die für die Ausübung seines Auskunftsrechts von Bedeutung sein könnten. Sie würde vielmehr bei dem Bürger Verwirrung stiften.

Ich habe deshalb die Auffassung vertreten, daß Magnetbänder, die lediglich als Zwischenträger im Datenträgeraustausch verwandt werden, nicht gesondert bekanntzugeben sind. Dies kann allerdings nur gelten, wenn die auf den Bändern gespeicherten Daten nach der Datenübermittlung gelöscht und nicht für andere Zwecke verwendet werden.

Eingaben von Bürgern machten im übrigen deutlich, daß Bekanntmachungen nach § 15 DSG NW durchaus auch aufmerksam verfolgt werden. Ein Bürger wandte sich dagegen, daß nach der Bekanntmachung seiner Gemeinde bestimmte sensible Daten regelmäßig an Zeitungen übermittelt werden (§ 15 Abs. 1 Satz 1 Nr. 4 DSG NW). Ich habe das Anliegen gegenüber der Gemeinde aufgegriffen. Diese hat mitgeteilt, daß sie die Daten nur mit schriftlicher Einwilligung des Betroffenen aus Anlaß von Jubiläen übermittelt.

3. Rechte des Betroffenen

a) Auskunftsrecht

Von den Rechten des Betroffenen, die diesem durch das Datenschutzgesetz Nordrhein-Westfalen gegeben sind, nimmt das Auskunftsrecht nach § 16 Abs. 1 Satz 1 DSG NW eine zentrale Stellung ein. In vielen Fällen schafft es für den Bürger erst die Voraussetzungen, andere Rechte wie etwa das auf Berichtigung, Sperrung und Löschung der zu seiner Person gespeicherten Daten, das Recht auf Unterlassung oder Beseitigung einer Beeinträchtigung schutzwürdiger Belange oder den Anspruch auf Schadensersatz gezielt geltend machen zu können. Damit ist auch das Interesse zu erklären, das ich den zahlreichen Eingaben entnehme, in denen Auskunft über gespeicherte Daten erbeten wurde. Trotz des klaren Wortlauts der Vorschrift war es immer wieder notwendig, Inhalt, Umfang und Adressat des Rechts auf Auskunft zu erläutern.

Häufig mußte ich einem offensichtlichen Mißverständnis entgegentreten, das den Bürger veranlaßt hatte, sein Auskunftsrecht beim Landesbeauftragten geltend zu machen. Zur Auskunft verpflichtet ist jedoch die jeweilige speichernde Stelle. Über einen Bürger können bei einer Vielzahl von Stellen Daten gespeichert sein. Soweit er annimmt, daß von einer Behörde oder sonstigen öffentlichen Stelle Daten über ihn gespeichert sind, muß er unmittelbar bei dieser Stelle die Auskunft beantragen.

Anhaltspunkte dafür, bei welchen Stellen Daten über ihn gespeichert sind, kann der Bürger in den Bekanntmachungen über die von den öffentlichen Stellen geführten Dateien finden, die nach § 15 Abs. 1 Satz 1 DSG NW in den jeweiligen Bekanntmachungsorganen veröffentlicht werden. Auf Antrag sind ihm von diesen Stellen auch die bisher schon erschienenen Bekanntmachungen zugänglich zu machen (§ 15 Abs. 1 Satz 2 DSG NW).

Sollte die speichernde Stelle ihm die Auskunft verweigern, so hat er das Recht, sich an den Landesbeauftragten zu wenden (§ 29 DSG NW). In diesen Fällen prüfe ich die Berechtigung der Auskunftsverweigerung und wirke gegebenenfalls darauf hin, daß dem Bürger die gewünschte Auskunft erteilt wird.

Oft ist dem Bürger unklar, an wen er bei einer Kommunalverwaltung seinen Antrag auf Auskunft richten soll. Speichernde Stelle ist in diesem Fall die Gemeinde oder der Gemeindeverband als Ganzes. Das bedeutet, daß der Bürger nicht gehalten ist, das für die Daten im Einzelfall jeweils zuständige Fachamt ausfindig zu machen. Um den Auskunftsanspruch geltend zu machen, genügt es, wenn er sich mit seinem Begehren an die betreffende Kommunalverwaltung wendet, ohne daß es darauf ankommt, welche der einzelnen Fachämter (Meldeamt, Ordnungsamt, Jugendamt usw.) über die ihn interessierenden Daten verfügen.

Allerdings gelangt der Betroffene umso schneller zum Ziele, je konkreter er sein Verlangen umschreibt. Dem dient auch die Regelung in § 16 Abs. 1 Satz 2 DSG NW, nach der in dem Antrag die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden soll. Geschieht dies, kann zudem ein unnötiger und damit — auch für den Bürger — kostenintensiverer Verwaltungsaufwand verhindert werden.

Nicht ohne Einfluß wird hier sein, mit welcher Genauigkeit und Sorgfalt die öffentliche Verwaltung ihrer Veröffentlichungspflicht nach § 15 Abs. 1 Satz 1 DSG NW nachkommt. Je genauer sie den Bürger über die bestehenden Dateien informiert, desto präziser kann der Antrag sein, mit dem dieser eine Auskunft begehrt.

Wie ich Mitteilungen von Gemeinden entnehme, liegt einem Teil der Auskunftsersuchen das Mißverständnis zugrunde, bei den Gemeinden gebe es eine zentrale Sammlung aller auf die Einzelperson bezogener Daten aus den verschiedensten Fachbereichen, die „auf Knopfdruck" abrufbar seien. Häufig führe schon der Hinweis, daß die Daten aufgabenbezogen in den einzelnen Fachämtern oder -abteilungen vorgehalten werden, zu einem Schwinden des Interesses.

Ich sehe dies nicht als gravierend an, soweit man davon ausgehen kann, daß ein nachlassendes Interesse seinen Grund durchaus in der Beruhigung haben kann, die viele Bürger bereits bei der Bestätigung des Nichtbestehens einer „Zentraldatei" empfinden. Nicht auszuschließen ist aber auch, daß Bürger in derartigen Fällen ein höheres Kostenrisiko fürchten, insbesondere im Hinblick darauf, daß eine vermutete Unrichtigkeit gespeicherter Daten im Regelfall nur einen Teil dieser Daten betrifft.

Nach § 16 Abs. 4 Nr. 2 DSG NW findet das Gebührengesetz für das Land Nordrhein-Westfalen mit der Maßgabe Anwendung, daß Ausnahmen von der Gebührenpflicht durch die Gebührenordnung in den Fällen vorzusehen sind, in denen durch besondere Umstände die Annahme gerechtfertigt wird, daß personenbezogene Daten unrichtig oder unzulässig gespeichert werden, oder in denen die Auskunft zur Berichtigung oder Löschung gespeicherter personenbezogener Daten geführt hat. Ich gehe davon aus, daß in derartigen Fällen von einer Gebührenerhebung auch dann Abstand genommen wird, wenn durch das Auskunftsersuchen die Unrichtigkeit gespeicherter personenbezogener

Daten **nur in Teilbereichen** offenbar geworden ist. Auf Eingaben von Bürgern wirke ich bei den speichernden Stellen darauf hin, daß so verfahren wird.

Dennoch bleibt die Frage nach der Berechtigung einer Gebührenpflicht überhaupt. Hier bestehen grundsätzliche Bedenken, mit denen sich auch die Konferenz der Datenschutzbeauftragten der Länder und des Bundes befaßt hat. In einer einvernehmlichen Stellungnahme, über die ich den Innenminister unterrichtet habe, hat sich gegen die Erhebung von Kosten ausgesprochen:

Die Erhebung von Kosten (Gebühren und Auslagen) für die Geltendmachung von Rechten nach den Datenschutzgesetzen laufen dem Grundgedanken des Datenschutzes zuwider: Das Recht auf Auskunft über gespeicherte Daten z. B. soll eine erhöhte Durchsichtigkeit der zunehmend automatisierten Verwaltung bewirken. Das Recht auf Sperrung gespeicherter Daten hat zum Ziel, daß vor allem die automatisierte Verarbeitung bei unklarem Sachverhalt nicht den Bürger überrollt. Die Erhebung von Kosten für Auskunft oder Sperrung würde eine Abschreckungswirkung auslösen, die grundsätzlich den Gehalt dieser Rechte in Frage stellt.

b) Anrufungsrecht

§ 29 DSG NW gibt jedermann das Recht, sich unmittelbar an den Landesbeauftragten für den Datenschutz zu wenden, wenn er sich bei der Verarbeitung seiner personenbezogenen Daten durch öffentliche Stellen in seinen schutzwürdigen Belangen verletzt glaubt. Von diesem Recht wurde in zahlreichen Fällen Gebrauch gemacht.

Nicht immer wird von dem Bürger erkannt, daß ein Anrufungsrecht nur dann besteht, wenn es um die Verarbeitung **seiner** personenbezogenen Daten geht. Gleichwohl habe ich stets versucht, in datenschutzrechtlichen Anliegen Aufklärung weitgehend auch dann zu geben, wenn die Eingabe nicht oder nicht erkennbar die Verarbeitung eigener personenbezogener Daten betraf. Ich habe mich hierbei davon leiten lassen, daß jede Information in Angelegenheiten des Datenschutzes dazu beiträgt, das Datenschutzbewußtsein zu fördern.

Schranken ergeben sich aus den Aufgaben des Landesbeauftragten. So kann von dem Landesbeauftragten nicht etwa Auskunft über die gespeicherten Daten nach § 16 DSG NW verlangt werden. Auch ist seine Kontrolltätigkeit nicht darauf gerichtet, bei der Beschaffung von personenbezogenen Daten Dritter behilflich zu sein.

Grenzen können sich auch bei der Vertretung der Belange des Bürgers ergeben. Dies gilt insbesondere dann, wenn eine notwendige Klärung des Sachverhalts mit den mir zur Verfügung stehenden Mitteln nicht möglich ist, weil Vermutungen des Bürgers Einlassungen derjenigen Stellen entgegenstehen, über deren Verhalten Beschwerde geführt wird.

In einem Falle glaubte ein Bürger, Mitglied einer Berufskammer, daß von der Kammer oder ihren Mitarbeitern Anschriften von Kammermitgliedern an ein Versicherungsunternehmen weitergegeben worden seien. Er bat um Überprüfung der Angelegenheit. Gewährspersonen wurden hierbei nicht benannt und konnten möglicherweise auch nicht benannt werden. Auf meine Bitte um Stellungnahme hat die Kammer den erhobenen Vorwurf mit Entschiedenheit als falsch zurückgewiesen.

Einem anderen Falle lag der Verdacht einer unzulässigen Datenübermittlung an einen Journalisten durch eine Behörde zugrunde. Auf mein Auskunftsersuchen hat mir die Behörde nach Anhörung der in Betracht kommenden Beamten mitgeteilt, daß diese keine derartigen Angaben gegenüber einem Dritten gemacht hätten.

Auch hier fehlte es an näheren Hinweisen, die zu einer Klärung des Sachverhalts hätten führen können.

Ich muß deshalb jeden Bürger um Verständnis bitten, dessen Eingabe trotz meiner Bemühungen in der Sache wenig Erfolg beschieden war, weil nur allgemein gehaltene Verdachtsmomente gegenüber einer datenverarbeitenden Stelle erhoben werden konnten.

Der Landesbeauftragte für den Datenschutz ist bei seiner Kontrolltätigkeit, soll sie zu befriedigenden Ergebnissen führen, auf die volle Unterstützung und Mitwirkung aller Beteiligten angewiesen.

Wenn ich keine Verstöße gegen Vorschriften über den Datenschutz feststellen kann, ist es nicht meine Aufgabe, den von mir kontrollierten Stellen zu bestätigen, daß sie solche Vorschriften nicht verletzt haben. In den Fällen, in denen der Sachverhalt nicht geklärt werden konnte, wäre ich hierzu auch nicht in der Lage.

c) Andere Rechte

Häufig wurde im Berichtszeitraum um Auskunft aus dem nach § 27 DSG NW vom Landesbeauftragten zu führenden Dateienregister gebeten. Allerdings lag dem meist die irrige Meinung zugrunde, daß das Register eine Sammlung aller personenbezogenen Daten enthalte, die über Bürger gespeichert sind. Vielfach verkennt der Bürger noch die Zweckbestimmung des Registers und glaubt, aus ihm diejenigen (Individual-)Angaben über die zu seiner Person gespeicherten Daten erhalten zu können, die ihm nur die speichernde Stelle selbst mit einer Auskunft nach § 16 DSG NW geben kann. In meinen Antworten versuche ich dies klarzustellen, insbesondere mit dem Hinweis, daß es eine „zentrale Speicherstelle" ohnehin nicht gibt und auch nicht geben darf. Sie würde dem Gedanken des Datenschutzes zuwiderlaufen.

Im übrigen war eine Einsicht in das Register noch nicht möglich, da dieses noch nicht eingerichtet ist (oben A.4.b).

Von den Rechten auf Berichtigung, Sperrung und Löschung von Daten (§ 17 DSG NW) wurde in zahlreichen Fällen Gebrauch gemacht. In einigen dieser Fälle habe ich zur Durchsetzung der Ansprüche des Betroffenen beigetragen.

In zwei Fällen konnte auf Eingaben der Betroffenen nach § 29 DSG NW erreicht werden, daß die speichernde Stelle die Folgen einer Beeinträchtigung schutzwürdiger Belange beseitigt hat (§ 4 Abs. 1 Nr. 6 DSG NW).

Ein Fall, in dem ein Betroffener einen Anspruch auf Schadensersatz (§ 4 Abs. 2 DSG NW) geltend gemacht hat, ist mir nicht bekannt geworden.

4. Gerichtliche Entscheidungen

Zum Grundrecht auf Datenschutz (Artikel 4 Abs. 2 der Landesverfassung) und zum Datenschutzgesetz Nordrhein-Westfalen ist bisher nur eine gerichtliche Entscheidung bekannt geworden (Beschluß des OVG Münster vom 4. 4. 1979, NJW 1979, S. 2221).

Es ist zu begrüßen, daß das Oberverwaltungsgericht Münster darin bestätigt hat, daß für die Erteilung einer Auskunft aus dem Melderegister nach Artikel 4 Abs. 2 der Landesverfassung eine gesetzliche Grundlage erforderlich ist. Der von dem Gericht vertretenen Auffassung, daß neben § 36 Abs. 2 DSG NW für Auskünfte aus dem Melderegister an Stellen außerhalb des öffentlichen Bereichs § 13 Abs. 1 Satz 1 DSG NW nicht ergänzend anzuwenden sei, kann allerdings nicht gefolgt werden (oben C.1.a).

5. Grenzüberschreitender Datenverkehr

Datenschutz ist nicht nur bei Datenverarbeitung im Inland, sondern auch bei grenzüberschreitendem Transport personenbezogener Daten zu gewährleisten. Nach § 13 Abs. 1 Satz 3 DSG NW gelten für die Übermittlung an Behörden oder sonstige Stellen außerhalb

des Geltungsbereichs des Grundgesetzes sowie an über- und zwischenstaatliche Stellen die Vorschriften über die Datenübermittlung an nicht-öffentliche Stellen, jedoch nach Maßgabe der für diese Übermittlung geltenden besonderen Gesetze und Vereinbarungen.

Vor dem Hintergrund zunehmender nationaler Datenschutzgesetzgebung der europäischen und außereuropäischen Staaten, des Aufbaus internationaler Informationsnetze und der damit verbundenen Erleichterungen für einen grenzüberschreitenden Datenverkehr bestehen für den betroffenen Bürger besondere Probleme, hierbei seine Rechte auf Datenschutz wahrzunehmen. Bei unterschiedlichen gesetzlichen Regelungen besteht zudem die Gefahr, daß Lücken in den Datenschutzbestimmungen zum Nachteil des Betroffenen ausgenutzt werden.

Im Berichtszeitraum bin ich mit zwei Entwürfen für internationale Übereinkommen befaßt worden, die auf eine Harmonisierung der nationalen Datenschutzrechte ausgerichtet sind. Es handelt sich einmal um ein „Übereinkommen zum Schutz des Einzelnen im Hinblick auf die automatisierte Verarbeitung personenbezogener Daten" (Europarat-Konvention), zum anderen um die „Leitlinien für den Schutz der Privatsphäre und den grenzüberschreitenden Verkehr personenbezogener Daten" (OECD-Leitlinien).

Zur Zeit noch nicht entschieden ist im Zusammenhang mit der erwarteten **Europarat-Konvention** die Frage, wer im Sinne der Konvention als hilfeleistende Behörde benannt werden soll.

Nach Artikel 13 Abs. 1 des Entwurfs verpflichten sich die Vertragsparteien, einander zur Durchführung dieses Übereinkommens gegenseitige Hilfe zu leisten; zu diesem Zweck benennt jede Vertragspartei eine oder mehrere Behörden. Nach Artikel 13 Abs. 2 des Entwurfs kann eine von einer Vertragspartei benannte Behörde auf Ersuchen einer von einer anderen Vertragspartei benannten Behörde

a) Informationen über ihre Rechts- und Verwaltungspraxis im Bereich des Datenschutzes liefern;
b) Sachinformationen über bestimmte Dateien mit personenbezogenen Daten liefern, die in ihrem Hoheitsgebiet verarbeitet werden, ausgenommen davon sind jedoch die in diesen Dateien enthaltenen personenbezogenen Daten;
c) in Übereinstimmung mit den innerstaatlichen Rechtsvorschriften die in dem Antrag erbetenen Ermittlungen bezüglich einer Datei oder zur Datenverarbeitung verwendeter Einrichtungen, Geräte oder Methoden anstellen.

Die Konferenz der Datenschutzbeauftragten der Länder und des Bundes hat zu der Benennung einer hilfeleistenden Behörde einen Vorschlag unterbreitet.

Die Frage der Ernennung nationaler Vertreter stellt sich in ähnlicher Weise bei den **OECD-Leitlinien**. Im Kapitel V „Internationale Zusammenarbeit" ist unter lfd. Nr. 21 geregelt, daß die Länder Verfahren festlegen sollten, um

(i) den mit diesen Leitlinien zusammenhängenden Informationsaustausch;

(ii) die gegenseitige Hilfe in den dabei auftretenden Verfahrens- und Ermittlungsfragen zu erleichtern.

Ich gehe davon aus, daß beide Probleme einheitlich gelöst werden.

E. Weiterer Ausbau des Datenschutzes

1. Änderung des Datenschutzgesetzes Nordrhein-Westfalen

Das Datenschutzgesetz Nordrhein-Westfalen ist seit 15 Monaten in Kraft. Der Landesbeauftragte für den Datenschutz hat sein Amt vor knapp 7 Monaten angetreten. Für ein Urteil darüber, ob das Gesetz sich praktisch bewährt habe, ist es noch zu früh. Mit diesem Vorbehalt sind jedoch seine Auswirkungen positiv zu bewerten. Insbesondere nötigt das Gesetz alle öffentlichen Stellen, sich und anderen Rechenschaft über die Notwendigkeit sowie über die Art und Weise der Verarbeitung personenbezogener Daten zu geben.

Auf Grund der bisherigen Erfahrungen mit dem Gesetz schlage ich jedoch folgende Änderungen vor:

a) Die Erhebung von Kosten (Gebühren und Auslagen) für das Wahrnehmen von Rechten nach dem Datenschutzgesetz Nordrhein-Westfalen widerspricht dem Grundgedanken des Datenschutzes, wonach nicht das Verbot des Umgangs mit personenbezogenen Daten, sondern der Umgang selbst einer Legitimierung bedarf. Insbesondere das Auskunftsrecht gehört zu den grundlegenden Datenschutzrechten des Bürgers. Erst die Auskunft über die über ihn gespeicherten Daten versetzt den Bürger in die Lage, von seinen weiteren Rechten gegen unrichtige oder unzulässige Datenverarbeitung Gebrauch zu machen. Die Erhebung von Kosten schreckt ihn hiervon ab. Damit wird grundsätzlich der Gehalt dieser Rechte in Frage gestellt. Die Regelung über die Erhebung von Kosten für das Erteilen von Auskünften über gespeicherte personenbezogene Daten (§ 16 Abs. 4 DSG NW) sollte deshalb aufgehoben werden. Stattdessen sollte hierfür sowie für das Geltendmachen anderer Rechte nach dem Datenschutzgesetz Nordrhein-Westfalen (wie Berichtigung, Sperrung und Löschung) ausdrücklich Kostenfreiheit vorgesehen werden.

b) Die Regelung für die Übermittlung an Personen und andere nicht-öffentliche Stellen in der 2. Alternative des § 13 Abs. 1 Satz 1 DSG NW hat sich nicht bewährt. Nach herrschender Auffassung fordert sie eine Abwägung zwischen den berechtigten Interessen des Empfängers und den Belangen des Betroffenen, die von den übermittelnden Stellen praktisch nicht zu leisten ist. Sofern der Empfänger nicht ein qualifiziertes (rechtliches oder öffentliches) Interesse geltend macht, wird kaum jemals auszuschließen sein, daß durch die Übermittlung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

   Diese Regelung sollte deshalb dahin geändert werden, daß eine Übermittlung zulässig ist, soweit sie zur Wahrung rechtlicher Interessen des Empfängers oder von Interessen der Allgemeinheit erforderlich ist und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden; dem Betroffenen ist die beabsichtigte Übermittlung vorher mitzuteilen. Bei einer solchen Regelung kann aus einem Schweigen des Betroffenen geschlossen werden, daß der Übermittlung keine schutzwürdigen Belange des Betroffenen entgegenstehen.

c) Die Regelung über das Datengeheimnis in § 5 Abs. 1 DSG NW hat zu Auslegungsschwierigkeiten geführt. Der Kreis der Personen, die „bei der Datenverarbeitung beschäftigt" sind, ist nach dem Wortlaut nicht eindeutig zu bestimmen. Zweifel haben sich insbesondere hinsichtlich des Hilfspersonals, das Zugang zu personenbezogenen Daten hat, sowie in Gemeinden hinsichtlich der Ratsmitglieder und sachkundigen Bürger ergeben.

   Das Datengeheimnis soll den Betroffenen vor unbefugter Nutzung seiner Daten schützen. Diesem Zweck würde es widersprechen, die Anwendung der Vorschrift von

der Art des Rechtsverhältnisses zwischen der speichernden Stelle und dem unbefugten Nutzer abhängig zu machen. Nach dem Zweck der Vorschrift muß das Datengeheimnis für alle Personen gelten, die bei der speichernden Stelle Zugang zu personenbezogenen Daten haben. Dies sollte durch eine entsprechende Änderung des § 5 Abs. 1 DSG NW klargestellt werden.

d) Von § 10 Abs. 2 DSG NW abgesehen ist die Datenerhebung im Gesetz nicht geregelt. § 3 Abs. 1 DSG NW, der die Zulässigkeit der Datenverarbeitung in allen vom Gesetz geregelten Phasen von einer Rechtsvorschrift oder der Einwilligung des Betroffenen abhängig macht, gilt deshalb nicht für die Datenerhebung. Diese ist jedoch ebenso wie die Speicherung und die Übermittlung ein Eingriff in das Grundrecht auf Datenschutz, der einer gesetzlichen Grundlage bedarf.

   Daher sollte die Datenerhebung in § 1 Abs. 2 Satz 1 DSG NW als erste Phase der Datenverarbeitung genannt werden. Damit wird klargestellt, daß sie nur zulässig ist, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat (§ 3 Satz 1 DSG NW). Auf eine Generalklausel im Datenschutzgesetz Nordrhein-Westfalen, die die Datenerhebung erlaubt, sollte verzichtet werden. Die gesetzliche Grundlage für die jeweilige Datenerhebung sollte, soweit noch nicht vorhanden, bereichspezifisch geschaffen werden.

e) Die Regelung für interne Dateien in § 1 Abs. 2 Satz 3 DSG NW hat zu Auslegungsschwierigkeiten geführt und darüber hinaus den Schutz des Bürgers in unvertretbarer Weise eingeschränkt. Es ist kein vernünftiger Grund erkennbar, bei Daten, die in Karteien verarbeitet werden, den Umfang des Schutzes davon abhängig zu machen, ob diese Daten (auch) zur Übermittlung an Dritte bestimmt sind. Für das Datengeheimnis, die Zulässigkeit der Speicherung, die Berichtigung, die Sperrung und die Löschung kann dies nicht entscheidend sein. Auch die Regelungen für die Übermittlung an Dritte sind für diese Daten nicht entbehrlich, da trotz interner Zweckbestimmung eine gelegentliche Übermittlung möglich ist.

   Die Vorschrift des § 1 Abs. 2 Satz 3 DSG NW sollte deshalb gestrichen werden. Allenfalls wäre eine Ausnahme von der Veröffentlichungs- und Auskunftspflicht (§§ 15 und 16 DSG NW) vertretbar. Insbesondere ist unverständlich, daß das Verbot des unbefugten Verarbeitens, Bekanntgebens, Zugänglichmachens oder sonstigen Nutzens davon abhängig gemacht wird, daß die Daten befugterweise einem Dritten übermittelt werden. Deshalb muß auf jeden Fall die Vorschrift über das Datengeheimnis (§ 5 DSG NW) Anwendung finden.

f) Die Beschränkung des Anwendungsbereichs des Datenschutzgesetzes Nordrhein-Westfalen auf Dateien (§ 1 Abs. 2 Satz 1 DSG NW) halte ich nicht für sachgerecht. Schutzwürdig und schutzbedürftig sind auch solche personenbezogenen Daten, die nicht in Dateien gespeichert, sondern in Akten, Listen oder sonstigen Unterlagen festgehalten werden. Für die Schutzwürdigkeit ist die Art der Datenverarbeitung ohne jede Bedeutung. Für das Maß der Schutzbedürftigkeit mag die Art der Datenverarbeitung zwar Anhaltspunkte geben; diese kann aber, wie die Eingaben an den Landesbeauftragten zeigen, nicht letztlich entscheidend sein.

   Der gegen einen Verzicht auf den Dateibegriff erhobene Einwand, daß der Anwendungsbereich des Gesetzes dann nicht mehr überschaubar wäre und ein korrekter Gesetzesvollzug sowie eine wirksame Datenschutzkontrolle mit vertretbarem Aufwand nicht mehr gewährleistet werden könne, überzeugt nach meiner Auffassung nicht. Zusätzlicher Verwaltungsaufwand kann, wenn es um die Verwirklichung des Grundrechts des Bürgers auf Datenschutz geht, kein entscheidender Gesichtspunkt sein. Allerdings müßten bei Wegfall des Dateibegriffs einige Vorschriften des Gesetzes (insbesondere über Veröffentlichung, Auskunft und Löschung) an die Gegebenheiten der Datenverarbeitung außerhalb einer Datei angepaßt werden.

   Auf jeden Fall sollten die Vorschriften über das Datengeheimnis (§ 5 DSG NW) und

über technische und organisatorische Maßnahmen (§ 6 DSG NW) auch auf Daten Anwendung finden, die nicht in Dateien verarbeitet werden.

g) Um Auseinandersetzungen über den Umfang der Kontrollbefugnis des Landesbeauftragten zu vermeiden, sollte in § 26 Abs. 1 Satz 1 DSG NW klargestellt werden, daß der Landesbeauftragte die Einhaltung anderer Vorschriften über den Datenschutz auch insoweit kontrolliert, als die Daten nicht in Dateien gespeichert, verändert, gelöscht oder aus Dateien übermittelt werden. Eine solche Klarstellung wäre allerdings dann entbehrlich, wenn die Beschränkung des Anwendungsbereichs des Gesetzes auf Dateien in § 1 Abs. 2 Satz 1 DSG NW gestrichen wird.

Die Bundestagsfraktionen haben Gesetzentwürfe zur Änderung des Bundesdatenschutzgesetzes eingebracht, die weitere Vorschläge enthalten. Einige dieser Vorschläge sind im Datenschutzgesetz Nordrhein-Westfalen bereits verwirklicht. Soweit sie über dieses Gesetz hinausgehen, sind sie auch für eine Änderung dieses Gesetzes erwägenswert (Zulässigkeit des Speicherns, Veränderns und Übermittelns nur zur Erfüllung von durch Rechtsnormen geregelten Aufgaben, Benachrichtigung bei erstmaliger Speicherung, Löschung statt Sperrung, verschuldensunabhängiger Schadensersatzanspruch ohne betragliche Begrenzung, Benachrichtigung des Datenschutzbeauftragten über den geplanten Aufbau personenbezogener automatisierter Informationssysteme).

2. Bereichspezifische Regelungen

Das Datenschutzgesetz Nordrhein-Westfalen findet nur Anwendung, soweit nicht besondere Rechtsvorschriften des Landes nach § 37 DSG NW oder Rechtsvorschriften des Bundes nach Artikel 31 GG vorgehen. Als Auffanggesetz enthält das Datenschutzgesetz Nordrhein-Westfalen notwendigerweise zahlreiche Generalklauseln und unbestimmte Rechtsbegriffe. Diese können den Besonderheiten der einzelnen Bereiche der Verwaltung nicht hinreichend Rechnung tragen. Deshalb sollten soweit als möglich bereichspezifische Datenschutzregelungen getroffen werden.

Der Bundesgesetzgeber hat inzwischen einige solche Regelungen geschaffen (etwa im Bundesstatistikgesetz, im Ersten Statistikbereinigungsgesetz und in der Novelle zum Gesetz über Personalausweise). Andere befinden sich im Gesetzgebungsverfahren (etwa die Entwürfe eines Melderechtsrahmengesetzes und eines Verkehrszentralregistergesetzes). Der Deutsche Bundestag hat anläßlich der Verabschiedung der Novelle zum Gesetz über Personalausweise in einer Entschließung einstimmig bereichspezifische Datenschutzregelungen für die Sicherheitsbehörden gefordert.

Für die Landesgesetzgebung kommen insbesondere folgende Bereiche in Betracht:

a) Gesetzliche Grundlage für das Sammeln, Nutzen und Übermitteln personenbezogener Daten durch die Polizei ist, soweit nicht besondere Vorschriften Anwendung finden, die polizeiliche Generalklausel (§ 20 Abs. 1 Satz 1 PolG (alt), § 8 Abs. 1 Satz 1 PolG NW).

   Danach können Polizeibehörden die notwendigen Maßnahmen treffen, um eine im Einzelfall bestehende Gefahr für die öffentliche Sicherheit oder Ordnung abzuwehren. Soweit die gesammelten Daten in einer Datei verarbeitet werden, wird für die Speicherung und die Übermittlung an Dritte die polizeiliche Generalklausel als Rechtsgrundlage durch die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen verdrängt.

   Unter dem Gesichtspunkt des Datenschutzes ist die Generalklausel einerseits zu weit, andererseits zu eng. Zu weit ist sie insofern, als sie nicht festlegt, welche Maßnahmen der personenbezogenen Informationsverarbeitung die Polizei unter welchen Voraus-

setzungen treffen darf. Zu eng ist sie deshalb, weil sie jede personenbezogene Informationsverarbeitung an das Vorliegen einer konkreten Gefahr knüpft. Die vorbeugende Abwehr von Gefahren einschließlich der vorbeugenden Verbrechensbekämpfung, also die Bekämpfung von Gefahren, bevor sie sich bereits zu konkreten Gefahren im polizeilichen Sinne verdichtet haben, ist einerseits in einem modernen Gemeinwesen eine unabweisbare Notwendigkeit; andererseits fehlt aber für sie die erforderliche gesetzliche Grundlage.

Ich habe davon abgesehen, zu dem Entwurf eines neuen Polizeigesetzes des Landes Nordrhein-Westfalen dem zuständigen Landtagsausschuß Vorschläge für bereichspezifische Datenschutzregelungen zu unterbreiten. Sie hätten einer eingehenden Beratung im Ausschuß bedurft. Dadurch wäre die Verabschiedung des Gesetzes in dieser Wahlperiode gefährdet worden. In der nächsten Wahlperiode sollte jedoch möglichst bald versucht werden, die für die personenbezogene Informationsverarbeitung durch die Polizei geltenden allgemeinen Regelungen durch bereichspezifische Datenschutzvorschriften zu ersetzen. Die in dem Alternativentwurf einheitlicher Polizeigesetze des Bundes und der Länder enthaltenen Vorschläge können hierfür, ohne daß ihnen in allen Fragen gefolgt werden müßte, eine Orientierungshilfe sein. In der nächsten Wahlperiode werde ich entsprechende Vorschläge zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen vorlegen.

b) Das Land Nordrhein-Westfalen hat als einziges Land der Bundesrepublik Deutschland noch kein Gesetz über den Verfassungsschutz. Gesetzliche Grundlage für das Sammeln, Nutzen und Übermitteln personenbezogener Daten durch die Verfassungsschutzbehörde ist § 3 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes vom 27. September 1950. Danach ist Aufgabe der Verfassungsschutzbehörden u. a. die Sammlung und Auswertung von Auskünften, Nachrichten und sonstigen Unterlagen über Bestrebungen, die gegen die freiheitliche demokratische Grundordnung gerichtet sind. Im Rahmen dieser und der anderen Aufgaben der Verfassungsschutzbehörden können auch personenbezogene Daten über Träger derartiger Bestrebungen gesammelt und verarbeitet werden. Soweit die gesammelten Daten in einer Datei verarbeitet werden, sind Rechtsgrundlage der Speicherung und der Übermittlung die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen.

   Umstritten ist der Umfang der zulässigen Amtshilfe zwischen Verfassungsschutz und Polizei. Der Bundesbeauftragte für den Datenschutz hat die Auffassung vertreten, daß über die Anforderungen der Datenschutzgesetze hinaus eine Übermittlung personenbezogener Daten von Verfassungsschutzbehörden an die Polizei nur zulässig sei, wenn dies zur Erfüllung der Aufgaben notwendig ist, die den Verfassungsschutzbehörden zugewiesen sind, etwa bei der Strafverfolgung von Staatsschutzdelikten (3.4.3.2. des Ersten Tätigkeitsberichts). Wegen der Versagung polizeilicher Befugnisse für den Verfassungsschutz hat er ferner Zweifel, ob eine Übermittlung von der Polizei an Verfassungsschutzbehörden zulässig ist (3.4.4.2. des Ersten Tätigkeitsberichts).

   Angesichts solcher Zweifel erscheint es geboten, die Datenübermittlung zwischen Verfassungsschutz und Polizei unter Beachtung der Erfordernisse des Datenschutzes bereichspezifisch zu regeln. In einem zu erlassenden Verfassungsschutzgesetz des Landes Nordrhein-Westfalen sollte deshalb festgelegt werden, unter welchen Voraussetzungen die Verfassungsschutzbehörde Daten an andere Stellen übermitteln und von anderen Stellen anfordern darf. Aber auch für die anderen Phasen der personenbezogenen Informationsverarbeitung durch den Verfassungsschutz sollte in diesem Gesetz eine bereichspezifische Rechtsgrundlage geschaffen werden.

c) Gesetzliche Grundlage für den Umgang mit Personalakten ist § 102 LBG in Verbindung mit den für die Bearbeitung von Personalangelegenheiten geltenden Rechtsvorschriften. Das Datenschutzgesetz Nordrhein-Westfalen kommt als gesetzliche

Grundlage nicht in Betracht, da es nur in Dateien gespeicherte personenbezogene Daten schützt und Personalakten keine Dateien sind (§ 1 Abs. 2 Satz 1, § 2 Abs. 3 Nr. 3 DSG NW). § 102 LBG, der die Einsicht des Beamten in seine Personalakten regelt, setzt voraus, daß alle Vorgänge über die dienstlichen oder persönlichen Verhältnisse des Beamten in Personalakten gesammelt werden. Die für die Bearbeitung von Personalangelegenheiten geltenden Rechtsvorschriften setzen voraus, daß die mit der Bearbeitung beauftragten Bediensteten Zugang zu den Personalakten haben, soweit die Kenntnis der in diesen gesammelten Vorgänge für die Bearbeitung erforderlich ist. Eine ausdrückliche und eindeutige Regelung des Umgangs mit Personalakten im Landesbeamtengesetz wäre zu begrüßen.

3. Datenschutz in der öffentlichen Diskussion

Der Datenschutz war im Berichtszeitraum mehrmals Gegenstand heftiger öffentlicher Diskussion. Sie wurde in keinem Bereich so kontrovers geführt wie im Zusammenhang mit den Sicherheitsbehörden. Dabei besteht die Gefahr, daß Eingriffe in die Persönlichkeitssphäre in anderen Bereichen der Verwaltung weniger ernst genommen werden. Dieser Bericht zeigt, daß in fast allen Bereichen mit personenbezogenen Daten gearbeitet wird und der Umgang mit ihnen sorgfältig beobachtet werden muß.

Kommentare in einer Zeitung nennen das Bedürfnis nach Datenschutz „halb künstlich", warnen vor hauptberuflichen Verfechtern des Datenschutzes und sprechen von einer Datenschutz-Manie, die bald nicht mehr nur kostspielig, sondern auch schädlich und vielleicht sogar gefährlich sein werde, insbesondere im Sicherheitsbereich. Ein anderes Presseorgan hingegen deutet an, daß die Datenschutzbeauftragten etwa bei der Rasterfahndung der Polizei vorschnell einen „Persilschein" ausgestellt hätten, und rügt ein angebliches „geheimes Zusammenspiel zwischen Kontrolleuren und Kontrollierten". Beides sind extreme Positionen, die für einen wirksamen Datenschutz im Interesse der Bürger wenig hilfreich sind. Dieser verlangt ein ausgewogenes Verhältnis zwischen dem Schutz der Persönlichkeitssphäre des Bürgers und der Erfüllung der staatlichen Aufgaben, die ebenfalls im Interesse des Bürgers liegt.

Der Datenschutzbeauftragte muß vor unangemessener Informationsverarbeitung warnen, aber auch darüber aufklären, wo eine solche Gefahr nicht oder noch nicht besteht. Dies ist oft eine schwierige Gradwanderung, bei der auf der einen Seite Verharmlosung, auf der anderen Übertreibung droht. Diese fördert Resignation, Apathie und sogar Angst und hindert damit den Bürger, die notwendigen Gegenaktivitäten zu entfalten.

Die bestehenden Informationssysteme rechtfertigen nach meiner Überzeugung nicht, die Bundesrepublik einen Überwachungsstaat zu nennen. Jedoch ist ständige Wachsamkeit geboten, um rechtzeitig Entwicklungen entgegentreten zu können, die zu weiterer Abhängigkeit der betroffenen Menschen führen können.

Die öffentliche Diskussion über Datenschutz hat zur Folge, daß die Behörden generell mit einer höheren, der Sache aber durchaus angemessenen Sensibilisierung der Bürger rechnen müssen. Es liegt im wohlverstandenen Interesse der Behörden, von sich aus die Öffentlichkeit über die praktizierten Methoden der Datenverarbeitung und die bestehenden Informationssysteme möglichst umfassend zu unterrichten. Dadurch würde in vielen Fällen unbegründetes Mißtrauen gar nicht erst entstehen. Erhöhte Transparenz kommt fast immer auch der Aufgabenerfüllung der Behörden zugute.

Allerdings wird gelegentlich versucht, den Datenschutz für Zwecke zu mißbrauchen, für die er nicht gedacht ist. Es kann nicht seine Aufgabe sein, Bürgern zu ermöglichen, sich ihren rechtlichen Verpflichtungen zu entziehen. Auch ist es nicht gerechtfertigt, etwa die zeitgeschichtliche Forschung, an der ein überwiegendes Interesse der Allgemeinheit be-

steht, unter Berufung auf den Datenschutz zu behindern. Derartige Bestrebungen sind geeignet, den Datenschutz zu diskreditieren. Ihnen muß deshalb mit Entschiedenheit entgegengetreten werden.

Häufig begegnet man bei Behörden, aber auch bei interessierten Bürgern der Haltung: Datenschutz ist notwendig, aber nicht in meinem Bereich, nur bei den Anderen. Demgegenüber kann nur mit Geduld versucht werden, die Wertmaßstäbe des Grundgesetzes verständlich zu machen, die der Menschenwürde und der freien Entfaltung der Persönlichkeit den höchsten Rang einräumen und Eingriffe in das Selbstbestimmungsrecht des Menschen über seine Daten nur unter eingrenzenden Voraussetzungen zulassen.

Dies gilt auch dann, wenn die Eingriffe plausibel erscheinen und durchaus anerkennungswerten Zielen dienen. Nicht das Verbot des Umgangs mit personenbezogenen Daten bedarf einer Rechtfertigung, sondern der Umgang selbst. Ob und in welchem Umfang Eingriffe in das Selbstbestimmungsrecht des Bürgers über seine Daten zugelassen werden, hat innerhalb der von der Verfassung gesetzten Schranken der Gesetzgeber zu bestimmen.

Düsseldorf, den 31. März 1980

Dr. Weyer