Der Landesbeauftragte für den Datenschutz Nordrhein-Westfalen

2. Tätigkeitsbericht

Zweiter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Nordrhein-Westfalen

für die Zeit vom 1. April 1980
bis zum 31. März 1981

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. Überblick

In meinem ersten Tätigkeitsbericht hatte ich zu einigen Grundsatzfragen des Datenschutzrechts Stellung genommen. Die Landesregierung ist in ihrer Stellungnahme in entscheidenden Fragen meiner Auffassung entgegengetreten. Sie legt sowohl die Kontrollbefugnis des Landesbeauftragten für den Datenschutz als auch den Anwendungsbereich materieller Datenschutzvorschriften (Grundrecht auf Datenschutz, Übermittlung aus einer Datei, Hinweispflicht bei Datenerhebung) restriktiv aus. Ich kann mich diesen Auslegungen nicht anschließen und halte an der im ersten Tätigkeitsbericht vertretenen Auffassung fest.

Der zweite Tätigkeitsbericht befaßt sich im wesentlichen mit der Anwendung der Datenschutzvorschriften in den einzelnen Bereichen der Verwaltung sowie mit organisatorischen und technischen Maßnahmen der Datensicherung. Demgegenüber treten Aussagen zu anderen allgemeinen Fragen des Datenschutzes zurück.

Schwerpunkte meiner Tätigkeit lagen in den Bereichen des Meldewesens, der Polizei, des Sozialwesens, des Schulwesens und der öffentlich-rechtlichen Kreditinstitute. Im Berichtszeitraum ist wiederum in zahlreichen Fällen gegen Datenschutzvorschriften verstoßen worden. Vorsätzliches Zuwiderhandeln gegen nicht weiter auslegungsbedürftige Vorschriften ist allerdings selten. In diesem Sinne hat es in Nordrhein-Westfalen keinen größeren „Datenskandal" gegeben.

Sorge bereitet mir jedoch die Datensicherung bei der Vernichtung nicht mehr benötigter Datenträger. Im Berichtszeitraum sind mehrere Fälle bekanntgeworden, in denen alte Akten, Karteikarten, Kontoauszüge und sonstige Unterlagen der Verwaltung mit personenbezogenen Daten, die vernichtet werden sollten, von Dritten an mehr oder weniger allgemein zugänglichen Orten aufgefunden wurden. Hier wird von vielen öffentlichen Stellen nicht sorgfältig genug verfahren.

2. Kontrolle der Einhaltung der Datenschutzvorschriften

a) Umfang der Kontrollbefugnis

Nach § 26 Abs. 1 Satz 1 DSG NW kontrolliert der Landesbeauftragte für den Datenschutz die Einhaltung der Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen sowie anderer Vorschriften über den Datenschutz. Die materiellen Vorschriften des Datenschutzgesetzes finden nur Anwendung, wenn personenbezogene Daten in einer Datei verarbeitet oder aus einer Datei übermittelt werden (§ 1 Abs. 2 Satz 1 DSG NW). Insoweit kann sich die Kontrolle nur auf die Datenverarbeitung in einer Datei oder die Datenübermittlung aus einer Datei beziehen.

Die anderen Vorschriften über den Datenschutz, wie etwa das Steuergeheimnis, das Sozialgeheimnis, das Statistikgeheimnis und auch das Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung, kennen den Dateibegriff nicht. Sie schützen den Bürger ohne Rücksicht darauf, ob seine Daten in einer Datei gespeichert sind oder in Akten oder sonstigen Unterlagen festgehalten werden. Ich habe seit Beginn meiner Tätigkeit die Auffassung vertreten, daß der Landesbeauftragte die Einhaltung dieser anderen Vorschriften über den Datenschutz auch dann zu kontrollieren hat, wenn die Daten nicht in

einer Datei gespeichert sind, sondern in Akten oder sonstigen Unterlagen festgehalten werden (vgl. A. 2. a meines ersten Tätigkeitsberichts, Vorlage 9/20).

Die Landesregierung ist in ihrer Stellungnahme zu meinem ersten Tätigkeitsbericht (Drucksache 9/151, S. 3-4) dieser Auffassung entgegengetreten. Sie ist der Ansicht, daß die Kontrollbefugnis des Landesbeauftragten auch hinsichtlich der anderen Vorschriften über den Datenschutz auf den Anwendungsbereich der materiellen Regelungen des Datenschutzgesetzes Nordrhein-Westfalen, also auf Datenverarbeitung in Dateien und Datenübermittlung aus Dateien beschränkt sei. Zur Begründung verweist sie auf die Entstehungsgeschichte des Gesetzes. Der Gesetzgeber sei davon ausgegangen, daß die Zusammenfassung personenbezogener Daten in einer Datensammlung, die durch ihre innere Organisation die Verfügbarkeit und Auswertbarkeit der Daten erhöhe, eine besondere Gefahrenlage schaffe. Ausschließlich diese besondere Gefahrenlage habe der Gesetzgeber durch besondere Regelungen und ein besonderes Kontrollorgan bekämpfen wollen.

Dieser restriktiven Auslegung des § 26 Abs. 1 Satz 1 DSG NW durch die Landesregierung kann ich nicht folgen. Sie liegt weder nahe, noch ist sie gar zwingend.

Maßgebend für die Auslegung einer Vorschrift ist ihr Wortlaut, der Zusammenhang in dem sie steht, ihr Zweck und ihre Entstehungsgeschichte. Dabei kommt der Entstehungsgeschichte nur insofern Bedeutung zu, als sie die Richtigkeit der nach den anderen Auslegungsmethoden ermittelten Auslegung bestätigt oder Zweifel behebt, die mit diesen allein nicht ausgeräumt werden können. Die Gesetzesmaterialien sind immer nur mit einer gewissen Zurückhaltung, in der Regel nur unterstützend zu verwerten (vgl. BVerfGE 1, 312; 8, 307; 10, 244; 11, 130-131; 13, 268).

Der Wortlaut des § 26 Abs. 1 Satz 1 DSG NW enthält keine Einschränkung der Art, daß die Einhaltung der „anderen Vorschriften über den Datenschutz" nur dann kontrolliert werden dürfe, wenn die Daten in einer Datei gespeichert oder aus einer Datei übermittelt werden. In der Vorschrift wird vielmehr die Einhaltung „der Vorschriften dieses Gesetzes" der Einhaltung „anderer Vorschriften über den Datenschutz" gegenübergestellt. Gegen die stillschweigende Ergänzung der zweiten Alternative um das ungeschriebene Merkmal „Dateibezug" spricht auch der Umstand, daß an anderen Stellen, bei denen Anlaß zu einer solchen Ergänzung bestand, diese ausdrücklich in den Text aufgenommen wurde (etwa in § 5 Abs. 1 und § 6 Abs. 1 Satz 1 DSG NW durch den Hinweis auf den „Rahmen des § 1 Abs. 2"). Hätte die Kontrollbefugnis hinsichtlich der „anderen Vorschriften über den Datenschutz" auf Dateien beschränkt werden sollen, so hätte etwa entsprechend dem Wortlaut des § 37 DSG NW angefügt werden müssen: „soweit sie auf in Dateien gespeicherte personenbezogene Daten anzuwenden sind".

Auch aus dem Zusammenhang, in dem § 26 Abs. 1 Satz 1 DSG NW steht, ergibt sich keine derartige Einschränkung. Die zweite Alternative dieser Vorschrift geht von dem gleichen Begriff des Datenschutzes aus wie die Leitvorschrift des § 1 Abs. 1 DSG NW, die keine Begrenzung auf Dateien enthält. Erst in § 1 Abs. 2 DSG NW wird der Anwendungsbereich der materiellen Vorschriften des Gesetzes auf die Datenverarbeitung in Dateien und die Datenübermittlung aus Dateien beschränkt.

Schließlich läßt sich auch aus dem Zweck des § 26 Abs. 1 Satz 1 DSG NW eine einschränkende Auslegung nicht herleiten. Der Zweck der Vorschrift gebietet vielmehr, auch den Umgang der Verwaltung mit personenbezogenen Daten in Akten einer externen Kontrolle durch eine unabhängige Instanz zu unterwerfen.

Zwar haben die besonderen Gefahren der automatisierten Datenverarbeitung den Gesetzgeber zu legislatorischer Initiative veranlaßt. Dieser hat in den Anwendungsbereich des Gesetzes aber auch die herkömmliche, nicht automatisierte Datenverarbeitung in Dateien einbezogen. Darüber hinaus hat der Gesetzgeber zahlreiche Rechtsvorschriften vorgefunden, die sowohl auf Datenverarbeitung in Dateien als auch auf den Umgang mit personenbezogenen Daten außerhalb von Dateien Anwendung finden. Diese Rechts-

vorschriften gelten weiter und gehen den Vorschriften des Datenschutzgesetzes vor. Es wäre nicht sachgerecht, die Kontrolle der Einhaltung dieser anderen Vorschriften, für die der Dateibegriff ohne jede Bedeutung ist, auf die Datenverarbeitung in Dateien zu beschränken.

Wie die Praxis immer wieder bestätigt, ist die Persönlichkeitssphäre des Bürgers bei dem Umgang der Verwaltung mit personenbezogenen Daten in Akten in gleicher Weise bedroht, wie bei der Datenverarbeitung in einer Datei. Für die Schutzwürdigkeit der Daten kommt es auf die Art der Datenverarbeitung nicht an. Für das Maß der Schutzbedürftigkeit mag die Art der Datenverarbeitung zwar Anhaltspunkte geben; dies kann aber, wie die Eingaben an den Landesbeauftragten zeigen, nicht letztlich entscheidend sein. Eine Trennung der Kontrolle zwischen Datenverarbeitung in Dateien und anderen Formen ist auch dem Bürger kaum verständlich zu machen. Der Zweck des Datenschutzgesetzes kann nur erreicht werden, wenn der Schutz des Bürgers vor rechtswidrigem Umgang mit seinen Daten in allen Bereichen der Kontrolle durch eine unabhängige Instanz unterworfen wird.

Ich gehe deshalb davon aus, daß der Kontrollbefugnis für die Einhaltung der „anderen Vorschriften über den Datenschutz" ein umfassender Begriff des Datenschutzes zugrunde liegt. Dieser schließt alle Vorschriften ein, die dem Schutz des Betroffenen vor rechtswidrigem Umgang mit seinen Daten dienen, also auch solche, die nicht oder nicht allein die Datenverarbeitung in Dateien betreffen.

Die einschränkende Auslegung des § 26 Abs. 1 Satz 1 DSG NW durch die Landesregierung ist für den Landesbeauftragten nicht bindend. Der unabhängige und nur dem Gesetz unterworfene Landesbeauftragte hat über den Umfang seiner Befugnis selbst zu befinden. Ich halte an meiner Auffassung fest, daß sich die Kontrollbefugnis des Landesbeauftragten für die Einhaltung der „anderen Vorschriften über den Datenschutz" nach dem Wortlaut des § 26 Abs. 1 Satz 1 DSG NW, nach dem Zusammenhang, in dem diese Vorschrift steht, und nach ihrem Zweck nicht auf die Datenverarbeitung in Dateien beschränkt, sondern auch auf den Umgang mit Daten in Akten und anderen Unterlagen erstreckt.

Diese Auffassung wird von den Datenschutzbeauftragten des Bundes und der anderen Länder für ihren Bereich geteilt (mit Ausnahme von Schleswig-Holstein, dessen Gesetz den Datenschutz in der Leitvorschrift auf Dateien beschränkt).

b) Auskunfts-, Einsichts- und Zutrittsrecht

Soweit es bei Eingaben, Beratungsersuchen und Kontrollen vom Amts wegen zur Aufklärung des Sachverhalts erforderlich war, habe ich **Auskunftsersuchen** an die betroffenen öffentlichen Stellen gerichtet. In den meisten Fällen wurde meinen Ersuchen durch umfassende und eingehende Auskunfterteilung Rechnung getragen.

Verzögerungen bei der Beantwortung meiner Auskunftsersuchen gab es, wenn die verantwortlichen Stellen zunächst Rückfragen bei ihren Aufsichtsbehörden für notwendig erachteten. In einigen Fällen mag dies mit den Meinungsverschiedenheiten über den Umfang meiner Prüfungskompetenz zusammenhängen (oben A.2.a). In anderen Fällen dürfte es darauf zurückzuführen sein, daß die allgemeinen Verwaltungsvorschriften, die nach dem Willen des Gesetzgebers von den obersten Landesbehörden zu erlassen sind (§ 9 DSG NW), im wesentlichen noch nicht vorliegen.

In einem Fall ist meiner Bitte um Auskunft nicht entsprochen worden. So hatte ich den Landesrechnungshof auf Grund des Beratungsersuchens einer obersten Landesbehörde und der Eingabe eines Personalrats unter Bezugnahme auf § 26 Abs. 1 Satz 1 und 2 sowie Abs. 3 DSG NW um Mitteilung gebeten, inwieweit bei Durchführung seiner Prüfung zur Feststellung der jährlichen Arbeitszeit die Erfassung personenbezogener Daten erforderlich sei. Demgegenüber hielt der Landesrechnungshof den Landesbeauftragten für den Datenschutz nicht für befugt, die Frage der Erforderlichkeit von Prüfungsmaßnahmen

des Landesrechnungshofs unter datenschutzrechtlichen Gesichtspunkten aufzugreifen (vgl. Vorlage 9/74).

Als wirksames Mittel, sich mit den Verfahrensabläufen in bestimmten Bereichen vertraut zu machen, haben sich **Informationsbesuche** erwiesen, die ich im Berichtszeitraum in verstärktem Umfang durchgeführt habe. Zweck war nicht die Überprüfung, sondern die Information. Im Vordergrund stand das Bestreben, sich einen möglichst umfassenden Überblick über Organisation und Durchführung der Datenverarbeitung sowie über die Handhabung des Datenschutzes zu verschaffen. Erfaßt werden sollten Aufgabenstellung und Arbeitsweise gleichermaßen wie etwaige Schwierigkeiten und Probleme „vor Ort".

Derartige Informationsbesuche fanden insbesondere im Bereich der Kommunalverwaltung, der Sozialversicherung, der Polizei und der öffentlich-rechtlichen Kreditinstitute statt. Soweit ich Verbände angesprochen habe, sollten damit zugleich überregional gesammelte Erfahrungen genutzt werden. Häufig konnte der mit den Besuchen gewonnene Kontakt erhalten und zum Vorteil beider Seiten später vertieft und ergänzt werden. Er wurde von den besuchten Stellen, die mit Bereitwilligkeit und Offenheit gewünschte Einblicke gewährten, ausnahmslos begrüßt.

Aussagen über Schwachstellen bei der Datenverarbeitung öffentlicher Stellen vermittelten insbesondere **Kontrollbesuche,** die im Gegensatz zu den Informationsbesuchen unmittelbar der Feststellung dienten, ob gegen Vorschriften über den Datenschutz verstoßen wurde. Sie reichten von der kurzfristigen Überprüfung einzelner durch Eingaben vorgegebener Sachverhalte bis zur längerfristig geplanten Gesamtkontrolle ausgewählter Einrichtungen des öffentlichen Bereichs ohne besonderen Anlaß.

Bei der Planung größerer Kontrollbesuche war ich bemüht, der Vielfalt der Datenverarbeitung bei öffentlichen Stellen Rechnung zu tragen. Dabei habe ich Stellen mit unterschiedlicher Aufgabenstellung ausgewählt, um mit etwaigen Empfehlungen einen möglichst weiten Bereich der Datenverarbeitung ansprechen zu können.

Größere Kontrollbesuche dauerten bis zu einer Woche; an ihnen waren jeweils mehrere meiner Mitarbeiter beteiligt. Sie wurden einige Wochen vorher angekündigt mit der Bitte, der Vorbereitung dienende Unterlagen vorab zur Verfügung zu stellen. Sie begannen jeweils mit einem Gespräch bei der verantwortlichen Leitung und endeten mit einer umfassenden Schlußerörterung, der eine detaillierte schriftliche Prüfungsmitteilung meiner Dienststelle nachfolgte.

Die Kontrollbesuche zeigten noch zahlreiche Mängel insbesondere auf dem Gebiet der organisatorischen und technischen Maßnahmen auf (unten D.). Gleichwohl konnte ich feststellen, daß die verantwortlichen Stellen den Besuch als sehr hilfreich empfunden haben. Er verhalf ihnen zu einer „Sicherheitsanalyse", die nicht nur als Antwort auf aufgetretene Einzelfragen des Datenschutzes, sondern für die sichere Abwicklung der automatisierten Datenverarbeitung schlechthin von Bedeutung ist.

So hat auch schon eine öffentliche Stelle von sich aus den Wunsch nach einem Kontrollbesuch des Landesbeauftragten geäußert, um durch die Prüfungsmitteilung einen Überblick über Schwachstellen der Datensicherheit im eigenen Hause zu erhalten.

c) Dateienregister

Die Landesregierung hat am 16. Dezember 1980 im Einvernehmen mit dem Ausschuß für Innere Verwaltung des Landtags die Verordnung über die Dateienregister des Landesbeauftragten für den Datenschutz Nordrhein-Westfalen (Dateienregisterverordnung Nordrhein-Westfalen — DRegVO NW) erlassen. Die Verordnung ist am 31. Dezember 1980 in Kraft getreten. Sie trägt meinen Vorschlägen überwiegend Rechnung.

Keine Berücksichtigung fand mein Vorschlag, in den Anmeldungen zum Dateienregister auch die Angabe der Rechtsgrundlage der Aufgaben vorzusehen, zu deren Erfüllung die Kenntnis der gespeicherten oder der übermittelten Daten erforderlich ist (Spalten 5 und 8 des Musters der Anlage zu der Verordnung). Diese Angabe schien mir notwendig zur Prü-

fung der Rechtmäßigkeit der Aufgabenerfüllung, die nach § 10 Abs. 1, § 11 Abs. 1 Satz 1 und der ersten Alternative des § 13 Abs. 1 Satz 1 DSG NW Voraussetzung für die Zulässigkeit der Speicherung oder Übermittlung ist. Ferner ist die von der Landesregierung zunächst vorgesehene Angabe des Auftragnehmers bei Auftragsdatenverarbeitung (§ 7 Abs. 1 DSG NW) in der von dem Ausschuß für Innere Verwaltung gebilligten Fassung wieder gestrichen worden.

Das Register kann nur dann seinen Zweck erfüllen, wenn die Angaben zu den Dateien klar, übersichtlich und vollständig sind. Das setzt möglichst fehlerfreie Meldungen voraus. Gestützt auf Erfahrungen aus Anfragen und Vorab-Meldungen speichernder Stellen habe ich deshalb den Innenminister gebeten, den meldepflichtigen Stellen erläuternde Hinweise an die Hand zu geben. Meinen Vorstellungen hierzu ist der Innenminister überwiegend gefolgt.

Nach § 2 Abs. 1 DRegVO NW hat die Anmeldung der Dateien unverzüglich nach der erstmaligen Speicherung der Daten zu erfolgen. Dateien, die bei Inkrafttreten der Dateienregisterverordnung bereits bestanden, sind innerhalb von sechs Monaten nach Inkrafttreten der Verordnung anzumelden (§ 5 Abs. 2 DRegVO NW). Der Aufbau des Registers wird deshalb noch einige Zeit in Anspruch nehmen. Gleichwohl hoffe ich, möglichst bald in der Lage zu sein, anfragenden Bürgern, die ich derzeit noch um Geduld bitten muß, Einsicht zu gewähren und Auskünfte zu erteilen. Nach § 4 Abs. 2 DRegVO NW ist dies für den Bürger kostenfrei.

Zunächst ist vorgesehen, das Register manuell zu führen. Mein Bestreben ist es, auch dem Bürger größtmögliche Transparenz zu bieten. Die Struktur des Registers wird dem Verwaltungsaufbau des Landes angeglichen sein. Für jede meldepflichtige Stelle wird eine eigene Registerakte geführt werden. Auf Grund des gefundenen Auswertungssystems wird der Inhalt des Registers auch regional erfaßbar sein. Damit ist es möglich, dem Bürger schnell und gezielt Auskunft über bestehende Dateien öffentlicher Stellen in seiner Wohngemeinde, dem Kreisgebiet oder dem Regierungsbezirk zu erteilen.

Das Register selbst wird keine personenbezogenen Daten enthalten, sondern lediglich Angaben über die Dateien, in denen personenbezogene Daten gespeichert sind (§ 27 Abs. 2 DSG NW). Hierauf mußte ich wiederholt anfragende Bürger hinweisen, die aus dem Register etwas über die zu ihrer Person gespeicherten Daten erfahren wollten.

d) Durchsetzungsmöglichkeiten

Auch in diesem Berichtszeitraum habe ich zur Durchsetzung meiner Vorstellungen zahlreiche **Empfehlungen** (§ 26 Abs. 2 DSG NW) gegeben. Diesen ist in den meisten Fällen gefolgt worden.

Von der Möglichkeit, Verstöße gegen die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen und andere Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten förmlich zu **beanstanden** (§ 30 DSG NW), habe ich wiederum nur in zwei Fällen Gebrauch gemacht. Dabei habe ich den eingeschlagenen Weg zunächst beibehalten, eine Beanstandung nur dann auszusprechen, wenn die Bedeutung der Angelegenheit, die Schwere des Verstoßes oder die datenschutzrechtliche Bewertung der Angelegenheit durch die verantwortliche Stelle dies verlangt. Häufig habe ich nur deshalb von einer Beanstandung noch abgesehen, weil ich glaubte davon ausgehen zu können, daß meine Empfehlungen ausreichten, Verstöße künftig zu vermeiden.

Von meinem Recht, mich jederzeit an den **Landtag** zu wenden (§ 31 Abs. 3 DSG NW), habe ich zweimal Gebrauch gemacht. In dem einen Fall habe ich zu dem Entwurf der Dateienregisterverordnung eine Änderung vorgeschlagen, die dem Dateienregister mehr Aussagekraft geben sollte (Vorlage 9/89). Ferner habe ich anläßlich der Beratung des Haushaltsplans 1981 dem Haushalts- und Finanzausschuß sowie dem Ausschuß für Innere Verwaltung des Landtags meine Vorstellungen zur Personalausstattung meiner Dienststelle dargelegt (Vorlage 9/225).

Auch **Öffentlichkeitsarbeit** ist ein Mittel, das Bewußtsein unserer Gesellschaft für das Rechtsgut Datenschutz zu fördern und dazu beizutragen, den Schutz des Bürgers vor Mißbrauch seiner personenbezogenen Daten zu verbessern. Die umfassende Unterrichtung des Bürgers und der Öffentlichkeit über den Datenschutz betrachte ich deshalb als einen wesentlichen Teil meiner Tätigkeit.

Bestärkt werde ich hierin durch eine stetige Nachfrage von Bürgern sowie Stellen des privaten und öffentlichen Bereichs nach Informationen über den Datenschutz, die neben zahlreichen Eingaben und Beratungsersuchen auf ein gestiegenes Informationsbedürfnis schließen läßt. Gerne nehme ich deshalb die Gelegenheit wahr, in Interviews, Vorträgen und Referaten auf Fragen des Datenschutzes einzugehen. Für die Verteilung und Versendung von Informationsmaterial stehen mir die Informationsschrift „Der Bürger und seine Daten" sowie die Informationsbroschüre des Innenministers zum Datenschutzgesetz Nordrhein-Westfalen zur Verfügung. Hinzu kommt mein erster Tätigkeitsbericht, der nunmmehr in gedruckter Form vorliegt.

Gute Resonanz ließ sich insbesondere dort feststellen, wo das Material an Stellen gelangte, die personenbezogene Daten in großem Umfange verarbeiten oder bei ihrer Tätigkeit mit einem großen Teil der Bevölkerung in Berührung kommen. Dies gilt vor allem für die Behörden der Kommunalverwaltung und für Büchereien. Besonders erfreulich ist es, daß Schulen, Erwachsenenbildungseinrichtungen, öffentliche Verwaltungen und auch Privatunternehmen Informationsunterlagen offenbar verstärkt zu Unterrichts- und Schulungszwecken einsetzen. Ich halte dies für einen guten Weg, Erfahrungen und Erkenntnisse im Bereich des Datenschutzes einem weiten Kreis betroffener Bürger nutzbar zu machen.

Viele Anfragen zeigen, daß noch immer ein erhebliches Informationsdefizit besteht. Dies gilt sowohl für das grundsätzliche Anliegen des Datenschutzes als auch für die allgemeinen und besonderen Datenschutznormen. Um dem Rechnung zu tragen, ist beabsichtigt, eine Broschüre herauszugeben, die die wichtigsten in Nordrhein-Westfalen geltenden Datenschutzvorschriften enthält.

3. Zusammenarbeit mit den anderen Datenschutzbeauftragten

Die Zusammenarbeit mit den anderen Datenschutzbeauftragten wurde fortgesetzt. Sie hat wesentlich zur Klärung vergleichbarer Sachverhalte beigetragen und häufig zu einer einheitlichen Auffassung über grundsätzliche Datenschutzprobleme geführt.

Die **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** hat im Berichtszeitraum dreimal getagt. In den Sitzungen im April, September und Dezember 1980 wurden unter anderem folgende Themen behandelt:

- Datenschutz bei den Sicherheitsbehörden (KpS-Richtlinien, Dateienrichtlinien, Neukonzeption des INPOL-Systems und Kriminalaktennachweis)
- Melderechtsrahmengesetz (Anpassung des Landesrechts)
- Personalausweisgesetz (Herstellungsverfahren des neuen Personalausweises)
- Zehntes Buch des Sozialgesetzbuchs
- Neue Medien (Bildschirmtext, Kabelfernsehen)
- Anordnung über Mitteilungen in Strafsachen (MiStra).

Schwerpunkt einer dritten „Kooperationssitzung" der Datenschutzbeauftragten und der obersten Aufsichtsbehörden der Länder für den Datenschutz im April 1980 war die Erörterung von Novellierungsvorschlägen zum Bundesdatenschutzgesetz. Sie stand im Zusammenhang mit einer Anhörung durch den Innenausschuß des Deutschen Bundestags, die dieser anläßlich der Beratung von Gesetzentwürfen der Bundestagsfraktionen durchführte.

4. Weiterer Ausbau der Dienststelle

a) Personal

Die stellenmäßige Ausstattung der Dienststelle des Landesbeauftragten für den Datenschutz ist im Haushaltsjahr 1980 gegenüber 1979 unverändert geblieben. Es standen 32 Planstellen und Stellen zur Verfügung, von denen inzwischen 27 besetzt werden konnten. Auch die Stellenbesetzungen waren im Berichtszeitraum das Ergebnis einer guten Zusammenarbeit mit dem Innenminister, der mich wie bisher nach besten Kräften unterstützte. Dank verständnisvoller Mitwirkung des Personalrats beim Innenminister gelang es wiederum, meinen Vorschlägen zu Stellenbesetzungen, Beförderungen, Höhergruppierungen und anderen Personalmaßnahmen zu entsprechen.

Noch nicht besetzt sind zwei Planstellen des gehobenen Dienstes und drei Stellen für Sachbearbeiter im Angestelltenverhältnis. Die Besetzung der drei Stellen mit geeigneten Bewerbern wird auch weiterhin nicht möglich sein, da die vorgesehene Eingruppierung in Vergütungsgruppe III nicht den Leistungsanforderungen entspricht.

Für den Haushaltsplan 1981 hatte ich die Umwandlung dieser Stellen in zwei Planstellen des höheren Dienstes, von denen eine allerdings für ein besonders belastetes Fachreferat benötigt wird, und eine Stelle der Vergütungsgruppe Ib/IIa beantragt. Diese Umwandlung ist zur Erfüllung meiner Aufgaben notwendig (§ 25 Abs. 1 DSG NW). Obwohl der Innenminister mein Anliegen für berechtigt hält, ist ihm bislang im Hinblick auf die angespannte Haushaltslage des Landes nicht Rechnung getragen worden. Ich habe den Haushalts- und Finanzausschuß sowie den Ausschuß für Innere Verwaltung des Landtags über meine Vorstellungen unterrichtet (Vorlage 9/225).

Entsprechend meinem Antrag sieht der Entwurf des Haushaltsplans 1981 drei neue Stellen für den Vorzimmer-, Schreib- und Fernsprechdienst vor.

b) Diensträume

Die ursprüngliche Unterbringung meiner Dienststelle im Gebäude Ulenbergstraße 1, die von allen Beteiligten nur als Übergangslösung angesehen wurde, war erfreulicherweise nicht von langer Dauer. Seit dem 16. Juni 1980 steht mir ein angemietetes Gebäude in Düsseldorf, Elisabethstraße 12, zur Verfügung. Die durch den Innenminister in Zusammenarbeit mit dem Finanzminister ermöglichte Unterbringung betrachte ich als langfristige Lösung. Die zur Verfügung stehenden Räumlichkeiten entsprechen dem Raumbedarf einschließlich der notwendigen Sonderräume. Inzwischen konnten auch notwendige Sicherheitsmaßnahmen verwirklicht werden.

B. Zum Grundrecht auf Datenschutz

Nach Artikel 4 Abs. 2 der Landesverfassung hat jeder Anspruch auf Schutz seiner personenbezogenen Daten; in dieses Grundrecht darf, sofern nicht Bundesrecht einen Eingriff zuläßt, nur im überwiegenden Interesse der Allgemeinheit auf Grund eines Landesgesetzes eingegriffen werden. Wie in meinem ersten Tätigkeitsbericht dargelegt, bedarf danach jeder Umgang öffentlicher Stellen mit personenbezogenen Daten, also jedes Erheben, Sammeln, Festhalten, Nutzen und Weitergeben solcher Daten einer gesetzlichen Grundlage. Fehlt eine solche und liegt auch keine Einwilligung des Betroffenen vor, so ist der Umgang mit seinen Daten unzulässig.

Das Datenschutzgesetz Nordrhein-Westfalen interpretiert und konkretisiert das Grundrecht auf Datenschutz für den Bereich der Verarbeitung personenbezogener Daten in Dateien. Dementsprechend wiederholt § 3 Satz 1 DSG NW für die Datenverarbeitung in Dateien, was sich allgemein bereits aus Artikel 4 Abs. 2 der Landesverfassung ergibt: daß die Datenverarbeitung in jeder ihrer Phasen nur zulässig ist, wenn entweder dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat.

Die Auffassung, daß nach Artikel 4 Abs. 2 der Landesverfassung jede personenbezogene Informationsverarbeitung öffentlicher Stellen einer gesetzlichen Grundlage bedarf, ist allerdings nicht unumstritten.

a) Die Landesregierung hält sie in ihrer Stellungnahme zu meinem ersten Tätigkeitsbericht für „problematisch weitgehend". Sie ist der Ansicht, daß diese Auslegung von Wortlaut, Zweck, systematischer Stellung und von der Entstehungsgeschichte der Norm her weder geboten noch gerechtfertigt und in den rechtlichen und praktischen Konsequenzen kaum absehbar sei, jedenfalls aber die gesetzesfreie Verwaltung weitgehend lahmlegen würde — ohne diese Aussagen allerdings näher zu begründen.

   Der Wortlaut spricht jedenfalls für die von mir vertretene Auffassung. Der kategorische Satz „jeder hat Anspruch auf Schutz seiner personenbezogenen Daten" verbietet eine einschränkende Auslegung. Aus dem Wortlaut ergibt sich der Zweck der Vorschrift, die personenbezogene Informationsverarbeitung einer Entscheidung des Gesetzgebers vorzubehalten. Einzelnen Äußerungen der am Gesetzgebungsverfahren Beteiligten kann demgegenüber keine entscheidende Bedeutung zukommen (vgl. BVerfGE 1, 312; 8, 307; 10, 244; 11, 130-131; 13, 268).

   Die Befürchtung, daß diese Auslegung die gesetzesfreie Verwaltung lahmlegen oder daß die danach gebotene Verrechtlichung der personenbezogenen Informationsverarbeitung eine Bürokratisierung zur Folge hätte, halte ich für unbegründet. Dem Gesetzesvorbehalt für Einschränkungen des Grundrechts könnte bereits dadurch Rechnung getragen werden, daß entweder die Beschränkung des Anwendungsbereichs des Datenschutzgesetzes Nordrhein-Westfalen auf Dateien aufgehoben oder ein ähnliches Auffanggesetz für die personenbezogene Informationsverarbeitung außerhalb von Dateien geschaffen wird. Soweit die Besonderheiten einzelner Bereiche der Verwaltung es gebieten, müßten dann allerdings bereichspezifische Regelungen geschaffen werden, die dem Auffanggesetz vorgehen, wie sie in zahlreichen Fällen für die Informationsverarbeitung sowohl innerhalb als auch außerhalb von Dateien schon erlassen worden sind.

b) Gegen die Auffassung, daß jeder Umgang mit personenbezogenen Daten einen Eingriff in das Grundrecht darstellt, wird ferner eingewandt, daß danach die Verwaltung zur Durchsetzung privater Interessen keine personenbezogenen Daten mehr verarbeiten dürfe, weil nach Artikel 4 Abs. 2 der Landesverfassung Eingriffe nur im überwiegenden Interesse der Allgemeinheit zugelassen werden dürfen. Bei dieser Auslegung des Grundrechts sei zumindest zweifelhaft, ob die Vorschriften des Datenschutz-

gesetzes Nordrhein-Westfalen, die eine Übermittlung an Private in deren Interesse zulassen, mit der Verfassung vereinbar seien.

Dem liegt jedoch ein Mißverständnis zugrunde. Das in Artikel 4 Abs. 2 der Landesverfassung als Eingriffsvoraussetzung genannte Interesse der Allgemeinheit ist nicht mit dem öffentlichen Interesse gleichzusetzen, sondern reicht weiter.

So liegt die einfache Melderegisterauskunft über Namen, akademische Grade und Anschrift eines von dem Empfänger bezeichneten Betroffenen, die § 36 Abs. 2 Satz 1 DSG NW ohne weitere Voraussetzungen zuläßt, durchaus im Interesse der Allgemeinheit. Denn diese Möglichkeit der Kontaktaufnahme mit namentlich bekannten Personen ist eine Grundvoraussetzung des Zusammenlebens in unserer Gesellschaft geworden.

Auch die Übermittlung anderer personenbezogener Daten an Private bei Vorliegen eines rechtlichen Interesses liegt im Interesse der Allgemeinheit. Die Durchsetzung von Rechtsansprüchen dient der Erhaltung oder Wiederherstellung des Rechtsfriedens. 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. Hierzu gehören auch die zur Durchsetzung dieser Ansprüche erforderlichen Daten. Entsprechendes gilt auch für Daten, die zur Rechtsverteidigung erforderlich sind. Soweit § 13 Abs. 1 Satz 1 DSG NW für solche Zwecke die Übermittlung personenbezogener Daten an Private zuläßt, habe ich keinen Zweifel, daß das Interesse der Allgemeinheit an der Erhaltung oder Wiederherstellung des Rechtsfriedens gegenüber dem Interesse des Betroffenen an dem Schutz seiner Daten überwiegt und deshalb diese Vorschrift mit Artikel 4 Abs. 2 der Landesverfassung auch bei weiter Auslegung seines Anwendungsbereichs vereinbar ist.

Nicht im Interesse der Allgemeinheit, jedenfalls aber nicht in ihrem überwiegenden Interesse liegt allerdings die Übermittlung, wenn sich der Empfänger lediglich auf ein einfaches berechtigtes Interesse berufen kann. Eine verfassungskonforme Auslegung des § 13 Abs. 1 Satz 1 DSG NW gebietet vielmehr, in diesen Fällen den schutzwürdigen Belangen des Betroffenen Vorrang einzuräumen und deshalb von einer Übermittlung abzusehen. Diese muß auf die Fälle beschränkt bleiben, in denen der Empfänger ein qualifiziertes Interesse, also entweder ein rechtliches oder aber ein öffentliches Interesse geltend macht.

c) Um den Anwendungsbereich des Grundrechts auf Datenschutz zu begrenzen, wird gelegentlich auf immanente Schranken des Grundrechts hingewiesen. Nach diesem Konzept läge bei einem Umgang mit personenbezogenen Daten, der diese Schranken nicht überschreitet, überhaupt kein Eingriff in das Grundrecht vor, so daß sich die Frage seiner Legitimierung durch den Gesetzgeber nicht stellen würde.

   Es ist allerdings nicht erkennbar, wo die Schranken liegen sollen. Vor allem spricht aber gegen ein derartiges Konzept das Datenschutzgesetz Nordrhein-Westfalen selbst. Dieses Gesetz, das das Grundrecht auf Datenschutz für den Bereich der Datenverarbeitung in Dateien interpretiert, geht von einem Verbot der Datenverarbeitung in Dateien ohne Rücksicht auf die Art der Daten und die Schwere der Belastung des Betroffenen aus und macht die Zulässigkeit jeder Datenverarbeitung von einer Rechtsvorschrift abhängig, sofern nicht die Einwilligung des Betroffenen vorliegt. Insbesondere kommt es dabei nicht darauf an, ob die Daten mehr oder weniger sensibel sind. Der Umstand, daß selbst die Verarbeitung einfacher Adreßdaten grundsätzlich verboten ist und nur durch Rechtsvorschrift erlaubt werden kann, ist mit einer einschränkenden Auslegung des Grundrechts auf Datenschutz kaum in Einklang zu bringen. Er bestätigt vielmehr, daß dem Datenschutzgesetz Nordrhein-Westfalen eine Auslegung des Grundrechts zugrundeliegt, die für jeden Umgang öffentlicher Stellen mit personenbezogenen Daten eine gesetzliche Grundlage verlangt.

d) Im Schrifttum wird gelegentlich die Ansicht vertreten, daß die in den Datenschutzgesetzen enthaltenen Generalklauseln nicht dem verfassungsrechtlichen Bestimmt-

heitsgebot entsprächen. Die Vertreter dieser Ansicht verweisen darauf, daß jedes zu Eingriffen in ein Grundrecht ermächtigende Gesetz Inhalt, Gegenstand, Zweck und Ausmaß des Eingriffs hinreichend bestimmen müsse. Diese Voraussetzung sei bei den Generalklauseln der Datenschutzgesetze nicht erfüllt. Da aber — unstreitig — auf solche Generalklauseln in einem Auffanggesetz nicht verzichtet werden kann, schließt man daraus, daß der in den Generalklauseln zugelassene Umgang mit personenbezogenen Daten — sofern nicht besondere Umstände hinzuträten — überhaupt kein Eingriff sei.

Dem ist entgegenzuhalten, daß das Bestimmtheitsgebot selbst auslegungsbedürftig ist, wobei Besonderheiten der jeweils zu regelnden Materie zu berücksichtigen sind. Beim Datenschutz genügen nach meiner Auffassung allgemein gehaltene Generalklauseln dann, wenn der Eingriff nicht besonders schwerwiegend ist. Handelt es sich um sensiblere Daten (wie etwa bei den Sicherheitsbehörden oder im Sozialbereich), so verlangt das Bestimmtheitsgebot eine gesetzliche Präzisierung der Eingriffsermächtigungen in bereichspezifischen Regelungen.

Die Forderung aller drei im Deutschen Bundestag vertretenen Parteien nach bereichspezifischen Datenschutzregelungen entspricht somit in Nordrhein-Westfalen einem Verfassungsgebot.

Nach alldem halte ich an meiner Auffassung fest, daß nach Artikel 4 Abs. 2 der Landesverfassung jeder Umgang öffentlicher Stellen mit personenbezogenen Daten einer gesetzlichen Grundlage bedarf. Das Oberverwaltungsgericht Münster hat in der bislang einzigen Entscheidung zum Datenschutzgesetz Nordrhein-Westfalen (NJW 1979, S. 2221) die gleiche Auffassung vertreten, indem es das Erfordernis einer gesetzlichen Grundlage für eine Melderegisterauskunft über Geburtsdatum, Geburtsort und Nummer des Reisepasses auf Artikel 4 Abs. 2 der Landesverfassung gestützt hat.

Bei der Prüfung, ob bei der personenbezogenen Informationsverarbeitung das Grundrecht auf Datenschutz beachtet wurde, haben sich in meiner bisherigen Tätigkeit fünf Fallgruppen ergeben:

Bei der Datenerhebung ist zu prüfen, ob hierfür die nach Artikel 4 Abs. 2 der Landesverfassung erforderliche gesetzliche Grundlage vorhanden ist. Diese Prüfung ist unabhängig davon, ob die erhobenen Daten anschließend in einer Datei gespeichert oder in Akten oder sonstigen Unterlagen festgehalten werden sollen. Das Datenschutzgesetz Nordrhein-Westfalen selbst enthält keine Ermächtigung zur Datenerhebung, sondern setzt eine durch eine andere Rechtsvorschrift zugelassene (oder eine mit Einwilligung des Betroffenen vorgenommene) Erhebung voraus. In mehreren Fällen hat die Prüfung ergeben, daß wegen Fehlens einer gesetzlichen Grundlage für die Datenerhebung das Grundrecht auf Datenschutz verletzt wurde.

Die zweite Fallgruppe betrifft die weitere Verarbeitung der erhobenen Daten. Soweit die Daten in einer Datei gespeichert werden, gilt hierfür das Datenschutzgesetz Nordrhein-Westfalen. Da dieses Gesetz das Grundrecht auf Datenschutz für diesen Bereich konkretisiert, braucht insoweit das Grundrecht in der Regel nicht herangezogen zu werden. Dagegen ist die weitere Verarbeitung der erhobenen Daten außerhalb von Dateien, also in Akten oder sonstigen Unterlagen, unmittelbar an dem Grundrecht zu messen mit der Folge, daß diese Verarbeitung einer gesetzlichen Grundlage bedarf. In mehreren Fällen war das Grundrecht verletzt worden, weil eine gesetzliche Grundlage für die Verarbeitung fehlte.

In einer dritten Fallgruppe war das Grundrecht auf Datenschutz zur Auslegung landesgesetzlicher Eingriffsermächtigungen heranzuziehen. Dies gilt insbesondere für Ermächtigungen, die nach ihrem Wortlaut so weit gefaßt sind, daß dem Erfordernis des überwiegenden Interesses der Allgemeinheit nicht hinreichend Rechnung getragen wird. Aus dem Grundrecht ergab sich in diesen Fällen eine Einschränkung der Ermächtigung.

Zur vierten Fallgruppe gehören die Ansprüche der Betroffenen auf Auskunft, Berichtigung, Sperrung oder Löschung von Daten. Für den Fall der Speicherung in einer Datei hat das Datenschutzgesetz Nordrhein-Westfalen diese Ansprüche in den entsprechenden Vorschriften konkretisiert. Es liegt nahe, die dort für den Bereich der Dateien vorgenommene Interpretation des Grundrechts auch für die unmittelbar aus dem Grundrecht herzuleitenden Ansprüche im Bereich der Akten und sonstigen Unterlagen heranzuziehen. Dies ist in mehreren Fällen geschehen.

Die fünfte Fallgruppe betrifft die Datensicherung. Soweit Daten nicht in einer Datei gespeichert werden, muß die Verpflichtung, organisatorische und technische Maßnahmen zum Schutz der Daten gegen unbefugtes Zugreifen, Nutzen oder Weitergeben zu treffen, unmittelbar aus Artikel 4 Abs. 2 der Landesverfassung hergeleitet werden. In mehreren Fällen wurde gegen diese Verpflichtung verstoßen.

Dieser Überblick macht deutlich, daß das Grundrecht auf Datenschutz insbesondere für den Umgang mit personenbezogenen Daten außerhalb von Dateien, also in Akten und sonstigen Unterlagen von Bedeutung ist. Hierbei ist zu berücksichtigen, daß in Akten oft wesentlich sensiblere Daten festgehalten werden, als in vielen Dateien.

C. Datenschutz in den Bereichen der Verwaltung

1. Meldewesen

a) Melderechtsrahmengesetz

Der Bundesgesetzgeber hat das Melderechtsrahmengesetz (MRRG) verabschiedet. Das Gesetz ist am 23. August 1980 in Kraft getreten. Die Länder sind verpflichtet, ihr Melderecht den Vorschriften des Gesetzes bis zum 22. August 1982 anzupassen (§ 23).

Der von der Bundesregierung vorgelegte Gesetzentwurf trug den Forderungen des Datenschutzes weitgehend Rechnung. Die vom Deutschen Bundestag beschlossene Fassung kommt zwar in einigen Punkten der aus der Sicht des Datenschutzes bedenklichen Stellungnahme des Bundesrates entgegen. Das Gesetz ist jedoch als bereichspezifische Datenschutzregelung insgesamt positiv zu bewerten.

Insbesondere ist zu begrüßen, daß der Katalog der Daten, die im Melderegister gespeichert werden dürfen, eingeschränkt wird (§ 2 Abs. 1), anderen öffentlichen Stellen im Regelfall nur bestimmte Grunddaten übermittelt werden dürfen (§ 18 Abs. 1), die Übermittlung weiterer Daten an die Sicherheitsbehörden einer Protokollierungspflicht unterliegt (§ 18 Abs. 3) und regelmäßige Datenübermittlungen an öffentliche Stellen nur auf Grund einer Rechtsverordnung zulässig sind (§ 18 Abs. 4). Die gespeicherten Daten unterliegen einer Zweckbindung (§ 3). Schutzwürdige Belange der Betroffenen dürfen durch die Verarbeitung oder sonstige Nutzung nicht beeinträchtigt werden (§ 6). Der Betroffene erhält das Recht auf gebührenfreie Auskunft über die gespeicherten Daten (§ 7 Nr. 1) und auf Benachrichtigung bei erweiterten Melderegisterauskünften (§ 7 Nr. 4). Die für die Aufgabenerfüllung nicht mehr erforderlichen Daten sind von Amts wegen zu löschen (§ 10 Abs. 1 Satz 1).

Unbefriedigend sind allerdings die Regelungen über die Übermittlung von Daten von Nichtmitgliedern an eine Religionsgesellschaft (§ 19 Abs. 2), über die erweiterte Melderegisterauskunft (§ 21 Abs. 2) und über die Melderegisterauskunft über Alters- und Ehejubiläen (§ 22 Abs. 2) sowie die lange Übergangsfrist für die Einsichtnahme der Polizei in das Melderegister (§ 24). Bei der Übermittlung von Daten der zur Familie gehörenden Nichtmitglieder an eine Religionsgesellschaft ist lediglich ein Widerspruchsrecht des Betroffenen vorgesehen (§ 19 Abs. 2 Satz 3). Das gleiche gilt für die Melderegisterauskunft über Alters- und Ehejubiläen (§ 22 Abs. 2 Satz 1). Die erweiterte Melderegisterauskunft wird nur davon abhängig gemacht, daß der Datenempfänger ein berechtigtes Interesse glaubhaft macht (§ 21 Abs. 2); der Betroffene kann die Daten nur sperren lassen, soweit er seinerseits ein berechtigtes Interesse nachweist (§ 21 Abs. 6).

Bei der Anpassung des Landesmelderechts an das Rahmengesetz muß auf jeden Fall die insgesamt datenschutzfreundliche Grundkonzeption dieses Gesetzes erhalten bleiben. Das Rahmengesetz läßt darüber hinaus für den Landesgesetzgeber Spielraum für noch datenschutzfreundlichere Lösungen im Einzelfall. Diese gesetzgeberischen Möglichkeiten gilt es zu nutzen.

b) Vorabanwendung des Melderechtsrahmengesetzes

Das Melderechtsrahmengesetz enthält, abgesehen von den §§ 20, 23 und 25 bis 28, keine unmittelbar wirkenden Vorschriften, sondern nur Rahmenbestimmungen für den Landesgesetzgeber.

Mit Runderlaß vom 9. Dezember 1980 (MBl. NW. 1980 S. 2930) hat der Innenminister des Landes Nordrhein-Westfalen den Meldebehörden für die Bearbeitung einschlägiger

meldebehördlicher Angelegenheiten empfohlen, bereits jetzt folgende Vorschriften des Melderechtsrahmengesetzes zu beachten:

- § 6 – Schutzwürdige Belange des Betroffenen,
- § 8 – Auskunft an den Betroffenen,
- § 9 Satz 1 – Berichtigung von Daten,
- § 19 – Datenübermittlung an öffentlich-rechtliche Religionsgesellschaften und
- § 21 – Melderegisterauskunft.

Durch Runderlaß vom 18. August 1980 hat der Innenminister darüber hinaus für die Melderegisterauskunft an Parteien und Wählergruppen aus Anlaß von Wahlen eine Regelung getroffen, die die Vorschrift des § 22 Abs. 1 MRRG berücksichtigt.

Der Innenminister hat mich vorab zu dem Entwurf des Runderlasses vom 9. Dezember 1980 um Stellungnahme gebeten.

Ich habe in meiner Stellungnahme darauf hingewiesen, daß nach Artikel 4 Abs. 2 der Landesverfassung in das Grundrecht auf Datenschutz, sofern nicht Bundesrecht einen Eingriff zuläßt, nur im überwiegenden Interesse der Allgemeinheit auf Grund eines Landesgesetzes eingegriffen werden darf. Danach dürfen Vorschriften des Melderechtsrahmengesetzes, die in die Rechtssphäre des Betroffenen eingreifen, nur insoweit vorab angewendet werden, als bereits das geltende Recht einen Eingriff zuläßt.

Die Vorabanwendung der §§ 6, 8 und 21 Abs. 5 MRRG ist zu begrüßen, weil diese Vorschriften die Rechtsstellung des Betroffenen verbessern. Die Anwendung des § 9 Satz 1 MRRG ist unbedenklich, weil er der Regelung in § 17 Abs. 1 DSG NW entspricht. Das gleiche gilt für § 21 Abs. 1 MRRG, der der Regelung in § 36 Abs. 2 DSG NW entspricht. Auch gegen die Anwendung des § 19 Abs. 1 MRRG sind keine durchgreifenden Bedenken zu erheben.

Erhebliche Bedenken bestehen gegen die Vorabanwendung des § 19 Abs. 2 MRRG sowie des § 21 Abs. 2 MRRG.

§ 19 Abs. 2 MRRG, der die Übermittlung bestimmter Daten von Nichtmitgliedern einer Religionsgesellschaft vorsieht, greift in den Kernbereich des Grundrechts der Nichtmitglieder ein (vgl. C.1.c meines ersten Tätigkeitsberichts). Ein solcher Eingriff wäre nach geltendem Recht nur mit Einwilligung des Betroffenen zulässig. Das in § 19 Abs. 2 Satz 3 MRRG vorgesehene Widerspruchsrecht des Betroffenen bietet keinen gleichwertigen Schutz, da es die Schutzwirkung des Grundrechts von einem Tätigwerden des Betroffenen abhängig macht. Eine Übermittlung von Daten von Nichtmitgliedern muß deshalb bis zum Inkrafttreten des neuen Meldegesetzes für das Land Nordrhein-Westfalen unterbleiben, sofern nicht eine ausdrückliche Einwilligung des Betroffenen vorliegt.

§ 21 Abs. 2 MRRG macht die Übermittlung allein davon abhängig, daß der Empfänger ein berechtigtes Interesse glaubhaft macht. Eine Abwägung zwischen diesem Interesse und den Belangen des Betroffenen, wie sie § 13 Abs. 1 Satz 1 DSG NW nach herrschender Meinung verlangt, ist nicht vorgesehen. Sofern der Empfänger nicht ein qualifiziertes (rechtliches oder öffentliches) Interesse geltend macht, hat eine solche Abwägung bei verfassungskonformer Auslegung des § 13 Abs. 1 Satz 1 DSG NW (vgl. oben B.) regelmäßig zur Folge, daß die Belange des Betroffenen überwiegen und eine Übermittlung ohne seine Einwilligung zu unterbleiben hat. Allerdings schreibt § 6 MRRG allgemein vor, daß schutzwürdige Belange der Betroffenen durch die Verarbeitung oder sonstige Nutzung nicht beeinträchtigt werden dürfen. Ob die Anwendung dieser Vorschrift zu dem gleichen Ergebnis wie die Interessenabwägung nach § 13 Abs. 1 Satz 1 DSG NW führt, ist jedoch im Hinblick auf die Spezialvorschrift des § 21 Abs. 6 MRRG zweifelhaft. § 21 Abs. 6 MRRG sieht keinen gleichwertigen Schutz des Betroffenen vor, da diese Vorschrift den Nachweis eines berechtigten Interesses an der Auskunftverweigerung verlangt.

Nach meiner Auffassung ist jedenfalls nicht auszuschließen, daß die Vorabanwendung des § 21 Abs. 2 MRRG zu Eingriffen führt, für die nach geltendem Recht keine gesetzliche

Grundlage vorhanden ist. Ich habe in meiner Stellungnahme an den Innenminister empfohlen, bis zum Inkrafttreten des neuen Meldegesetzes für das Land Nordrhein-Westfalen erweiterte Melderegisterauskünfte nur nach § 13 Abs. 1 Satz 1 DSG NW (in der genannten verfassungskonformen Auslegung) zu erteilen.

Zu begrüßen ist, daß der Innenminister für Auskünfte über Jubiläumsdaten bis zur Anpassung des Landesmelderechts an die Vorschriften des Melderechtsrahmengesetzes an dem Erfordernis der ausdrücklichen Einwilligung des Betroffenen festhält und deshalb von einer Empfehlung der Vorabanwendung der Widerspruchsregelung in § 22 Abs. 2 Satz 1 MRRG abgesehen hat.

c) Datenübermittlung an nicht-öffentliche Stellen

Vor Inkrafttreten des Datenschutzgesetzes Nordrhein-Westfalen wurden Auskünfte aus dem Melderegister nach der Verwaltungsvorschrift zur Durchführung des Meldegesetzes für das Land Nordrhein-Westfalen — VV. MG. NW. — (SMBl. NW. 2101) erteilt. Soweit diese Verwaltungsvorschrift im Widerspruch zu den Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen steht, ist sie nicht mehr anzuwenden.

Nach § 36 Abs. 2 DSG NW 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 (vom Empfänger nicht bezeichneter) Betroffener dürfen nur übermittelt werden, wenn dies im öffentlichen Interesse liegt (Satz 2). § 13 Abs. 1 Satz 1 DSG NW läßt eine Übermittlung weiterer Daten zu, soweit der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

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 Auskünfte über die letzte frühere Wohnung nicht in Betracht. Auch Auskünfte darüber, wer Bewohner eines bestimmten Hauses ist, läßt diese Vorschrift nicht zu, da der Empfänger den Betroffenen zu bezeichnen hat.

Derartige Angaben wie auch Auskünfte über Tag und Ort der Geburt, Beruf, Staatsangehörigkeit, Familienstand, Geburtsname und Name aus der letzten früheren Ehe sind nur unter den Voraussetzungen des § 13 Abs. 1 Satz 1 DSG NW zulässig. Bei der hiernach gebotenen Abwägung der Interessen überwiegt in der Regel das Interesse des Betroffenen. Lediglich dann, wenn der Empfänger nicht nur ein berechtigtes (im Einklang mit der Rechtsordnung stehendes), sondern ein rechtliches (seine Rechtsverhältnisse unmittelbar betreffendes) Interesse glaubhaft macht oder wenn sein Interesse zugleich ein öffentliches Interesse ist, kann in der Regel davon ausgegangen werden, daß das Interesse des Empfängers überwiegt. In allen anderen Fällen bedarf eine Auskunft der Einwilligung des Betroffenen (§ 3 Satz 1 Nr. 2 DSG NW).

Auf Eingaben von Bürgern habe ich die betreffenden Gemeinden auf die Rechtslage hingewiesen und gebeten, andere Daten als Namen, akademische Grade und Anschriften an Privatpersonen und andere nicht-öffentliche Stellen nur noch mit Einwilligung des Betroffenen zu übermitteln, sofern nicht die Voraussetzungen des § 13 Abs. 1 Satz 1 DSG NW vorliegen.

In meinem ersten Tätigkeitsbericht (C. 1. a) habe ich die Auffassung vertreten, daß gegen die Übermittlung von Namen, akademischen Graden und Anschriften an **Adreßbuchverlage** zum Zweck der Herausgabe von Adreßbüchern keine Bedenken bestehen, da die Herausgabe im öffentlichen Interesse liegt (§ 36 Abs. 2 DSG NW). Inzwischen haben sich Bürger bei mir darüber beschwert, daß sich in Adreßbüchern, die jeder käuflich erwerben kann, ein nach Straßen und Häusern gegliedertes Einwohnerverzeichnis befindet, aus dem entnommen werden kann, welche Personen in einem Haus wohnen. Beunruhigung besteht unter anderem wegen der Möglichkeit, auf einfache Weise Informationen zur Vorbereitung von Straftaten (wie etwa Einbruchdiebstählen) zu erlangen.

Soweit eine Auskunft nach § 36 Abs. 2 Satz 1 DSG NW über eine Person gewünscht wird, ist diese Person vom Empfänger zu bezeichnen. Eine Auskunft darüber, welche Personen in einem vom Empfänger bezeichneten Haus wohnen, läßt § 36 Abs. 2 Satz 1 DSG NW nach meiner Ansicht nicht zu. Dies spricht dafür, daß einem Dritten derartige Informationen auch nicht durch ein nach Straßen und Häusern gegliedertes Einwohnerverzeichnis in einem Adreßbuch zugänglich gemacht werden dürfen. Bedenken gegen die Veröffentlichung dieser Informationen wäre gegebenenfalls durch eine entsprechende Beschränkung des Verwendungszwecks der an einen Adreßbuchverlag zu übermittelnden Daten Rechnung zu tragen (§ 13 Abs. 2 in Verbindung mit § 34 DSG NW). Ich habe wegen dieser Frage mit dem Innenminister des Landes Nordrhein-Westfalen Verbindung aufgenommen.

Der Innenminister hat mir mitgeteilt, daß nach seiner Meinung an der Herausgabe sogenannter Straßenverzeichnisse durch die Adreßbuchverlage auf der Grundlage von Daten, die von den Meldeämtern gemäß § 36 Abs. 2 DSG NW übermittelt worden sind, keine aus den Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen abzuleitenden Bedenken beständen.

Er vertritt die Ansicht, daß in § 36 Abs. 2 DSG NW keine verbindliche Entscheidung des Gesetzgebers getroffen sei, auf Grund dieser Vorschrift übermittelte personenbezogene Daten nur in der dort genannten Reihenfolge zu nutzen.

Dem ist zwar zuzustimmen. Daraus folgt aber nicht, daß die genannten Daten auch für eine Nutzung übermittelt werden dürfen, durch die jedermann Zugang zu Daten erhält, die ihm die Meldebehörde selbst nicht übermitteln darf.

Der Innenminister verweist weiter darauf, daß nach § 32 Abs. 3 BDSG bei der zusammengefaßten Übermittlung personenbezogener Daten — um einen solchen Tatbestand handele es sich bei der Herausgabe von Adreßbüchern — kein Grund zu der Annahme bestehen darf, daß dadurch schutzwürdige Belange der Betroffenen beeinträchtigt werden. Bei der gebotenen summarischen Betrachtung (vgl. Simitis in Simitis/Dammann/Mallmann, BDSG, 2. Aufl., § 23 Rdnr. 65) sei er jedoch zu dem Schluß gekommen, daß die insoweit denkbaren Belange wie zum Beispiel die Offenbarung des familiären Umfeldes, die mittelbare Information, wie ein Gebäude genutzt werde, und auch gegebenenfalls die Offenbarung von Nachbarschaftsverhältnissen nicht so gewichtig seien, daß sie gegenüber dem öffentlichen Interesse, das an der Herausgabe von sogenannten Straßenverzeichnissen bestehe, einen Vorrang haben müßten. Das Straßenverzeichnis ermögliche eine gezielte Ansprache des Bürgers in seinem durch die jeweilige Umgebung geprägten sozialen Umfeld. Dies sei zum Beispiel von Bedeutung für die Kommunikation der Parteien mit dem Bürger im Rahmen ihrer Aufgabe, an der politischen Willensbildung mitzuwirken. Gleiches gelte für die verschiedenen, oft auch im öffentlichen Interesse liegenden Aktivitäten von Verbänden, Vereinen und Interessengruppen. An der Herausgabe eines Adreßbuches in Form eines Straßenverzeichnisses bestehe deshalb ein öffentliches Interesse, dem keine entsprechend qualifizierten Belange des Betroffenen entgegenständen.

Der Auffassung des Innenministers kann ich nicht folgen. Meines Erachtens führt sie zu einer Umgehung der in § 36 Abs. 2 und § 13 Abs. 1 Satz 1 DSG NW getroffenen Regelungen. Nach § 36 Abs. 2 Satz 2 ist bei jeder Übermittlung einer Vielzahl personenbezogener Daten zu prüfen, ob diese Übermittlung im öffentlichen Interesse liegt. Wenn die Informationen, die ein nach Straßen und Häusern gegliedertes Einwohnerverzeichnis bietet, aus einem jedermann zugänglichen Adreßbuch entnommen werden können, kann bei den unzähligen Benutzern nicht mehr geprüft werden, ob bei dem einen oder anderen Benutzer auch das erforderliche öffentliche Interesse vorhanden ist. Nach § 13 Abs. 1 Satz 1 DSG NW muß bei der Übermittlung von Daten, die über Namen, akademische Grade und Anschriften eines oder mehrerer vom Empfänger bezeichneter Betroffener hinausgehen, im Einzelfall geprüft werden, ob schutzwürdige Belange des Betroffenen beeinträchtigt werden. Dies ist bei der dem Straßenverzeichnis zu entnehmenden Angabe, wer Bewohner eines bestimmten Hauses ist, nicht möglich.

Adreßbuchverlage fordern bei den Einwohnermeldeämtern auch Daten über eine Altersgruppenzugehörigkeit oder die Zugehörigkeit zu der Gruppe der berufstätigen Ehefrauen, der Gewerbetreibenden oder freiberuflich Tätigen an. Diese Daten dürfen — wie Angaben über Beruf oder Hauseigentümerschaft — nur mit Einwilligung des Betroffenen übermittelt werden, da eine Beeinträchtigung schutzwürdiger Belange des Betroffenen nicht auszuschließen ist.

Die Auffassung, daß Jubiläumsdaten nur mit Einwilligung des Betroffenen an die **Presse** übermittelt werden dürfen, hat sich inzwischen allgemein durchgesetzt. Hierbei ist die Frage aufgeworfen worden, ob ein Unterschied zwischen einem „normalen" Bürger und einer Persönlichkeit des öffentlichen Lebens gemacht werden kann. Eine Gemeinde vertritt die Auffassung, daß bei Persönlichkeiten des öffentlichen Lebens die Weitergabe von Jubiläumsdaten ohne Einwilligung des Betroffenen an die Presse zulässig ist.

Dieser Auffassung vermag ich nicht zu folgen. Nach dem Datenschutzgesetz hat jeder Bürger einen Anspruch auf Schutz seiner personenbezogenen Daten. Hierbei kann kein Unterschied zwischen Persönlichkeiten des öffentlichen Lebens und anderen Bürgern gemacht werden. Auch bei Persönlichkeiten des öffentlichen Lebens können durch die Weitergabe von Jubiläumsdaten schutzwürdige Belange des Betroffenen beeinträchtigt werden. Die Einholung der erforderlichen Einwilligung dürfte in diesen Fällen im übrigen auch keine Schwierigkeiten bereiten.

Es ist erfreulich, daß Kurverwaltungen dazu übergegangen sind, personenbezogene Daten in **Kurzeitungen** nur noch mit Einwilligung des Betroffenen zu veröffentlichen. Für die Zulässigkeit der Übermittlung von Angaben über Kurgäste gilt § 13 Abs. 1 Satz 1 DSG NW. Das erforderliche berechtigte Interesse des Empfängers dürfte zwar meist vorliegen. Durch die Bekanntgabe können jedoch schutzwürdige Belange des Betroffenen beeinträchtigt werden, da es sicher viele Kurgäste gibt, die nicht möchten, daß bekannt wird, wo sie sich aufhalten. Hier muß das Informationsinteresse der Datenempfänger gegenüber dem Interesse des einzelnen Betroffenen am Schutz seiner Privatsphäre zurücktreten. Die Bekanntmachung in einer Kurzeitung bedarf daher der Einwilligung des Betroffenen.

Gelegentlich legen Gemeinden datenschutzrechtliche Bestimmungen zu eng aus. So hat sich ein **Unternehmen** an mich gewandt, das Schwierigkeiten bei der Ermittlung von neuen Anschriften seiner Kunden gehabt hatte. Das Einwohnermeldeamt der Fortzugsgemeinde teilte nur noch den neuen Wohnort, nicht aber die Straße und die Hausnummer mit. Diese Angaben sollten beim Einwohnermeldeamt der Zuzugsgemeinde erfragt werden.

§ 36 Abs. 2 Satz 1 DSG NW, der die Übermittlung von Namen, akademischen Graden und Anschriften eines oder mehrerer vom Empfänger bezeichneter Betroffener an Personen oder andere nicht-öffentliche Stellen zuläßt, enthält keine Beschränkung auf Auskünfte durch die für die derzeitige Wohnung zuständige Meldebehörde. Auch die für den früheren Wohnsitz zuständige Meldebehörde darf die neue Anschrift übermitteln. Da § 36 Abs. 2 Satz 1 DSG NW die Auskunfterteilung auch von keinen weiteren Voraussetzungen abhängig macht und es abweichend von § 13 Abs. 1 Satz 1 DSG NW weder auf ein berechtigtes Interesse des Empfängers noch auf schutzwürdige Belange des Betroffenen ankommt, ist nach meiner Auffassung die Übermittlung der vollständigen neuen Anschrift auch durch die Fortzugsgemeinde zulässig.

Ein beträchtlicher Teil der Eingaben im Bereich des Meldewesens betraf wie im Vorjahr wiederum die Erteilung von Auskünften über die Zugehörigkeit zu bestimmten Gruppen an Vereine.

So wurde angefragt, ob Namen und Anschriften

— der Bürger der Jahrgänge 1957 — 1961 an den Bundesverband der Sozialversicherten e. V. zur Information dieser Bürger über Sozialversicherungsprobleme,

- der im Jahre 1977 geborenen Kinder an die Landesverkehrswacht NRW e. V. zur Information über Möglichkeiten der Unfallverhütung,
- der Kinder im Alter von 1 – 8 Jahren an Nachbargemeinschaften und Schützenbruderschaften zur Durchführung von Nikolaus- und Sankt-Martins-Veranstaltungen,
- der 70-jährigen und älteren Bürger an Schützenbruderschaften für die Veranstaltung von Altenfesten und Altenfahrten

übermittelt werden dürfen.

Bei der Übermittlung dieser Daten, deren Zulässigkeit nach § 13 Abs. 1 Satz 1 DSG NW zu beurteilen ist, überwiegt in der Regel das Interesse der einzelnen Betroffenen an dem Schutz ihrer Privatsphäre gegenüber dem Interesse der Vereine. Die Übermittlung bedarf der Einwilligung des Betroffenen (§ 3 Satz 1 Nr. 2 DSG NW).

Lediglich gegen die Datenübermittlung an die Landesverkehrswacht habe ich keine Bedenken erhoben.

Die Landesverkehrswacht verfolgt mit ihren Bemühungen um eine gezielte Verkehrserziehung von Kleinkindern ein gemeinschaftsdienliches Anliegen. Aus diesem Grunde überwiegt bei der Abwägung der Interessen das Interesse der Landesverkehrswacht gegenüber dem Interesse des einzelnen Betroffenen.

Damit jedoch auch in diesem Falle den Belangen des Datenschutzes wirksam Rechnung getragen werden kann, habe ich empfohlen, die Daten nur in Form von Adreßaufklebern, nicht aber in Form von Listen bereitzustellen. Damit wäre sichergestellt, daß bei der Landesverkehrswacht keine Daten verbleiben.

Am besten wäre den Belangen des Datenschutzes Rechnung getragen, wenn die Gemeinde selbst die von der Verkehrswacht vorbereiteten Schreiben adressieren und versenden würde. Damit würde die Übermittlung von Anschriften an Dritte entfallen.

Wiederholt bin ich ersucht worden, Unbedenklichkeitserklärungen für eine Datenübermittlung an nicht-öffentliche Stellen zu **Forschungszwecken** abzugeben. Ich habe in diesen Fällen darauf hingewiesen, 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. Die Zulässigkeit von Datenübermittlungen bedarf der Prüfung in jedem Einzelfall; die Entscheidung trifft dabei die übermittelnde Stelle in eigener Verantwortung.

Nicht jedes Forschungsvorhaben rechtfertigt die Übermittlung personenbezogener Daten an einen Empfänger außerhalb des öffentlichen Bereichs. Lediglich dann, wenn an dem Forschungsvorhaben auch ein öffentliches Interesse besteht, kann in der Regel davon ausgegangen werden, daß das Interesse des Empfängers gegenüber dem Interesse des Betroffenen an dem Schutz seiner Daten überwiegt. Das Vorliegen eines öffentlichen Interesses müßte zumindest von einer obersten Bundes- oder Landesbehörde bestätigt werden. In allen anderen Fällen bedarf eine Übermittlung der Einwilligung des Betroffenen (§ 3 Satz 1 Nr. 2 DSG NW).

Gegen die Weitergabe von Namen und Anschriften ausländischer Familien mit Kindern im Kindergartenalter an **Kindergärten** habe ich keine datenschutzrechtlichen Bedenken geäußert. Die Mitteilung der in Betracht kommenden Daten an **kommunale Kindergärten** ist zwar keine Übermittlung im Sinne des Datenschutzgesetzes, weil diese keine Dritten sind (§ 2 Abs. 2 Nr. 2, Abs. 3 Nr. 2 DSG NW). Die Gemeinden haben aber 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 Abs. 1 Satz 1 DSG NW). Danach muß die Weitergabe zur rechtmäßigen Erfüllung einer in der Zuständigkeit des kommunalen Kindergartens liegenden Aufgabe erforderlich sein. Diese Voraussetzung liegt hier vor. Wie ich der

Presse entnommen habe, besuchen zum Beispiel nur 30% der türkischen Kinder eines Jahrgangs einen Kindergarten. Die gewollte Integration der hier lebenden Ausländerkinder kann aber nicht nur Aufgabe der Schulen sein. Die Bemühungen müssen schon früher einsetzen. Für eine rasche Eingewöhnung in die deutschen Verhältnisse und als Vorbereitung zur Eingliederung in deutsche Schulen kommt dem Besuch eines Kindergartens besondere Bedeutung zu. Die sich hier stellenden Aufgaben können die Kindergärten nur erfüllen, wenn sie möglichst lückenlos Namen und Anschriften der ausländischen Familien erhalten, um mit ihnen Kontakt aufzunehmen. Allerdings dürfen nur die Anschriften solcher Familien weitergegeben werden, die im Einzugsbereich des jeweiligen Kindergartens wohnen.

Für die Übermittlung der Anschriften an **Kindergärten der öffentlich-rechtlichen Religionsgesellschaften** gilt § 11 Abs. 2 in Verbindung mit § 11 Abs. 1 DSG NW. Ebenso wie bei den kommunalen Kindergärten kann davon ausgegangen werden, daß die Übermittlung der Anschriften zur Erfüllung der in der Zuständigkeit der konfessionellen Kindergärten liegenden Aufgaben erforderlich ist.

Für die Zulässigkeit der Übermittlung dieser Daten an **Kindergärten sonstiger freier Träger,** die als Träger der freien Jugendhilfe öffentlich anerkannt sind, gilt § 13 Abs. 1 Satz 1 DSG NW. Bei einer Abwägung der Interessen überwiegt das Interesse der Kindergärten gegenüber dem Interesse des einzelnen Betroffenen am Schutz seiner Privatsphäre, da jeder Beitrag der Kindergärten zur Integration der Ausländerkinder nicht nur den Kindern und ihren Eltern dient, sondern auch dem Interesse der Allgemeinheit.

Um eine Verletzung des Datengeheimnisses auszuschließen, dürfen grundsätzlich keine **telefonischen Auskünfte** erteilt werden; sofern ausnahmsweise aus zwingenden Gründen eine telefonische Auskunft erforderlich ist, muß durch Rückruf bei der anfragenden Stelle deren Identität eindeutig festgestellt sein (D. 2. d meines ersten Tätigkeitsberichts). Dies gilt jedoch nur für Auskünfte, bei denen es auf die Identität des Auskunftsuchenden ankommt.

Bei der Erteilung von Auskünften nach § 36 Abs. 2 Satz 1 DSG NW ist eine Identitätsfeststellung nicht erforderlich, da diese Vorschrift die Übermittlung der dort genannten Daten eines oder mehrerer vom Empfänger bezeichneter Betroffener ohne weitere Voraussetzung zuläßt.

d) Datenübermittlung an öffentliche Stellen

Ein Mitglied des Landtags hat mich unter Hinweis auf die Antwort der Landesregierung auf seine Kleine Anfrage (Drucksache 9/254) um Stellungnahme zu der Datenübermittlung durch die Meldebehörden an die Polizei für Zwecke der Nachwuchswerbung gebeten. Die Meldebehörden übermitteln den Polizeibehörden für die Versendung von Werbebriefen entweder listenmäßig oder durch Übersenden von Aufklebern Namen und Anschriften bestimmter Geburtsjahrgänge. Die Listen werden von der Polizei unmittelbar nach der Versendung der Werbebriefe an den in Betracht kommenden Personenkreis vernichtet. Soweit die Polizeibehörden Aufkleber erhalten, werden diese unmittelbar zur Adressierung verwendet. Im Anschluß an den Versand sind die Daten bei der Polizei nicht mehr erfaßt.

Für die Übermittlung durch Meldebehörden an die Polizei gilt § 11 Abs. 1 Satz 1 DSG NW. Danach ist die Übermittlung zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist. Nach der hier allein in Betracht kommenden zweiten Alternative dieser Vorschrift ist die Übermittlung nur dann erforderlich, wenn der Empfänger seine Aufgaben ohne Kenntnis der Daten nicht rechtmäßig erfüllen kann. An die Erforderlichkeit sind strenge Anforderungen zu stellen; es reicht nicht aus, wenn zur Aufgabenerfüllung die Kenntnis der Daten nur dienlich, aber nicht unbedingt notwendig ist.

Zwar ist zur rechtmäßigen Erfüllung der Aufgaben der Polizei eine ausreichende Personalausstattung notwendig. Auch kann nach der Antwort der Landesregierung auf die

Kleine Anfrage davon ausgegangen werden, daß nur mit einer individuellen Direktwerbung durch Einstellungsberater die angestrebte Polizeidichte erreicht werden kann. Nach meiner Auffassung ist jedoch für diese Werbemethode die Übermittlung der Namen und Anschriften der in Betracht kommenden Geburtsjahrgänge an die Polizei nicht erforderlich. Die von der Polizei vorbereiteten Werbebriefe können gegen Kostenerstattung von den Meldebehörden adressiert und versandt werden. Auf diese Weise können die Angehörigen der in Betracht kommenden Jahrgänge ohne Übermittlung ihrer Daten angeschrieben werden. Für die Polizei würde dies an dem Ergebnis der Werbeaktion nichts ändern. Die individuelle Direktwerbung durch Einstellungsberater setzt ohnehin erst dann ein, wenn die Antworten der potentiellen Bewerber vorliegen. Unter diesen Umständen halte ich eine Übermittlung der genannten Daten durch die Meldebehörden an die Polizei nach geltendem Recht nicht für zulässig.

Sofern gleichwohl aus Gründen der Zweckmäßigkeit an dem Versand der Werbebriefe durch die Polizei festgehalten werden soll, müßte für die regelmäßige Datenübermittlung an die Polizei eine Rechtsgrundlage geschaffen werden. Hierfür käme entweder eine Rechtsverordnung nach § 14 DSG NW oder eine Regelung gemäß § 18 Abs. 4 MRRG in dem neuen Meldegesetz für das Land Nordrhein-Westfalen in Betracht.

Datenschutzrechtlich unbedenklich wäre auch eine Verteilung der Werbebriefe durch die Schulen. Die Übermittlung von Listen der für eine Einstellung in Betracht kommenden Schülerjahrgänge an die Polizei wäre hingegen ebenfalls nicht zulässig.

Ich habe dem Innenminister über meine Bedenken gegen die Übermittlung der genannten Daten durch die Meldebehörden an die Polizei unterrichtet und ihm empfohlen, zur Vermeidung von Verstößen gegen Vorschriften über den Datenschutz auf die Datenübermittlung an die Polizei zu verzichten und die Werbebriefe durch die Meldebehörden versenden oder durch die Schulen verteilen zu lassen. Bei einem Versand durch die Meldebehörden sollte in dem Werbebrief auf die Art der Versendung hingewiesen werden, um bei den Betroffenen den Eindruck zu vermeiden, daß ihre Daten der Polizei übermittelt werden.

e) Datenübermittlung an die Kirchen

Mehrere Gemeinden und eine Kommunale Datenverarbeitungszentrale haben mich zu der Frage des zulässigen Umfangs der Datenübermittlung an öffentlich-rechtliche Religionsgesellschaften um Stellungnahme gebeten.

Hinsichtlich der Zulässigkeit der Datenübermittlung an die öffentlich-rechtlichen Religionsgesellschaften durch Kommunale Datenverarbeitungszentralen habe ich darauf hingewiesen, daß über die Übermittlung nicht die Kommunale Datenverarbeitungszentrale, sondern jede einzelne speichernde Stelle zu entscheiden hat. Diese ist Normadressat des Datenschutzgesetzes Nordrhein-Westfalen (§ 1 Abs. 2 Satz 1, § 2 Abs. 3 Nr. 1 DSG NW). Für die Kommunalen Datenverarbeitungszentralen gelten von den Vorschriften dieses Gesetzes nur die §§ 1 bis 9 und 24 bis 31 (§ 7 Abs. 2 Satz 1 DSG NW). Sie sind bei der Datenverarbeitung in jeder ihrer Phasen an die Weisung der speichernden Stellen gebunden (§ 7 Abs. 2 Satz 2 DSG NW).

Auch nach Inkrafttreten des Melderechtsrahmengesetzes dürfen nach meiner Auffassung bis zum Inkrafttreten des neuen Meldegesetzes für das Land Nordrhein-Westfalen den öffentlich-rechtlichen Religionsgesellschaften lediglich Daten ihrer Mitglieder übermittelt werden. Die Übermittlung personenbezogener Daten von Familienangehörigen eines Mitglieds, die nicht selbst Mitglieder der jeweiligen Religionsgesellschaft sind, ist nach geltendem Recht unzulässig, sofern nicht eine ausdrückliche Einwilligung des Betroffenen vorliegt (oben C. 1. b).

Ich habe deshalb auf die Frage einer Gemeinde nach der Zulässigkeit der Übermittlung von Namen und Anschriften

- der 70-jährigen und älteren Bürger für die Vorbereitung von Altentagen und Altenfahrten,
- der bis zu 14 Jahre alten Kinder zur Durchführung von Sankt-Martins-Veranstaltungen,
- der 18-jährigen und älteren katholischen Bürger anläßlich von Kirchenvorstandswahlen

an die Pfarrgemeinderäte und Kirchenvorstände mitgeteilt, daß aus datenschutzrechtlicher Sicht nur dann keine Bedenken gegen die Weitergabe von Listen mit diesen Daten bestehen, wenn die jeweilige Kirchengemeinde lediglich die Daten ihrer Mitglieder erhält.

Nach § 11 Abs. 2 DSG NW ist die Datenübermittlung an die öffentlich-rechtlichen Religionsgesellschaften darüber hinaus nur zulässig, wenn sichergestellt ist, daß bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen sind. Nach den Feststellungen des Innenministers haben die evangelischen Landeskirchen und die römisch-katholische Kirche im Bereich des Landes Nordrhein-Westfalen entsprechende Rechtsvorschriften erlassen und hinreichende Vorkehrungen zu deren Vollzug getroffen. Damit kann das Erfordernis, daß bei diesen Datenempfängern ausreichende Datenschutzmaßnahmen getroffen sind, nach Auffassung des Innenministers als erfüllt angesehen werden. Falls an weitere öffentlich-rechtliche Religionsgesellschaften Daten übermittelt werden sollen, ist hier das Vorliegen ausreichender Datenschutzmaßnahmen gesondert zu prüfen (Runderlaß vom 9. Dezember 1980, MBl. NW. S. 2930).

f) Lohnsteuerkarten

Bei der Ausstellung und der Zustellung der Lohnsteuerkarten durch die Gemeinden ergaben sich auch in diesem Jahr wieder datenschutzrechtliche Probleme. Bürger haben sich darüber beschwert, daß die Lohnsteuerkarten ohne Umschlag oder in einem Umschlag mit dem Aufdruck „Inhalt: Lohnsteuerkarte" übersandt wurden und daß auf der Lohnsteuerkarte der Familienstand angegeben war.

Die Gemeinden werden bei der Ausstellung der Lohnsteuerkarten als örtliche Landesfinanzbehörden tätig und unterliegen insoweit dem Steuergeheimnis nach § 30 der Abgabenordnung (AO). Das Steuergeheimnis wird durch jede unbefugte Offenbarung der Verhältnisse eines anderen verletzt (§ 30 Abs. 2 AO).

Zu den Verhältnissen eines Steuerpflichtigen im Sinne des § 30 Abs. 2 Ziffer 1 AO gehören die persönlichen, wirtschaftlichen und steuerlichen Verhältnisse. Demnach unterliegen auch die auf der Steuerkarte enthaltenen Angaben dem Steuergeheimnis. Es muß daher sichergestellt werden, daß das Steuergeheimnis auch bei der Zustellung der Lohnsteuerkarten gewahrt wird. Die Handhabung in einigen Gemeinden, die Lohnsteuerkarten noch immer ohne Umschlag zu übersenden und die offenen Lohnsteuerkarten teilweise sogar im Hausflur oder vor der Haustür abzulegen, verstößt gegen die Verpflichtung zur Wahrung des Steuergeheimnisses.

Ich habe die Gemeinden auf die Rechtslage hingewiesen und gebeten, zur Vermeidung von Verstößen gegen das Steuergeheimnis und andere Vorschriften über den Datenschutz Lohnsteuerkarten nur noch in einem verschlossenen Umschlag zuzustellen. Die Zusendung von Lohnsteuerkarten durch die Post im offenen Umschlag oder in einem Adhäsionsumschlag als Drucksache genügt dieser Anforderung nicht.

Zu den Verhältnissen eines anderen gehört auch dessen Eigenschaft als Arbeitnehmer. Da eine Lohnsteuerkarte in der Regel nur für Arbeitnehmer ausgestellt wird, wird durch die Versendung in einem Umschlag mit dem Aufdruck „Inhalt: Lohnsteuerkarte" die Arbeitnehmereigenschaft des Betroffenen den Postbediensteten und gegebenenfalls auch anderen Personen offenbart, die Zugang zu dem Umschlag haben, bevor dieser den Betroffenen erreicht. Die Arbeitnehmereigenschaft ist für die Postbediensteten nicht offenkundig; es kann auch nicht davon ausgegangen werden, daß sie für alle anderen Personen, die Zugang zu dem Umschlag haben, offenkundig ist.

Eine Befugnis zur Offenbarung an die genannten Personen ist nicht ersichtlich. Die Offenbarung dient nicht der Durchführung des Zustellungsverfahrens, da der Aufdruck für die Postbeförderung nicht erforderlich ist (§ 30 Abs. 4 Nr. 1 AO). Auch liegt kein anderer Fall zulässiger Offenbarung vor (§ 30 Abs. 4 Nr. 2 bis 5 AO). Ich habe darauf hingewiesen, daß durch die Versendung der Lohnsteuerkarten in einem Umschlag mit dem genannten Aufdruck das Steuergeheimnis (§ 30 Abs. 1 AO) verletzt wird.

Die Angabe des Familienstandes auf der Lohnsteuerkarte ist für die Berechnung der Lohnsteuer durch den Arbeitgeber nicht erforderlich. Hierfür reichen die Steuerklasse und die Zahl der Kinder aus. Der Familienstand kann jedoch für die Nachprüfung der Besteuerung durch das Finanzamt erheblich sein.

Rechtsgrundlage für die Aufnahme des Familienstandes in die Lohnsteuerkarte ist § 39 Abs. 3 Satz 1 des Einkommenssteuergesetzes. Danach hat die Gemeinde auf der Lohnsteuerkarte insbesondere den Familienstand, die Steuerklasse und die Zahl der Kinder des Steuerpflichtigen einzutragen. Nach § 39 Abs. 3 Satz 3 dieses Gesetzes ist die Eintragung der genannten Angaben die gesonderte Feststellung von Besteuerungsgrundlagen, die unter dem Vorbehalt der Nachprüfung steht. Für eine Änderung der Rechtsvorschrift, die die Gemeinde zur Eintragung des Familienstandes verpflichtet, wäre der Bundesgesetzgeber zuständig.

2. Paß- und Personalausweiswesen

Das Gesetz zur Änderung des Gesetzes über Personalausweise (BPersAG) sieht die Einführung eines neuen fälschungssicheren und maschinenlesbaren Personalausweises ab 1. Oktober 1981 vor. Gegen das vorgesehene Herstellungsverfahren bestehen datenschutzrechtliche Bedenken.

Die für die Vorderseite des Ausweises vorgesehenen Angaben werden bei der Bundesdruckerei vom Antragsformular auf das Ausweisblankett übertragen und danach sofort gelöscht. Die auf der Rückseite aufzubringenden Daten bleiben gespeichert, bis nach Fertigstellung der Vorderseite die Rückseite beschrieben werden kann. Die Daten bleiben mittels der Seriennummer identifizierbar. Sie werden gelöscht, wenn der Ausweis die Dienststelle verläßt. Personenbezogene Daten nach § 1 Abs. 2 BPersAG werden also in der Bundesdruckerei, wenn auch nur für einen begrenzten Zeitraum, gespeichert. Dies ist nach § 3 Abs. 3 Satz 2 BPersAG unzulässig.

Durch Initiativen der Datenschutzbeauftragten des Bundes und der Länder ist zwar erreicht worden, daß die Verarbeitungsdauer bei der Bundesdruckerei erheblich verkürzt wird. Wenngleich durch die Verkürzung der Speicherungsdauer die Gefahr eines Mißbrauchs verringert wurde, verstößt auch eine zeitlich begrenzte Speicherung gegen das Gesetz. Der Bundesbeauftragte für den Datenschutz hat dies nach § 20 des Bundesdatenschutzgesetzes beanstandet.

Ich habe dem Innenminister des Landes Nordrhein-Westfalen meine Bedenken gegen das Herstellungsverfahren mitgeteilt und ihn von der Beanstandung des Bundesbeauftragten für den Datenschutz in Kenntnis gesetzt. Darüber hinaus habe ich ihn gebeten, sich in den zuständigen Gremien für eine gesetzeskonforme Lösung einzusetzen. Wenn an dem bisher vorgesehenen Herstellungsverfahren festgehalten werden soll, müßte durch Änderung des Gesetzes über Personalausweise eine Ausnahme von dem Speicherungsverbot vorgesehen werden.

3. Wahlen

Anläßlich der Bundes- und der Landtagswahl haben viele Bürger **Werbeschreiben von Parteien** erhalten. Bei diesen Schreiben handelte es sich nicht um Postwurfsendungen,

sondern um persönlich adressierte Briefe. Zahlreiche Bürger wollten wissen, auf welche Weise die Parteien ihre Anschriften erhalten hatten und ob die Übermittlung der Anschriften datenschutzrechtlich zulässig sei.

Die Übermittlung von Namen und Anschriften von Wahlberechtigten, auch bestimmter Gruppen wie Jungwähler oder Senioren, an Parteien oder zu einer Wahl zugelassenen Wählergruppen kann durch die Anfertigung von Auszügen oder Abschriften des Wählerverzeichnisses oder durch Auskunft aus dem Melderegister erfolgen.

Gesetzliche Grundlage für die Anfertigung von Auszügen oder Abschriften des Wählerverzeichnisses sind die Vorschriften der Wahlordnungen. Danach kann die Gemeindebehörde die Anfertigung von Auszügen oder Abschriften des Wählerverzeichnisses innerhalb der Auslegungsfrist durch an der Wahl teilnehmende Parteien zulassen oder auch selbst Auszüge und Abschriften erteilen, wenn ein berechtigtes Interesse im Zusammenhang mit der Wahl besteht; dabei ist auch die Kenntlichmachung bestimmter Altersgruppen zulässig. Die Auszüge oder Abschriften dürfen jedoch nicht die Geburtsdaten der Wähler enthalten.

Gesetzliche Grundlage für Auskünfte aus dem Melderegister über Namen und Anschriften von Wahlberechtigten an Parteien ist § 13 Abs. 1 Satz 1 DSG NW. Ein berechtigtes Interesse der Parteien an der Kenntnis der Daten liegt vor. Die Parteien wirken nach Artikel 21 Abs. 1 des Grundgesetzes 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 und dabei auch bestimmte Gruppen von Bürgern wie Jungwähler oder Senioren gezielt anzusprechen. Bei der Abwägung der Interessen überwiegt dieses Interesse der Parteien gegenüber dem Interesse des Bürgers an dem Schutz vor einer Mitteilung seiner personenbezogenen Daten. Das Interesse des Bürgers muß hier gegenüber dem Interesse der Parteien an einer Verbesserung der Kommunikation mit den Bürgern, das zugleich ein öffentliches Interesse ist, zurücktreten.

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.

Die Vorschriften über den Datenschutz gebieten nach meiner Auffassung nicht, die Übermittlung auf die Zeit eines halben Jahres vor einer Wahl oder auf Angaben über die Zugehörigkeit zur Gruppe der Erstwähler zu beschränken.

In einem Fall haben meine Ermittlungen ergeben, daß eine Wählergemeinschaft aus Anlaß der Kommunalwahlen 1979 Adressenmaterial von Wahlberechtigten bei einer Kommunalen Datenverarbeitungszentrale angefordert und gegen Zahlung eines Entgelts von dieser erhalten hat. Die Wählergemeinschaft wurde darauf hingewiesen, daß die Adressenaufkleber nur für Zwecke der Wahl verwendet werden dürfen. Die betreffende Wählergemeinschaft hat die Anschriften jedoch nicht nur zu diesem Zweck, sondern für die Versendung eines Schreibens zur Gewinnung von Kaufinteressenten für die darin beschriebenen Immobilienobjekte verwendet. Dies ist ein Verstoß gegen § 13 Abs. 2 DSG NW, der nach § 34 DSG NW als Ordnungswidrigkeit mit Geldbuße geahndet werden kann. Da meiner Kontrolle nur die in § 26 Abs. 1 Satz 1 DSG NW genannten Stellen unterliegen, hatte ich selbst keine Möglichkeiten, gegen diese Wählergemeinschaft vorzugehen.

Zwar dürfen nach § 13 Abs. 5 Satz 3 der Kommunalwahlordnung und § 17 Abs. 5 Satz 5 der Landeswahlordnung Auszüge und Abschriften des Wählerverzeichnisses ebenfalls nur für Zwecke der Wahl verwandt und Dritten nicht zugänglich gemacht werden. Es fehlt aber eine dem § 34 DSG NW für die Ahndung von Verletzungen des § 13 Abs. 2 DSG NW entsprechende Bußgeldvorschrift.

Ich habe dem Innenminister empfohlen, eine entsprechende Bestimmung in die Wahlvorschriften aufzunehmen. Dadurch könnte den datenschutzrechtlichen Belangen der Betroffenen wirksamer Rechnung getragen werden.

Eine Eingabe betraf den **Wahlvorgang.** Um den Datenschutzbelangen der Betroffenen Rechnung zu tragen, sieht § 56 Abs. 4 Satz 4 der Bundeswahlordnung (BWO) vor, daß die Mitglieder des Wahlvorstandes nicht befugt sind, Angaben zur Person des Wählers — also auch Angaben zu einer Stimmabgabe — so zu verlautbaren, daß sie von sonstigen im Wahlraum Anwesenden zur Kenntnis genommen werden können, sofern nicht die Feststellung der Wahlberechtigung dies erfordert. Außerdem sind die Mitglieder von Wahlausschüssen und Wahlvorständen zur Verschwiegenheit über die ihnen bei ihrer amtlichen Tätigkeit bekanntgewordenen Tatsachen, insbesondere über alle dem Wahlgeheimnis unterliegenden Angelegenheiten zu verpflichten (§ 5 Abs. 5 BWO, §§ 6 Abs. 3 Satz 1, 53 Abs. 1 BWO).

Entsprechende datenschutzrechtliche Regelungen sind bisher in der Landeswahlordnung und der Kommunalwahlordnung nicht enthalten. Ich habe deshalb diese Eingabe zum Anlaß genommen, dem Innenminister des Landes Nordrhein-Westfalen zu empfehlen, entsprechende Regelungen auch in diese Wahlordnungen aufzunehmen. Der Innenminister hat mir mitgeteilt, daß er Regelungen über die Verpflichtung der Wahlausschuß- und Wahlvorstandsmitglieder zur Verschwiegenheit sowie über eine Diskretionspflicht der Wahlvorstandsmitglieder im Wahllokal zur Aufnahme in die Landes- und Kommunalwahlordnung vorgemerkt habe.

4. Personenstandswesen

Eingaben im Bereich des Personenstandswesens betrafen unter anderem die Datenerhebung bei dem Standesamt im Falle einer Geburt und die Erteilung von Auskünften aus den Personenstandsbüchern für Zwecke der Familienforschung.

Einem Bürger, der bei dem zuständigen Standesbeamten die **Geburt** seines Kindes anzeigen wollte, wurde mittels eines Vordrucks eine Vielzahl von Fragen gestellt; die Rechtsgrundlage für diese Datenerhebung wurde ihm nicht genannt.

Eine Datenerhebung bei dem Betroffenen ist nur auf Grund einer Rechtsvorschrift oder auf freiwilliger Grundlage zulässig. Nach § 10 Abs. 2 Satz 1 DSG NW ist der Betroffene auf die Rechtsvorschrift oder auf die Freiwilligkeit hinzuweisen. Derartige Hinweise fehlten in dem von dem betreffenden Standesamt verwendeten Vordruck.

Rechtsgrundlagen für die Datenerhebung im Fall einer Geburt sind § 21 des Personenstandsgesetzes (PStG), § 70 Nr. 1 PStG in Verbindung mit der Verordnung zur Ausführung des Personenstandsgesetzes (PStV) sowie das Gesetz über die Statistik der Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes in der Fassung vom 14. März 1980 (BGBl. I S. 308). Soweit die Datenerhebung nach diesen Rechtsvorschriften nicht erforderlich ist, besteht keine Verpflichtung zu entsprechenden Angaben.

Die Prüfung des Vordrucks ergab, daß für die Angabe der Amtsbezeichnung bei Beamten sowie des akademischen Grades keine Rechtsgrundlage vorhanden ist. Die Erhebung dieser Daten wird auf die Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden gestützt. Diese ist jedoch nur eine Verwaltungsvorschrift, keine Rechtsvorschrift. Amtsbezeichnung und akademischer Grad können deshalb nur auf freiwilliger Grundlage erhoben werden.

Auch für die in dem Vordruck vorgesehene Angabe des Geburtsdatums des Vaters und der Mutter sowie der Erwerbstätigkeit des Vaters besteht keine Rechtsgrundlage. Nach dem Gesetz über die Statistik der Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes ist nur die Angabe des Alters der Eltern sowie der Erwerbstätigkeit der Mutter erforderlich.

Für die Erhebung der anderen in dem Vordruck genannten Daten ist eine Rechtsgrundlage vorhanden. Der Vordruck ist inzwischen neugestaltet und mit einem Hinweis nach § 10 Abs. 2 DSG NW versehen worden.

Zu der Einsichtnahme in Personenstandsbücher zum Zwecke der **Familienforschung** habe ich wie folgt Stellung genommen.

Die Benutzung der seit dem 1. Juli 1938 geführten Personenstandsbücher ist in § 61 Abs. 1 des Personenstandsgesetzes (PStG) geregelt. Nach § 61 der Verordnung zur Ausführung des Personenstandsgesetzes (PStV) gilt § 61 Abs. 1 PStG auch für die Benutzung der vom 1. Januar 1876 bis zum 30. Juni 1938 geführten Standesregister.

Nach § 61 Abs. 1 PStG kann Einsicht in die Personenstandsbücher oder Durchsicht dieser Bücher 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 oder Durchsicht, wenn sie ein rechtliches Interesse glaubhaft machen (Satz 3).

Ein rechtliches Interesse an der Einsicht oder Durchsicht liegt nur dann vor, wenn die Kenntnis der Personenstandsdaten eines anderen zur Verfolgung oder Wahrung von Rechten erforderlich ist. Genealogische Forschungen erfüllen diese Voraussetzung nicht.

Die Standesämter dürfen deshalb zu diesen Forschungszwecken nur dann Einsicht und Durchsicht gewähren, wenn die Person, auf die sich der Eintrag bezieht, ihr Ehegatte, ein Vorfahre oder ein Abkömmling eine entsprechende schriftliche Vollmacht erteilt hat. Die Durchsicht der Personenstandsbücher ist allerdings auch unter dieser Voraussetzung nur gezielt möglich, weil bei allgemeiner Durchsicht nicht nur der gesuchte Eintrag, sondern alle in diesem Personenstandsbuch enthaltenen Einträge zur Kenntnis des Lesers gelangen und der Schutz der eingetragenen Personen nicht gewährleistet wäre (vgl. Runderlaß des Innenministers des Landes Nordrhein-Westfalen vom 9. September 1980, MBl. NW. S. 2124).

Für die Benutzung der vor dem 1. Januar 1876 geführten Zweitregister der Zivilstandsregister, die in den Personenstandsarchiven Brühl und Detmold aufbewahrt werden, gilt § 4 Abs. 2 Satz 2 der Verordnung zur Durchführung des Personenstandsgesetzes (PStVO.NW.) vom 10. Dezember 1974 (SGV. NW. 211) in Verbindung mit § 61 PStG. Danach kann Einsicht und Durchsicht unter den gleichen Voraussetzungen wie bei den Personenstandsbüchern und Standesregistern gewährt werden. Für die Einsicht in die vor dem 1. Oktober 1874 geführten Zivilstandsregister und deren Durchsicht genügt es jedoch, ein berechtigtes Interesse glaubhaft zu machen. Auch auf diese Register finden die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen keine Anwendung.

Da das Interesse an der Durchführung von Familienforschungen ein berechtigtes ist, kann für diese Zwecke bei den vor dem 1. Oktober 1874 geführten Registern Einsicht oder Durchsicht gewährt werden, ohne daß es einer Vollmacht einer der in § 61 Abs. 1 Satz 1 PStG genannten Personen bedarf.

5. Staatsangehörigkeitsangelegenheiten

Eine Eingabe gab Anlaß zu der Prüfung, ob es erforderlich und mit dem Datenschutz vereinbar ist, für die Erlangung eines Staatsangehörigkeitsausweises zahlreiche personenbezogene Daten, insbesondere auch Daten über die Großeltern eines Betroffenen zu erheben.

Die deutsche Staatsangehörigkeit wird nach § 3 des Reichs- und Staatsangehörigkeitsgesetzes (RuStAG) unter anderem durch die Geburt erworben (Abstammungsprinzip). Der Nachweis des Erwerbs der Staatsangehörigkeit durch Abstammung kann schwierig sein. Um nachzuweisen, daß jemand die deutsche Staatsangehörigkeit eines Elternteils erworben hat, muß zunächst die Staatsangehörigkeit dieses Elternteils nachgewiesen werden. Falls dieser Elternteil seine deutsche Staatsangehörigkeit ebenfalls durch Abstammung erworben hat, muß der Nachweis der Staatsangehörigkeit des Großeltern-

teils erbracht werden, von dem der Elternteil die Staatsangehörigkeit erworben hat. Falls auch der Großelternteil seine Staatsangehörigkeit durch Abstammung erworben hat, müßte in aufsteigender Linie weiter zurückgegangen werden, bis ein Vorfahre festgestellt wird, der die Staatsangehörigkeit auf andere Weise erworben hat, etwa auf Grund des in Preußen bis 1842 geltenden Wohnsitzprinzips oder durch Einbürgerung.

In der Praxis begnügen sich die für die Ausstellung von Staatsangehörigkeitsausweisen zuständigen Behörden in der Regel damit, bis auf den Großvater zurückzugehen. Die Bundesländer sind übereingekommen, daß die deutsche Staatsangehörigkeit in der Regel festgestellt werden kann, wenn der Antragsteller glaubhaft macht, daß er oder die Personen, von denen er seine Staatsangehörigkeit ableitet, seit dem 1. Januar 1914 als deutsche Staatsangehörige behandelt worden sind (vgl. Runderlaß des Innenministers des Landes Nordrhein-Westfalen vom 17. März 1958, SMBl. NW. 102).

Zur Feststellung des Erwerbs der deutschen Staatsangehörigkeit kann es deshalb auch erforderlich sein, auf Daten der Großeltern zurückzugreifen, um Meldeunterlagen und gegebenenfalls auch Standesamtsakten heranziehen zu können. Da der Staatsangehörigkeitsnachweis einen höheren Beweiswert für den Besitz der deutschen Staatsangehörigkeit hat als ein Personalpapier, läßt sich der für die Feststellung der Staatsangehörigkeit erforderliche Verwaltungsaufwand nicht vermeiden.

Die dargelegten Schwierigkeiten bei dem Nachweis des Staatsangehörigkeitserwerbes durch Abstammung haben in Nordrhein-Westfalen dazu geführt, daß von Behörden nur in Zweifelsfällen Staatsangehörigkeitsausweise gefordert werden, während im allgemeinen Personalausweis oder Reisepaß als Beleg für den Besitz der deutschen Staatsangehörigkeit angesehen werden.

Eine Vereinfachung des Verfahrens zur Feststellung der Staatsangehörigkeit durch Aufstellung gesetzlicher Vermutungsregeln wäre zweckmäßig und aus der Sicht des Datenschutzes zu begrüßen. Sie stößt jedoch wegen des gebotenen Festhaltens an der einheitlichen deutschen Staatsangehörigkeit und damit an dem Reichs- und Staatsangehörigkeitsgesetz auf Schwierigkeiten. Diese deutschlandpolitische Notwendigkeit muß vor den Belangen des Datenschutzes Vorrang haben.

6. Öffentliche Ordnung

Ein Bürger hat mich auf den Artikel in einer Tageszeitung „Für Katastrophenfall Schwerbehinderte dem Ordnungsamt melden" aufmerksam gemacht. In diesem Artikel ist der Aufruf einer Gemeinde wiedergegeben, im Rahmen von vorbeugenden **Katastrophenschutzmaßnahmen** dem Ordnungsamt Behinderte unter Angabe von Namen, Anschrift, Alter und Art der Behinderung zu benennen.

Gegen diesen Aufruf habe ich datenschutzrechtliche Bedenken erhoben. Gewiß ist es notwendig, in die Sicherheitsvorkehrungen für den Brand- und Katastrophenfall gerade die Behinderten einzubeziehen. Dies muß aber in rechtlich einwandfreier Weise geschehen.

Nach Artikel 4 Abs. 2 der Landesverfassung bedarf jedes Erheben, Sammeln und Festhalten personenbezogenener Daten einer gesetzlichen Grundlage, sofern keine Einwilligung des Betroffenen vorliegt.

Eine gesetzliche Grundlage für die Datenerhebung über Behinderte für Zwecke des Katastrophenschutzes ist nicht ersichtlich. Dies gilt sowohl für die Datenerhebung beim Betroffenen selbst wie auch bei anderen über ihn. Damit bleibt nur die Möglichkeit der Datenerhebung beim Betroffenen auf der Grundlage der Freiwilligkeit. Auf die Freiwilligkeit ist bei der Erhebung hinzuweisen (§ 10 Abs. 2 Satz 1 DSG NW).

Nur wenn der Betroffene selbst nicht in der Lage ist, die erforderlichen Auskünfte zu geben, ist im Hinblick auf den in diesem Fall höherrangigen Sozialstaatsgrundsatz die Erhebung bei nahen Angehörigen (Ehegatte, Eltern, Kinder), gesetzlichen Vertretern und Heim- oder Anstaltsleitern gerechtfertigt.

Auf die Freiwilligkeit wird auch in einem Erlaß des Innenministers des Landes Nordrhein-Westfalen vom 3. September 1979 betreffend Sicherheitsvorkehrungen für Behinderte im Brand- und Katastrophenfall ausdrücklich hingewiesen.

Eine Bürgerin hat in einer **Friedhofsangelegenheit** ein Auskunftsersuchen an eine Behörde gerichtet. Sie bat um Auskunft über die früheren Nutzungsberechtigten sowie über die Daten der jeweiligen Umschreibung des Nutzungsrechts an der Grabstätte ihrer Eltern. Die Auskunft wurde ihr unter Hinweis auf das Datenschutzgesetz Nordrhein-Westfalen verweigert. Ich wurde um Überprüfung dieser Auskunftsverweigerung ersucht.

Die Daten, über die Auskunft begehrt wurde, sind Einzelangaben über sachliche Verhältnisse sowohl der derzeitigen Nutzungsberechtigten als auch der anderen Personen, deren Angehörige in der Grabstätte beerdigt sind, also auch der Auskunftsuchenden (§ 2 Abs. 1 DSG NW). Es handelt sich somit um Daten mit Doppelbezug.

Bei Daten mit Doppelbezug können die in § 4 DSG NW genannten Rechte, also auch das Auskunftsrecht nach § 16 DSG NW, grundsätzlich von jedem der Betroffenen geltend gemacht werden. Die Auskunftserteilung unterbleibt — von hier nicht in Betracht kommenden Fällen abgesehen — nur dann, wenn die personenbezogenen Daten wegen der überwiegenden berechtigten Interessen einer dritten Person geheimgehalten werden müssen (§ 16 Abs. 3 Nr. 3 DSG NW).

Ein Geheimhaltungsinteresse der derzeitigen Nutzungsberechtigten, das höher zu bewerten wäre als das Interesse der Auskunftsuchenden, war nicht erkennbar. Ich habe deshalb den Oberstadtdirektor der betreffenden Stadt gebeten, die gewünschte Auskunft zu erteilen. Er hat mir inzwischen mitgeteilt, daß er der von mir vertretenen Rechtsauffassung folge und der Antragstellerin die gewünschten Auskünfte erteilen werde.

7. Kommunalwesen

Im kommunalen Bereich betrafen mehrere Beratungsersuchen und Eingaben wiederum die Weitergabe von Jubiläumsdaten, und zwar an Ratsfraktionen, Kreisverwaltungen, Bürgermeister und Ortsvorsteher.

Soweit Jubiläumsdaten von der Verwaltung an Ratsfraktionen weitergegeben werden, halte ich dies nach wie vor für unzulässig (vgl. C. 4. meines ersten Tätigkeitsberichts). Diese Datenübermittlung ist nach dem Datenschutzgesetz Nordrhein-Westfalen zu beurteilen. Dessen Vorschriften werden insbesondere nicht durch § 3 Abs. 1 des ADV-Organisationsgesetzes (ADVG NW) verdrängt. Nach § 3 Abs. 1 ADVG NW können die Fraktionen der kommunalen Vertretungsorgane von dem Hauptverwaltungsbeamten im Rahmen ihrer Aufgaben Auskünfte auf Grund der gespeicherten Daten verlangen. Der Datenschutzgesichtspunkt wurde bei der Schaffung dieser Bestimmung bewußt ausgeklammert. Diese Vorschrift kann daher auch nicht als eine „andere Rechtsvorschrift" im Sinne von § 3 Satz 1 Nr. 1 DSG NW angesehen werden.

Nicht zu beanstanden war die Weitergabe von Jubiläumsdaten an eine Kreisverwaltung. Es kann davon ausgegangen werden, daß es auch zu den Aufgaben eines Kreises — etwa im Rahmen der Öffentlichkeitsarbeit — gehört, Bürgern aus kreisbezogenen Anlässen zu bestimmten Jubiläen zu gratulieren.

Gegen die Weitergabe von Listen mit den Namen aller über 75 Jahre alten Bürger einer Stadt an den Bürgermeister zur Ehrung des ältesten Teilnehmers auf einem Seniorenfest oder einer ähnlichen Veranstaltung habe ich Bedenken geäußert.

Zwar dürfte es zu den Aufgaben einer Gemeinde gehören, den ältesten Teilnehmer auf einem Seniorenfest durch den Bürgermeister zu ehren. Diese Ehrung muß jedoch rechtmäßig sein, darf also nicht gegen Datenschutzvorschriften verstoßen.

Mit der Ehrung im Rahmen derartiger Veranstaltungen ist eine Bekanntgabe personenbezogener Daten (zumindest des Namens und des Alters des Betroffenen) an Dritte verbunden. Die Bekanntgabe stellt damit eine Übermittlung personenbezogener Daten an Personen außerhalb des öffentlichen Bereichs im Sinne des § 13 Abs. 1 Satz 1 DSG NW dar.

Bei der nach § 13 Abs. 1 Satz 1 DSG NW erforderlichen Interessenabwägung überwiegt das Interesse des Betroffenen am Schutz seiner Privatsphäre gegenüber dem Interesse der Teilnehmer von Senioren- oder Altenfesten an der Kenntnis dieser Daten. Die mit der Ehrung auf Senioren- oder Altenfesten verbundene Bekanntgabe personenbezogener Daten durch den Bürgermeister bedarf daher der Einwilligung des Betroffenen.

Nach § 3 Satz 2 DSG NW ist die Einwilligung im Regelfall schriftlich zu erteilen. Dies dürfte allerdings bei der Ehrung der ältesten Teilnehmer an einer solchen Veranstaltung nicht praktikabel sein, weil vor einer Veranstaltung noch nicht feststeht, wer an ihr teilnimmt. Die besonderen Umstände lassen deshalb eine andere Form der Einwilligung angemessen erscheinen. Als datenschutzkonforme und zugleich zweckmäßige Lösung bietet es sich an, die ältesten Teilnehmer an der Veranstaltung aus dem Kreis der Anwesenden zu ermitteln, indem gefragt wird, ob jemand einem bestimmten Jahrgang angehört und — bei mehreren Meldungen — in welchem Monat er geboren ist. Bei diesem Verfahren würde das Alter des Betroffenen nicht vom Bürgermeister, sondern von dem Betroffenen selbst den Anwesenden bekanntgegeben werden. Auch wäre die Weitergabe der Daten der ältesten eingeladenen Personen durch die Verwaltung an den Bürgermeister entbehrlich.

Da die Befragung eine Datenerhebung bei dem Betroffenen ist, muß auf die Freiwilligkeit der Meldung hingewiesen werden (§ 10 Abs. 2 Satz 1 DSG NW). Wer sein Alter nicht bekanntgeben will, kann auf die Meldung verzichten.

In einer Gemeinde war es bis zum Inkrafttreten des Datenschutzgesetzes Nordrhein-Westfalen üblich, daß bei der Ehrung von Altersjubilaren sowohl der Bürgermeister als auch der jeweilige Ortsvorsteher gemeinsam die Glückwünsche der Gemeinde überbrachten. Nach Inkrafttreten des Datenschutzgesetzes werden die Ortsvorsteher unter Berufung auf datenschutzrechtliche Bestimmungen von der Teilnahme an derartigen Ehrungen ausgeschlossen.

Sofern der Bürgermeister wegen der großen Zahl der in Betracht kommenden Personen oder aus anderen Gründen daran gehindert ist, die Glückwünsche selbst zu übermitteln, ist es datenschutzrechtlich unbedenklich, wenn er sich hierbei vertreten läßt. Dies kann auch durch den zuständigen Ortsvorsteher geschehen.

Übermittelt der Bürgermeister die Glückwünsche selbst, so kann er sich von dem zuständigen Ortsvorsteher begleiten lassen, sofern dies in der Gemeinde zu den Aufgaben eines Ortsvorstehers gehört. Auch in diesem Fall bestehen keine datenschutzrechtlichen Bedenken dagegen, daß der Ortsvorsteher hierbei Kenntnis von den Jubiläumsdaten erhält.

Eine Gemeinde bat mich um datenschutzrechtliche Prüfung der Zulässigkeit der Übermittlung von Namen und Anschriften aller 70-jährigen und älteren Bürger und aller bis zu 14 Jahre alten Kinder an die Ortsvorsteher zur Durchführung von Altenfesten und Sankt-Martins-Veranstaltungen.

Soweit in einer Gemeinde den Ortsvorstehern die Durchführung von Altenfesten und Sankt-Martins-Veranstaltungen zulässigerweise übertragen worden ist, bestehen keine datenschutzrechtlichen Bedenken gegen die Weitergabe dieser Daten an den Ortsvorsteher.

a) KpS-Richtlinien und Dateienrichtlinien

Die Innenminister/-senatoren haben einen neuen Musterentwurf für Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien) sowie den Entwurf der Richtlinien für die Errichtung und Führung von Dateien beim Bundeskriminalamt (Dateienrichtlinien) gebilligt. Sie haben in Aussicht genommen, beide Richtlinien zu überarbeiten, sobald ausreichende Erfahrungen mit ihnen vorliegen. In Nordrhein-Westfalen sind die neuen KpS-Richtlinien durch Runderlaß des Innenministers vom 10. Februar 1981 (MBl. NW. S. 192) bereits in Kraft gesetzt worden; sie sind an die Stelle der bisher in Nordrhein-Westfalen geltenden KpS-Richtlinien getreten.

Zu den KpS-Richtlinien hatten die Datenschutzbeauftragten des Bundes und der Länder einen eigenen Musterentwurf erarbeitet. Diesen hatte ich dem Innenminister zugeleitet. Auch zu dem Entwurf der Dateienrichtlinien hatte ich Stellung genommen.

Die Datenschutzbeauftragten des Bundes und der Länder haben vor der Verabschiedung der beiden Entwürfe durch die Innenminister/-senatoren festgestellt, daß einige ihrer Vorschläge übernommen worden sind und in anderen Punkten ein aus der Sicht des Datenschutzes akzeptabler Kompromiß gefunden wurde. Sie haben insbesondere die Regelung für die Auskunft an den Betroffenen über die zu seiner Person gespeicherten Daten begrüßt. Diese stellt klar, daß Auskunft erteilt wird, es sei denn, daß die Belange des Bürgers hinter dem öffentlichen Interesse an der Nichtherausgabe der jeweiligen Daten zurücktreten müssen.

Gleichwohl halten die Datenschutzbeauftragten in mehreren Punkten Änderungen der Entwürfe für geboten. So muß nach ihrer Auffassung in den Dateienrichtlinien klargestellt werden, daß bei den Verbunddateien, aber auch bei den Zentraldateien die anliefernde Stelle die Verantwortung für die Rechtmäßigkeit der Speicherung im Einzelfall trägt. Die Datenschutzbeauftragten halten ferner an ihrer Auffassung fest, daß im Bereich der Polizei eine Speicherung nur zur Erfüllung von Aufgaben erfolgen darf, die durch Rechtsnorm zugewiesen sind. Im übrigen darf nach ihrer Auffassung auch innerhalb der Polizei ein unmittelbarer Abruf personenbezogener Daten aus automatisiert geführten Dateien nur unter Berücksichtigung der jeweiligen Aufgabenstellung zugelassen werden.

Es ist zu hoffen, daß die Änderungsvorschläge der Datenschutzbeauftragten bei der von den Innenministern/-senatoren in Aussicht genommenen Überarbeitung der Richtlinien Berücksichtigung finden werden.

b) Neukonzeption des INPOL-Systems und Kriminalaktennachweis (KAN)

Der Arbeitskreis II der Innenministerkonferenz hat die überarbeitete Fassung des Konzepts für die Fortentwicklung des polizeilichen Informationssystems INPOL und des Konzepts für Aufbau und Führung des Kriminalaktennachweises (KAN) vorgelegt.

Der KAN wird nach diesem Konzept als Teil des polizeilichen Informationssystems INPOL beim Bundeskriminalamt geführt. Er ist ein Verzeichnis von Kriminalakten, die beim Bund und bei den Ländern nach den KpS-Richtlinien in Fällen schwerer oder überregional bedeutsamer Straftaten über Beschuldigte oder sonst tatverdächtige Personen angelegt sind. Durch ihn soll insbesondere erreicht werden, daß überregionale Straftäter erkannt und wirkungsvoller bekämpft werden können. Hinweise auf Akten über Straftaten von ausschließlich regionaler Bedeutung sollen in den KAN nicht aufgenommen werden. Den Ländern bleibt es überlassen, insoweit einen eigenen Aktennachweis zu führen.

Das vom Arbeitskreis II überarbeitete KAN-Konzept, in das die Vorschläge der Datenschutzbeauftragten des Bundes und der Länder Eingang gefunden haben, stellt aus der Sicht des Datenschutzes eine erhebliche Verbesserung gegenüber der ursprünglichen Fassung dar. Insbesondere sind die Forderungen der Datenschutzbeauftragten nach

Eingrenzung des Datenumfanges und der Beschränkung auf Aktenhinweise über Straftaten von ausschließlich überregionaler Bedeutung berücksichtigt worden. Auch ist zu begrüßen, daß nach dem Konzept Auskünfte aus dem KAN nur an mit der Bearbeitung von Ermittlungsvorgängen befaßte Polizeidienststellen erteilt werden sollen.

Wenngleich gegen das jetzt vorliegende Konzept nach dem derzeitigen Erkenntnisstand keine Bedenken bestehen, wird aber darauf zu achten sein, daß die vorgesehenen Beschränkungen nicht durch die Ausweitung anderer Konzeptionen unterlaufen werden.

c) Jugendschutzdatei (ZJD)

Die Zentrale Jugendschutzdatei (ZJD) wurde durch Runderlaß des Innenministers des Landes Nordrhein-Westfalen vom 3. Februar 1978 (MBl. NW. 1978 S. 228) eingerichtet. Nach diesem Erlaß werden in der ZJD Hinweise auf bei den Polizeibehörden vorhandene Unterlagen über tatverdächtige strafunmündige Minderjährige (bis zur Vollendung des 14. Lebensjahres) und gefährdete Minderjährige (bis zur Vollendung des 18. Lebensjahres) gespeichert. Gefährdete Minderjährige sind insbesondere Selbstmord-, Drogen- und Alkoholgefährdete sowie Vermißte im weitesten Sinne.

Die tatverdächtigen strafunmündigen Minderjährigen und die gefährdeten Minderjährigen werden dem Landeskriminalamt Nordrhein-Westfalen mittels eines Personalbogens von den zuständigen Polizeibehörden benannt. Der untere Teil des Personalbogens enthält Sozial- und Gefährdungsdaten, die der Ursachenforschung und der Kriminalstatistik dienen. Er wird getrennt vom Personalteil übersandt, so daß eine namensmäßige Zuordnung ausgeschlossen ist.

Für die Führung, Einsichtnahme und Auswertung der ZJD, nicht aber für die Aussonderung, gelten die Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien) entsprechend. Der Runderlaß des Innenministers vom 3. Februar 1978 sieht vor, daß die Unterlagen über tatverdächtige Kinder mit Erreichen des 14. Lebensjahres, über gefährdete Minderjährige mit Erreichen des 18. Lebensjahres ausgesondert und vernichtet werden, es sei denn, es liegen Anhaltspunkte dafür vor, daß der Betroffene weiterhin polizeilich in Erscheinung treten wird. In diesem Fall wird der Hinweis in die Zentrale Auskunftsdatei des automatisierten Informationssystems der Polizei übernommen; die vorhandenen Unterlagen gehen in die Kriminalakte ein.

Nr. 5.2.3 der KpS-Richtlinien (n. F.) bestimmt, daß bei Kindern nach 2 Jahren, bei Jugendlichen nach 5 Jahren zu prüfen ist, ob eine Aussonderung der Unterlagen möglich ist. Auf meine Veranlassung ist klargestellt worden, daß für die Aussonderung jeweils der für den Betroffenen günstigere Termin (Erreichen der Altersgrenze oder Ablauf der genannten Frist) gilt.

d) Häftlingsüberwachung

Personen, die Kontakt zu Strafgefangenen aufnehmen, die der Häftlingsüberwachung unterliegen, werden von der Justizvollzugsanstalt dem Landeskriminalamt Nordrhein-Westfalen gemeldet. Verstöße gegen Vorschriften über den Datenschutz habe ich hierbei nicht feststellen können.

Die Übermittlung und Speicherung dieser Daten ist zur Erfüllung von Aufgaben der Gefahrenabwehr, insbesondere zur vorbeugenden Verbrechensbekämpfung erforderlich. Rechtsgrundlage war bis Juni 1980 § 20 Abs. 1 Satz 1 des alten Polizeigesetzes und ist seitdem § 8 Abs. 1 des neuen Polizeigesetzes für das Land Nordrhein-Westfalen (PolG NW), jeweils in Verbindung mit § 34 des Strafvollzugsgesetzes (StVollzG). Nach § 8 Abs. 1 PolG NW kann die Polizei die notwendigen Maßnahmen treffen, um eine im einzelnen Falle bestehende Gefahr für die öffentliche Sicherheit oder Ordnung abzuwehren, soweit nicht andere Vorschriften die Befugnisse der Polizei besonders regeln. Nach § 34 Abs. 1 Nr. 1 StVollzG dürfen Kenntnisse aus der Überwachung der Besuche oder des Schriftwechsels verwertet werden, soweit dies notwendig ist, um Straftaten zu verhüten, zu

unterbinden oder zu verfolgen. Nach § 34 Abs. 2 StVollzG dürfen diese Kenntnisse den Behörden mitgeteilt werden, die hierfür zuständig sind.

e) Örtliche Ausschreibung zur polizeilichen Beobachtung

Eine Polizeibehörde hatte zum Zwecke einer effektiveren Kriminalitätsbekämpfung und zur Verbesserung des Informationsaustausches zwischen der Schutzpolizei und den Fachkommissariaten der Kriminalpolizei zu Beginn des Jahres 1980 eine auf ihren Bereich begrenzte Ausschreibung von Intensivtätern veranlaßt. Diese erfolgte auf Grund kriminalpolizeilicher Erkenntnisse über früher verübte Straftaten dieser Personen. Die Ausschreibung hatte zur Folge, daß im Falle einer — zufälligen — Überprüfung eines Betroffenen durch einen Polizeibeamten die Polizeibehörde hiervon eine Meldung erhielt.

Es handelte sich um ein zeitlich beschränktes, auf den Bereich dieser Polizeibehörde begrenztes Testprogramm, das nicht fortgeführt wurde. Meine Ermittlungen haben ergeben, daß alle in diesem Zusammenhang gespeicherten personenbezogenen Daten bereits vor meinem Auskunftsersuchen wegen rechtlicher Bedenken gelöscht worden sind.

f) Angaben über Homosexualität

In mehreren Eingaben wurde angefragt, ob bei der Polizei eine „Homosexuellen-Kartei" geführt werde.

§ 10 Abs. 1 des Datenschutzgesetzes Nordrhein-Westfalen läßt das Speichern personenbezogener Daten in einer Datei nur zu, wenn es zur rechtmäßigen Erfüllung der Aufgaben der speichernden Stelle erforderlich ist. Eine Aufgabe, zu deren rechtmäßiger Erfüllung eine „Homosexuellen-Kartei" erforderlich sein könnte, kann ich mir nicht vorstellen. Das Führen einer derartigen Kartei wäre somit bereits wegen Fehlens einer gesetzlichen Grundlage unzulässig.

Nach meinen Feststellungen werden weder beim Landeskriminalamt Nordrhein-Westfalen noch bei den anderen Polizeibehörden des Landes Angaben über abweichendes Sexualverhalten in Dateien gespeichert oder in sonstigen Sammlungen festgehalten. Eine Ausnahme gilt für abweichendes Sexualverhalten von Beschuldigten, soweit es im Zusammenhang mit einer strafbaren Handlung von Bedeutung ist. Hier kommen insbesondere Handlungen nach §§ 174 bis 184 b StGB, Beischlafdiebstahl, Erpressung auf sexueller Grundlage, Beraubung homosexueller Personen und Tötungshandlungen auf Grund sexueller Motive in Betracht. In diesen Fällen werden entsprechende Angaben gespeichert oder in Einzelakten festgehalten. Diese Unterlagen werden nach den KpS-Richtlinien ausgesondert. Die ausgesonderten Unterlagen werden vernichtet. Die auf elektronischen Datenträgern gespeicherten Daten werden physikalisch vernichtet.

Für die Aussonderung und Vernichtung von Altakten, die Angaben über strafbares abweichendes Sexualverhalten vor der Rechtsänderung enthalten, gelten ebenfalls die genannten Richtlinien. Nach Auskunft des Landeskriminalamtes hat eine generelle Bereinigung noch nicht stattgefunden. Sie ist nach Auffassung der Polizeibehörden wegen des Umfangs des zu überprüfenden Aktenbestandes mit dem vorhandenen Personal nicht möglich. Die Überprüfung der Akten, die im Zuge der laufenden Sachbearbeitung erfolgt, führt in der Regel zur Aussonderung und Vernichtung. Einige wenige Einzelfälle werden weiterhin ausgewertet, wenn dies zur Verfolgung einschlägiger Straftaten des geltenden Rechts erforderlich ist. Eine Übermittlung der in diesen Akten enthaltenen Angaben findet nur unter dieser Voraussetzung statt. Im übrigen sind die Kriminalpolizeilichen personenbezogenen Sammlungen vertraulich.

g) Datengeheimnis und Datensicherung

Im Bereich der Polizei werden in großem Umfang besonders sensible personenbezogene Daten verarbeitet. Gerade hier kann eine Zweckentfremdung der Daten für den Betroffenen besonders einschneidende nachteilige Folgen haben.

Deshalb ist ein Mitarbeiter einer Polizeibehörde, der unbefugt personenbezogene Daten eines Dritten im automatisierten Informationssystem der Polizei abgerufen und genutzt hat, von dem Behördenleiter scharf gemaßregelt worden. Nur die besonderen Umstände des Falles und die persönlichen Verhältnisse dieses Mitarbeiters und des Betroffenen haben mich davon Abstand nehmen lassen, von meinem Strafantragsrecht nach § 33 Abs. 3 DSG NW Gebrauch zu machen.

In einem anderen Fall war Schriftgut einer Polizeibehörde in die Hände Dritter gelangt. Es bestand der Verdacht, daß dieses über einen jedermann zugänglichen Müllcontainer nach draußen gelangt war.

Meine Ermittlungen ergaben, daß das Altpapier, das personenbezogene Daten enthielt, im Bereich dieser Polizeibehörde wie folgt behandelt wurde: Das Papier wurde von den Bediensteten zerrissen und in den Papierkorb geworfen. Der Reinigungsdienst sortierte den Inhalt der Papierkörbe, um Schriftgutabfall von dem übrigen Abfall zu trennen. Das aussortierte Altpapier wurde vom Reinigungsdienst in Plastiksäcken gesammelt und in verschlossenen Abstellräumen aufbewahrt. Die Plastiksäcke wurden von Zeit zu Zeit von Altpapierfirmen, mit denen vertragliche Regelungen bestanden, abgeholt und samt Inhalt vernichtet.

Ich habe dieses Verfahren als unzureichend bezeichnet und empfohlen, das Sammeln des Altpapiers, das personenbezogene Daten enthält, nicht dem Reinigungsdienst zu überlassen, sondern jeweils von denjenigen Bediensteten durchführen zu lassen, die mit den personenbezogenen Daten arbeiten. Ferner sollte die Vernichtung des gesammelten Altpapiers, das personenbezogene Daten enthält, nicht von privaten Altpapierfirmen vorgenommen werden. Es sollte vielmehr mit Hilfe eines Reißwolfes vernichtet werden, bevor die nicht mehr lesbaren Reste an Altpapierfirmen abgegeben werden.

Der Behördenleiter hat mir mitgeteilt, daß er die Bediensteten seiner Behörde angewiesen habe, die Vernichtung des Altpapiers entsprechend meinem Vorschlag durchzuführen. Zu diesem Zweck seien weitere Aktenvernichter angeschafft worden.

h) Auskunft an den Betroffenen

Auch in diesem Berichtsjahr wollten zahlreiche Bürger wissen, ob und in welchem Umfang personenbezogene Daten über sie bei der Polizei gespeichert sind.

§ 16 Abs. 1 Satz 1 DSG NW gibt dem Betroffenen das Recht, von den Behörden des Landes Nordrhein-Westfalen Auskunft über die zu seiner Person in einer Datei gespeicherten Daten zu verlangen. Nach § 16 Abs. 2 in Verbindung mit § 15 Abs. 2 Nr. 1 DSG NW gilt dies allerdings nicht für die Behörden der Polizei. Diese haben ein Auskunftsverweigerungsrecht.

Das Auskunftsverweigerungsrecht bedeutet nicht, daß die genannten Behörden keine Auskunft erteilen dürfen. Sie haben vielmehr nach pflichtgemäßem Ermessen zu entscheiden, ob sie dem Auskunftersuchen eines Betroffenen entsprechen wollen.

Bei der Entscheidung muß zunächst festgestellt werden, ob im konkreten Fall, bezogen auf die einzelnen Unterlagen über den Betroffenen, überhaupt ein öffentliches Interesse an der Geheimhaltung besteht. Von einem solchen Geheimhaltungsinteresse kann nur ausgegangen werden, wenn die Auskunfterteilung die Arbeit der Polizei erheblich erschweren oder ihre Wirksamkeit in Frage stellen würde.

Sodann ist dieses Geheimhaltungsinteresse gegen das Auskunftsinteresse des Betroffenen abzuwägen. Dabei kann es von Bedeutung sein, ob der Antragsteller über das allgemeine Auskunftsinteresse eines jeden Betroffenen hinaus Umstände dargelegt hat, die ein besonderes Auskunftsinteresse des Antragstellers erkennen lassen.

Wenn eine speichernde Stelle dem Betroffenen die Auskunft darüber verweigert, ob und gegebenenfalls welche Daten zu seiner Person gespeichert sind, so hat er nach § 29 DSG NW das Recht, sich an den Landesbeauftragten für den Datenschutz zu wenden.

Dieser hat die Berechtigung der Auskunftsverweigerung zu überprüfen und gegebenenfalls darauf hinzuwirken, daß die gewünschte Auskunft erteilt wird.

Das den Behörden der Polizei zustehende Auskunftsverweigerungsrecht darf allerdings auch der Landesbeauftragte für den Datenschutz nicht durch Mitteilungen der ihm bei seiner Prüfung zugänglich gemachten Erkenntnisse an den Betroffenen umgehen. Hält die speichernde Stelle an der Auskunftsverweigerung fest, so kann auch ich keine Auskunft erteilen.

In mehreren Fällen war wiederum meiner Einschaltung eine vergebliche Anfrage des Betroffenen bei der Polizei vorausgegangen. Diese hatte die Auskunft unter Berufung auf ihr Auskunftsverweigerungsrecht abgelehnt. Unter Hinweis auf Nr. 6 Satz 1 der Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen (a. F.) habe ich die Polizeibehörden gebeten, ihre Entscheidung noch einmal zu überprüfen.

In der Mehrzahl der Fälle haben daraufhin die Polizeibehörden dem Betroffenen die gewünschte Auskunft gegeben oder sie waren damit einverstanden, daß ich diese Auskunft erteilte. Dies gilt auch für die Auskunft, daß keine Daten zur Person des Betroffenen gespeichert sind. Nur in wenigen Fällen mußte ich mich dem Betroffenen gegenüber auf die Mitteilung beschränken, daß ich keine Verstöße gegen Vorschriften über den Datenschutz festgestellt habe.

Diese datenschutzfreundliche Auskunftspraxis hat sich nicht zuletzt auch auf Grund zahlreicher Gespräche mit Vertretern des Innenministeriums, dem Landeskriminalamt und den Polizeibehörden „vor Ort" eingespielt. Ich gehe davon aus, daß sie sich — zumal nach Inkrafttreten der neuen KpS-Richtlinien — bei allen Polizeibehörden auch ohne Einschaltung des Landesbeauftragten für den Datenschutz durchsetzen wird.

i) Löschung

In einigen Fällen habe ich unter Hinweis auf § 17 Abs. 3 DSG NW und die KpS-Richtlinien bei den Polizeibehörden angefragt, wann mit einer Löschung der gespeicherten oder festgehaltenen Daten zu rechnen sei. Mehrfach konnte ich den Betroffenen mitteilen, daß auf meine Veranlassung die über sie geführten Kriminalpolizeilichen Sammlungen ausgesondert und vernichtet und die entsprechenden Hinweise im automatisierten Informationssystem der Polizei gelöscht worden sind.

In einigen Fällen sahen sich die Polizeibehörden allerdings zu einer Vernichtung der Unterlagen und einer Löschung der dazu im automatisierten Informationssystem der Polizei gespeicherten personenbezogenen Daten nicht in der Lage. Verstöße gegen Vorschriften über den Datenschutz habe ich hierbei nicht feststellen können. Bei der Prüfung war auch zu berücksichtigen, daß den Polizeibehörden nach den Vorschriften über die vorzeitige Aussonderung ein Beurteilungsspielraum verbleibt. Ich habe mich in diesen Fällen dafür eingesetzt, daß die Polizeibehörde nach angemessener Frist erneut prüft, ob die Unterlagen vorzeitig, d. h. vor Ablauf der in den KpS-Richtlinien festgelegten Regelfristen, vernichtet werden können.

k) Sonstige Eingaben von Bürgern

Auf eine Eingabe hatte ich die Rechtmäßigkeit des Festhaltens personenbezogener Daten, die bei einer Feststellung der Identität einer Person in ein **Streifenbuch** aufgenommen worden waren, zu überprüfen.

Zwar läßt § 9 Abs. 1 PolG NW die Feststellung der Identität einer Person unter bestimmten Voraussetzungen zu. Dies rechtfertigt jedoch nicht, die dabei erhobenen personenbezogenen Daten länger festzuhalten, als es der Zweck der Identitätsfeststellung erfordert. Auch als Tätigkeitsvermerk zu einem innerbetrieblichen Nachweis ist das Festhalten der Personalien des Betroffenen nicht zu rechtfertigen. Für diesen Zweck genügt eine Notiz in anonymisierter Form. Das Festhalten personenbezogener Daten ist hierfür nicht erforderlich.

Für vertretbar halte ich allenfalls, die Personalien im Streifenbuch für begrenzte Zeit festzuhalten, um eine nachträgliche Überprüfung der Rechtmäßigkeit des Eingriffs zu ermöglichen. Dabei gehe ich von der Erwägung aus, daß die Unmöglichkeit einer solchen Überprüfung den Betroffenen stärker belasten kann als das Festhalten seiner Personalien für eine begrenzte Zeit. Als angemessene Frist können in Anlehnung an die Strafantragsfrist nach § 77b StGB drei Monate angesehen werden. Spätestens nach Ablauf dieser Frist sind die festgehaltenen Daten zu löschen.

Das Datenschutzgesetz Nordrhein-Westfalen findet im vorliegenden Fall keine Anwendung, da das Streifenbuch, in dem die Personalien der überprüften Person festgehalten werden, mangels Umordnungsmöglichkeit keine Datei ist (§ 1 Abs. 2 Satz 1 in Verbindung mit § 2 Abs. 3 Nr. 3 DSG NW). Der Anspruch auf Löschung der Daten ergibt sich unmittelbar aus Artikel 4 Abs. 2 der Landesverfassung. Da die Aktenordnung der Polizei eine von dieser Forderung abweichende Regelung enthält, hat die von mir angeschriebene Polizeibehörde die Frage nach der Löschungsfrist dem Innenminister vorgelegt. Von dort ist in Kürze eine allgemeine Regelung zu erwarten.

Durch die Eingabe eines Bürgers erhielt ich Kenntnis von folgendem Vorfall: Eine Polizeibehörde hatte die Daten mehrerer Fahrzeughalter beim Kraftfahrt-Bundesamt angefordert und nach deren Übermittlung ausgewertet, um Namen und Anschrift eines Bürgers für eine andere Person festzustellen, die diese Daten für einen privaten Zweck nutzen wollte.

Die **Datenübermittlung vom Kraftfahrt-Bundesamt an die Polizeibehörde** war nicht zulässig, da sie zur rechtmäßigen Erfüllung der Aufgaben der Polizeibehörde nicht erforderlich war (§ 10 Abs. 1 Satz 1 BDSG) und auch keine Einwilligung der betroffenen Fahrzeughalter vorlag (§ 3 Satz 1 Nr. 2 BDSG). Die Verantwortung dafür, daß die Kenntnis der zu übermittelnden Daten zur rechtmäßigen Erfüllung der Aufgaben des Empfängers erforderlich ist, liegt in erster Linie bei dem Empfänger, hier also bei der Polizeibehörde. Darüber hinaus verstieß das Anfordern und Auswerten der übermittelten Daten durch die Polizeibehörde für einen privaten Zweck mangels einer gesetzlichen Grundlage gegen Artikel 4 Abs. 2 der Landesverfassung.

Ich habe die Polizeibehörde auf die Rechtslage hingewiesen und sie gebeten, künftig derartigen Ersuchen nur dann nachzukommen, wenn dies ohne Verstoß gegen Vorschriften über den Datenschutz möglich ist. Von einer Beanstandung nach § 30 DSG NW habe ich wegen der besonderen Umstände des Falles abgesehen.

9. Verfassungsschutz

Die Mitte des Jahres 1980 in Kraft getretene Neufassung der Dienstanweisung für die Auswertung der Verfassungsschutzabteilung des Innenministeriums des Landes Nordrhein-Westfalen enthält unter anderem Regelungen über die Verarbeitung personenbezogener Daten im Nachrichtendienstlichen Informationssystem (NADIS) und in der Kartei einschließlich der Löschung dieser Daten. Zusammen mit den Richtlinien für die Löschung von personenbezogenen Daten der Verfassungsschutzbehörden im Nachrichtendienstlichen Informationssystem (NADIS) aus dem Jahre 1979, nach denen auch im Lande Nordrhein-Westfalen gearbeitet wird, stellt diese Dienstanweisung eine deutliche Verbesserung des Datenschutzes in diesem Bereich dar. Gleichwohl werden die Datenschutzbeauftragten des Bundes und der Länder zu prüfen haben, ob weitere Verbesserungen möglich sind.

Mehrere Eingaben betrafen den Verfassungsschutz. In den meisten Fällen war zu prüfen, ob und gegebenenfalls welche personenbezogenen Daten beim Verfassungsschutz festgehalten oder von ihm übermittelt worden sind. Die erforderlichen Prüfungen habe ich in den Diensträumen der Verfassungsschutzabteilung des Innenministeriums durchge-

führt und dabei keine Hinweise auf Verstöße gegen Vorschriften über den Datenschutz festgestellt.

Für die Verfassungsschutzbehörde besteht weder eine Veröffentlichungspflicht über gespeicherte personenbezogene Daten (§ 15 Abs. 2 Nr. 1 DSG NW), noch eine Auskunftspflicht gegenüber dem Betroffenen (§ 16 Abs. 2 DSG NW). Der Landesbeauftragte für den Datenschutz kann die Einhaltung der Datenschutzvorschriften bei dieser Behörde zwar ohne Einschränkung kontrollieren. Er darf jedoch das Auskunftsverweigerungsrecht dieser Behörde nicht durch Mitteilung über die ihm bei seiner Prüfung zugänglich gemachten Erkenntnisse umgehen. Allerdings enthält § 16 Abs. 2 in Verbindung mit § 15 Abs. 2 Nr. 1 DSG NW nur eine Ermächtigung, nicht aber eine Verpflichtung zur Auskunftsverweigerung. In vielen Fällen ist es mir gelungen, die Verfassungsschutzbehörde zu einer Auskunftspraxis zu veranlassen, die auch den Belangen der Betroffenen Rechnung trägt.

In mehreren Eingaben wurde nach der Existenz einer „Homosexuellen-Kartei" beim Verfassungsschutz gefragt. Nach meinen Feststellungen werden bei der Verfassungsschutzabteilung des Innenministeriums des Landes Nordrhein-Westfalen Erkenntnisse über einfache Homosexualität weder in automatisierten Dateien noch in Karteien gespeichert. Eine generelle Bereinigung der Altakten hat auch hier noch nicht stattgefunden. Die in diesen festgehaltenen Daten über abweichendes Sexualverhalten, die zur rechtmäßigen Erfüllung der Aufgaben des Verfassungsschutzes nicht mehr erforderlich sind, werden im Zuge der laufenden Bearbeitung gelöscht.

Die Landesregierung hat den Entwurf eines Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen eingebracht, der auch bereichspezifische Datenschutzregelungen vorsieht (Drucksache 9/430). Ich werde hierzu Stellung nehmen.

10. Bauwesen

Auf Anfrage einer Gemeinde habe ich geprüft, ob die Übermittlung von Namen und Anschriften der Bauherren, die dort während einer bestimmten Zeit gebaut haben, an einen Studenten zur Durchführung einer Befragung zulässig ist.

Die Übermittlung der Anschriften der Bauherren richtet sich nach § 13 Abs. 1 Satz 1 DSG NW. Ein berechtigtes Interesse des Studenten an der Kenntnis der Daten dürfte zwar vorliegen. Zumindest ein Teil der Betroffenen würde jedoch die Befragung als Belästigung empfinden. Bei einer Abwägung der Interessen überwiegt in diesen Fällen das Interesse der Betroffenen an dem Schutz ihrer Privatsphäre.

Gegen die Handhabung einer Gemeinde, zu dem Bauleitplan nach § 2a Abs. 6 des Bundesbaugesetzes (BBauG) auch ein Eigentümerverzeichnis zu jedermanns Einsicht öffentlich auszulegen, habe ich datenschutzrechtliche Bedenken geäußert.

§ 2a Abs. 6 Satz 1 BBauG erlaubt nur die Auslegung des Entwurfes der Bauleitpläne mit dem Erläuterungsbericht oder der Begründung. Die öffentliche Auslegung eines Eigentümerverzeichnisses ist nicht vorgesehen. Eine andere Rechtsvorschrift, die als gesetzliche Grundlage für die öffentliche Auslegung eines solchen Verzeichnisses in Betracht käme und die nach Artikel 31 des Grundgesetzes oder nach § 37 DSG NW den Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen vorgehen würde, ist nicht ersichtlich. Die Zulässigkeit der Übermittlung dieser Daten durch die Auslegung des Eigentümerverzeichnisses ist daher nach § 13 Abs. 1 Satz 1 DSG NW zu beurteilen.

Es ist nicht ersichtlich, daß die Auslegung des Eigentümerverzeichnisses zur rechtmäßigen Aufgabenerfüllung des Bauverwaltungsamtes erforderlich ist. Eine Übermittlung nach der ersten Alternative des § 13 Abs. 1 Satz 1 DSG NW kommt daher nicht in Betracht.

Ein berechtigtes Interesse derjenigen, die ein Eigentümerverzeichnis einsehen wollen, dürfte zwar vorliegen. Durch die Bekanntgabe solcher Daten können jedoch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Zwar mögen einige Grundstückseigentümer damit einverstanden sein, daß ihr Name bekannt wird; andere hingegen möchten dies auf keinen Fall. Bei der Abwägung der Interessen überwiegt in der Regel das Interesse des Betroffenen an dem Schutz seiner Daten. Deshalb scheidet auch eine Übermittlung nach der zweiten Alternative des § 13 Abs. 1 Satz 1 DSG NW aus.

Ich habe empfohlen, zur Vermeidung von Verstößen gegen Vorschriften über den Datenschutz künftig von einer Auslegung des Eigentümerverzeichnisses abzusehen. Die Gemeinde hat mir mitgeteilt, daß sie meiner Empfehlung folgen werde.

11. Rechtswesen

a) Strafsachen

In meinem ersten Tätigkeitsbericht (C. 8. a) habe ich dargelegt, daß nach § 26 Abs. 1 Satz 1 DSG NW die Behörden der **Staatsanwaltschaft** ohne Einschränkung der Kontrolle des Landesbeauftragten für den Datenschutz unterliegen, da nach § 32 Abs. 1 Nr. 1 DSG NW lediglich die Gerichte, soweit sie nicht Verwaltungsaufgaben wahrnehmen, von seiner Kontrolle ausgenommen sind. Ob die Behörden der Staatsanwaltschaft Verwaltungsaufgaben erledigen oder als Organe der Rechtspflege tätig werden, ist nach meiner Auffassung nur für die Frage von Bedeutung, ob die materiellen Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen oder die des Bundesdatenschutzgesetzes anzuwenden sind (§ 1 Abs. 2 Satz 2 DSG NW, § 7 Abs. 2 Satz 1 Nr. 2 BDSG).

Die Landesregierung ist in ihrer Stellungnahme zu meinem ersten Tätigkeitsbericht (S. 4) dieser Auffassung entgegengetreten. Sie ist der Ansicht, daß die Kontrollbefugnis des Landesbeauftragten gegenüber den Behörden der Staatsanwaltschaft auf den Anwendungsbereich der materiellen Regelungen des Datenschutzgesetzes Nordrhein-Westfalen beschränkt sei. Danach unterlägen die Behörden der Staatsanwaltschaft der Kontrolle des Landesbeauftragten nur insoweit, als sie Verwaltungsaufgaben wahrnähmen (§ 1 Abs. 2 Satz 2 DSG NW). § 32 DSG NW habe keinen eigenständigen Regelungsgehalt.

Dieser einschränkenden Auslegung des § 26 Abs. 1 Satz 1 DSG NW durch die Landesregierung kann ich mich nicht anschließen. Sie findet weder in dem Wortlaut der Vorschrift, noch in dem Zusammenhang der Regelungen des Gesetzes, noch in deren Zweck eine Stütze. Gegen sie spricht insbesondere § 32 Abs. 1 Nr. 1 DSG NW. Der Ansicht, daß dieser Vorschrift keine eigenständige Bedeutung zukomme, kann nicht gefolgt werden. Grundsätzlich ist davon auszugehen, daß eine gesetzliche Vorschrift einen Regelungsgehalt hat. Wenn der Gesetzgeber in einer Vorschrift (wie in § 32 Abs. 1 Nr. 1 DSG NW) eine ausdrückliche und präzise Regelung trifft, muß daraus geschlossen werden, daß sich diese Regelung nicht bereits aus einer anderen, allgemein gehaltenen Vorschrift (wie § 1 Abs. 2 Satz 2 DSG NW) ergibt. Hätte die Kontrollbefugnis gegenüber den Behörden der Staatsanwaltschaft ausgeschlossen werden sollen, so hätte dies im Gesetz ebenso ausdrücklich und präzise wie für die Gerichte festgelegt werden müssen. Im übrigen spricht auch § 32 Abs. 1 Nr. 2 DSG NW, der den Westdeutschen Rundfunk Köln von der Kontrolle ausnimmt und dessen eigenständiger Regelungsgehalt nicht bestritten werden kann, gegen die Auffassung der Landesregierung. Aus dem Zusammenhang der Vorschriften ergibt sich, daß der Gesetzgeber in § 32 Abs. 1 DSG NW abschließend festgelegt hat, welche der in § 26 Abs. 1 Satz 1 DSG NW genannten Stellen nicht der Kontrolle des Landesbeauftragten unterliegen.

Ich muß deshalb an meiner Auffassung festhalten, daß die Behörden der Staatsanwaltschaft auch insoweit der Kontrolle des Landesbeauftragten unterliegen, als sie nicht Verwaltungsaufgaben erledigen.

Um einen Einblick in Zweck, Aufbau und Führung der **Zentralnamenkartei der Staatsanwaltschaft** zu erhalten, habe ich einen Informationsbesuch bei einer Staatsanwaltschaft durchgeführt.

Durch die Rundverfügung des Justizministers des Landes Nordrhein-Westfalen vom 8. Dezember 1980 sind Zweck, Aufbau, Führung der Zentralnamenkartei, Auskunft aus der Kartei und die Aussonderung der Karteikarten neu geregelt worden, um den Anforderungen des Datenschutzes einerseits und der Notwendigkeit der Führung einer Zentralnamenkartei andererseits gerecht zu werden. In Nordrhein-Westfalen ist nicht vorgesehen, die Zentralnamenkartei zu automatisieren.

Nach den neuen Bestimmungen dient die Zentralnamenkartei ausschließlich der staatsanwaltschaftlichen Tätigkeit, und zwar als Zugangsschlüssel zu den Akten und für die Aktenzusammenführung. Bei der Aktenzusammenführung bildet sich der ermittelnde Staatsanwalt jedoch nicht bereits durch die Eintragungen in der Kartei ein Urteil über den Betroffenen, sondern erst nach Beiziehung der entsprechenden Akten.

Bei der von mir besuchten Staatsanwaltschaft hat die in Karteiform geführte Zentralnamenkartei folgenden Inhalt:

- Name (ggf. mit Geburtsnamen),
- Vorname,
- Geburtsdatum (wenn nicht bekannt: Wohnort und Wohnung),
- Aktenzeichen.

Es werden Beschuldigte und Betroffene sowie bei Nachteilssachen (UJs-Sachen) Antragsteller, Verletzte und Anzeigende sowie die Tagebuchnummer der sachbearbeitenden Polizeidienststelle eingetragen.

Gerichten, anderen Staatsanwaltschaften, anderen Behörden und Stellen sowie Privatpersonen darf weder Einsicht noch Auskunft über Eintragungen in der Kartei erteilt werden. Die schriftlich erteilten Auskünfte aus der Zentralnamenkartei an die einzelnen Abteilungen der jeweiligen Staatsanwaltschaft sind mit dem Aufdruck „Datenschutz! Nur für Handakten!" zu versehen. Die Auskünfte aus der Kartei werden zu den Handakten genommen. Die Handakten werden nicht versandt und keinem Dritten zugänglich gemacht.

Obwohl die Zentralnamenkartei eine interne Kartei ist, wird dem Betroffenen, der wissen möchte, ob er in der Kartei eingetragen ist, Auskunft erteilt. Bei negativer Auskunft wird sie unmittelbar durch die Geschäftsstellenbeamtin, bei positiver Auskunft durch den Datenschutzdezernenten erteilt.

Die Karteikarten werden nach Ablauf von 10 Jahren vernichtet. Nach den früheren Bestimmungen wurden die Karten 5 Jahre aufbewahrt und sodann in eine Ablagekartei übernommen. Die Führung einer Ablagekartei ist nunmehr entfallen.

Sofern die Zentralnamenkartei der Staatsanwaltschaft nach den Vorschriften der Rundverfügung des Justizministers geführt wird, ist sie nach meiner Auffassung als interne Kartei für Zwecke der Rechtspflege anzusehen, für die nach § 7 Abs. 2 Satz 1 Nr. 2, § 1 Abs. 2 Satz 2 BDSG von den Vorschriften des Bundesdatenschutzgesetzes lediglich § 6 (technische und organisatorische Maßnahmen) gilt.

Dem in meinem ersten Tätigkeitsbericht (C. 8. a) angesprochenen Fall von **Akteneinsicht** durch ein Versicherungsunternehmen bin ich im Hinblick auf besondere Umstände des Falles im Einvernehmen mit dem Betroffenen nicht weiter nachgegangen. Ich halte jedoch an meiner Auffassung fest, daß die Gewährung von Einsicht in Straf- und Ermittlungsakten, die personenbezogene Daten enthalten, ohne Einwilligung des Betroffenen einen Eingriff in dessen Grundrecht auf Datenschutz darstellt und deshalb einer gesetzlichen Grundlage bedarf (Artikel 4 Abs. 2 der Landesverfassung).

Nach Nr. 185 Abs. 4 der Richtlinien für das Straf- und Bußgeldverfahren (RiStBV) wird einem bevollmächtigten Rechtsanwalt oder Rechtsbeistand Akteneinsicht gewährt, wenn er ein berechtigtes Interesse darlegt und wenn sonst Bedenken nicht bestehen. Als Rechtsgrundlage für die Gewährung von Akteneinsicht kommt diese Vorschrift nicht in Betracht, da es sich lediglich um eine Verwaltungsvorschrift handelt.

Der Justizminister ist jedoch der Ansicht, daß sie als Ausprägung eines bundesrechtlichen Gewohnheitsrechtssatzes verstanden werden müsse, der nach Artikel 31 des Grundgesetzes den in Artikel 4 Abs. 2 der Landesverfassung enthaltenen Gesetzesvorbehalt überlagere.

Ich habe nach wie vor Zweifel, ob ein solches Gewohnheitsrecht im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts zum Schutz der Menschenwürde und zur freien Entfaltung der Persönlichkeit Geltung beanspruchen kann, und halte eine Regelung durch Gesetz für geboten. Diese darf allerdings die Gewährung von Akteneinsicht nicht allein von der Darlegung eines beliebigen berechtigten Interesses eines Dritten abhängig machen, sondern muß schutzwürdige Belange des Betroffenen zumindest gleichrangig berücksichtigen.

Die Datenschutzbeauftragten des Bundes und der Länder haben die datenschutzrechtliche Überprüfung der **Anordnung über Mitteilungen in Strafsachen (MiStra)** fortgesetzt (vgl. C. 8. b meines ersten Tätigkeitsberichts). Sie haben dazu einstimmig eine Stellungnahme beschlossen, die ich dem Justizminister zugeleitet und auch dem Innenminister und dem Chef der Staatskanzlei zur Kenntnis gegeben habe.

Kernpunkte der Feststellungen und Forderungen der Datenschutzbeauftragten sind:

- Die MiStra entspricht wichtigen Grundentscheidungen des Gesetzgebers und des Bundesverfassungsgerichts nicht mehr. Die Datenschutzgesetzgebung des Bundes und der Länder hat die Verarbeitung personenbezogener Daten rechtlichen Beschränkungen unterworfen. Bereichspezifische Gesetze wie das Bundeszentralregistergesetz und das Bundespersonalausweisgesetz sowie einschlägige Entscheidungen des Bundesverfassungsgerichts sind Belege dafür, daß der Staat nunmehr in vielen Fällen bewußt davon absieht, die verfügbaren Informationen allen daran möglicherweise interessierten Stellen zur Kenntnis zu geben. Demgegenüber ist die MiStra von der gegenteiligen Auffassung geprägt. Ihre Anwendung führt vielfach zu einer globalen und schematischen Übermittlung besonders sensibler Daten, die im Regelfall eine Einzelfallprüfung unter Beachtung des Grundsatzes der Verhältnismäßigkeit vermissen läßt.
- Jede Mitteilung dieser Art stellt einen Eingriff in die nach Artikel 2 Abs. 1 des Grundgesetzes geschützte Rechtssphäre des Betroffenen dar. Ein solcher Eingriff bedarf einer gesetzlichen Grundlage. Als interne Verwaltungsvereinbarung kommt die MiStra selbst als Rechtsgrundlage nicht in Betracht. Für einzelne Arten von Mitteilungen mag eine Rechtsgrundlage vorhanden sein; für die meisten fehlt sie jedoch. Sie kann auch nicht aus allgemeinen Rechtsgrundsätzen hergeleitet werden. Soweit derartige Mitteilungen für erforderlich gehalten werden, muß der Gesetzgeber die Voraussetzungen festlegen, unter denen sie zulässig sein sollen.
- Neben der Regelung der Mitteilungspflichten sind Vorkehrungen zu treffen, daß die Grundsätze des Datenschutzes auch auf die nach der MiStra mitgeteilten Daten angewendet werden, sie also beispielsweise nach Ablauf bestimmter Fristen aus den Akten entfernt werden. Ansätze dafür finden sich in den Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien).

In ihrer Stellungnahme bitten die Datenschutzbeauftragten des Bundes und der Länder die Justizverwaltungen, die MiStra insoweit zu überprüfen, daß nur noch die Vorschriften bestehen bleiben, für die eine Rechtsgrundlage besteht, oder aber eine weitergehende gesetzliche Grundlage zu schaffen.

Unabhängig von der Notwendigkeit einer Rechtsgrundlage habe ich unter dem Gesichtspunkt der Erforderlichkeit der einzelnen Mitteilungen vorgeschlagen, eine Reihe von Vorschriften der MiStra zu ändern oder zu streichen.

b) Ordnungswidrigkeitenverfahren

Im Zusammenhang mit der Ausweisung eines seit Jahren in einer nordrhein-westfälischen Großstadt lebenden türkischen Staatsangehörigen warf ein Bürger die Frage nach der Zulässigkeit der Führung örtlicher „Verkehrssünderkarteien" bei den Ordnungsbehörden auf.

Nach Mitteilung des Oberstadtdirektors werden in die von ihm geführte Kartei lediglich Namen und Anschrift des Betroffenen sowie das Aktenzeichen rechtskräftig abgeschlossener oder eingestellter Bußgeldverfahren aufgenommen. Die Kartei diene dem Auffinden der Akten solcher Verfahren. Ausnahmsweise werde der Ausländerbehörde aus der Kartei Auskunft über Bußgeldverfahren gegen Ausländer erteilt. Die Karteikarten würden für die Dauer der längsten Aufbewahrungsfrist für Bußgeldakten (5 Jahre) aufbewahrt und dann vernichtet.

Sofern diese Kartei ausschließlich als Suchkartei zum Auffinden der Akten für einen rechtmäßigen Zweck verwendet wird, ist das Speichern der genannten Daten in der Kartei nach dem derzeitigen Erkenntnisstand nicht zu beanstanden. Als Rechtsgrundlage kann § 1 Abs. 2 Satz 3 DSG NW in Verbindung mit den Rechtsvorschriften angesehen werden, die eine Verwendung der Akten abgeschlossener Verfahren zulassen (wie etwa § 85 des Ordnungswidrigkeitengesetzes für den Fall der Wiederaufnahme des Verfahrens). § 1 Abs. 2 Satz 3 DSG NW stellt Daten, die in nicht-automatisierten Verfahren verarbeitet werden und nicht zur Übermittlung an Dritte bestimmt sind, von der Anwendung der Vorschrift des Datenschutzgesetzes Nordrhein-Westfalen über die Zulässigkeit der Datenspeicherung (§ 10 Abs. 1 DSG NW) frei. Danach setzt die Speicherung derartiger Daten nicht voraus, daß sie zur rechtmäßigen Erfüllung der Aufgaben der speichernden Stelle „erforderlich" ist. Es genügt, wenn die Verwendung der Daten rechtmäßig ist.

Die Erteilung von Auskünften an die Ausländerbehörde über Verkehrsordnungswidrigkeitsverfahren erfüllt diese Voraussetzung allerdings nicht. Nach der Rechtsprechung des Bundesverwaltungsgerichts zu den Vorschriften des Straßenverkehrsgesetzes über das Verkehrszentralregister ist dieses die allein maßgebende Sammel- und Auskunftsstelle über verkehrsrechtliche Entscheidungen und sonst erhebliche Vorgänge auf dem Gebiet des Straßenverkehrsrechts, durch die örtliche Karteien ersetzt worden sind (BVerwGE 51, 359, 368-369). Daraus folgt, daß es nach dem Willen des Gesetzgebers unzulässig ist, bei den örtlichen Behörden „Verkehrssünderkarteien" zu führen oder andere, an sich zulässige Karteien, in denen auch Hinweise auf derartige Vorgänge enthalten sind, für Auskünfte darüber zu verwenden, ob über eine Person solche Vorgänge vorhanden sind.

Zwar kann nach der Rechtsprechung der Verwaltungsgerichte eine Vielzahl von Bußgeldbescheiden etwa wegen ordnungswidrigen Parkens, die nicht in das Verkehrszentralregister eingetragen werden, die Entziehung der Fahrerlaubnis rechtfertigen. Um festzustellen, ob ein derartiger Wiederholungsfall vorliegt, darf jedoch ebenso wie bei der Verfolgung von Ordnungswidrigkeiten nicht auf örtliche Karteien, sondern lediglich auf die ohne dieses Hilfsmittel vorhandene Kenntnis des Bearbeiters von durchgeführten Bußgeldverfahren zurückgegriffen werden (vgl. hierzu die Begründung zu § 22 des Entwurfs eines Verkehrszentralregistergesetzes, Bundestagsdrucksache 8/3900, S. 17).

Auf jeden Fall muß aus dem Grundgedanken der Regelungen über das Verkehrszentralregister der Grundsatz entnommen werden, daß Verkehrsordnungswidrigkeiten für andere als die in § 30 StVG genannten Zwecke überhaupt nicht verwertet werden dürfen, sofern nicht eine andere Rechtsvorschrift dies ausdrücklich zuläßt. Eine solche ist hier

jedoch nicht ersichtlich. Auskünfte über Verkehrsordnungswidrigkeiten an die Ausländerbehörde sind deshalb nicht zulässig.

Eine Suchkartei, in die auch Verfahren über Verkehrsordnungswidrigkeiten aufgenommen werden, darf danach nur dazu verwendet werden, das Aktenzeichen eines dem Auskunftsuchenden bereits bekannten Bußgeldverfahrens gegen einen Betroffenen festzustellen. Dagegen darf eine solche Kartei nicht dazu verwendet werden festzustellen, **ob** gegen eine Person ein Bußgeldverfahren durchgeführt worden ist, weil damit dem Auskunftsuchenden auch Bußgeldverfahren wegen Verkehrsordnungswidrigkeiten bekannt werden und dadurch gegen das Verbot örtlicher „Verkehrssünderkarteien" verstoßen wird.

Gegen die Aufbewahrung der Karteikarten für die Dauer der Aufbewahrung der dazugehörigen Akten nach dem Runderlaß des Innenministers des Landes Nordrhein-Westfalen vom 5. Juli 1973 (SMBl. NW. 453) habe ich keine Bedenken. Spätestens bei Vernichtung der Akten müssen jedoch auch die Karteikarten vernichtet werden. Mit dem Zweck einer Suchkartei wäre es unvereinbar, die Karteikarte 5 Jahre aufzubewahren, wenn die Akte bereits nach 3 Jahren vernichtet wird. Wird bei der Bearbeitung eine Karteikarte gezogen, bei der der Ablauf der Aufbewahrungsfrist festgestellt wird, so muß sie ebenso wie die Akte unverzüglich vernichtet werden.

Eine Frage nach der Zulässigkeit von Anfragen bei dem Kraftfahrt-Bundesamt über den Halter eines Kraftfahrzeuges bei ordnungswidrigem Parken ohne Parkscheibe durch die zuständige Behörde für die Verfolgung von Ordnungswidrigkeiten habe ich wie folgt beantwortet:

Nach § 24 des Straßenverkehrsgesetzes, § 49 Abs. 1 Nr. 13 der Straßenverkehrsordnung in Verbindung mit § 46 Abs. 1 und 2 des Ordnungswidrigkeitengesetzes (OWiG) und § 160 Abs. 1, § 161 Satz 1 der Strafprozeßordnung kann der Stadtdirektor als Verfolgungsbehörde für die genannte Verkehrsordnungswidrigkeit zur Erforschung des Sachverhalts von allen Behörden Auskunft verlangen.

Nach § 65 OWiG wird die Ordnungswidrigkeit, soweit das Gesetz nichts anderes bestimmt, durch Bußgeldbescheid geahndet. Allerdings kann nach § 56 Abs. 1 OWiG die Verwaltungsbehörde bei geringfügigen Ordnungswidrigkeiten den Betroffenen verwarnen und ein Verwarnungsgeld erheben. Die Verwarnung ist gemäß § 56 Abs. 2 OWiG jedoch nur wirksam, wenn der Betroffene nach Belehrung über sein Weigerungsrecht mit ihr einverstanden ist und das Verwarnungsgeld entsprechend der Bestimmung der Verwaltungsbehörde entweder sofort oder innerhalb festgesetzter Frist zahlt.

Für diese Verwarnung wäre die Halteranfrage nicht erforderlich. Für den Fall aber, daß der Betroffene mit der Verwarnung nicht einverstanden ist und das Verwarnungsgeld innerhalb der festgesetzten Frist nicht einzahlt, hat die Verwaltungsbehörde unverzüglich ein Bußgeldverfahren nach den Bestimmungen des Ordnungswidrigkeitengesetzes einzuleiten. Hierbei ist die Verwaltungsbehörde auf die Kenntnis des Namens und der Anschrift des Fahrzeughalters angewiesen. Um ein mögliches Bußgeldverfahren rechtzeitig einleiten zu können, darf die Halterauskunft bereits unmittelbar nach der festgestellten Ordnungswidrigkeit unabhängig vom Ausgang des Verwarnungsverfahrens eingeholt werden. Die Halteranfrage erst nach Durchführung eines erfolglosen Verwarnungsverfahrens zu stellen, wäre möglicherweise zu spät. Die erforderliche Übersendung des Anhörungsbogens an den Kraftfahrzeughalter würde dann erst zu einem Zeitpunkt erfolgen, zu dem das Erinnerungsvermögen des Betroffenen für eine verantwortliche Anhörung nicht mehr ausreichen könnte (OVG Lüneburg, Deutsches Autorecht 1977, S. 223).

Sofern durch die Zahlung des Verwarnungsgeldes eine Verwarnung wirksam geworden ist, brauchen die Halterdaten nicht weiter festgehalten zu werden. Die Auskunft des Kraftfahrt-Bundesamts ist deshalb bei rechtzeitiger Zahlung des Verwarnungsgeldes zu vernichten.

c) Zivilsachen

Am 1. Januar 1981 ist das **Gesetz über die Prozeßkostenhilfe** in Kraft getreten. Wie ich in meinem ersten Tätigkeitsbericht (C. 8. f) ausgeführt habe, wurden bei dem Verfahren über die Gewährung der Prozeßkostenhilfe Daten über die persönlichen und wirtschaftlichen Verhältnisse der beantragenden Partei sehr weitgehend offengelegt. Ich habe daher empfohlen, die in diesem Verfahren anfallenden Daten in einem Beiheft festzuhalten, das den Prozeßparteien nicht zugänglich ist.

Der Justizminister des Landes Nordrhein-Westfalen ist in den Durchführungsbestimmungen zum Gesetz über die Prozeßkostenhilfe (Allgemeine Verfügung vom 10. Dezember 1980, JMBl. NW. 1981 S. 14) meiner Empfehlung nur teilweise gefolgt. Er hat angeordnet, daß der Vordruck mit der Erklärung über die persönlichen und wirtschaftlichen Verhältnisse sowie die bei der Durchführung der Prozeßkostenhilfe entstehenden Vorgänge in einem Beiheft zu vereinigen sind. Eine Regelung über die Akteneinsicht hat er unter Hinweis auf die Unabhängigkeit der Gerichte nicht getroffen. Aus der Sicht des Datenschutzes ist dies zu bedauern.

Dem Justizminister erscheint die Aufnahme der persönlichen Erklärung in einem Beiheft allerdings geeignet, die Gerichte bei der Entscheidung über die Gewährung von Akteneinsicht an die Schutzbedürftigkeit der in der Erklärung offenbarten Daten zu erinnern. Es ist zu hoffen, daß die Gerichte bei der Gewährung von Akteneinsicht den Datenschutzbelangen des Betroffenen Rechnung tragen werden.

Mehrere Eingaben, die die Erteilung von Auskünften aus dem **Schuldnerverzeichnis** betrafen, haben wieder gezeigt, daß eine Neugestaltung der Allgemeinen Vorschriften über die Erteilung und die Entnahme von Abschriften oder Auszügen aus dem Schuldnerverzeichnis (AV) vom 1. August 1955 dringend erforderlich ist.

In meinem ersten Tätigkeitsbericht (C. 8. d) habe ich meine Bedenken gegen die bisherige Regelung dargelegt. Die gemeinsam mit den anderen Datenschutzbeauftragten erarbeiteten Änderungsvorschläge sind bei den Landesjustizverwaltungen und den Wirtschaftsverbänden auf Ablehnung gestoßen. Umso mehr ist es zu begrüßen, daß der Bundesminister der Justiz dennoch einen Entwurf für eine Verordnung über Abschriften aus den Schuldnerverzeichnissen vorgelegt und den Landesjustizverwaltungen zur Stellungnahme übermittelt hat.

Der Entwurf sieht vor, daß einem Antrag auf Erteilung von Abschriften aus dem bei den Amtsgerichten geführten Schuldnerverzeichnis zu entsprechen ist, wenn der Antrag von einer öffentlich-rechtlichen Berufsvertretung oder von einer der im Vierten Abschnitt (Geschäftsmäßige Datenverarbeitung für fremde Zwecke) des Bundesdatenschutzgesetzes genannten Stelle gestellt wird. Durch diese Vorschrift ist dem Vorschlag der Datenschutzbeauftragten gefolgt worden, den Empfängerkreis der vom Gericht erstellten Abschriften auf die Stellen einzugrenzen, die einer datenschutzrechtlichen Aufsicht unterliegen. Leider nicht berücksichtigt wurde mein Vorschlag, die vorgesehene Höchstdauer für die Bewilligung der Abschrifterteilung von 5 Jahren auf 3 Jahre zu verkürzen.

Erhebliche Bedenken bestehen dagegen, daß auch nach dem Entwurf für die neuen Bestimmungen die öffentlich-rechtlichen Berufsvertretungen die Möglichkeit haben sollen, Abschriften aus dem Schuldnerverzeichnis ihren Mitgliedern und den Mitgliedern einer gleichen öffentlich-rechtlichen Berufsvertretung zugänglich zu machen. Zwar haben die Empfänger und die Zweitempfänger die Abschriften und aus ihnen zusammengestellte Datenträger unverzüglich zu vernichten, wenn die Frist nach § 915 Abs. 2 Satz 1 der Zivilprozeßordnung und des § 107 Abs. 2 Satz 3 der Konkursordnung abgelaufen ist oder eine vorzeitige Löschung erfolgte. Auch müssen sich die Empfänger gegenüber dem Präsidenten des Amtsgerichts bzw. dem Präsidenten des Landgerichts, die Zweitempfänger gegenüber den Empfängern schriftlich verpflichten, die Bestimmungen über die Auskunfterteilung, den Verwendungszweck und die Löschung einzuhalten, und die Zweitempfänger haben im Falle der Zuwiderhandlung eine Vertragsstrafe bis zu 1000 Deut-

sche Mark zu zahlen. Diese Vorkehrungen können jedoch bei der großen Zahl der Zweitempfänger eine vertrauliche Behandlung der Daten eines Schuldners nicht gewährleisten. Ich halte deshalb an dem Vorschlag fest, die öffentlich-rechtlichen Berufsvertretungen wie die anderen Empfänger von Abschriften aus dem Schuldnerverzeichnis auf die Erteilung von Einzelauskünften zu beschränken.

d) Zustellungen

Datenschutzrechtliche Probleme ergaben sich bei der Zustellung von Bußgeldbescheiden und Schriftstücken in Bußgeldverfahren sowie bei der Übersendung von Gerichtskostenrechnungen. Bürger beschwerten sich darüber, daß ihr Geburtsdatum in das Adressenfeld aufgenommen worden war. Bei der Zustellung eines Bußgeldbescheides war darüber hinaus noch der Geburtsort und der Beruf im Sichtfenster des Briefumschlages zu lesen.

Ich verkenne nicht, daß es in einigen wenigen Fällen, wenn mehrere Träger des gleichen Familien- und Vornamens die gleiche Anschrift haben, im Interesse der Betroffenen liegen kann, zur Übersendung der Kostenrechnung, eines Bußgeldbescheides, eines Strafbefehls oder einer Terminsladung das Geburtsdatum im Adressenfeld aufzuführen, sofern nicht anderweitig, etwa durch Zusätze wie „jun." oder „sen.", eine eindeutige Bestimmung des Betroffenen erreicht werden kann.

Gerade auch bei einer Gerichtskostenrechnung und bei der Übersendung von Schriftstücken im Bereich der Strafsachen ist es wichtig, daß diese an den richtigen Empfänger gelangen. Wird eine Gerichtskostenrechnung nicht bezahlt, können sich Mahnungen und Zwangsvollstreckungsmaßnahmen anschließen, die bei richtiger Übermittlung der Kostenrechnung durch eine genaue Bezeichnung des Kostenschuldners hätten vermieden werden können. Bei der Zustellung eines Bußgeldbescheides oder eines Strafbefehls an den falschen Adressaten kann nach Ablauf der Rechtsmittelfrist irrtümlich von der Rechtskraft des Bußgeldbescheides oder Strafbefehls ausgegangen werden. Die fehlgeleitete Ladung eines Zeugen oder eines Beschuldigten kann zum Erlaß eines Vorführungs- oder Haftbefehls führen. Bei richtiger Übermittlung der Schriftstücke infolge genauerer Bezeichnung der Adressaten können solche für den Betroffenen und einen unbeteiligten Dritten gleichermaßen unliebsamen Folgen vermieden werden.

Die Fälle, in denen eine Verwechslungsgefahr naheliegt, rechtfertigen nach meiner Auffassung aber nicht die regelmäßige Aufnahme des Geburtsdatums in das Adressenfeld bei allen Schriftstücken der genannten Art. Von den betreffenden Justizbehörden wurde mir zugesagt, künftig darum bemüht zu sein, in Fällen hinreichender Identifikation von der Angabe des Geburtsdatums abzusehen.

Die bisher verwendeten Vordrucksätze für Ordnungswidrigkeitsanzeigen waren so gestaltet, daß zwischen Anschrift und Geburtsdatum nur ein geringer Abstand bestand. Bei ungenauem Falten der Vordrucke konnte es vorkommen, daß im Umschlagfenster Geburtsdatum oder weitere geschützte personenbezogene Daten sichtbar wurden.

Damit den datenschutzrechtlichen Belangen der Betroffenen wirksamer Rechnung getragen werden kann, habe ich dem Innenminister des Landes Nordrhein-Westfalen empfohlen, in den Vordrucksätzen den Abstand zwischen Anschrift und anderen Daten zu vergrößern oder die mit der Erstellung von Bußgeldbescheiden betrauten Stellen anzuweisen, zwischen Anschrift und Geburtsdatum mehr Abstand zu lassen. Der Innenminister hat meine Empfehlung aufgegriffen und die Vordrucksätze entsprechend geändert.

e) Vormundschaftsangelegenheiten

Durch das Gesetz zur Neuregelung des Rechts der elterlichen Sorge vom 18. Juli 1979 (BGBl. I S. 1061) wurde § 1668 BGB neu gefaßt. Nach dieser Bestimmung hat das zuständige Gericht nunmehr auch bei einem Antrag auf Abnahme der eidesstattlichen Versicherung (§ 807 ZPO), der die Eltern oder einen Elternteil betrifft, das zuständige Vormund-

schaftsgericht zu benachrichtigen. Sinn dieser Vorschrift ist, bei Anträgen nach § 807 ZPO rechtzeitig die Gefährdung des Kindesvermögens festzustellen. In der überwiegenden Zahl der Fälle werden die Kinder jedoch kein Vermögen haben, das gefährdet werden könnte. Es ist auch zweifelhaft, ob die Feststellung der Gefährdung im Zeitpunkt des Antrags auf Abgabe der eidesstattlichen Versicherung überhaupt noch rechtzeitig sein kann.

Die Vollstreckungsgerichte sind auf Grund von § 1668 BGB gehalten, alle Anträge auf Abgabe der eidesstattlichen Versicherung dem Vormundschaftsgericht anzuzeigen, da zunächst nicht bekannt ist, ob die Betroffenen Kinder haben. Die Vormundschaftsgerichte reagieren recht unterschiedlich auf diese Mitteilungen der Vollstreckungsgerichte.

Einzelne Vormundschaftsgerichte warten den Termin zur Abgabe der eidesstattlichen Versicherung ab und lassen im Termin durch das Vollstreckungsgericht die notwendigen personenbezogenen Daten erheben. In einer Vielzahl der Fälle kommt es jedoch gar nicht erst zur Terminsbestimmung, sondern es erfolgt die Einstellung des Verfahrens wegen zwischenzeitlicher Bezahlung der Forderung oder Ratenzahlungsvereinbarungen. Die Möglichkeit der Gefährdung des Kindesvermögens besteht allerdings schon bei der Stellung des Antrages auf Abgabe der eidesstattlichen Versicherung, so daß die Handhabung dieser Gerichte zwar eine praktikable Lösung darstellt, jedoch nicht ganz dem Sinn des § 1668 BGB entspricht.

Andere Vormundschaftsgerichte dagegen werden unmittelbar nach Eingang der Mitteilung durch das Vollstreckungsgericht tätig und holen Auskünfte über Namen, Anschriften und Geburtsdaten der Ehegatten und Kinder eines Schuldners bei dem zuständigen Einwohnermeldeamt ein. Bei der Menge der Anträge nach § 807 ZPO gingen bei dem Einwohnermeldeamt einer Stadt innerhalb von drei Monaten 300 Anfragen eines Vormundschaftsgerichts ein. Dies nahm die Stadt zum Anlaß, sich an mich mit der Bitte um Prüfung zu wenden, ob die Anfragen des Vormundschaftsgerichts zu dessen Aufgabenerfüllung erforderlich und eine Datenübermittlung somit zulässig sei. Ich habe den Justizminister und den Innenminister des Landes Nordrhein-Westfalen um Stellungnahme zu dieser Problematik gebeten, insbesondere zu der Frage, ob bei diesem Verfahren der Grundsatz der Verhältnismäßigkeit gewahrt ist.

Der Justizminister hat mir mitgeteilt, daß sich die bereits vor Inkrafttreten dieser Bestimmung befürchteten Schwierigkeiten in der Praxis bestätigt hätten. Deshalb seien die Landesjustizverwaltungen an den Bundesminister der Justiz herangetreten und hätten vorgeschlagen, § 1668 BGB aufzuheben. Der Bundesjustizminister habe den Landesjustizverwaltungen Vorschläge für Gesetzesänderungen unterbreitet, die bei geeigneter Gelegenheit in das Gesetzgebungsverfahren eingebracht werden sollen. Hierzu gehört auch die Aufhebung des § 1668 BGB. Der Innenminister und ich teilen aus datenschutzrechtlicher Sicht die Auffassung des Justizministers, daß § 1668 BGB im Hinblick auf die Schwierigkeiten bei der praktischen Durchführung und die geringe Wirksamkeit dieser Bestimmung entfallen sollte.

Bis zur Aufhebung dieser Vorschrift sind jedoch die Gerichte gehalten, der gesetzlichen Verpflichtung des § 1668 BGB nachzukommen. Auf welche Weise der Rechtspfleger, auf den diese Aufgaben nach dem Rechtspflegergesetz übertragen sind, seine Ermittlungen anstellt, unterliegt seiner Entscheidung. Zu diesen Ermittlungen können auch die Anfragen an das Einwohnermeldeamt gehören. Eine Einflußnahme auf die Entscheidung des Rechtspflegers ist mit Rücksicht auf die Selbständigkeitsgarantie des § 9 des Rechtspflegergesetzes unzulässig.

f) Grundbuchwesen

Die Eingaben im Bereich des Grundbuchwesens bezogen sich auf die Einsicht in das Grundbuch und die Erteilung von Abschriften aus dem Grundbuch.

Gesetzliche Grundlage für die Einsichtnahme in das Grundbuch, die Erteilung von Abschriften aus dem Grundbuch und von Urkunden, auf die im Grundbuch zur Ergänzung

einer Eintragung Bezug genommen wird, ist § 12 Abs. 1 und 2 der Grundbuchordnung (GBO). Diese Vorschrift geht nach Artikel 31 des Grundgesetzes als Bundesrecht den Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen und auch der Landesverfassung vor. Da sie die Erteilung von Abschriften abschließend regelt, finden die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen insoweit keine Anwendung.

Nach der genannten Vorschrift kann die Einsichtnahme in das Grundbuch und die Erteilung von Abschriften gewährt werden, wenn ein berechtigtes Interesse dargelegt wird; ein Notar ist von der Darlegung des berechtigten Interesses befreit (§ 43 der Grundbuchverfügung). Der Begriff des berechtigten Interesses ist weiter als der des rechtlichen Interesses. Das berechtigte Interesse umfaßte auch das Interesse einer Antragstellerin zu erfahren, ob und gegebenenfalls aus welchem Grund sie von einer vorweggenommenen Erbfolge ausgeschlossen wurde, das Interesse eines Notars an einer Wertermittlung für seine Gebührenberechnung und das Interesse eines Bauunternehmers, die Angaben zu erhalten, die zur Vorbereitung eines Antrags auf Eintragung einer Sicherungshypothek benötigt werden.

g) Vorschlagslisten für Schöffen

Im Mitteilungsblatt einer Gemeinde waren die Vorschlagslisten der Parteien zur Schöffenwahl unter Angabe der vorschlagenden Parteien abgedruckt. Neben dem Namen, Vornamen, Beruf, der Anschrift und dem Geburtsdatum waren auch die Telefonnummern der Vorgeschlagenen aufgeführt.

Gesetzliche Grundlage für den Inhalt und die Bekanntgabe der Vorschlagsliste für Schöffen sind die Vorschriften des § 36 Abs. 2 und 3 des Gerichtsverfassungsgesetzes (GVG), die eine abschließende Regelung enthalten.

Nach § 36 Abs. 2 Satz 2 GVG muß die Vorschlagsliste folgende Angaben über die vorgeschlagene Person enthalten:

- Geburtsnamen
- Familiennamen
- Vornamen
- Tag und Ort der Geburt
- Wohnungsanschrift
- Beruf.

Für die Angabe der vorschlagenden Partei und der Telefonnummer der vorgeschlagenen Person ist keine gesetzliche Grundlage vorhanden.

Die Vorschlagsliste ist nach § 36 Abs. 3 GVG in der Gemeinde eine Woche lang zu jedermanns Einsicht aufzulegen. Der Zeitpunkt der Auflegung ist vorher unter Hinweis auf die gesetzliche Einspruchsmöglichkeit (§ 37 GVG) öffentlich bekanntzumachen (§ 36 Abs. 3 Satz 2 GVG). Die Handhabung, die Vorschlagsliste im Mitteilungsblatt der Gemeinde zu veröffentlichen, entspricht nicht den gesetzlichen Bestimmungen.

Meine Ermittlungen bei dieser Gemeinde haben ergeben, daß Niederschriften über Ratssitzungen, soweit sie den öffentlichen Teil betreffen, zur Information der Bürger im Mitteilungsblatt der Gemeinde veröffentlicht wurden. Die von den Parteien eingereichten Vorschlagslisten waren Bestandteil einer solchen Niederschrift und dieser als Anlage beigefügt gewesen. Irrtümlicherweise wurde auch diese Anlage (Vorschlagsliste der Parteien) veröffentlicht. Es wurde mir zugesichert, daß zur Vermeidung von Verstößen gegen Bestimmungen des Datenschutzes künftig darauf geachtet wird, daß derartige Listen nicht im Mitteilungsblatt veröffentlicht werden.

h) Personalakten für Rechtsbeistände

In einem Rechtsstreit wurde Beweis darüber erhoben, ob ein Verzicht auf die Erlaubnis zur Besorgung fremder Rechtsangelegenheiten gemäß Artikel 1 § 1 des Rechtsberatungs-

gesetzes (RBerG) wirksam oder unwirksam war. Die Beweiserhebung erfolgte durch die Vernehmung der Personalsachbearbeiterin des zuständigen Amtsgerichtes zu dem in den Personalakten des Beklagten befindlichen Schreiben. Der Beklagte bat mich um Prüfung der Zulässigkeit der Erteilung dieser Auskunft aus seiner Personalakte.

Gesetzliche Grundlage für die Auskunft der zuständigen Sachbearbeiterin über das in den Personalakten befindliche Schreiben in dem Rechtsstreit sind die Vorschriften der Zivilprozeßordnung über den Zeugenbeweis. Danach sind Zeugen zur Aussage verpflichtet, sofern sie kein Zeugnisverweigerungsrecht haben. Beamte und andere Personen des öffentlichen Dienstes bedürfen für die Aussage über Angelegenheiten, über die sie Verschwiegenheit zu bewahren haben, der Genehmigung des Dienstvorgesetzten (§ 376 Abs. 1 ZPO, § 64 Abs. 2 Satz 1 und 2 LBG).

Zwar bestimmt § 65 Abs. 1 LBG, daß die Aussagegenehmigung nur versagt werden darf, wenn die Aussage dem Wohl des Bundes oder eines deutschen Landes Nachteile bereiten oder die Erfüllung öffentlicher Aufgaben ernstlich gefährden oder erheblich erschweren würde. Bei Aussagen, die in den Anspruch eines Betroffenen auf Schutz seiner personenbezogenen Daten eingreifen, darf jedoch nach Artikel 4 Abs. 2 der Landesverfassung die Genehmigung nur erteilt werden, wenn ein überwiegendes Interesse der Allgemeinheit an der Aussage vorliegt.

Bei Aussagen über den Inhalt von Personalakten genügt nach meiner Auffassung das bei einem Rechtsstreit immer vorhandene rechtliche Interesse der Prozeßparteien nicht. In dem geschilderten Fall überwog allerdings das schutzwürdige Interesse der Allgemeinheit an einer gerichtlichen Klärung, ob der Beklagte zur Besorgung fremder Rechtsangelegenheiten berechtigt war, gegenüber seinem Geheimhaltungsinteresse. Somit verstießen die erteilte Aussagegenehmigung und die auf Grund dieser Genehmigung erteilte Auskunft der Sachbearbeiterin aus den Personalakten nicht gegen Vorschriften über den Datenschutz.

12. Sozialwesen

a) Neuregelung des Sozialgeheimnisses

Ein Schwerpunkt meiner Tätigkeit lag im Bereich des Sozialwesens. Für diesen Bereich ist der Datenschutz im Berichtsjahr neu geregelt worden. Der Bundesgesetzgeber hat das Zehnte Buch des Sozialgesetzbuches (SGB X) verabschiedet, das am 1. Januar 1981 in Kraft getreten ist. In diesem Gesetz ist § 35 des Ersten Buchs des Sozialgesetzbuchs (SGB I) als Grundnorm für den Schutz des Sozialgeheimnisses neu gefaßt und durch einen abschließenden Katalog von Offenbarungsbefugnissen sowie Vorschriften über den Schutz der Sozialdaten bei der Datenverarbeitung (§§ 67 bis 85 SGB X) ergänzt worden.

Diese erste umfassende bereichspezifische Datenschutzregelung für den besonders bedeutsamen und sensiblen Sozialbereich ist als solche durchaus zu begrüßen. Sie entspricht im Grundsatz meiner Forderung, soweit als möglich bereichspezifische Datenschutzregelungen zu treffen, um den Besonderheiten der einzelnen Verwaltungsbereiche hinreichend Rechnung zu tragen (vgl. E. 2 meines ersten Tätigkeitsberichts).

Umso mehr bedauere ich, daß die Absicht des Gesetzgebers für einen wirksameren Datenschutz im Sozialbereich zu sorgen, nur zum Teil verwirklicht wird. Zwar hat die Neuregelung den Datenschutz gegenüber dem früheren Recht in mancher Hinsicht verbessert; sie führt andererseits aber in einer Reihe von Punkten zu einer Verschlechterung des Datenschutzes. Ich habe deshalb während des Gesetzgebungsverfahrens mehrere Änderungen vorgeschlagen.

Dies gilt insbesondere für die in § 68 SGB X vorgesehene Offenbarung bestimmter Sozialdaten im Rahmen der allgemeinen Amtshilfe. Das Sozialgeheimnis gewährleistet,

daß die Bürger der Sozialverwaltung vertrauen können. Dieses Vertrauensverhältnis ist notwendig, da sonst insbesondere viele Dienstleistungen und alle persönlichen und erzieherischen Hilfen kaum möglich sind. Die in § 68 SGB X vorgesehene Freigabe bestimmter personenbezogener Daten für nicht ausdrücklich festgelegte Fälle der Amtshilfe beeinträchtigt das Vertrauensverhältnis zwischen dem Sozialleistungsträger und dem Bürger. Die Übermittlung von Sozialdaten im Wege der Amtshilfe darf nur für bestimmte Zwecke unter Beachtung des Verhältnismäßigkeitsgrundsatzes zugelassen werden. Von diesen Ausnahmefällen abgesehen muß das Sozialgeheimnis nach meiner Auffassung „amtshilfefest" bleiben. Ich habe mich deshalb für eine Streichung des § 68 SGB X eingesetzt und vorgeschlagen, die Offenbarung der dort genannten Daten einzelner Betroffener lediglich an Polizeibehörden für Zwecke der Gefahrenabwehr zuzulassen.

Ferner habe ich die Änderung des § 71 Nr. 3 SGB X gefordert, soweit er eine Offenbarung personenbezogener Daten durch Vorlage von Urkunden und Akten nach § 97 AO zur Durchführung der Besteuerung vorsieht. Ich halte eine solche Offenbarung in Abwägung mit den schutzwürdigen Belangen des Bürgers an der Geheimhaltung seiner Sozialdaten für nicht gerechtfertigt. Der Verhältnismäßigkeitsgrundsatz verbietet es, den Finanzbehörden Akten der Sozialverwaltung zu übersenden oder ihnen Einsicht in diese Akten zu gewähren. In aller Regel ist davon auszugehen, daß den Finanzbehörden durch die Übersendung oder Akteneinsicht mehr Daten zugänglich gemacht werden, als für die Durchführung der Besteuerung erforderlich sind. Zur Durchführung der Besteuerung hätte deshalb die Offenbarung von Sozialdaten auf die gesetzlichen Mitteilungspflichten nach den §§ 93 und 116 AO beschränkt werden müssen.

Mit § 78 SGB X ist der Gesetzgeber insofern auf halbem Wege stehengeblieben, als er die Zweckbindung nur für die Empfänger von Daten vorschreibt. Sie sollte auch für die in § 35 SGB I genannten Stellen gelten, die solche Daten erheben. Deshalb hätte bestimmt werden sollen, daß jede Stelle die Daten nur zu dem Zweck verwenden darf, zu dem sie sie erhoben oder empfangen hat.

Ich habe außerdem vorgeschlagen, § 79 SGB X zu streichen. Diese Vorschrift erstreckt den Anwendungsbereich des Bundesdatenschutzgesetzes auf die landesunmittelbaren Sozialleistungsträger und verdrängt insoweit die Datenschutzgesetze der Länder. Den damit erreichten „Vorteil" eines bundeseinheitlichen Schutzes der Sozialdaten stehen folgende — nach meiner Überzeugung überwiegende — Nachteile gegenüber.

Die Behörden im Landesbereich, insbesondere die Gemeinden und Gemeindeverbände, müssen zweierlei Datenschutzrecht anwenden, und zwar das Bundesdatenschutzgesetz, soweit sie Leistungsträger im Sinne des § 35 SGB I sind, im übrigen das Landesdatenschutzgesetz. Dies dient weder der Verwaltungsvereinfachung noch dem Interesse der betroffenen Bürger. Ihnen werden zudem, soweit sie es mit Sozialleistungsträgern zu tun haben, nach den Datenschutzgesetzen der Länder zustehende Rechte wie z. B. der verschuldensunabhängige Schadensersatzanspruch (§ 4 Abs. 2 DSG NW) und der Unterlassungs- und Folgenbeseitigungsanspruch (§ 4 Abs. 1 Nr. 6 DSG NW) entzogen. Insgesamt verlangt § 79 SGB X damit von den Bürgern einen zu hohen Preis für die Bundeseinheitlichkeit des Sozialdatenschutzes.

In diesem Zusammenhang habe ich auch empfohlen, die Regelung der Datenverarbeitung im Auftrag in § 80 Abs. 2 Satz 3 SGB X zu ändern, da sie hinter den Anforderungen einer wirksamen Datenschutzkontrolle zurückbleibt. Diese ist nur möglich, wenn nicht nur der Auftraggeber, sondern auch der für ihn zuständige Datenschutzbeauftragte die Einhaltung der Datenschutzvorschriften bei dem Auftragnehmer überwachen kann, wie dies durch § 7 Abs. 1 Satz 2 DSG NW sichergestellt ist. Schließlich habe ich vorgeschlagen, bei besonders sensiblen Daten (z. B. über gesundheitliche Verhältnisse, strafbare Handlungen oder Ordnungswidrigkeiten) eine Datenverarbeitung im Auftrag nur dann zuzulassen, wenn der Auftragnehmer eine öffentliche Stelle ist.

Die Landesregierung hat zwar einen Teil meiner Vorschläge aufgegriffen und im Bundesrat entsprechende Anträge auf Anrufung des Vermittlungsausschusses gestellt, die vom Bundesrat auch angenommen wurden. Der Vermittlungsausschuß ist diesem Anrufungsbegehren jedoch nicht gefolgt. Im Ergebnis hat keiner meiner Vorschläge im Gesetz Berücksichtigung gefunden.

Es bleibt abzuwarten, wie sich die neuen Vorschriften auswirken und ob sie die Erwartungen der interessierten Öffentlichkeit erfüllen werden.

b) Sozialversicherung

Die Rentenversicherungsträger verlangen seit 1979 im Verfahren zur **Rehabilitation Abhängigkeitskranker** (Alkohol-, Medikamenten- und Drogenabhängige) von den Suchtberatungsstellen einen „Sozialbericht — psychosoziale Grunddaten —" unter Verwendung eines bundeseinheitlich eingeführten Vordrucks. Der Bericht enthält neben Angaben zur Person eine Vielzahl sensibler Informationen, z. B. Angaben über Entmündigungen, Pflegschaften, Zahl der Kinder, Wohn- und finanzielle Verhältnisse, frühere Krankheiten, Suizidversuche, verwendete Suchtmittel sowie Dosis und Häufigkeit der Einnahme, Verhalten unter Einfluß von Suchtmitteln, seelisch-geistige Veränderungen, Zahl und Zeitpunkt durchgeführter Entgiftungen und Entwöhnungen. Außerdem gibt der Bericht im Rahmen einer eingehenden Sozialanamnese Aufschluß über das soziale Umfeld des Betreuten und die gegen ihn anhängigen Strafverfahren.

Der Betreute wird gebeten, in einer dem Sozialbericht beigefügten Erklärung zu bestätigen, daß er über dessen Inhalt unterrichtet wurde und mit der Übermittlung des Berichts an den Leistungsträger und die Behandlungsstätte zum Zwecke der Antragserledigung und zur Durchführung der Behandlung einverstanden ist.

Die datenschutzrechtliche Problematik des Sozialberichts ist in einer Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder eingehend erörtert worden. Dabei war insbesondere zu untersuchen, ob die Erhebung der im Sozialbericht festgehaltenen Daten des Betreuten in diesem Umfang erforderlich ist. Insoweit bestehende Zweifel konnten zwar — auch nach Anhörung der beratend hinzugezogenen Vertreter der Rentenversicherung — nicht völlig ausgeräumt werden; sie rechtfertigen jedoch nach dem derzeitigen Erkenntnisstand nicht, einen Verstoß gegen Vorschriften über den Datenschutz festzustellen.

Das Muster für die recht allgemein gehaltene Einverständniserklärung des Betreuten bedurfte allerdings der Überarbeitung. Es ist inhaltlich konkretisiert und durch aufklärende Hinweise auf die Rechtslage, insbesondere auf den Umfang der Mitwirkungspflicht des Leistungsberechtigten ergänzt worden.

Mir ist bekannt geworden, daß die Kassenärztlichen Vereinigungen in Fällen einer **Krebs-Früherkennungsuntersuchung** bei Frauen die Übersendung eines Untersuchungsvordrucks mit sämtlichen Eintragungen verlangen.

Nach Artikel 4 Abs. 2 der Landesverfassung bedarf das Anfordern einer mit sämtlichen Eintragungen einschließlich der Personalien des Versicherten versehenen Ausfertigung des Untersuchungsvordrucks durch die Kassenärztliche Vereinigung einer gesetzlichen Grundlage. Eine solche ist nicht ersichtlich. Die gemäß § 368 p Abs. 5 RVO vom Bundesausschuß der Ärzte und Krankenkassen beschlossenen Krebsfrüherkennungs-Richtlinien in der geänderten Fassung vom 26. April 1976 sehen zwar vor, daß der eine Teil des dreiteiligen Berichtsvordrucks nach abschließenden Eintragungen vom untersuchenden Arzt der zuständigen Kassenärztlichen Vereinigung zur Erfassung und Auswertung eingereicht wird. Diese Richtlinien sind jedoch keine Rechtsvorschrift.

Auch § 369 Abs. 2 RVO kommt als gesetzliche Grundlage nicht in Betracht. Nach dieser Vorschrift haben die Kassenärztlichen Vereinigungen die bei Durchführung von Maßnahmen zur Früherkennung von Krankheiten anfallenden Ergebnisse zu sammeln und auszuwerten; dabei ist sicherzustellen, daß Rückschlüsse auf die Person der Untersuchten

ausgeschlossen sind. Für die Sammlung und Auswertung der Untersuchungsergebnisse ist eine personenbezogene Erhebung nicht erforderlich. Es genügt, wenn der untersuchende Arzt die Ergebnisse anonymisiert an die Kassenärztliche Vereinigung weitergibt.

Unter diesen Umständen halte ich das Anfordern der Untersuchungsergebnisse mit den Personalien der Untersuchten durch die Kassenärztliche Vereinigung für unzulässig. Das gleiche gilt für die anschließende Speicherung der Daten in der als Datei (§ 2 Abs. 3 Nr. 3 DSG NW) anzusehenden Sammlung der Untersuchungsergebnisse, da die Speicherung eine rechtmäßige, also eine durch Gesetz zugelassene oder mit Einwilligung des Betroffenen vorgenommene Datenerhebung voraussetzt.

Mehrere **Eingaben** betrafen den Umgang mit personenbezogenen Daten bei Kassenärztlichen Vereinigungen und bei gesetzlichen Krankenkassen. Mitglieder einer Kassenzahnärztlichen Vereinigung sind mit der Frage an mich herangetreten, ob es den Datenschutzvorschriften entspricht, wenn sie von ihrer Vereinigung dazu angehalten werden, die Einwilligung zur Weitergabe personenbezogener Daten von RVO-Kassen angehörenden Patienten an zahntechnische Laboratorien bei den Betroffenen einzuholen.

Die Aufforderung, die Einwilligung der betroffenen Patienten zur Weitergabe ihrer Daten einzuholen, stellt keinen Umgang mit personenbezogenen Daten dar. Ihr stehen Datenschutzvorschriften nicht entgegen. Gleichwohl bin ich der Auffassung, daß diese Aufforderung gegen den Grundsatz der Verhältnismäßigkeit, der nach der Rechtsprechung des Bundesverfassungsgerichts übergreifende Leitregel allen staatlichen Handelns ist, verstößt und das Vertrauensverhältnis zwischen Arzt und Versicherten beeinträchtigen kann. Eine Weitergabe der personenbezogenen Daten des Versicherten durch den Arzt an das zahntechnische Labor ist nicht erforderlich. Es genügen vielmehr anonymisierte Zuordnungsmerkmale (z. B. eine Nummer), um das Abrechnungsverfahren mit den Krankenkassen durchzuführen.

Ich habe der Kassenzahnärztlichen Vereinigung daher empfohlen, ihre Mitglieder künftig nicht mehr zur Einholung der vorgesehenen Einverständniserklärung der Versicherten anzuhalten.

Eine Bürgerin hat sich dagegen gewandt, daß eine kassenzahnärztliche Vereinigung Behandlungsausweise, die von bestimmten Zahnärzten zur Abrechnung eingereicht werden, von Studenten fotokopieren läßt.

Bei meiner Prüfung habe ich festgestellt, daß das Fotokopieren von Abrechnungen zur rechtmäßigen Erfüllung der Aufgaben der Kassenzahnärztlichen Vereinigung nach § 368 n Abs. 1 RVO erforderlich ist. Denn nur auf diese Weise kann die Kassenzahnärztliche Vereinigung auch nach Versendung der Originale an die Krankenkassen diesen gegenüber auf Grund entsprechender Prüfung die Gewähr dafür übernehmen, daß die Einzelabrechnungen den gesetzlichen und vertraglichen Erfordernissen entsprechen.

Die zum Zwecke der Überprüfung gefertigten Fotokopien werden weder an Dritte weitergegeben, noch erhalten Dritte Kenntnis von deren Inhalt. Im übrigen werden alle Beschäftigten der Kassenzahnärztlichen Vereinigung nach § 5 Abs. 2 DSG NW auf das Datengeheimnis verpflichtet.

Allerdings müssen die in der Sammlung der Fotokopien gespeicherten personenbezogenen Daten nach Abschluß der Überprüfung und Auswertung zumindest gesperrt werden (§ 17 Abs. 2 Satz 2 DSG NW). Auf Antrag des Betroffenen sind sie durch Vernichtung der Fotokopien zu löschen (§ 17 Abs. 3 Satz 2 DSG NW).

Unabhängig davon habe ich der Kassenzahnärztlichen Vereinigung empfohlen, sämtliche Fotokopien nach Abschluß der Überprüfung und Auswertung auch ohne Antrag des Betroffenen zu vernichten.

Ein Bürger hat mich vor Inkrafttreten des Zehnten Buches des Sozialgesetzbuches um Auskunft gebeten, ob es gegen Vorschriften über den Datenschutz verstößt, wenn eine

Krankenkasse mit Hilfe eines Rechenzentrums eine sogenannte „Schuldnerdatei" aufbaut, in der ihre Mitglieder gespeichert werden, und diese Krankenkasse von dem Rechenzentrum Mitteilungen über An- oder Abmeldungen bei einer anderen, demselben Rechenzentrum angeschlossenen Kasse erhält.

Nach § 35 Abs. 1 Satz 1 SGB I a. F. hatte jeder Anspruch darauf, daß seine Geheimnisse, insbesondere die zum persönlichen Lebensbereich gehörenden Geheimnisse von den Leistungsträgern nicht unbefugt offenbart werden (Sozialgeheimnis). Die Tatsache der An- und Abmeldung bei einer gesetzlichen Krankenkasse war ein Geheimnis, die Bekanntgabe dieser Tatsache an eine andere Krankenkasse war eine Offenbarung im Sinne dieser Vorschrift.

Eine Offenbarung war nur dann nicht unbefugt, wenn der Betroffene zugestimmt hatte oder eine gesetzliche Mitteilungspflicht bestand (§ 35 Abs. 1 Satz 2 SGB I a. F.). Beide Voraussetzungen lagen in diesem Fall offensichtlich nicht vor.

Darüber hinaus ließ allerdings § 35 Abs. 2 SGB I a. F. die Amtshilfe unter den Leistungsträgern zu, soweit die ersuchende Stelle zur Erfüllung ihrer Aufgaben die geheimzuhaltende Tatsache kennen muß. Der Umstand, daß andere Krankenkassen offenbar ohne eine Schuldnerdatei auskommen, spricht gegen die Notwendigkeit der Kenntnis dieser Daten. Auf jeden Fall muß Amtshilfe nach herrschender Auffassung auf Ausnahmefälle beschränkt bleiben; sie setzt ein Ersuchen im Einzelfall voraus. Diese Voraussetzung fehlt, wenn die Krankenkasse von dem Rechenzentrum regelmäßig Listen mit dem Hinweis auf die An- oder Abmeldung bei anderen Krankenkassen erhält, ohne die Daten im Einzelfall bei diesen Kassen angefordert zu haben.

Allerdings hat sich die Rechtslage durch das Zehnte Buch des Sozialgesetzbuchs geändert. Nach § 69 Abs. 1 Nr. 1 SGB X ist eine Offenbarung zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach diesem Gesetzbuch durch einen Leistungsträger erforderlich ist. Diese Vorschrift ermöglicht, soweit die genannte sachliche Voraussetzung erfüllt ist, einen regelmäßigen Datenfluß zwischen Leistungsträgern. Das Erfordernis eines Amtshilfeersuchens im Einzelfall entfällt.

Ebenfalls noch vor Inkrafttreten der Neuregelung des Sozialdatenschutzes hat ein anderer Bürger bei mir angefragt, ob ein Sozialversicherungsträger der Polizei auf Ersuchen die Anschrift eines Versicherten sowie Name und Anschrift des Arbeitgebers bekanntgeben darf.

Sowohl Name und Anschrift in Verbindung mit dem Sozialversicherten-Status als auch Name und Anschrift des Arbeitgebers eines Sozialversicherten sind Geheimnisse im Sinne von § 35 Abs. 1 Satz 1 SGB I a. F. Nach meiner Auffassung, die vom Bundesminister für Arbeit und Sozialordnung geteilt wird, bestand gegenüber der Polizei zu dieser Zeit keine gesetzliche Mitteilungspflicht nach § 35 Abs. 1 Satz 2 SGB I a. F. Somit durfte ein Sozialversicherungsträger nach altem Recht die Anschrift eines Versicherten und Namen und Anschrift seines Arbeitgebers der Polizei nicht bekanntgeben.

Auch hier hat sich die Rechtslage mit dem Inkrafttreten des Zehnten Buches des Sozialgesetzbuchs geändert. Nach § 68 Abs. 1 Satz 1 SGB X sind im Rahmen der Amtshilfe Vor- und Familiennamen, Geburtsdatum, Geburtsort, derzeitige Anschrift des Betroffenen sowie Namen und Anschriften seines derzeitigen Arbeitgebers zu offenbaren, soweit kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Dies gilt auch gegenüber der Polizei. Die ersuchte Stelle ist jedoch zur Offenbarung dann nicht verpflichtet, wenn sich die ersuchende Behörde die Angaben auf andere Weise beschaffen kann (§ 68 Abs. 2 SGB X), wenn die ersuchte Stelle die Hilfe nur mit unverhältnismäßig großem Aufwand leisten könnte oder wenn sie unter Berücksichtigung der Aufgaben der ersuchenden Behörde durch die Hilfeleistung die Erfüllung der eigenen Aufgaben ernstlich gefährden würde (§ 4 Abs. 3 Nr. 2 und 3 SGB X).

In einem weiteren Fall hat sich ein Abiturient gegen die Übermittlung seines Namens, seiner Anschrift und der Zugehörigkeit zu einer bestimmten Altersgruppe an die AOK gewandt.

Die AOK hatte die bei ihr versicherten Eltern von Kindern, die voraussichtlich im Jahre 1980 aus der Schule entlassen wurden, zum Zwecke der Mitgliederwerbung angeschrieben. Vermutlich ist von einer der angeschriebenen Personen, die sich daraufhin gemeldet hatten, im Rahmen der üblichen Befragung nach weiteren bekannten Schulabgängern auch der Name und die Anschrift dieses Abiturienten genannt worden. Die auf diese Weise bekannt gewordenen Schulabgänger sind Anfang 1980 von der AOK ebenfalls angeschrieben worden.

Gegen diese Art der Datenerhebung habe ich gegenüber der AOK datenschutzrechtliche Bedenken geäußert. Ich habe darauf hingewiesen, daß jede Erhebung von Daten entweder einer gesetzlichen Grundlage oder der Einwilligung des Betroffenen bedarf. Eine gesetzliche Grundlage für die Erhebung von Daten bei Dritten zum Zwecke der Mitgliederwerbung ist nicht ersichtlich. Ich habe deshalb die AOK gebeten, von Fragen an Dritte über Namen und Anschriften von Schulabgängern abzusehen und die bisher auf diese Weise erhobenen Daten zu löschen, sofern nicht inzwischen eine Einwilligung des Betroffenen vorliegt.

c) Sozialhilfe

In der Öffentlichkeit hat folgender Fall Aufsehen erregt.

Das Sozialamt einer kreisfreien Stadt ist im Januar 1971 in ein neues Verwaltungsgebäude umgezogen und hat aus Raummangel einen Teil der Altakten weiter in dem nicht mehr genutzten Gebäude gelagert. Im Jahre 1979 wurde dieses alte Dienstgebäude verkauft. Vor Abbruch des Gebäudes durch den neuen Eigentümer wurde versäumt, die Altakten zu entfernen, so daß Teile davon beim Abbruch in die Hände Dritter gelangt sind.

Auf Grund meiner Ermittlungen habe ich gemäß § 30 Abs. 1 DSG NW festgestellt, daß die Stadt sowohl das Sozialgeheimnis (§ 35 Abs. 1 Satz 1 SGB I a. F.) als auch das Grundrecht der Betroffenen auf Datenschutz (Artikel 4 Abs. 2 der Landesverfassung) verletzt hat, indem sie es unterlassen hat, die erforderlichen Maßnahmen zu treffen, um einen Zugang Dritter zu Akten des Sozialamts mit Geheimnissen und anderen personenbezogenen Daten der Betroffenen zu verhindern.

Ich habe der Stadt Maßnahmen vorgeschlagen, um derartige Verstöße gegen den Datenschutz in Zukunft zu vermeiden. Diesen Empfehlungen ist der Oberstadtdirektor gefolgt, indem er die Allgemeine Dienstanweisung und die Aktenordnung entsprechend geändert hat.

Ein Arbeitgeber hat mich um datenschutzrechtliche Prüfung des von einer Gemeinde für die Einholung von Lohnauskünften verwendeten Fragebogens gebeten. Der Arbeitgeber wird unter anderem gefragt,

- ob der Arbeitnehmer eine Rente oder ein Ruhegeld bezieht;
- in welcher Krankenkasse er versichert ist;
- ob und wie lange die Arbeit wegen Krankheit, Arbeitsmangels oder aus einem anderen Grund unterbrochen worden ist;
- welche Lohnpfändungen vorliegen.

Meine Prüfung hat ergeben, daß insbesondere für diese Fragen eine gesetzliche Grundlage fehlt. Der Arbeitgeber ist nach § 116 Abs. 2 BSHG nur verpflichtet, dem Träger der Sozialhilfe über die Art und Dauer der Beschäftigung, die Arbeitsstätte und den Arbeitsverdienst der bei ihm beschäftigten Hilfesuchenden oder Hilfeempfänger, Unterhaltspflichtigen oder Kostenersatzpflichtigen Auskunft zu geben, soweit die Durchführung dieses Gesetzes es erfordert. Ich habe dem Oberstadtdirektor empfohlen, sich bei der Einholung von Lohnauskünften nach § 116 Abs. 2 BSHG auf Fragen zu beschränken, die durch die in dieser Vorschrift geregelte Auskunftspflicht des Arbeitgebers gedeckt sind. Gleichzeitig habe ich den Minister für Arbeit, Gesundheit und Soziales gebeten, bei den Gemeinden darauf hinzuwirken, daß künftig entsprechend verfahren wird.

Um Unterhaltsansprüche gegen den getrennt lebenden Ehemann geltend machen zu können, hat mich eine Bürgerin gebeten, ihr behilflich zu sein, in die Sozialhilfeakten des Sozialamtes Einsicht zu nehmen, die ihr von dort unter Berufung auf das Datenschutzgesetz verweigert worden war.

Zwar findet das Datenschutzgesetz Nordrhein-Westfalen in diesem Falle keine Anwendung, da es nur in Dateien gespeicherte personenbezogene Daten schützt (§ 1 Abs. 2 Satz 1 DSG NW), Akten aber keine Dateien sind (§ 2 Abs. 3 Nr. 3 DSG NW). Soweit die Akten Geheimnisse des Ehemannes enthalten, hätte die Einsichtgewährung jedoch gegen § 35 Abs. 1 Satz 1 SGB I a. F. verstoßen, weil weder der Betroffene zugestimmt hatte noch eine gesetzliche Mitteilungspflicht bestand.

Auch hier hat sich die Rechtslage durch das Zehnte Buch des Sozialgesetzbuches geändert. Nach § 74 SGB X ist eine Offenbarung zulässig, soweit sie für die Durchführung eines gerichtlichen Verfahrens wegen eines gesetzlichen oder vertraglichen Unterhaltsanspruchs (Nr. 1a) oder für die Geltendmachung eines solchen Anspruchs außerhalb eines gerichtlichen Verfahrens (Nr. 2a) erforderlich ist. In dem zuletzt genannten Fall setzt die Offenbarung allerdings voraus, daß der Betroffene nach den Vorschriften des bürgerlichen Rechts zur Auskunft verpflichtet ist und diese Pflicht innerhalb angemessener Frist, nachdem er unter Hinweis auf die Offenbarungsbefugnis des Leistungsträgers gemahnt wurde, nicht oder nicht vollständig erfüllt hat.

In einem weiteren Fall hat ein im Ausland lebender Bürger gerügt, daß ein Sozialamt seiner geschiedenen Ehefrau personenbezogene Daten offenbart hat, um ihr die Pfändung seiner Rente zur Durchsetzung ihres Unterhaltsanspruchs zu ermöglichen.

Die für eine Rentenpfändung erforderlichen personenbezogenen Daten waren Geheimnisse im Sinne von § 35 SGB I a. F. Der Betroffene hatte weder der Offenbarung gegenüber seiner geschiedenen Ehefrau zugestimmt, noch lag eine gesetzliche Mitteilungspflicht vor. Eine solche konnte insbesondere nicht aus dem gesetzlichen Auskunftsanspruch der geschiedenen Ehefrau gegenüber dem geschiedenen Ehemann (§ 1580 in Verbindung mit § 1605 BGB) hergeleitet werden. Entgegen der Ansicht des Oberstadtdirektors ergab sich eine Befugnis zur Offenbarung auch nicht aus dem Gedanken des rechtfertigenden Notstandes (§ 34 StGB). Dabei konnte die Frage, ob über die Regelung in § 35 Abs. 1 Satz 2 SGB I a. F. hinaus eine Offenbarungsbefugnis auch in Fällen des rechtfertigenden Notstandes anzunehmen war, dahingestellt bleiben. Auf jeden Fall hätte eine derartige Durchbrechung des Sozialgeheimnisses vorausgesetzt, daß das zu schützende Rechtsgut einen wesentlich höheren Rang als das Sozialgeheimnis hat. Diese Voraussetzung lag hier nicht vor. Eine Durchbrechung des Sozialgeheimnisses mag bei einer anders nicht abwendbaren Gefahr für Leib, Leben oder Freiheit gerechtfertigt sein. Das Interesse an der Durchsetzung von Unterhaltsansprüchen oder an der Entlastung des Haushalts des Sozialleistungsträgers rechtfertigt sie jedenfalls nicht.

Die Offenbarung der für die Rentenpfändung erforderlichen personenbezogenen Daten war somit unbefugt und verstieß deshalb gegen § 35 Abs. 1 Satz 1 SGB I a. F. Im Hinblick darauf, daß dieser Verstoß schon längere Zeit zurücklag und damals noch Unklarheit hinsichtlich der Tragweite der Vorschrift über das Sozialgeheimnis bestand, habe ich von einer Beanstandung nach § 30 DSG NW abgesehen, den Leistungsträger jedoch zugleich gebeten, durch das Sozialgeheimnis geschützte personenbezogene Daten künftig zur Durchsetzung von Unterhaltsansprüchen nur unter den Voraussetzungen des § 74 SGB X zu offenbaren.

Nach dieser Vorschrift ist seit dem 1. Januar 1981 eine Offenbarung zulässig, soweit sie für die Durchführung eines Vollstreckungsverfahrens wegen eines gesetzlichen oder vertraglichen Unterhaltsanspruchs erforderlich ist. Ich habe Zweifel, ob diese Voraussetzung bei der Offenbarung der für die Rentenpfändung erforderlichen Daten vorgelegen hätte. Dem Sozialamt dürfte es möglich gewesen sein, die Unterhaltsansprüche der geschiedenen Ehefrau nach bewirktem Rechtsübergang gemäß §§ 90, 91 BSHG durch Rentenpfändung bei der Bundesversicherungsanstalt für Angestellte selbst durchzusetzen,

ohne personenbezogene Daten des geschiedenen Ehemannes gegenüber der geschiedenen Ehefrau zu offenbaren.

Ein Träger der freien Wohlfahrtspflege hat mich darauf aufmerksam gemacht, daß Sozialhilfeempfängern, die einen Antrag auf Bekleidungsbeihilfe stellen, von einem Sozialamt nahegelegt wurde, ihren Bedarf zunächst bei der Kleidersammelstelle des Deutschen Roten Kreuzes zu decken. Die Kleidersammelstelle erhielt Durchschrift dieses Bescheides sowie den Antrag selbst.

Dieses Verfahren verstieß gegen § 35 Abs. 1 Satz 1 SGB I a. F. Zwar sind Name und Anschrift allein in der Regel keine Geheimnisse im Sinne dieser Vorschrift. Unstreitig ist aber die Tatsache, daß eine bestimmte Person Sozialhilfe empfängt oder beantragt, ein solches Geheimnis. Da durch das Gebot der Zusammenarbeit zwischen den Sozialhilfeträgern und den Trägern der freien Wohlfahrtspflege (§ 28 Abs. 2 Halbsatz 2 SGB I) eine gesetzliche Mitteilungspflicht nicht begründet wurde, hätten Durchschriften des Antrages auf Bekleidungsbeihilfe und des auf die Kleidersammelstellen hinweisenden Bescheides nur mit Zustimmung des Antragstellers an das Deutsche Rote Kreuz übersandt werden dürfen.

Ich halte es auch für bedenklich, stattdessen vom Antragsteller nach § 60 Abs. 1 Nr. 1 SGB I eine Bestätigung des Deutschen Roten Kreuzes zu verlangen, daß der Bekleidungsbedarf von der Kleidersammelstelle nicht gedeckt werden konnte. Eine Mitwirkungspflicht des Antragstellers besteht nach § 65 Abs. 1 Nr. 2 SGB I nicht, wenn ihre Erfüllung dem Betroffenen aus einem wichtigen Grund nicht zugemutet werden kann. Ein solcher wichtiger Grund ist meines Erachtens die Preisgabe eines Sozialgeheimnisses einem Dritten gegenüber. Der Antragsteller kommt in dieser Situation nicht umhin, die Tatsache, hilfsbedürftig zu sein, gegenüber dem Deutschen Roten Kreuz preiszugeben.

Ein Oberstadtdirektor hat vor der Neufassung des § 35 SGB I die Frage an mich herangetragen, ob einer Steuerfahndungsstelle zur Einleitung eines Strafverfahrens wegen Steuerhinterziehung Auskunft aus bzw. Einsicht in Sozialhilfeakten gewährt werden darf. Ich bin damals zu dem Ergebnis gekommen, daß im Bereich der Abgabenordnung das Sozialgeheimnis lediglich durch eine durch den verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz begrenzte Anzeigepflicht nach § 116 Abs. 1 AO sowie durch eine ebenso begrenzte Auskunftspflicht nach § 93 Abs. 1 Satz 2 AO durchbrochen wird. Der Gesetzgeber ist dieser Auffassung jedoch nicht gefolgt, sondern hat eine Offenbarung personenbezogener Daten zur Durchführung der Besteuerung auch durch Vorlage von Urkunden und Akten nach § 97 AO zugelassen (§ 71 Nr. 3 SGB X).

d) Ausbildungsförderung

Zahlreiche Eingaben betrafen datenschutzrechtliche Fragen aus dem Bereich der Ausbildungsförderung nach dem Bundesausbildungsförderungsgesetz. Mehrere Eltern von Auszubildenden haben sich besorgt darüber geäußert, daß das Amt für Ausbildungsförderung von ihnen Auskunft über ihre Einkommens- und Vermögensverhältnisse verlangt. Sie wollten insbesondere wissen, was mit ihren persönlichen Daten geschieht und wem sie zugänglich gemacht werden.

Ein Bürger, der seiner in der Ausbildung befindlichen Tochter nach seinen Angaben monatlich Unterhalt in einer Höhe zahlt, die eine zusätzliche Förderung nach dem Bundesausbildungsförderungsgesetz ausschließt, war unter Festsetzung eines Zwangsgeldes aufgefordert worden, Auskunft über seine Einkommens- und Vermögensverhältnisse zu erteilen. Er wollte wissen, ob er dieser Aufforderung nachkommen muß.

Gesetzliche Grundlage für das Anfordern einer Einkommenserklärung der Eltern eines Antragstellers nach dem Bundesausbildungsförderungsgesetz ist § 47 Abs. 4 BAföG in Verbindung mit § 60 Abs. 1 Nr. 1 SGB I. Nach § 60 Abs. 1 Nr. 1 SGB I hat derjenige, der Sozialleistungen beantragt, alle Tatsachen anzugeben, die für die Leistung erheblich sind. Nach § 47 Abs. 4 BAföG gilt dies auch für die Eltern eines Auszubildenden, der Ausbil-

dungsförderung beantragt hat. Das Einkommen der Eltern ist für die Gewährung von Ausbildungsförderung erheblich, da es nach § 11 Abs. 2 BAföG auf den Bedarf anzurechnen ist.

Ich habe dem Betroffenen mitgeteilt, daß er grundsätzlich verpflichtet ist, die geforderte Einkommenserklärung abzugeben. Diese Verpflichtung entfällt allerdings dann, wenn ihre Erfüllung nicht in einem angemessenen Verhältnis zu der in Anspruch genommenen Sozialleistung steht (§ 65 Abs. 1 Nr. 1 SGB I). Diese Voraussetzung dürfte vorliegen, wenn der Antrag auf Ausbildungsförderung bereits aus anderen Gründen abzulehnen ist. Hängt dagegen die Entscheidung über den Antrag von der Höhe seines Einkommens ab, so ist der Betroffene zur Abgabe einer Einkommenserklärung verpflichtet. Die Erfüllung dieser Verpflichtung erscheint weder unzumutbar (§ 65 Abs. 1 Nr. 2 SGB I), noch kann das Amt für Ausbildungsförderung sich die erforderlichen Kenntnisse durch einen geringeren Aufwand selbst beschaffen (§ 65 Abs. 1 Nr. 3 SGB I).

Die auf Grund der Auskunftspflicht nach § 47 Abs. 4 BAföG dem Amt für Ausbildungsförderung erteilten Auskünfte werden jedoch grundsätzlich nicht an Dritte weitergegeben. Sie unterliegen dem Sozialgeheimnis (§ 35 Abs. 1 SGB I) und dürfen somit von den Leistungsträgern nicht unbefugt offenbart werden. Ihre unbefugte Offenbarung ist nach § 203 StGB strafbar.

Allerdings sind nach § 55 Abs. 2 Nr. 3 BAföG für jeden geförderten Auszubildenden im Rahmen der jährlichen Bundesstatistik bestimmte Daten der Eltern zu erfassen. Sie werden ohne Angabe des Namens an das Landesamt für Datenverarbeitung und Statistik weitergegeben und gelangen von dort an das Statistische Bundesamt. Durch die Anonymisierung sind keinerlei Rückschlüsse auf die Identität des geförderten Auszubildenden und der Eltern möglich.

Einige Eltern sehen bereits in der Tatsache, daß ihre persönlichen Einkommens- und Vermögensverhältnisse dem Auszubildenden zur Kenntnis gelangen, einen Eingriff in ihre Privatsphäre. So hat sich ein Vater bei mir darüber beklagt, daß das Amt für Ausbildungsförderung auf seine Anträge ergangene Bescheide nicht an ihn selbst, sondern an seinen Sohn gerichtet und diesem dadurch die Tatsache einer Darlehnsaufnahme sowie die Verschlechterung seiner Einkommensverhältnisse offenbart hat.

Sowohl die Darlehnsaufnahme als auch die Verschlechterung der Einkommensverhältnisse sind Geheimnisse im Sinne von § 35 SGB I a. F. Der Betroffene hatte weder der Offenbarung gegenüber seinem Sohn zugestimmt noch lag eine gesetzliche Mitteilungspflicht vor. Insbesondere kann eine solche nicht aus den Vorschriften des Bundesausbildungsförderungsgesetzes hergeleitet werden. Die Offenbarung dieser Geheimnisse war somit unbefugt und verstieß deshalb gegen § 35 Abs. 1 Satz 1 SGB I a. F. und gegen Artikel 4 Abs. 2 Satz 1 der Landesverfassung.

Zur Wahrung des Sozialgeheimnisses wie auch nach allgemeinen Verfahrensgrundsätzen hätten die Bescheide auf die Anträge des Vaters nicht an den Sohn, sondern nur an den Vater gerichtet werden dürfen. Wenn nach den Vorschriften des Bundesausbildungsförderungsgesetzes eine Entscheidung nur gegenüber dem Auszubildenden möglich war, hätten die Anträge des Vaters als unzulässig abgelehnt werden müssen, ohne dem Sohn die Tatsache der Antragstellung und die Begründung der Anträge mitzuteilen.

Im Hinblick darauf, daß die Bescheide fast ein Jahr zurücklagen und seinerzeit möglicherweise noch Unsicherheit hinsichtlich der Tragweite der Vorschrift über das Sozialgeheimnis und des Grundrechts auf Datenschutz bestand, habe ich von einer Beanstandung nach § 30 DSG NW abgesehen.

Eine Bürgerin, deren Sohn in einem anderen Bundesland Ausbildungsförderung nach dem Bundesausbildungsförderungsgesetz beantragt hatte, teilte mir mit, sie sei von diesem Amt aufgefordert worden, einen Bescheid über den Lohnsteuer-Jahresausgleich vorzulegen. Dieser Bescheid enthalte aber auch Angaben über die Einkommensverhält-

nisse ihres Ehemannes (und Stiefvaters des Auszubildenden). Da einerseits ihr Ehemann einer Weitergabe seiner personenbezogenen Daten nicht zustimme, andererseits das zuständige Finanzamt die Fertigung eines Auszuges aus dem Bescheid mit den nur sie betreffenden Angaben ablehne, sei sie nicht in der Lage, die geforderten Angaben zu erbringen.

Meine Ermittlungen bei dem meiner Kontrolle unterliegenden Finanzamt haben ergeben, daß im Wege der Amtshilfe dem Amt für Ausbildungsförderung Angaben über die steuerlichen Verhältnisse des Stiefvaters weitergegeben worden sind. Dies war datenschutzrechtlich nicht zulässig.

Nach § 47 Abs. 3 BAföG (ab 1. Januar 1981: § 21 Abs. 4 SGB X) haben die Finanzbehörden dem Amt für Ausbildungsförderung Auskünfte über die Einkommens- und Vermögensverhältnisse des Auszubildenden, seiner Eltern und seines Ehegatten zu erteilen, soweit die Durchführung dieses Gesetz es erfordert. Der Ehemann, dessen Einkommensverhältnisse aus dem gemeinsamen Bescheid über den Lohnsteuer-Jahresausgleich ersichtlich sind, gehört als Stiefvater des Antragstellers nicht zu dem in § 47 Abs. 3 BAföG genannten Personenkreis. Demnach hätte das Finanzamt die steuerlichen Verhältnisse des Ehemannes nicht offenbaren dürfen. Wie mir der Finanzminister hierzu mitgeteilt hat, wird das Finanzamt dies künftig beachten.

Mehrere bei einer Stadtverwaltung als Honorarkräfte beschäftigte Studenten haben mir mitgeteilt, daß ihre Namen, Anschriften und Einkommen einem bestimmten Amt für Ausbildungsförderung weitergegeben worden seien, obwohl weder eine Auskunftspflicht bestanden noch ein Auskunftsersuchen vorgelegen habe. Sie seien auch nicht über die Weitergabe der Daten unterrichtet worden. Von der Weitergabe der Daten seien auch Studenten betroffen, deren Ausbildung nicht gefördert werde oder für deren Ausbildungsförderung ein anderes Amt zuständig sei.

Die Stadt darf nach § 3 Abs. 1 DSG NW personenbezogene Daten, also auch Namen, Anschriften und Einkommen, nur dann an Dritte übermitteln, wenn das Datenschutzgesetz Nordrhein-Westfalen oder eine andere Rechtsvorschrift es erlaubt oder der Betroffene eingewilligt hat. § 47 Abs. 5 BAföG verpflichtet den Arbeitgeber, dem Amt für Ausbildungsförderung auf Verlangen eine Bescheinigung über den Arbeitslohn und den auf der Lohnsteuerkarte eingetragenen steuerfreien Jahresbetrag auszustellen, soweit dies zur Durchführung des Bundesausbildungsförderungsgesetzes erforderlich ist. Diese Voraussetzung lag hier nicht vor, da das Amt für Ausbildungsförderung die Bescheinigung nicht verlangt hatte.

Die Vorschrift des Datenschutzgesetzes Nordrhein-Westfalen, die die Übermittlung personenbezogener Daten zuläßt, wenn diese zur rechtmäßigen Erfüllung der Aufgaben des Empfängers erforderlich ist (§ 11 Abs. 1 DSG NW), kam hier als Rechtsgrundlage für die Übermittlung nicht in Betracht, weil sie durch die bundesrechtliche Vorschrift des § 47 Abs. 5 BAföG verdrängt wird. Sie hätte im übrigen — ebenso wie § 47 Abs. 5 BAföG — eine Übermittlung nur auf Ersuchen zugelassen.

Ich habe diesen Verstoß gegen § 3 Satz 1 DSG NW gemäß § 30 Abs. 1 Satz 1 DSG NW beanstandet. Zur Vermeidung künftiger Verstöße habe ich die Stadt gebeten, Namen, Anschriften und Einkommen von Aushilfskräften dem Amt für Ausbildungsförderung nur noch dann bekanntzugeben, wenn dieses nach § 47 Abs. 5 BAföG eine entsprechende Bescheinigung für einen Auszubildenden, der einen Antrag auf Ausbildungsförderung gestellt hat, verlangt.

Durch die Eingabe eines anderen Studenten habe ich erfahren, daß die Medizinischen Einrichtungen einer Universität dem zuständigen Studentenwerk die Höhe der Vergütung von studentischen Aushilfskräften ohne Ersuchen im Einzelfall und unabhängig davon melden, ob die Studierenden einen Antrag auf Ausbildungsförderung gestellt haben. Die studentischen Aushilfskräfte haben die Kenntnis folgender Erklärung schriftlich zu bestätigen.

„Das zuständige Studentenwerk erhält am Ende eines Kalenderjahres eine Aufstellung über die gesamte Vergütung aus jeglicher Aushilfstätigkeit (mit Namen, Geburtstag und Matrikelnummer)."

Diese Praxis verstößt gegen § 3 Satz 1 DSG NW, da weder das Datenschutzgesetz Nordrhein-Westfalen noch eine andere Rechtsvorschrift die Übermittlung der genannten Daten an das Studentenwerk erlaubt noch eine Einwilligung des Betroffenen eingeholt wird. Die Einwilligung des Betroffenen in die Weitergabe seiner personenbezogenen Daten an das Studentenwerk wird nicht dadurch ersetzt, daß er schriftlich bestätigt, über die Weitergabe informiert worden zu sein.

Als Rechtsgrundlage für die Übermittlung kommt weder § 47 Abs. 5 BAföG noch § 11 Abs. 1 Satz 1 DSG NW in Betracht.

§ 47 Abs. 5 BAföG verpflichtet den Arbeitgeber, dem Amt für Ausbildungsförderung auf Verlangen eine Bescheinigung über den Arbeitslohn und den auf der Lohnsteuerkarte eingetragenen steuerfreien Jahresbetrag auszustellen, soweit dies zur Durchführung des Bundesausbildungsförderungsgesetzes erforderlich ist. Diese Voraussetzung lag hier nicht vor, da der Betroffene keinen Antrag auf Ausbildungsförderung gestellt hatte.

Die Übermittlungsvorschrift des § 11 Abs. 1 Satz 1 DSG NW scheidet als Rechtsgrundlage aus, weil sie durch die bundesrechtliche Vorschrift des § 47 Abs. 5 BAföG verdrängt wird. Sie würde im übrigen eine Übermittlung nur zulassen, wenn eine Prüfung im Einzelfall ergibt, daß die Kenntnis der angeforderten Daten, bezogen auf eine bestimmte Person, zur Aufgabenerfüllung erforderlich ist. Eine Übermittlung „auf Vorrat" für den Fall, daß die Daten später einmal zur Erfüllung einer Aufgabe gebraucht werden könnten, wäre nach dieser Vorschrift unzulässig.

Ich habe die Medizinischen Einrichtungen der Universität auf die Rechtslage hingewiesen und gebeten, zur Vermeidung von Verstößen gegen Vorschriften über den Datenschutz die Vergütung von Aushilfskräften dem Studentenwerk nur noch dann bekanntzugeben, wenn dieses nach § 47 Abs. 5 BAföG eine entsprechende Bescheinigung für einen Auszubildenden, der einen Antrag auf Ausbildungsförderung gestellt hat, verlangt.

Da die von dem Betroffenen zu Recht beanstandete Praxis auch an anderen Hochschulen zu bestehen scheint, habe ich die Angelegenheit auch gegenüber dem Minister für Wissenschaft und Forschung aufgegriffen. Dieser hat mir inzwischen mitgeteilt, daß das von ihm durch Erlaß eingeführte Muster für einen Dienstvertrag mit wissenschaftlichen/studentischen Hilfskräften folgende Klausel enthält:

„Die wissenschaftliche/studentische Hilfskraft ist damit einverstanden, daß das zuständige Studentenwerk über das Beschäftigungsverhältnis, dessen Dauer und die Höhe der Vergütung unterrichtet wird."

Gegen eine derartige Einwilligungserklärung, von der der Abschluß eines Dienstvertrages abhängig gemacht wird, habe ich Bedenken. Zwar bestimmt § 3 DSG NW nicht ausdrücklich, daß dem Betroffenen aus einer Verweigerung der Einwilligung keine Rechtsnachteile entstehen dürfen. Nach dem Grundgedanken dieser Vorschrift soll der Betroffene jedoch über die Verarbeitung seiner personenbezogenen Daten frei entscheiden können, soweit nicht ein gesetzlicher Erlaubnistatbestand für die Verarbeitung vorliegt. Mit diesem Grundgedanken ist das in dem Erlaß vorgesehene Verfahren nicht vereinbar. Die Einwilligung in die Übermittlung der genannten Daten an das Studentenwerk könnte nach meiner Auffassung allenfalls dann verlangt werden, wenn die Übermittlung in einem sachlichen Zusammenhang mit dem Vertragsverhältnis stünde. Diese Voraussetzung liegt hier jedoch nicht vor, da die Übermittlung allein der Überprüfung der Inanspruchnahme von Ausbildungsförderung dient.

Darüber hinaus wird mit einer solchen vertraglichen Vereinbarung die gesetzliche Übermittlungsregelung in § 47 Abs. 5 BAföG umgangen. Der Gesetzgeber hat in dieser Vorschrift Auskünfte des Arbeitgebers an das Amt für Ausbildungsförderung von bestimmten

Voraussetzungen abhängig gemacht. Es muß davon ausgegangen werden, daß damit nach dem objektiven Willen des Gesetzes ein anderes Verfahren für die Übermittlung solcher Angaben ausgeschlossen wird.

Schließlich verstößt das vorgesehene Verfahren auch gegen den verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz, da die Einwilligungserklärung von allen Hilfskräften verlangt wird, obwohl nur ein Teil Ausbildungsförderung in Anspruch nimmt.

Ein staatliches Prüfungsamt für Erste Staatsprüfungen für Lehrämter an Schulen hat bei mir angefragt, ob dem Amt für Ausbildungsförderung Auskunft über Prüfungstermine von Studenten ohne deren Zustimmung erteilt werden darf.

Gesetzliche Grundlage für das Auskunftersuchen des Amtes für Ausbildungsförderung ist § 47 Abs. 2 in Verbindung mit §§ 15 Abs. 2, 15a Abs. 3 BAföG. Nach § 47 Abs. 2 BAföG hat die Ausbildungsstätte dem Amt für Ausbildungsförderung auf Verlangen alle zur Durchführung des Bundesausbildungsförderungsgesetzes erforderlichen Auskünfte zu erteilen. Nach §§ 15 Abs. 2, 15a Abs. 3 BAföG ist bei der Hochschulausbildung für die Beendigung der Ausbildungsförderung der Zeitpunkt des letzten Prüfungsteils maßgebend. Da dieser Zeitpunkt aus dem Zeugnis des staatlichen Prüfungsamtes nicht zu entnehmen ist, muß er dem Amt für Ausbildungsförderung zusätzlich nachgewiesen werden. Hiernach ist das staatliche Prüfungsamt gesetzlich verpflichtet, die verlangte Auskunft zu erteilen. Einer Einwilligung bedarf es insoweit nicht.

e) Jugendwesen

Im Zusammenhang mit der Jahreserhebung der Erziehungsberatungsstellen (vgl. C. 9. c meines ersten Tätigkeitsberichts) hat mich der Minister für Arbeit, Gesundheit und Soziales um Stellungnahme gebeten, ob der Klient vor der Erhebung seiner personenbezogenen Daten durch die Erziehungsberatungsstelle darauf hingewiesen werden muß, daß ein Teil dieser Daten in anonymisierter Form für statistische Zwecke an den Landschaftsverband weitergegeben wird.

Bei den in der Erziehungsberatungsstelle von dem Klienten erfragten Angaben handelt es sich um personenbezogene Daten (§ 2 Abs. 1 DSG NW). Ihre Erhebung ist nach § 10 Abs. 2 DSG NW nur zulässig, wenn der Betroffene auf die zugrunde liegende Rechtsvorschrift oder auf die Freiwilligkeit seiner Angaben hingewiesen worden ist.

Die Hinweispflicht dient dem Schutz des Betroffenen durch Aufklärung über seine Rechtspflichten. Dieser Schutzzweck wird nur erreicht, wenn der Hinweis auf die Rechtslage **vor** der Erhebung, spätestens aber bei ihrem Beginn erfolgt. Dabei sollte dem Betroffenen zugleich die vorgesehene Nutzung seiner Angaben erläutert werden. Es empfiehlt sich, ihm eindeutig zu erklären, was mit seinen Daten geschehen wird, wie sie verarbeitet werden (personenbezogen oder anonymisiert) und welchem Verwendungszweck sie dienen werden. Nur auf Grund einer solchen umfassenden Unterrichtung ist der Betroffene in der Lage, sich frei zu entscheiden, ob er die von ihm erfragten Angaben machen will.

Soweit die erfragten Angaben nicht oder nicht nur für die Jahreserhebung, sondern allein oder auch für die Durchführung der Erziehungsberatung benötigt werden, muß der Betroffene nach § 10 Abs. 2 DSG NW wie auch nach § 66 Abs. 3 SGB I auf seine Mitwirkungspflicht (§ 60 Abs. 1 Nr. 1 SGB I) und die Folgen ihrer Nichterfüllung (§ 66 Abs. 1 SGB I) hingewiesen werden. Soweit die erfragten Angaben nur für die Jahreserhebung benötigt werden, ist der Betroffene nach § 10 Abs. 2 DSG NW auf die Freiwilligkeit hinzuweisen. Bei sämtlichen für die Jahreserhebung benötigten Daten, mögen sie auf Grund der Mitwirkungspflicht oder auf freiwilliger Grundlage erhoben werden, muß der Betroffene darüber unterrichtet werden, daß sie in anonymisierter Form für statistische Zwecke an den Landschaftsverband weitergegeben werden.

In einem anderen Fall hat mich der Minister für Arbeit, Gesundheit und Soziales um Prüfung gebeten, ob die Einwohnermeldeämter und die Standesämter die Anschriften der

Eltern erstgeborener Kinder an das Kreisjugendamt weitergeben dürfen, damit ihnen von dort regelmäßig Elternbriefe zugesandt werden können.

Die Übermittlung der Namen und Anschriften junger Eltern durch das Einwohnermeldeamt an das Kreisjugendamt ist zulässig, da sie zur rechtmäßigen Erfüllung von Aufgaben dieses Amtes erforderlich ist (§ 11 Abs. 1 DSG NW). Nach § 5 Abs. 1 Nr. 1 JWG ist es Aufgabe des Jugendamtes, die für die Wohlfahrt der Jugend erforderlichen Einrichtungen und Veranstaltungen anzuregen, zu fördern und gegebenenfalls zu schaffen, insbesondere auch für die Beratung in Fragen der Erziehung. Diesem Zweck dient auch die Zusendung von Elternbriefen. Diese ist aber nur möglich, wenn das Jugendamt die Namen und Anschriften der Eltern erstgeborener Kinder kennt.

Entsprechendes gilt für die Weitergabe dieser Daten durch das Einwohnermeldeamt an das Jugendamt derselben Gemeinde (§ 8 Satz 1 in Verbindung mit § 11 Abs. 1 DSG NW).

Rechtsgrundlage für die Weitergabe der Namen und Anschriften durch das Standesamt ist § 61 Abs. 1 PStG, der als Bundesrecht nach Artikel 31 GG den Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen vorgeht. Hiernach ist die Einsicht in und damit die Erteilung von Auskünften aus Personenstandsbüchern an das Jugendamt zulässig, sofern dieses im Rahmen seiner Zuständigkeit darum ersucht (§ 61 Abs. 1 Satz 1 PStG) und den Zweck des Ersuchens angibt (§ 61 Abs. 1 Satz 2 PStG).

Als Mitglied eines nach dem Kindergartengesetz gewählten Elternrates eines kommunalen Kindergartens hat sich eine Bürgerin an mich gewandt, die für vom Kindergarten weiter entfernt wohnende Kinder einen privaten Zubringerdienst organisieren wollte und dafür die Anschriften der entsprechenden Eltern von der Stadtverwaltung erbeten hatte. Diese hatte die Bekanntgabe der Anschriften unter Hinweis auf das Datenschutzgesetz abgelehnt.

Aus datenschutzrechtlicher Sicht bestehen jedoch gegen die Weitergabe der Anschriften an den Elternrat keine Bedenken. Diese Weitergabe ist zwar keine Übermittlung im Sinne des Datenschutzgesetzes, weil der kommunale Kindergarten kein Dritter ist (§ 2 Abs. 2 Nr. 2, Abs. 3 Nr. 2 DSG NW). Die Stadt hat aber für die Beachtung der Grundsätze über die Zulässigkeit der Übermittlung (§ 11 Abs. 1 DSG NW) auch dann zu sorgen, wenn Daten von einer Stelle der Stadt an eine andere weitergegeben werden (§ 8 Satz 1 DSG NW). Danach muß die Weitergabe zur rechtmäßigen Erfüllung einer in der Zuständigkeit des Elternrates liegenden Aufgabe erforderlich sein. Diese Voraussetzung liegt hier vor. Nach § 3 Satz 2 des Kindergartengesetzes hat der Elternrat unter anderem die Aufgabe, die Zusammenarbeit zwischen den Erziehungsberechtigten zu fördern. Um diese Aufgabe wirksam erfüllen zu können, muß der Elternrat die Möglichkeit haben, die Erziehungsberechtigten gezielt anzusprechen. Hierzu ist es erforderlich, daß dem Elternrat die Erziehungsberechtigten mit Namen und Anschriften bekannt sind.

f) Entscheidung über Offenbarungsersuchen nach dem Sozialgesetzbuch

Über Offenbarungsersuchen im Rahmen der Amtshilfe entscheidet der Leiter der ersuchten Stelle, sein allgemeiner Stellvertreter oder ein besonders bevollmächtigter Bediensteter (§ 68 Abs. 2 SGB X). Über Offenbarungsersuchen für den Schutz der inneren und äußeren Sicherheit entscheidet bei der ersuchten Stelle der Behördenleiter oder sein allgemeiner Stellvertreter (§ 72 Abs. 2 Satz 3 SGB X). Zur Auslegung der Begriffe „Leiter der ersuchten Stelle" in § 68 Abs. 2 SGB X und „Behördenleiter" in § 72 Abs. 2 Satz 3 SGB X habe ich auf ein Beratungsersuchen einer Gemeinde wie folgt Stellung genommen.

Das Zehnte Sozialgesetzbuch verwendet in den Amtshilfevorschriften des Zweiten Kapitels — anders als in den Amtshilfevorschriften der §§ 3 ff. — anstelle des Begriffs „Behörde" den Begriff „Stelle". Bei der Auslegung der Begriffe „Leiter der ersuchten Stelle" in § 68 Abs. 2 SGB X und „Behördenleiter" in § 72 Abs. 2 Satz 3 SGB X ist von § 35 Abs. 1

SGB I auszugehen. Die §§ 68 ff. SGB X sind, indem sie Offenbarungsbefugnisse regeln, lediglich Ausnahmen von dem in § 35 Abs. 1 SGB I enthaltenen Geheimhaltungsgebot. Daraus folgt, daß der in der Grundnorm des § 35 Abs. 1 SGB I bestimmte Kreis der Adressaten des Geheimhaltungsgebots identisch ist mit dem Kreis der nach §§ 68 ff. SGB X Offenbarungsberechtigten. „Ersuchte Stelle" im Sinne von § 68 Abs. 2 und § 72 Abs. 2 Satz 3 SGB X kann demnach nur eine in § 35 SGB I genannte Stelle sein. Adressat des Geheimhaltungsgebots nach § 35 Abs. 1 Satz 1 SGB I und damit „ersuchte Stelle" im Sinne der §§ 68 Abs. 2, 72 Abs. 2 Satz 3 SGB X ist der jeweilige Leistungsträger (§ 12 SGB I). Dies ist immer die Gemeinde, der Kreis, der Landschaftsverband, nicht das Sozialamt, das Jugendamt, die Wohngeldstelle usw.

Folglich ist ungeachtet des unterschiedlichen Wortlauts — „Leiter" (§ 68 Abs. 2), „Behördenleiter" (§ 72 Abs. 2 Satz 3) — in beiden Amtshilfefällen der Hauptverwaltungsbeamte des jeweiligen Leistungsträgers zur Entscheidung berufen. In den Fällen des § 68 SGB X kann die Entscheidung auch durch einen von dem Hauptverwaltungsbeamten besonders bevollmächtigten Bediensteten getroffen werden.

13. Gesundheitswesen

a) Einschulungsuntersuchungen

Durch den Minister für Arbeit, Gesundheit und Soziales ist mir bekannt geworden, daß verschiedene Gesundheitsämter des Landes Nordrhein-Westfalen den vom Institut für Dokumentation und Information über Sozialmedizin und öffentliches Gesundheitswesen (IDIS) in Bielefeld herausgegebenen Elternfragebogen „Angaben für den Schularzt zur Einschulungsuntersuchung" verwenden und diesen zusammen mit einem Anschreiben den Erziehungsberechtigten übersenden. Ich prüfe zur Zeit, ob die Betroffenen vor der mit dem Fragebogen vorgenommenen Erhebung personenbezogener Daten auf die entsprechenden Rechtsvorschriften oder auf die Freiwilligkeit der Angaben ausreichend hingewiesen werden (§ 10 Abs. 2 DSG NW).

b) Krankenhäuser

Von einem Bürger ist die Frage an mich herangetragen worden, ob die Weitergabe personenbezogener Daten von der Verwaltung eines Krankenhauses an andere Abteilungen (z. B. Labor) innerhalb des Krankenhauses zulässig ist. Ich bin davon ausgegangen, daß diese Sammlung personenbezogener Daten eine Datei im Sinne des § 2 Abs. 3 Nr. 3 DSG NW ist und habe zur Zulässigkeit der Weitergabe wie folgt Stellung genommen.

Nach § 8 Satz 1 in Verbindung mit § 11 Abs. 1 Satz 1 DSG NW dürfen personenbezogene Daten auch innerhalb derselben öffentlichen Stelle nur dann weitergegeben werden, wenn dies zur rechtmäßigen Erfüllung der in der Zuständigkeit der weitergebenden Abteilung oder des Empfängers liegenden Aufgabe erforderlich ist.

An die Erforderlichkeit ist im Interesse des Datenschutzes ein strenger Maßstab zu legen. Danach dürfen nur solche Daten weitergegeben werden, deren Kenntnis notwendig ist, um den angestrebten Zweck zu erreichen. Es ist daher nicht erforderlich und mithin unzulässig, alle bei der Einlieferung in das Krankenhaus erhobenen personenbezogenen Daten an die einzelnen Abteilungen des Krankenhauses weiterzugeben. Es dürfen nur diejenigen Daten innerhalb des Krankenhauses weitergegeben werden, die der jeweilige Empfänger zur Erledigung der in seiner Zuständigkeit liegenden Aufgaben benötigt.

In einer anderen Eingabe wurde die Besorgnis geäußert, das Datenschutzgesetz Nordrhein-Westfalen unterbinde die Übermittlung der Namen der in ein Krankenhaus aufgenommenen Gemeindemitglieder an ihre Pfarrgemeinde und die Weitergabe an den Besuchsdienst der Gemeinde. Ich habe wie folgt Stellung genommen.

Rechtsgrundlage für die Datenübermittlung durch Krankenhäuser mit öffentlich-rechtlicher Trägerschaft ist § 11 Abs.2 in Verbindung mit Abs. 1 DSG NW.

Danach ist eine Übermittlung an Stellen der öffentlich-rechtlichen Religionsgesellschaften zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist. Ihre Aufgaben und Ziele legen die Religionsgesellschaften im Rahmen ihrer Autonomie selbst fest. Damit können sie auch bestimmen, daß die seelsorgerische und karitative Betreuung der in ein Krankenhaus aufgenommenen Gemeindemitglieder zu den Aufgaben ihrer Pfarrgemeinde gehört.

Allerdings muß nach § 11 Abs. 2 DSG NW sichergestellt werden, daß bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen werden. Insbesondere muß bei der Pfarrgemeinde gewährleistet sein, daß die haupt- oder ehrenamtlichen Mitglieder der Gemeinde die von dem Krankenhaus übermittelten Daten nur zur Erfüllung der genannten Aufgaben nutzen und keinem Dritten zugänglich machen.

Unter diesen Voraussetzungen bestehen keine Bedenken gegen die Übermittlung der Namen der in ein Krankenhaus aufgenommenen Gemeindemitglieder an ihre Pfarrgemeinde und die Weitergabe an den Besuchsdienst der Gemeinde, sofern er rechtlich der Gemeinde zuzuordnen ist. Das Arztgeheimnis steht dem nicht entgegen, da die Angaben über die Aufnahme in das Krankenhaus und über die Konfession dem Krankenhaus nicht von einem Arzt übermittelt (§ 11 Abs. 1 Satz 2 DSG NW), sondern bei dem Patienten selbst erhoben worden sind.

Eine rechtliche Verpflichtung des Patienten zur Angabe seiner Konfession besteht nicht. Das Krankenhaus hat deshalb bei der Erhebung auf die Freiwilligkeit der Angabe hinzuweisen (§ 10 Abs. 2 Satz 1 DSG NW). Wenn ein Patient eine seelsorgerische oder karitative Betreuung nicht wünscht, hat er die Möglichkeit, die Angabe der Konfession zu verweigern.

Ist der Besuchsdienst eine Vereinigung von Gemeindemitgliedern, die mit der Gemeinde zusammenarbeitet, ihr aber rechtlich nicht zuzuordnen ist, so sind die Vorschriften über die Übermittlung an nicht-öffentliche Stellen anzuwenden. Da eine Beeinträchtigung schutzwürdiger Belange des Betroffenen (§ 13 Abs. 1 Satz 1 DSG NW) jedenfalls nicht auszuschließen ist, dürfen die Daten in diesem Fall nur mit Einwilligung des Betroffenen übermittelt werden (§ 3 Satz 1 Nr. 2 DSG NW).

c) Berufskammern

Durch die Eingabe eines Zahnarztes habe ich erfahren, daß der Bundesverband der Deutschen Zahnärzte e.V. (BDZ) die Anschriften der Zahnärzte an den Deutschen Ärzteverlag in Köln zum Zwecke der Verwendung der vom BDZ und von der Kassenzahnärztlichen Bundesvereinigung herausgegebenen „Zahnärztlichen Mitteilungen" weitergibt. Der Verlag verschickte darüber hinaus mit dem Einverständnis des BDZ Werbematerial „seriöser" Firmen an die Zahnärzte.

Auf den BDZ finden die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen Anwendung. Dieses Gesetz schützt auch Daten, die von Vereinigungen der Landesaufsicht unterstehender juristischer Personen des öffentlichen Rechts übermittelt werden (§1 Abs. 2 Satz 1 DSG NW). Zu diesen Vereinigungen gehört auch der BDZ; er ist eine Arbeitsgemeinschaft der Zahnärztekammern, der unter anderem die Zahnärztekammern Nordrhein und Westfalen-Lippe angehören und die ihren Sitz in Nordrhein-Westfalen hat.

Soweit der BDZ dem Deutschen Ärzteverlag die Anschriften der Zahnärzte zum Zweck der Versendung der von dem BDZ herausgegebenen „Zahnärztlichen Mitteilungen" übermittelt, bestehen keine datenschutzrechtlichen Bedenken, da es als Aufgabe des BDZ angesehen werden kann, die Mitglieder der ihm angehörenden Zahnärztekammern durch ein Mitteilungsblatt zu informieren (§ 13 Abs. 1 Satz 1 DSG NW). Dies rechtfertigt jedoch nicht die Verwendung von Anschriften für die Versendung von Werbematerial an Firmen. Nach § 13 Abs. 2 DSG NW darf der Empfänger die übermittelten Daten nur für den

Zweck verwenden, für dessen Erfüllung sie ihm übermittelt wurden. Ein Verstoß gegen diese Vorschrift kann nach § 34 DSG NW als Ordnungswidrigkeit mit Geldbuße geahndet werden.

§ 13 Abs. 1 Satz 1 DSG NW läßt eine Übermittlung an nicht-öffentliche Stellen darüber hinaus zu, soweit der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Der Übermittlung steht die Erklärung des Einverständnisses mit der Verwendung bereits übermittelter Daten für einen anderen Zweck gleich. Zwar dürfte ein berechtigtes Interesse des Deutschen Ärzteverlages an der Kenntnis der Anschriften zum Zwecke der Versendung von Werbematerial von Firmen vorliegen. Dadurch können jedoch schutzwürdige Belange der Betroffenen beeinträchtigt werden. Zwar mögen manche Zahnärzte die Übersendung von Werbematerial wünschen. Andere hingegen empfinden sie als Belästigung. Bei einer Abwägung der Interessen überwiegt das Interesse des Betroffenen an dem Schutz seiner Daten gegenüber dem rein kommerziellen Interesse des Verlages. Auch die Tatsache, daß nur Werbematerial „seriöser" Firmen versandt wird, kann zu keiner anderen Beurteilung führen.

Da weder § 13 Abs. 1 Satz 1 DSG NW noch eine andere Rechtsvorschrift die Übermittlung an nicht-öffentliche Stellen zum Zweck der Versendung von Werbematerial privater Unternehmen erlaubt und auch keine Einwilligung der Betroffenen vorlag, verstieß die Erklärung des BDZ, er sei mit der Verwendung der Anschriften für die Versendung von Werbematerial seriöser Firmen durch den deutschen Ärzteverlag einverstanden, gegen § 3 Satz 1 DSG NW. Ich habe deshalb den BDZ gebeten, die Einverständniserklärung zu widerrufen. Der BDZ hat meiner Bitte entsprochen.

Auch das Vorhaben des BDZ, Namen, Anschrift, Geburtsjahr, Jahr der Bestallung, akademischen Grad und weitere personenbezogene Daten aller Zahnärzte an einen Fachverlag für die Herausgabe des „Deutschen Zahnärztlichen Adreßbuches" zu übermitteln, erfüllt nicht die Voraussetzungen des § 13 Abs. 1 Satz 1 DSG NW. Es erscheint bereits zweifelhaft, ob der Fachverlag ein berechtigtes Interesse an der Kenntnis aller Daten hat, die er bislang in dem Deutschen Zahnärztlichen Adreßbuch veröffentlicht hat. Auf jeden Fall können durch die Bekanntgabe dieser Daten schutzwürdige Belange der Betroffenen beeinträchtigt werden. Bei einer Abwägung der Interessen überwiegt in jedem Fall das Interesse der Betroffenen an dem Schutz ihrer Persönlichkeitssphäre gegenüber dem Veröffentlichungsinteresse des Verlages und dem Informationsinteresse der Benutzer des Adreßbuchs. Da die Verletzung schutzwürdiger Belange der Betroffenen jedenfalls nicht auszuschließen ist, bedarf die Übermittlung der von dem Verlag zur Veröffentlichung im Deutschen Zahnärztlichen Adreßbuch vorgesehenen Daten der Einwilligung der Betroffenen (§ 3 Satz 1 Nr. 2 DSG NW). Die Einwilligung ist grundsätzlich schriftlich zu erteilen, nachdem die Betroffenen über ihre Bedeutung aufgeklärt worden sind (§ 3 Abs. 2 und 3 DSG NW).

14. Personalwesen

a) Bearbeitung von Personalangelegenheiten

In meinem ersten Tätigkeitsbericht (C. 11. a) habe ich empfohlen, in das Landesbeamtengesetz eine ausdrückliche gesetzliche Regelung für das Sammeln personenbezogener Daten in Personalakten und für den Zugang zu diesen Akten aufzunehmen. Die Landesregierung hat in ihrer Stellungnahme (S. 11 — 12) die Auffassung vertreten, daß es schon zweifelhaft sein könne, ob der Umgang mit personenbezogenen Daten in Personalakten einen Eingriff in das Grundrecht auf Datenschutz darstelle. Auf jeden Fall entspreche dieser Umgang mit personenbezogenen Daten einem Bundes-Gewohnheitsrecht, das gemäß Artikel 31 des Grundgesetzes jeder landesverfassungsrechtlichen Regelung vorgehe.

Dieser Auffassung kann ich nicht folgen. Ein Bundes-Gewohnheitsrecht kann nur gelten, soweit der Bund eine Gesetzgebungskompetenz hat. Zwar hat der Bund nach Artikel 75 Nr. 1 des Grundgesetzes das Recht, Rahmenvorschriften über die Rechtsverhältnisse der im öffentlichen Dienst der Länder, Gemeinden und anderen Körperschaften des öffentlichen Rechts stehenden Personen zu erlassen. In einem Rahmengesetz kann er auch unmittelbar geltende Regelungen treffen, die dem Landesrecht vorgehen. Ein unmittelbar geltendes Bundes-Gewohnheitsrecht auf Grund der Gesetzgebungskompetenz für Rahmenvorschriften über die Rechtsverhältnisse der im öffentlichen Dienst stehenden Personen dürfte jedoch rechtlich nicht möglich sein. Ich halte an meiner Empfehlung fest.

b) Weitergabe von Daten an den Personalrat

Eine Gemeinde hat mich um Stellungnahme gebeten, ob datenschutzrechtliche Bedenken dagegen bestehen, sämtliche im automatisiert verarbeiteten Stellenplan aufgeführten Angaben an den Personalrat weiterzugeben. Der Stellenplan enthält im einzelnen folgende Angaben: Stellenbewertung, Personalnummer, Dienstbezeichnung, Name, Vorname, Geburtsdatum, Eingruppierung, Daten der Einweisung in die Gruppe und in die Stelle.

Der Informationsaustausch zwischen Dienststelle und Personalrat ist bereichspezifisch und abschließend durch das Landespersonalvertretungsgesetz 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 der Personalnummer im Stellenplan zur Durchführung der Aufgaben des Personalrats erforderlich ist. Von der Übermittlung der Personalnummer an den Personalrat ist daher abzusehen. Dagegen dürfte die Übermittlung der übrigen im Stellenplan enthaltenen Daten an den Personalrat zur Durchführung seiner Aufgaben notwendig sein. Ohne Kenntnis dieser Daten ist es dem Personalrat oft nicht möglich, in den nach § 72 LPVG beteiligungspflichtigen Angelegenheiten eine sachgerechte Entscheidung zu treffen. Dies gilt auch für die Übermittlung von Geburtsdaten, deren Kenntnis bei der Zustimmung des Personalrats zu Beförderungen oder Höhergruppierungen in Fällen gleicher Eignung erforderlich sein kann. Ich habe deshalb gegen die Übermittlung der im Stellenplan enthaltenen personenbezogenen Daten — mit Ausnahme der Personalnummer — aus datenschutzrechtlicher Sicht keine Bedenken.

Eine andere Gemeinde hat bei mir angefragt, ob dem Verlangen des Personalrats, die Namen derjenigen Bediensteten zu benennen, die das vermögenswirksame Sparen nicht wahrnehmen, stattzugeben sei.

Nach § 64 Nr. 2 LPVG hat der Personalrat die allgemeine Aufgabe, darüber zu wachen, daß die zu Gunsten der Beschäftigten geltenden Gesetze, Verordnungen, Tarifverträge, Dienstvereinbarungen und Verwaltungsanordnungen durchgeführt werden. Hierzu gehören auch das Gesetz über vermögenswirksame Leistungen für Beamte, Richter, Berufssoldaten und Soldaten auf Zeit sowie der Tarifvertrag über vermögenswirksame Leistungen an Angestellte. Zwar ist es danach Aufgabe des Personalrats, die den Beschäftigten durch die genannten Vorschriften zugestandenen Ansprüche auf vermögenswirksame Leistungen durch entsprechende Kontrollen zu sichern und für ihre Erfüllung einzutreten. Diese Aufgabe kann der Personalrat jedoch in der Weise wahrnehmen, daß er in einem Rundschreiben an alle Bediensteten auf die Regelungen über die Gewährung vermögenswirksamer Leistungen hinweist. Dazu ist es nicht erforderlich und deshalb unzulässig, dem Personalrat die Namen derjenigen Bediensteten mitzuteilen, die die vermögenswirksamen Leistungen nicht in Anspruch nehmen.

c) Weitergabe von Daten an den Schulträger

Die Gewerkschaft Erziehung und Wissenschaft, Landesverband Nordrhein-Westfalen, hat mich gebeten, die Zulässigkeit der Weitergabe personenbezogener Daten von Leh-

rern an den Schulträger im Rahmen seiner Beteiligung bei der Anstellung, Beförderung und Versetzung datenschutzrechtlich zu überprüfen.

Das Datenschutzgesetz Nordrhein-Westfalen scheidet als gesetzliche Grundlage für die Weitergabe der Personalakten eines Lehrers aus, da dieses Gesetz nur in Dateien gespeicherte Daten schützt und Personalakten keine Dateien sind (§ 1 Abs. 2 Satz 1, § 2 Abs. 3 Nr. 3 DSG NW). Das gleiche gilt für ergänzende Auskünfte durch den Schulaufsichtsbeamten oder den Schulleiter, da auch diese Daten nicht in einer Datei gespeichert sein dürften. Als gesetzliche Grundlage für die Weitergabe dürfte wohl nur § 23 des Schulverwaltungsgesetzes in Verbindung mit § 7 Abs. 1 des Landesbeamtengesetzes (LBG) in Betracht kommen. Soweit hiernach der Schulträger bei der Anstellung, Beförderung und Versetzung eines Lehrers zu beteiligen ist, müssen ihm diejenigen Daten des Lehrers zur Verfügung stehen, die für eine sachgerechte Ausübung der Rechte des Schulträgers unter Beachtung der beamtenrechtlichen Vorschriften für die Auslese der Bewerber erforderlich sind.

Bedenken bestehen allerdings gegen die Weitergabe der gesamten Personalakten. Der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz verbietet, mehr Daten weiterzugeben, als zur Aufgabenerfüllung erforderlich sind. Ich habe meine Bedenken dem Kultusminister dargelegt, dessen Stellungnahme zur Zeit noch nicht vorliegt.

d) Erfassung von Telefongesprächen

Ein im öffentlichen Dienst beschäftigter Bürger sowie Personalräte verschiedener Behörden haben mich um Stellungnahme gebeten, inwieweit die automatische Gesprächsdatenerfassung durch die jeweilige Telefonanlage zulässig sei.

Die von den verschiedenen Gesprächsdatenerfassungsanlagen aufgezeichneten Daten (Datum, Uhrzeit, Gesprächsdauer, Anzahl der Gebühreneinheiten, Rufnummer der Anlagennebenstelle und des angewählten Fernsprechteilnehmers) sind personenbezogene Daten, da die gesprächführenden Personen durch die Rufnummer der Nebenstelle und des angewählten Fernsprechteilnehmers bestimmbar sind (§ 2 Abs. 1 DSG NW).

Die Speicherung dieser Daten über **dienstliche Gespräche** ist nach meiner Auffassung zulässig, da sie zur rechtmäßigen Erfüllung der Aufgaben der speichernden Stelle erforderlich ist (§ 10 Abs. 1 DSG NW). Der Dienstherr hat bei dem Betrieb der Fernsprechnebenstellenanlage die Grundsätze der Wirtschaftlichkeit und Sparsamkeit zu beachten (§ 7 Abs. 1 der Landeshaushaltsordnung, § 62 Abs. 2 der Gemeindeordnung). Zur Überwachung ist die Speicherung der von der Gesprächsdatenerfassungsanlage aufgezeichneten Daten erforderlich. Jeder Bedienstete ist seinem Dienstherrn oder öffentlichen Arbeitgeber zur Rechenschaft über die Führung seiner Dienstgeschäfte verpflichtet; dazu gehört auch Auskunft über dienstlich geführte Telefongespräche. Das Fernmeldegeheimnis (Artikel 10 Abs. 1 des Grundgesetzes) steht dem nicht entgegen, weil der Schutz der Vertraulichkeit im dienstlichen Fernsprechverkehr von seinem Schutzzweck nicht erfaßt wird (OVG Bremen, NJW 1980, S. 606). Dies gilt auch für dienstliche Gespräche mit einem Dritten.

Bedenken bestehen jedoch gegen die Speicherung der Rufnummer des anderen Gesprächsteilnehmers bei **privaten Gesprächen**. Sie ist nach meiner Auffassung zur Erfüllung der Aufgaben der speichernden Stelle nicht erforderlich und deshalb unzulässig. Zwar muß die Behörde Einnahmen rechtzeitig einziehen und ihren Eingang überwachen (§ 34 Abs. 1 der Landeshaushaltsordnung, § 25 der Gemeindehaushaltsverordnung). Für die Abrechnung der Kosten privater Gespräche reicht es jedoch aus, die übrigen Daten zu speichern. Auch wenn Nebenstellen mehreren Bediensteten zugänglich sind, dürfte der Gesprächführende auf Grund des Datums, der Uhrzeit und der Gesprächsdauer durch Rückfrage bei den in Betracht kommenden Bediensteten festgestellt werden können.

Darüber hinaus unterliegen private Gespräche dem Schutz des Fernmeldegeheimnisses (Artikel 10 Abs. 1 des Grundgesetzes). Dieser erstreckt sich auch darauf, mit welchem

Teilnehmer der Bedienstete ein privates Gespräch geführt hat (vgl. Maunz-Dürig-Herzog-Scholz, Kommentar zum Grundgesetz, Artikel 10 Rdnr. 18). Aufzeichnungen über den Gesprächsteilnehmer ohne dessen Einwilligung würden daher auch das Fernmeldegeheimnis verletzen.

Sämtliche zulässigerweise gespeicherten personenbezogenen Daten sowohl über dienstliche als auch über private Gespräche müssen nach Ausdruck zumindest gesperrt werden, da ihre weitere Speicherung zur Aufgabenerfüllung nicht mehr erforderlich ist (§ 17 Abs. 2 Satz 2 DSG NW). Sie dürfen dann nur noch genutzt werden, wenn dies zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich ist oder der Betroffene in die Nutzung eingewilligt hat (§ 17 Abs. 2 Satz 3 DSG NW).

e) Bewerbungen

Ein Bürger hat sich dagegen gewandt, daß Bewerber für den Vorbereitungsdienst für ein Lehramt das vollständige Abiturzeugnis mit den Punktzahlen der Kurse und Prüfungsfächer sowie der Durchschnittsnote vorzulegen haben. Er ist der Ansicht, daß für den Nachweis der Hochschulreife das Deckblatt des Abiturzeugnisses genügt. Insbesondere befürchtet er, daß aus der Durchschnittsnote unzutreffende Rückschlüsse auf die Leistungsfähigkeit und die Leistungsbereitschaft des Bewerbers gezogen werden könnten.

Nach § 7 Abs. 1 LBG ist die Auslese der Bewerber nach Eignung, Befähigung und fachlicher Leistung vorzunehmen. Bei der Anforderung von Bewerbungsunterlagen ist der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz zu beachten. Dieser verbietet, mehr Daten zu erheben, als zur Beurteilung von Eignung, Befähigung und fachlicher Leistung erforderlich sind. Ich habe Zweifel, ob für die Auslese nach § 7 Abs. 1 LBG die Kenntnis der Punktzahlen und der Durchschnittsnote des Abiturzeugnisses notwendig ist. Für die Beurteilung von Eignung, Befähigung und fachlicher Leistung müßten die Prüfungsleistungen der Ersten Staatsprüfung entscheidend sein.

Der Kultusminister, den ich zu dieser Eingabe um Stellungnahme gebeten hatte, weist demgegenüber auf folgendes hin: Der nach § 3 Abs. 2 Ziffer 2 der Ordnung des Vorbereitungsdienstes und der Zweiten Staatsprüfung für Lehrämter an Schulen dem Einstellungsantrag beizufügende Nachweis der Hochschulreife werde durch ein Zeugnis geführt, dessen Form und Inhalt vorgeschrieben seien.

Das Abiturzeugnis sei eine einheitliche Urkunde, bestehend aus vier Seiten. Entgegen der Auffassung des Betroffenen lasse es sich nicht in ein „Deckblatt" und einen anderen (Leistungs-) Teil aufgliedern. Dem Charakter der Urkunde als geschlossene Einheit widerspräche es, jeweils nur bestimmte Teile herauszulösen und als Nachweis für die Einstellungen genügen zu lassen. Gerade bei den strengen Anforderungen des Beamtenrechts — dies gelte nicht nur für Lehrer — müsse die Zugangsberechtigung eines Bewerbers vollständig nachprüfbar sein. Im übrigen würden die Einzelbeurteilungen des Abiturzeugnisses zu Recht als ein Kriterium für den Einsatz eines Bewerbers herangezogen, wenn auch mit unterschiedlicher Intensität. Der Kultusminister hält deshalb daran fest, daß Bewerber für den Vorbereitungsdienst für ein Lehramt das vollständige Abiturzeugnis vorzulegen haben. Nach meiner Auffassung bedarf die Angelegenheit weiterer Erörterung.

f) Erklärung K, O, A und S

Das Landesamt für Besoldung und Versorgung (LBV) verlangt im Zweijahresrythmus von allen Personen, die in einem öffentlich-rechtlichen Amts- oder Dienstverhältnis, einem Arbeitsverhältnis oder Ausbildungsverhältnis zum Land stehen und die im Erklärungszeitraum Kindergeld und/oder einen höheren Ortszuschlag als den der Stufe 1, Anwärter-Verheirateten-Zuschlag oder Sozialzuschlag bezogen haben, die „Erklärung K, O, A und S". Mehrere Bürger haben mich in dieser Angelegenheit nach der Rechts-

grundlage gefragt und um Stellungnahme zur Notwendigkeit des Umfanges der Datenerhebung gebeten.

Die mit der „Erklärung K, O, A und S" erhobenen Daten sind zur Nachprüfung der Voraussetzungen für den Anspruch auf Kindergeld, Ortszuschlag, Anwärter-Verheiratetenzuschlag und Sozialzuschlag erforderlich. Rechtsgrundlage für die Erhebung dieser Daten sind die für die genannten Leistungen maßgebenden Vorschriften des Bundeskindergeldgesetzes, des Bundesbesoldungsgesetzes und der Tarifverträge für den öffentlichen Dienst. Die von Ledigen und Geschiedenen geforderten Angaben (C und D der Erklärung) sind notwendig, weil die dort genannten Personen, die sonst Ortszuschlag nach Stufe 1 erhalten, Anspruch auf Ortszuschlag nach Stufe 2 haben, wenn sie eine andere Person nicht nur vorübergehend in ihre Wohnung aufgenommen haben und ihr Unterhalt gewähren, weil sie gesetzlich oder sittlich dazu verpflichtet sind oder aus beruflichen oder gesundheitlichen Gründen ihrer Hilfe bedürfen (§ 40 Abs. 2 Nr. 4 BBesG) oder wenn sie gegenüber ihrem früheren Ehegatten zum Unterhalt verpflichtet sind (§ 40 Abs. 2 Nr. 3 BBesG). Die Erhebung dieser Daten ist somit datenschutzrechtlich nicht zu beanstanden.

Ein weiterer Bürger hat bei mir angefragt, ob das LBV berechtigt sei, von ihm die Anschrift des Arbeitgebers seiner Ehefrau und deren Personalnummer zu erfragen. Seiner Meinung nach müsse die Erklärung, seine Ehefrau sei mit einer bestimmten Stundenzahl bei der evangelischen Kirche teilzeitbeschäftigt, ausreichen, um seinen Anspruch auf Ortszuschlag zu ermitteln.

Nach § 40 Abs. 5 in Verbindung mit Abs. 7 Satz 1 und 3 BBesG ist bei der Ermittlung, in welcher Höhe dem Beamten der Unterschiedsbetrag zwischen den Stufen 1 und 2 des für ihn maßgebenden Ortszuschlages zusteht, insbesondere zu prüfen, ob der Ehegatte im öffentlichen Dienst steht oder seine Beschäftigung bei einem sonstigen Arbeitgeber dem öffentlichen Dienst gleichzusetzen ist. Die Feststellung, ob die Tätigkeit der Ehefrau bei der evangelischen Kirche öffentlicher Dienst ist oder ihm gleichsteht, konnte das LBV auf Grund der gemachten Angaben nicht treffen, weil innerhalb der evangelischen Kirche sowohl Beschäftigungsverhältnisse im Sinne von § 40 Abs. 7 Satz 1 und 3 BBesG wie auch solche anderer Art bestehen können. Für diese Feststellung waren weitere Angaben erforderlich.

Nach § 2 Abs. 3 BBesG kann der Beamte auf die ihm gesetzlich zustehende Besoldung, zu der auch der Ortszuschlag gehört (§ 1 Abs. 2 Nr. 3 BBesG), weder ganz noch teilweise verzichten. Das LBV durfte deshalb nicht ohne weiteres davon ausgehen, daß auf Grund der Erklärung des Betroffenen, seine Ehefrau sei bei der evangelischen Kirche mit einer bestimmten Stundenzahl teilzeitbeschäftigt, ihm der Unterschiedsbetrag zwischen den Stufen 1 und 2 des Ortszuschlages nur zur Hälfte zustehe. Um die zur Prüfung dieser Frage notwendigen Auskünfte einholen zu können, benötigte das LBV die Anschrift des Arbeitgebers der Ehefrau. Die Erhebung dieser Angabe verstieß somit nicht gegen Vorschriften über den Datenschutz.

g) Beihilfen

Ein Bürger hat mich um Auskunft gebeten, wie die Erhebung seiner personenbezogenen Daten anläßlich eines Beihilfeantrags seiner Ehefrau datenschutzrechtlich zu beurteilen ist.

Nach § 88 LBG in Verbindung mit der Verordnung über die Gewährung von Beihilfen in Krankheits-, Geburts- und Todesfällen (BVO) ist unter anderem zu prüfen, ob und inwieweit dem Beihilfeberechtigten oder einer berücksichtigungsfähigen Person Heilfürsorge, Krankenhilfe oder Kostenerstattung auf Grund anderer Rechtsvorschriften zusteht und ob der Antragsteller von der Krankenversicherung einer anderen Person (beispielsweise des Ehegatten) erfaßt wird (§ 3 Abs. 4 BVO).

Zur Klärung dieses Sachverhalts ist es erforderlich, daß derjenige, der einen Anspruch auf Beihilfe geltend macht, alle Tatsachen mitteilt, die die Festsetzungsstelle zur Prüfung der

Anspruchsberechtigung benötigt. Dies gilt insbesondere für den Fall, daß der Beihilfeberechtigte auch Beihilfe für den Ehegatten oder die berücksichtigungsfähigen Kinder beantragt. Es kann auch nicht davon ausgegangen werden, daß durch die den Ehegatten betreffenden Fragen im Beihilfeantrag der Grundsatz der Verhältnismäßigkeit verletzt ist. Im übrigen sind Anträge auf Beihilfe nach § 13 Abs. 2 Satz 4 BVO vertraulich zu behandeln.

Die in dem Vordruck vorgesehene Erhebung personenbezogener Daten des Ehegatten verstößt demnach nicht gegen Vorschriften über den Datenschutz.

Im Kreis der Datenschutzbeauftragten des Bundes und der Länder ist die Frage erörtert worden, ob die Vorlage des vollständigen ärztlichen Schlußberichtes bei der Stellung eines Antrages auf Gewährung von Beihilfe für stationäre Sanatoriumsbehandlung unter Berücksichtigung datenschutzrechtlicher Erfordernisse notwendig ist.

§ 6 Abs. 1 Satz 1 BVO regelt eindeutig und abschließend die Voraussetzungen für die Beihilfefähigkeit der Aufwendungen bei Sanatoriumsaufenthalt. Die Vorlage des ärztlichen Schlußberichtes gehört nicht zu diesen Voraussetzungen. Dementsprechend wird in Nordrhein-Westfalen — soweit ersichtlich — die Vorlage des ärztlichen Schlußberichtes nach Sanatoriumsbehandlung nicht verlangt. Eine derartige Praxis fände in § 6 Abs. 1 Satz 1 BVO keine Stütze.

Im übrigen ist eine Kontrolle, ob der Beihilfeberechtigte sich tatsächlich einer Sanatoriumsbehandlung (und nicht etwa nur einer heilkurähnlichen Behandlung) unterzogen hat und ob dabei das im amts- oder vertrauensärztlichen Gutachten attestierten Leiden (nicht etwa eine andere Krankheit) behandelt worden ist, durchaus ohne Vorlage des vollständigen ärztlichen Schlußberichtes möglich. Ich gehe davon aus, daß eine solche Kontrolle durch die nicht mit Ärzten besetzte Festsetzungsstelle ebenso auf Grund einer entsprechenden Erklärung des behandelnden Arztes erfolgen kann. Die Vorlage des vollständigen ärztlichen Schlußberichtes ist daher zur Entscheidung über die Beihilfefähigkeit der Aufwendungen für eine Sanatoriumsbehandlung nicht erforderlich. Soweit die Festsetzungsstelle gleichwohl den ärztlichen Schlußbericht anfordert, liegt darin ein Verstoß gegen den Grundsatz der Verhältnismäßigkeit.

h) Überweisung von Bezügen

Bereits im vorigen Berichtszeitraum hatte ich auf Grund mehrerer Eingaben von Landesbediensteten datenschutzrechtliche Bedenken gegen die detaillierte Aufschlüsselung der Bezüge in den vom LBV verwendeten Überweisungsträgern geäußert (C. 11. a meines ersten Tätigkeitsberichts).

Wie mir der Innenminister inzwischen mitgeteilt hat, ist der Gesamtkomplex der Benachrichtigung der Zahlungsempfänger über die erfolgten Zahlungen und deren Aufschlüsselung inzwischen überprüft worden. Es ist nun beabsichtigt, zum 1. August 1981 das gesamte Verfahren neu zu regeln. Von diesem Zeitpunkt an werden den Geldinstituten ausschließlich die für die Überweisung erforderlichen Daten übermittelt. Über die Zusammensetzung der Zahlung werden die Zahlungsempfänger bei jeder Veränderung der Brutto- und Nettobezüge durch eine gesonderte, in Leseschrift ausgedruckte, verschlossene Mitteilung informiert, die teils über die Beschäftigungsbehörden und teils durch die Post übermittelt wird.

Damit wird den datenschutzrechtlichen Bedenken gegen das bisherige Verfahren voll Rechnung getragen.

i) Datenübermittlung an nicht-öffentliche Stellen

Mehrere Bürger haben mir ihr Befremden darüber mitgeteilt, daß ihnen vor Einstellung in den Vorbereitungsdienst als Lehramtsanwärter von privaten Krankenkassen und anderen Unternehmen unaufgefordert Werbematerial mit unmittelbarem Bezug auf die bevorstehende Einstellung in den öffentlichen Dienst zugesandt worden ist. Die vom Kultus-

minister bereits nach den Einstellungsterminen für das Schuljahr 1979/80 in diesem Zusammenhang geführten Ermittlungen sind nicht zuletzt deshalb ohne Ergebnis geblieben, weil im Laufe des Einstellungsverfahrens eine Vielzahl von Personen bei den beteiligten Dienststellen (Regierungspräsidenten, Bezirkspersonalräte, Ausbildungsgruppen, Gesamtseminare, Kultusminister, Landesamt für Datenverarbeitung und Statistik) Kenntnis von diesen personenbezogenen Daten erhält. Der Kultusminister hat die beteiligten Stellen durch Erlaß darauf hingewiesen, daß es unzulässig ist, die Namen und Anschriften von Lehramtsanwärtern an Wirtschaftsunternehmen weiterzugeben.

Wie weitere Eingaben gezeigt haben, ist dieser Erlaß bei den Einstellungen für das Schuljahr 1980/81 in einigen Fällen offenbar nicht beachtet worden. Ohne nähere Anhaltspunkte war es mir jedoch nicht möglich festzustellen, von welcher Seite gegebenenfalls gegen Vorschriften über den Datenschutz verstoßen worden ist.

Im vorigen Berichtszeitraum hatte ich datenschutzrechtliche Bedenken dagegen geäußert, daß die Gymnasien und Gesamtschulen in Nordrhein-Westfalen dem Verlag des Philologen-Jahrbuches personenbezogene Daten von Lehrern ohne deren Einwilligung mitteilen (C.11.c meines ersten Tätigkeitsberichts). Der Kultusminister hat inzwischen auf meine Empfehlung durch Runderlaß die Regierungspräsidenten, Schulkollegien und Gesamtseminare darauf hingewiesen, daß die Weitergabe personenbezogener Daten durch die Schulen an den Philologen-Verband nur zulässig ist, wenn eine schriftliche Einwilligung der Betroffenen vorliegt.

In gleicher Weise habe ich auch gegenüber einem anderen Herausgeber eines Lehrer-Jahrbuches Stellung genommen.

Ein privater Verlag, der die Herausgabe eines Verzeichnisses der Fachhochschullehrer vorbereitete, hat mich um Stellungnahme zu folgendem Verfahren gebeten. Er beabsichtige, die in sein Verzeichnis aufzunehmenden Daten wie Name, Vorname, akademische Grade, dienstrechtliche Stellung, Fachgebiet, dienstliche und private Anschrift mit Fernsprechanschlüssen, Fachbereich und Fachhochschule den jeweiligen Vorlesungsverzeichnissen, also jedermann zugänglichen Quellen, zu entnehmen. Aus Gründen der Aktualität der Einträge sei er darauf angewiesen, die Fachbereiche um Korrektur der aufgenommenen Einträge zu bitten.

Hiergegen bestehen datenschutzrechtliche Bedenken. Die Rücksendung der den Fachhochschulen übersandten Listen nach Kontrolle der Vollständigkeit und Richtigkeit der Angaben unter Mitteilung etwaiger Ergänzungen, Streichungen und Änderungen ist eine Übermittlung personenbezogener Daten. Der Umstand, daß derartige Veränderungen später dem Vorlesungsverzeichnis entnommen werden können, steht dem nicht entgegen. Die nach § 13 Abs. 1 Satz 1 DSG NW gebotene Interessenabwägung führt dazu, daß das berechtigte Interesse des Verlages an der Kenntnis der Daten gegenüber dem Interesse des Betroffenen am Schutz seiner personenbezogenen Daten zurücktreten muß. Da die Beeinträchtigung schutzwürdiger Belange jedenfalls nicht auszuschließen ist, bedarf die Übermittlung solcher Daten der Einwilligung des Betroffenen (§ 3 Satz 1 Nr. 2 DSG NW). Ob die Fachhochschule die erforderliche Einwilligung einholen oder auf die Mitteilung solcher Daten an den Verlag verzichten will, steht in ihrem Ermessen. Eine rechtliche Verpflichtung, sich um die Einwilligung zu bemühen, besteht nicht. Die Fachhochschule hat in eigener Verantwortung zu entscheiden, ob sie diese Aufgabe im Interesse der an einem Hochschullehrerverzeichnis interessierten Bürger unter Inkaufnahme des für die Einholung der Einwilligung erforderlichen Verwaltungsaufwandes übernehmen will.

Im übrigen bedarf auch die bisherige Praxis der Veröffentlichung personenbezogener Daten von Hochschullehrern in Vorlesungsverzeichnissen einer datenschutzrechtlichen Überprüfung. Soweit dort Daten veröffentlicht werden, die nicht dienstbezogen sind (wie etwa die private Anschrift und die private Rufnummer), ist die Einwilligung des Betroffenen erforderlich.

15. Statistik

a) Sozialhilfestatistik

In meinem ersten Tätigkeitsbericht (C. 12. c) hatte ich auf die fehlende Rechtsgrundlage für die Weitergabe von Namen und Anschriften von Hilfeempfängern durch die Sozialhilfeträger an das Landesamt für Datenverarbeitung und Statistik (LDS) zum Zwecke der Durchführung der Jahresstatistik für Sozialhilfe hingewiesen. Der zuständige Bundesminister für Jugend, Familie und Gesundheit hat inzwischen die mit der Durchführung der Sozialhilfestatistik beauftragten statistischen Landesämter von der Unzulässigkeit der Erhebung dieser persönlichen Grunddaten unterrichtet.

b) Hochschulstatistik

Zum Zwecke der Planung im Hochschulbereich werden nach § 7 Nr. 1 in Verbindung mit § 3 Nr. 4 und § 2 Nr. 3 des Hochschulstatistikgesetzes bei den Schülern des Abschlußjahrganges der Sekundarstufe II unter anderem Angaben über den Berufswunsch erhoben. Auf dem Erhebungsbogen, der von der Schule an das LDS weitergegeben wird, ist auch die Angabe des Namens des jeweiligen Schülers vorgesehen.

Ich bin der Auffassung, daß zur Durchführung der Statistik, auch für Vollzähligkeits- und Plausibilitätskontrollen, die Angabe des Namens in dem Erhebungsbogen nicht erforderlich ist. Wie das LDS bestätigt hat, kann die Vollständigkeit der Erhebung auch durch die Schulen (zum Beispiel über dort verbleibende Namenslisten mit zugeordneten Kennummern) sichergestellt werden. Das Erheben der Namen in dem an das LDS weiterzugebenden Erhebungsbogen verstößt gegen den Grundsatz der Verhältnismäßigkeit und ist deshalb unzulässig.

16. Wissenschaft und Forschung

a) Hochschulen

Ein Kontrollbesuch bei einer Universität hat ergeben, daß für die **Matrikel** nach der Einschreibungsordnung mehr Daten erhoben werden, als nach § 64 Abs. 2 des Gesetzes über die wissenschaftlichen Hochschulen des Landes Nordrhein-Westfalen erforderlich ist. Für einen Teil dieser weitergehenden Erhebungen ist zwar eine gesetzliche Grundlage in § 4 des Hochschulstatistikgesetzes (HStatG) vorhanden. Die Speicherung dieser für die Bundesstatistik bestimmten Daten in einer Hochschuldatei ist jedoch nicht erlaubt, es sei denn, daß sie zur rechtmäßigen Erfüllung der Hochschulaufgaben benötigt werden (§ 10 Abs. 1 DSG NW). Nach diesem Erforderlichkeitsgrundsatz dürfen Daten über die Ausbildung und beruflichen Stellung der Eltern sowie über das Berufsziel der Studenten in der Hochschulmatrikel nicht mehr gespeichert werden.

Hinsichtlich des Berufsziels der Studenten fehlt nach dem Hochschulstatistikgesetz auch eine Rechtsgrundlage für die Speicherung in der Bundesstatistik. Auch für Zwecke der Bundesstatistik dürfen die Hochschulen deshalb diese Daten ohne Einwilligung der Studenten nicht mehr erheben (anders dagegen die Regelung für Schüler nach § 7 Nr. 2 HStatG).

Soweit die Daten, die nach dem Hochschulstatistikgesetz an das Landesamt für Datenverarbeitung und Statistik weiterzuleiten sind, von der Hochschule selbst nicht gespeichert werden dürfen, ist es erforderlich, unterschiedliche Erhebungsbogen für das Studentenstammblatt und für die Erhebung nach dem Hochschulstatistikgesetz zu verwenden.

Der Kontrollbesuch bei einer Universität hat ferner zu der Feststellung geführt, daß die **Veröffentlichung über gespeicherte Daten** nach § 15 DSG NW im gegebenen Fall

nicht vollständig ist. Insbesondere fehlt ein Hinweis darauf, daß der Zentralstelle für die Vergabe von Studienplätzen nach §§ 11 Abs. 4 Satz 1, 26 Abs. 1 der Vergabeordnung und dem Sozialversicherungsträger nach § 7 der Meldeverordnung für die Krankenversicherung der Studenten regelmäßig die Immatrikulation der einzelnen Studenten aus der Matrikel bestätigt wird und daß aus dieser Datei auch der Bundesversicherungsanstalt für Angestellte regelmäßig Auskünfte gegeben werden.

Der Kontrollbesuch gibt Anlaß zu einer umfassenden Prüfung, inwieweit auch anderen Stellen aus der Matrikel regelmäßig Daten übermittelt werden.

Eine Bürgereingabe betraf die **Bekanntgabe von Prüfungsergebnissen durch öffentlichen Aushang**. Die Ergebnisse der schriftlichen Klausuren im Grundstudium des Faches Volkswirtschaftslehre werden in einer Universität ausschließlich durch namentlichen Aushang an den Schwarzen Brettern bekanntgegeben.

Das geschilderte Verfahren der Bekanntgabe von Klausurergebnissen verstößt gegen Artikel 4 Abs. 2 der Landesverfassung. Eine gesetzliche Grundlage für die Bekanntgabe der Klausurergebnisse in der Weise, daß nicht nur der Betroffene, sondern auch Dritte Kenntnis nehmen können, ist nicht ersichtlich.

Ich habe der Universität empfohlen, die Klausurergebnisse künftig in der Weise mitzuteilen, daß die Klausuren nach der Bewertung den einzelnen Teilnehmern persönlich ausgehändigt werden. Für vertretbar halte ich allerdings auch, die Klausurergebnisse an den Schwarzen Brettern ohne Namensnennung lediglich unter Angabe der Matrikelnummer auszuhängen.

Der Minister für Wissenschaft und Forschung hat sich meiner Auffassung angeschlossen, daß eine namentliche Bekanntgabe der Prüfungsergebnisse, die eine Kenntnisnahme durch Dritte nicht ausschließt, bedenklich ist. Er hat die Hochschulen gebeten sicherzustellen, daß die Prüfungsergebnisse in einer datenschutzrechtlich unbedenklichen Weise bekanntgegeben werden.

b) Studienplatzvergabe

In einem Fall wurde gerügt, daß Studienbewerber, die sich bei der Zentralen Vergabestelle für Studienplätze (ZVS) für den Studiengang Medizin beworben haben, **Werbematerial eines Studienverlags** erhalten haben. Meine Ermittlungen haben ergeben, daß der Verlag Studienbewerber angeschrieben hat, um ihnen ein Trainingsseminar für den Test an den medizinischen Studiengängen anzubieten. Der Verlag hat die Anschriften der betreffenden Studienbewerber von der „Initiative abgelehnter medizinischer Studienbewerber" erhalten.

Die ZVS hat mir versichert, daß sie im Rahmen ihrer Aufgabenerfüllung personenbezogene Daten von Studienbewerbern ausschließlich an die am Vergabeverfahren beteiligten wissenschaftlichen Hochschulen und Fachhochschulen übermittelt. Ich habe keine Veranlassung, an der Richtigkeit dieser Versicherung zu zweifeln, zumal der zugrunde liegende Vorgang aufgeklärt ist und Anhaltspunkte für die Übersendung von Angeboten anderer Verlage nicht vorliegen.

Eine Übermittlung personenbezogener Daten durch die ZVS an private Unternehmen zu Werbezwecken wäre nur mit Einwilligung des Betroffenen (§ 3 Satz 1 Nr. 2 DSG NW) zulässig, da eine Beeinträchtigung schutzwürdiger Belange des Betroffenen (§ 13 Abs. 1 Satz 1 DSG NW) nicht auszuschließen ist.

In einem weiteren Fall hat mir ein Bürger ein ihn nicht betreffendes **Originalzeugnis** der allgemeinen Hochschulreife übersandt, das ihm von der ZVS versehentlich zugeleitet worden war.

Die Studienbewerber werden nach der von mir eingeholten Stellungnahme der Zentralstelle für die Vergabe von Studienplätzen im „ZVS-info" darüber unterrichtet, daß eine Aufbewahrung der Anträge und Belege nicht möglich ist; gleichzeitig wird darauf hingewie-

sen, auf keinen Fall Originaldokumente dem Antrag beizufügen, da eine Rücksendung auf Grund der großen Zahl von Unterlagen, die zudem in sehr kurzer Zeit bearbeitet werden müssen, nicht gewährleistet werden kann.

Die ZVS hält diese Verfahrensweise nach § 3 Abs. 4 der Vergabeverordnung für gerechtfertigt. Dieser Ansicht vermag ich nicht zu folgen.

Nach Artikel 4 Abs. 2 Satz 1 der Landesverfassung ist die Zentralstelle verpflichtet, Originaldokumente sorgfältig zu behandeln und durch organisatorische Maßnahmen sicherzustellen, daß solche Dokumente nicht verloren gehen. Dies erfordert für die Rücksendung der Originaldokumente an den Antragsteller ein Verfahren, das eine Verwechslung von Unterlagen ausschließt.

Nach Artikel 4 Abs. 2 Satz 2 der Landesverfassung bedarf eine Einschränkung des Anspruchs auf sorgfältige Behandlung und Rücksendung von Originaldokumenten einer gesetzlichen Grundlage. Eine solche ist nicht ersichtlich. § 3 Abs. 4 Vergabeverordnung kommt hierfür nicht in Betracht. Zwar ermächtigt § 3 Abs. 4 Satz 2 der Vergabeverordnung die ZVS, die Form der Unterlagen zu bestimmen, die den Anträgen mindestens beizufügen sind. Dies ist in der Weise geschehen, daß die ZVS nur amtlich beglaubigte Kopien verlangt. Eine Ermächtigung, den Anspruch auf sorgfältige Behandlung und Rücksendung von Originaldokumenten einzuschränken, läßt sich aus der Vorschrift jedoch nicht herleiten. Die Aufforderung, dem Antrag auf keinen Fall Originaldokumente beizufügen, mit dem Hinweis, daß „die ZVS die Rücksendung bei der großen Zahl von Unterlagen, die in sehr kurzer Zeit bearbeitet werden müssen, nicht gewährleisten kann", hat deshalb lediglich die Bedeutung einer Empfehlung. Der Anspruch des Betroffenen aus Artikel 4 Abs. 2 Satz 1 der Landesverfassung wird dadurch nicht eingeschränkt.

Der Allgemeine Studentenausschuß einer Universität hat mir mitgeteilt, daß ein an die Universität adressiertes Päckchen bei ihm eingegangen und versehentlich geöffnet worden sei. In dem Päckchen habe sich ein Magnetband der ZVS befunden. Das Band habe ausweislich eines beiliegenden Schreibens der ZVS „Daten zum Sommersemester 1980 für das besondere Verteilungsverfahren" enthalten. Aus dem Begleitschreiben habe sich auch der Code des Datenträgers ergeben.

Nach § 6 DSG NW in Verbindung mit Nr. 9 der Anlage zu diesem Gesetz haben die Behörden und sonstigen öffentlichen Stellen des Landes die technischen und organisatorischen Maßnahmen zu treffen, die geeignet sind zu gewährleisten, daß beim **Transport von Datenträgern** diese nicht unbefugt gelesen, verändert oder gelöscht werden können (Transportkontrolle).

Meine Nachforschungen haben ergeben, daß die ZVS im Rahmen des Vergabeverfahrens mit verschiedenen Hochschulen personenbezogene Daten von zugelassenen Bewerbern austauscht. Die Hochschulen benötigen diese Daten zur Vorbereitung der mit der Einschreibung der Studienanfänger zusammenhängenden Arbeiten. Für die Beförderung dieser Unterlagen wird der Postweg benutzt; die Empfängeranschriften werden mit den beteiligten Hochschulen abgestimmt. Nach den weiteren Feststellungen war aus dem Begleitschreiben der ZVS nicht die spezielle Codierung des Datenträgers ersichtlich, sondern lediglich datenverarbeitungstechnische Arbeitshinweise für die Behandlung des Bandes durch das Rechenzentrum der Universität. Der eigentliche Code zur Entschlüsselung der gespeicherten Informationen ergibt sich erst aus den Angaben zum Bandsatzaufbau. Diese Angaben werden dem Rechenzentrum der jeweiligen Hochschule auf getrennten Wegen mitgeteilt.

Allem Anschein nach ist der Eingang des Magnetbandes beim AStA der Universität auf ein einmaliges Versehen der Postverteilungsstelle zurückzuführen.

Gleichwohl hat der Kanzler der betreffenden Universität den Vorfall zum Anlaß genommen anzuordnen, daß in den Fällen, in denen Einrichtungen der Universität selbst ohne Einschaltung eines Boten Post aus der Hausverwaltung bei der Anlieferungsstelle abholen, die eingegangene Post vor der Übergabe nochmals auf korrekte Aussortierung über-

prüft wird. Im übrigen ist die ZVS gebeten worden, beim Versand von Magnetbändern zukünftig die vollständige Adresse anzugeben. Diese Maßnahmen scheinen geeignet zu sein, die Wiederholung eines derartigen Versehens für die Zukunft auszuschließen.

Ich habe den Vorfall zum Anlaß genommen, die beteiligten öffentlichen Stellen zu bitten, ihre Mitarbeiter auf die besonderen Sorgfaltspflichten beim Umgang mit personenbezogenen Daten der Bürger hinzuweisen. Darüber hinaus habe ich empfohlen, Magnetbänder mit personenbezogenen Daten in Zukunft nur unter Wertangabe zu versenden. Nur bei dieser Versendungsform unterliegt die Weiterleitung bei der Deutschen Bundespost einer besonderen Sicherung.

17. Bildung und Kultur

a) Schulen

Eingaben mehrerer Bürger betrafen die Frage, welche personenbezogene Daten über Schüler und Erziehungsberechtigte bei welchen Stellen zu welchem Zweck gesammelt werden dürfen. Daten über Schüler und Erziehungsberechtigte werden insbesondere bei der Anmeldung der Schüler zu Grundschulen und weiterführenden Schulen erhoben. Die Anmeldevordrucke werden gesammelt. Die bei der Anmeldung erhobenen Daten werden in den mir bekanntgewordenen Fällen in das **Schülerstammblatt**, das bei Aufnahme eines Schülers in der Schule anzulegen ist, übertragen (§ 5 Abs. 4 der Allgemeinen Schulordnung — ASchO).

In einem mir mitgeteilten Fall wird darüber hinaus beim Schulverwaltungsamt, das auch die Aufgaben des Schulamtes wahrnimmt, im automatisierten Verfahren eine Datei „Einschulung Lernanfänger" geführt.

Wegen der datenschutzrechtlichen Probleme, die sich im Hinblick auf die Datenerhebung und — verarbeitung bei der schulärztlichen Untersuchung aus Anlaß der Einschulung ergeben, wird auf die Ausführungen über Datenschutz im Gesundheitswesen (oben C.13.a) verwiesen.

In einem zur Überprüfung der Datenerhebung bei der Anmeldung zur Aufnahme in weiterführenden Schulen vorgelegten **Anmeldevordruck** werden unter anderem Angaben über die Zahl der Geschwister, den Beruf des Vaters und der Mutter, den Namen der Krankenkasse und die Art der Versicherung erhoben.

Nach meiner Auffassung sind die Erziehungsberechtigten zu diesen Angaben nicht verpflichtet. Auch unter Berücksichtigung des gesetzlich festgelegten Erziehungsauftrags der Schule (§ 1 des Ersten Gesetzes zur Ordnung des Schulwesens im Lande Nordrhein-Westfalen — Sch OG —) ist eine allgemeine Erhebung über **Zahl der Geschwister** und **Beruf der Eltern** aus Anlaß des Übergangs eines Schülers in eine weiterführende Schule nicht erforderlich. Zwar wird nicht verkannt, daß der Lehrer zur Erfüllung erzieherischer Aufgaben bei schulischen Schwierigkeiten einzelner Schüler Kenntnis über deren Sozialverhältnisse haben muß. Dazu reicht es jedoch aus, wenn der Lehrer diese Daten im jeweiligen Einzelfall in geeigneter Weise erhebt.

Die vorsorgliche Erhebung dieser Daten bereits bei der Anmeldung zu der weiterführenden Schule kann deshalb nur auf freiwilliger Grundlage erfolgen. Nach § 10 Abs. 2 DSG NW ist, soweit in dem Anmeldevordruck nach der Geschwisterzahl und dem Beruf der Eltern gefragt wird, unmißverständlich auf die Freiwilligkeit hinzuweisen.

Soweit die auf freiwilliger Grundlage allgemein erhobenen Daten in das Schülerstammblatt übertragen und in der Sammlung der Stammblätter gespeichert werden, bedarf es darüber hinaus auch für die Datenverarbeitung der schriftlichen Einwilligung des Betroffenen nach § 3 Satz 1 Nr. 2 DSG NW. Nur wenn der Betroffene in dem Vordruck auch auf die beabsichtigte Speicherung hingewiesen wurde, kann in der Mitteilung der Daten eine

schlüssige Einwilligungserklärung des Betroffenen gesehen werden. Eine Speicherung ohne Einwilligung des Betroffenen kommt nicht in Betracht, da die Speicherung der Daten aller Schüler zur Aufgabenerfüllung der Schule nicht erforderlich ist (§ 10 Abs. 1 DSG NW).

Das Erheben von Angaben über die **Krankenkasse** und die Art der Versicherung halte ich auch auf freiwilliger Grundlage für bedenklich. Ein Bezug zur Erfüllung der Aufgaben der Schule ist nicht erkennbar. Zwar hat die Schule während der Zeit, in der die Schüler am Unterricht oder an einer sonstigen Schulveranstaltung teilnehmen, eine Aufsichtspflicht (§ 12 ASchO). Sie kann diese Pflicht jedoch auch ohne Kenntnis der genannten Daten erfüllen. Auch bei einer plötzlich auftretenden Erkrankung, die eine unverzügliche ambulante oder stationäre ärztliche Versorgung des Schüler erfordert, ist die Kenntnis dieser Daten nicht notwendig, da die Ärzte und Krankenhäuser auf jeden Fall zur Hilfeleistung verpflichtet sind. Es muß den Erziehungsberechtigten vorbehalten bleiben, im Einzelfall zu entscheiden, ob sie Leistungen einer Krankenkasse in Anspruch nehmen und, wenn sie bei verschiedenen Krankenkassen versichert sind, an welche sie sich wenden wollen.

Hierzu habe ich den Kultusminister um Stellungnahme gebeten.

Soweit in den Anmeldebögen nach der **Religionszugehörigkeit** des Schülers gefragt wird, ist diese Erhebung durch § 31 Abs. 2 SchOG gerechtfertigt. Nach dieser Vorschrift ist der Religionsunterricht ordentliches Lehrfach an allen allgemein bildenden Schulen und an allen Schulen, durch deren Besuch der Schulpflicht genügt wird; ausgenommen sind die Weltanschauungsschulen und die bekenntnisfreien Schulen. Der Schüler ist zur Teilnahme am Religionsunterricht verpflichtet, soweit nicht die Erziehungsberechtigten oder der religionsmündige Schüler eine schriftliche Willenserklärung auf Befreiung vom Religionsunterricht abgeben (§ 34 SchOG). Unter diesen Umständen muß davon ausgegangen werden, daß die Erziehungsberechtigten verpflichtet sind, bei der Anmeldung die Religionszugehörigkeit des Schülers anzugeben.

Sofern nicht bereits bei der Anmeldung des Schülers zur Schule die Abmeldung vom Religionsunterricht erfolgt, darf die Angabe über die Religionszugehörigkeit des Schülers auch in der Sammlung der Schülerstammblätter gespeichert werden, da ihre Kenntnis zur Erfüllung der Aufgaben der Schule erforderlich ist (§ 10 Abs. 1 DSG NW).

In einem weiteren Fall wurden im Bereich eines Schulamtes sämtliche **Grundschulzeugnisse** der Schüler **bei Übergang auf weiterführende Schulen** der jeweils aufnehmenden Schule zugeleitet. Ein wesentlicher Grund für die Weitergabe der Zeugnisse soll die Vermeidung einer Archivierung bei der jeweiligen Grundschule sein.

Die Zeugnisse der Schüler enthalten zahlreiche personenbezogene Daten. Die Zeugnisse der Klassen 1 und 2 enthalten Aussagen über die Lernentwicklung im Arbeits- und Sozialverhalten sowie in den Lernbereichen/Fächern. Die Zeugnisse der Klasse 3 enthalten darüber hinaus Noten. Die Zeugnisse der Klasse 4 enthalten ausschließlich Noten.

Die Sammlung der Grundschulzeugnisse stellt eine Datei im Sinne von § 1 Abs. 2 Satz 1 DSG NW dar. Sie ist eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen erfaßt und geordnet, nach anderen bestimmten Merkmalen umgeordnet und ausgewertet werden kann (§ 2 Abs. 3 Nr. 3 DSG NW).

Nach meiner Auffassung ist die Abgabe der über einen Zeitraum von vier Grundschuljahren gesammelten Zeugnisse an die weiterführende Schule aus Anlaß des Übergangs des Schülers zur Erfüllung der Aufgaben der weiterführenden Schulen nicht erforderlich. Nach § 4 Abs. 4 Satz 2 Nr. 2 ASchO reicht für die Anmeldung zur weiterführenden Schule die Vorlage des Abgangs- oder Abschlußzeugnisses aus. Nach den Verwaltungsvorschriften zu § 14 Abs. 1 der Verordnung über den Bildungsgang in der Grundschule (AO-GS) ist bei der Anmeldung das Halbjahrszeugnis der Klasse 4 vorzulegen. Darüber hinaus beschränkt sich § 14 Abs. 2 AO-GS darauf, daß die weiterführende Schule ein Gut-

achten der Grundschule erhält. Hiernach geht der Verordnungsgeber grundsätzlich davon aus, daß eine Übermittlung weiterer Zeugnisse an die weiterführende Schule nicht geboten ist. Sie hat deshalb nach §§ 3 Satz 1 und 8 Satz 1 in Verbindung mit § 11 Abs. 1 Satz 1 DSG NW zu unterbleiben.

Der Kultusminister hat meine Auffassung bestätigt, daß nicht alle während des Besuches der Grundschule ausgestellten Zeugnisse der weiterführenden Schule auszuhändigen sind.

In den Verwaltungsvorschriften zu § 5 Abs. 4 ASchO, die zur Zeit vorbereitet werden, soll nach Mitteilung des Kultusministers im übrigen geregelt werden, welche Daten eines Schülers in das von der Schule zu führende Schülerstammblatt aufzunehmen sind und unter welchen Voraussetzungen sie weitergegeben werden können. Ich werde mich dafür einsetzen, daß in diesen Verwaltungsvorschriften die Weitergabe der Zeugnisdaten der Grundschulen an die weiterführenden Schulen ausdrücklich ausgeschlossen wird. Für die Erfüllung der Aufgaben der weiterführenden Schulen reicht es aus, bei der Anmeldung zur weiterführenden Schule das Halbjahreszeugnis der Klasse 4 vorzulegen und der weiterführenden Schule das Gutachten der Grundschule zuzuleiten.

Durch eine weitere Eingabe ist mir bekannt geworden, daß in einzelnen Schulen neben den allgemeinen Schülerdaten auch **Zeugnisdaten im automatisierten Verfahren** verarbeitet werden.

Um einen Überblick über diese Datenverarbeitung zu erhalten und gegebenenfalls notwendig werdende Kontrollen durchführen zu können, habe ich den Kultusminister um Auskunft gebeten, an welchen Schulen des Landes Computer zur Verarbeitung personenbezogener Daten, insbesondere von Schülern, eingesetzt werden und welche Erfahrungen über den Einsatz von Schulcomputern bei der Verarbeitung personenbezogener Daten vorliegen.

Mehrere Eingaben betrafen die **Führung des Klassenbuches**. Auch das Klassenbuch, das zahlreiche personenbezogene Daten von Schülern, Erziehungsberechtigten und Lehrern enthält, unterliegt dem Datenschutz. Zwar finden die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen keine Anwendung, weil das Klassenbuch mangels Umordnungsmöglichkeit der Daten keine Datei ist (§ 1 Abs. 2 Satz 1 in Verbindung mit § 2 Abs. 3 Nr. 3 DSG NW). Es gilt jedoch das Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung.

Ich habe deshalb dem Kultusminister empfohlen, das Festhalten personenbezogener Daten im Klassenbuch sowie den Zugang zum Klassenbuch ausdrücklich durch Rechtsvorschrift zu regeln. Dabei sollte ausgeschlossen werden, daß Schüler Zugang zu Daten von Erziehungsberechtigten erhalten, die über die in § 36 Abs. 2 Satz 1 DSG NW genannten Grunddaten (Namen, akademische Grade und Anschriften) hinausgehen.

Bei Fachoberschulen werden neben dem Klassenbuch besondere **Anwesenheitslisten** geführt. In den Anwesenheitslisten haben die Schüler ihre Teilnahme am Unterricht durch Unterschrift jeweils zu bestätigen.

Die Notwendigkeit der Führung einer Anwesenheitsliste ergibt sich aus § 9 Abs. 1 und 2 des Bundesausbildungsförderungsgesetzes (BAföG). Hiernach wird die Ausbildung gefördert, wenn die Leistungen der Auszubildenden erwarten lassen, daß sie das angestrebte Ziel erreichen. Dies wird in der Regel angenommen, solange die Auszubildenden die Ausbildungsstätte besuchen und entsprechende Studienfortschritte erkennen lassen. Das örtlich zuständige Amt für Ausbildungsförderung ist im Rahmen des § 48 BAföG zu benachrichtigen, wenn die Auszubildenden mehr als 3 Tage dem Unterricht unentschuldigt fernbleiben oder keine Aussicht auf Erlangung der angestrebten und geförderten Abschlüsse besteht.

Über die gesetzliche Auskunftspflicht der Ausbildungsstätten gegenüber dem Amt für Ausbildungsförderung (§ 47 Abs. 2 BAföG) hinaus wird Dritten die Anwesenheitsliste nicht zugänglich gemacht.

Auf Grund der genannten Vorschriften habe ich gegen die Führung der Anwesenheitsliste keine datenschutzrechtlichen Bedenken.

Auf eine weitere Bürgereingabe habe ich zu der Frage Stellung genommen, ob im Rahmen des **Sachkundeunterrichts** in der Grundschule mit Hilfe eines Arbeitsbogens **Daten von Familienmitgliedern** erhoben werden dürfen. Die Schüler sollen durch die Verwendung des Arbeitsbogens unter anderem die Generationsfolge anhand der Altersangaben erfahren. Die Arbeitsbögen verbleiben in der Arbeitsmappe des einzelnen Schülers.

Nach meiner Auffassung kann das Erheben, Sammeln und Auswerten der in dem Arbeitsbogen genannten Daten der Schüler und ihrer Familienangehörigen auf die Bildungsaufgabe der Schule nach § 1 Abs. 3 SchOG gestützt werden. Danach hat die Schule die Aufgabe, die Jugend auf der Grundlage des abendländischen Kulturgutes und deutschen Bildungserbes in lebendiger Beziehung zu der wirtschaftlichen und sozialen Wirklichkeit sittlich, geistig und körperlich zu bilden und ihr das für Leben und Arbeit erforderliche Wissen und Können zu vermitteln. Hierzu gehört auch die Vermittlung der genannten Erfahrungen und Erkenntnisse. Eine Rechtspflicht der Eltern zur Mitwirkung bei der Erhebung der Daten besteht allerdings nicht.

Unter den gegebenen Umständen vermag ich einen Verstoß gegen Vorschriften über den Datenschutz nicht zu erkennen. Die ausgefüllten Arbeitsbögen dürfen jedoch nicht an andere Personen oder Stellen weitergegeben werden. Gegen ihren Verbleib in der Arbeitsmappe des einzelnen Schülers bestehen keine Bedenken.

Zum **Schulsparen** hat mir ein Bürger mitgeteilt, daß eine Sparkasse anläßlich der Einschulung in die Grundschule den **Schulanfängern** jeweils ein auf ihren Namen ausgestelltes und mit voller Anschrift versehenes Sparbuch mit einem Guthaben von 5 DM durch die Schule habe aushändigen lassen. Nach dem Ergebnis meiner Ermittlungen sind der Sparkasse die personenbezogenen Daten der in Frage kommenden Schüler auf Anforderung von den Schulleitern der Grundschulen ihres Geschäftsbereiches übermittelt worden.

In einem anderen Fall hat sich ein Bürger dagegen gewandt, daß eine Sparkasse personenbezogene Daten der in Frage kommenden Schüler bei einem städtischen Schulverwaltungsamt angefordert und erhalten hat, um bei den **Schulabgängern** eine Werbeaktion auf Einrichtung eines Girokontos durchzuführen.

Die Datenübermittlung verstößt in beiden Fällen gegen datenschutzrechtliche Vorschriften.

Die Übermittlung personenbezogener Daten der Schulanfänger und Schulabgänger von den Schulbehörden an die Sparkasse wäre nach § 11 Abs. 1 Satz 1 DSG NW nur unter der Voraussetzung zulässig, daß sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist. Die Voraussetzung der Erforderlichkeit ist bei der vorliegenden Datenübermittlung nicht erfüllt. Zwar gehört es nach § 3 Satz 2 des Sparkassengesetzes zu den gesetzlichen Aufgaben der Sparkassen, den Sparsinn und die Vermögensbildung zu fördern; dies ist hier jedoch keine Rechtfertigung für die Datenübermittlung. Für diese Aufgabenerfüllung ist eine Übermittlung von Schülerdaten zwar nützlich, aber nicht im Sinne des § 11 Abs. 1 Satz 1 DSG NW erforderlich.

Insbesondere die Übergabe eines auf den Namen des jeweiligen Kindes ausgestellten Sparbuches geht über die Erziehungsaufgabe der Förderung des Sparsinns hinaus und stellt sich als gezielte Kundenwerbung gegenüber Kindern dar. Insoweit beschränkt sich die Durchführung des Schulsparens durch die Sparkassen entgegen dem Runderlaß des Kultusministers des Landes Nordrhein-Westfalen vom 17. Juli 1973 (GABl. NW. S. 437) nicht auf den schulischen Zweck.

Auch die Übermittlung der Daten von Schulabgängern, um Sparkassen eine gezielte

Werbeaktion für die Einrichtung von Girokonten zu ermöglichen, ist mit dem schulischen Zweck nicht mehr vereinbar.

Die Sparkassen als öffentliche Wettbewerbsunternehmen sind für ihre Werbung ebensowenig auf die Datenübermittlung durch öffentliche Stellen angewiesen wie private Wettbewerbsunternehmen.

Hierbei ist zu berücksichtigen, daß die Sparkassen den privat-rechtlichen Kreditinstituten datenschutzrechtlich gleichgestellt sind. Dies ergibt sich aus den im wesentlichen gleichlautenden Vorschriften der §§ 18 bis 23 DSG NW und der §§ 22 bis 27 BDSG. Bei dieser vom Gesetzgeber gewollten Gleichstellung wäre der Wettbewerbsvorteil, der sich aus einer Datenübermittlung nach § 11 Abs. 1 Satz 1 DSG NW ergäbe, nicht gerechtfertigt.

Zwei an mich herangetragene Fälle betreffen datenschutzrechtliche Belange im Rahmen des Schulmitwirkungsgesetzes.

In einem Fall hat sich ein Bürger dagegen gewandt, daß die Erziehungsberechtigten einer **Klassenpflegschaft** jeweils eine **Liste** mit den Namen und Anschriften der Schüler und ihrer Erziehungsberechtigten unter Angabe des Berufes erhalten.

Der Kultusminister hat dazu wie folgt Stellung genommen:

Gemäß § 1 des Schulmitwirkungsgesetzes (SchMG) sei es Ziel der Mitwirkung, die Eigenverantwortung in der Schule zu fördern und das notwendige Zusammenwirken aller Beteiligten in der Bildungs- und Erziehungsarbeit der Schule zu stärken. Gemäß § 11 Abs. 2 SchMG seien Mitglieder der Klassenpflegschaft die Erziehungsberechtigten der Schüler der Klasse, mit beratender Stimme der Klassenlehrer. Um die Aufgaben in diesem Mitwirkungsorgan erfüllen zu können, sei es erforderlich, die Beteiligten zu kennen, etwa um zu den Versammlungen einladen zu können oder um gemeinsame Gespräche zu initiieren. Daher sei es zunächst berechtigt, im Rahmen dieser Aufgabenstellung die Namen und Adressen der Schüler den Erziehungsberechtigten bekanntzugeben. Auf der anderen Seite dürfe nicht verkannt werden, daß manche Eltern ein berechtigtes Interesse daran hätten, daß ihre Adressen nicht weitergegeben würden. In einem solchen Fall sollten auf den Widerspruch des Erziehungsberechtigten Name und Adresse nicht bekanntgegeben werden. Die Abwägung zwischen der ordnungsgemäßen Aufgabenerfüllung nach dem Schulmitwirkungsgesetz und den schutzwürdigen Belangen des Einzelnen könne nicht pauschal erfolgen, sondern sei im Einzelfall zu treffen. Eine Weitergabe der Berufe der Erziehungsberechtigten sollte jedenfalls unterbleiben oder nur dann durchgeführt werden, wenn alle ihr Einverständnis erklärt hätten. Die Listen dürften im übrigen nur im Rahmen des Schulmitwirkungsgesetzes verwendet werden. Ein zweckentfremdeter Gebrauch etwa in privatem Interesse sei unzulässig.

Diese Auffassung des Kultusministers des Landes Nordrhein-Westfalen wird von mir geteilt.

In dem anderen Fall aus dem Bereich der **Schulmitwirkung** hat sich ein Bürger dagegen gewandt, daß Vertreter der Erziehungsberechtigten und Schüler **bei der Entscheidung über Ordnungsmaßnahmen** durch die Klassenkonferenz mitwirken.

Das Datenschutzgesetz Nordrhein-Westfalen findet auf die Bekanntgabe der persönlichen Verhältnisse von Schülern und ihrer Erziehungsberechtigten an Eltern- und Schülervertreter im Zusammenhang mit der Entscheidung über Ordnungsmaßnahmen keine Anwendung, weil die genannten Daten nicht aus einer Datei übermittelt werden (§ 1 Abs. 2 Satz 1, § 2 Abs. 3 Nr. 3 DSG NW).

Wohl ist aber bei der Bekanntgabe solcher Daten das Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung zu beachten, dessen Anwendungsbereich nicht auf Dateien beschränkt ist.

Nach § 26a Abs. 5 des Schulverwaltungsgesetzes (SchVG) ist die Zuständigkeit der Klassenkonferenz für Ordnungsmaßnahmen auf die Erteilung eines schriftlichen Verweises

(Nr. 1) und den vorübergehenden Ausschluß vom Unterricht von einem Tag bis zu zwei Wochen und von sonstigen Schulveranstaltungen (Nr. 3) beschränkt. Nach § 9 Abs. 2 Satz 2 SchMG nehmen der Vorsitzende der Klassenpflegschaft sowie ein weiterer von der Klassenpflegschaft benannter Erziehungsberechtigter und ab Klasse 7 der Klassensprecher sowie ein weiterer von der Klasse benannter Schüler an der Sitzung der Klassenkonferenz mit beratender Stimme teil; dies gilt nicht, soweit es um die Beurteilung eines Schülers oder die Bewertung seiner Leistungen geht.

Nach Sinn und Zweck dieser Vorschrift ist über ihren Wortlaut hinaus die Mitwirkung der Eltern- und Schülervertreter in der Klassenkonferenz immer dann ausgeschlossen, wenn es sich um Erziehungsangelegenheiten eines einzelnen Schülers handelt. Deshalb beruft der Klassenlehrer nach heutiger Auslegung der Vorschrift der Klassenkonferenz ohne Eltern- und Schülervertreter ein, wenn es sich um einen Fall handelt, der voraussichtlich zu einem schriftlichen Verweis oder vorübergehenden Ausschluß vom Unterricht führen wird (Pöttgen in Pöttgen/Jehkul/Esser, Allgemeine Schulordnung, 3. Aufl., § 15 Anm. 7).

Diese Auslegung des § 9 Abs. 2 Satz 2 SchMG ist nach Artikel 4 Abs. 2 der Landesverfassung geboten. Es besteht kein überwiegendes Interesse der Allgemeinheit an der Bekanntgabe der genannten Daten an Eltern- und Schülervertreter. Hiernach dürfen, soweit es sich um Entscheidungen über Ordnungsmaßnahmen durch die Klassenkonferenz handelt, weder Eltern- noch Schülervertreter mitwirken.

Für die Überweisung in eine parallele Klasse oder Lerngruppe, die Androhung der Entlassung von der Schule und die Entlassung von der Schule ist die Lehrerkonferenz zuständig (§ 26a Abs. 5 Nr. 2, 4 und 5 SchVG). Nach § 15 Abs. 4 der Allgemeinen Schulordnung hört die Lehrerkonferenz vor der Entscheidung über Ordnungsmaßnahmen einen Vertreter der Schulpflegschaft und des Schülerrates, soweit der betroffene Schüler oder seine Erziehungsberechtigten nicht widersprechen. Unter der Voraussetzung, daß der Schüler und seine Erziehungsberechtigten auf ihr Widerspruchsrecht vor der Anhörung hingewiesen werden, ist dieses Verfahren mit Artikel 4 Abs. 2 der Landesverfassung vereinbar. Es ist deshalb datenschutzrechtlich nicht zu beanstanden.

Ein Bürger hat sich darüber beschwert, daß das für ihn zuständige **Kreiswehrersatzamt** bereits vor Erfassung durch die Meldebehörde personenbezogene Daten über seine Person speichert. Das Kreiswehrersatzamt hatte ihm mitgeteilt, daß er sich vorzeitig einberufen lassen könne, um einen Zeitverlust bei der Berufsausbildung bzw. Hochschulbildung zu vermeiden.

Der Bundesminister der Verteidigung hat hierzu dem Bundesbeauftragten für den Datenschutz mitgeteilt, daß die zuständige Wehrbereichsverwaltung mit dem Kultusminister des Landes Nordrhein-Westfalen die Vereinbarung getroffen habe, daß den zuständigen Kreiswehrersatzämtern im Herbst jeden Jahres von den Schulen Listen übergeben werden, aus denen die Schüler ersichtlich sind, die vor der Erfassung und Musterung ihre Schulausbildung beenden.

Gegen dieses Verfahren bestehen datenschutzrechtliche Bedenken. Nach §§ 3 Satz 1, 11 Abs. 1 Satz 1 DSG NW ist eine Datenübermittlung an öffentliche Stellen nur zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist. Es ist sicher keine in der Zuständigkeit der Schule liegende Aufgabe, anderen öffentlichen Stellen Listen der Schulabgänger zur Verfügung zu stellen. Zwar kann es als Aufgabe der Kreiswehrersatzämter angesehen werden, Schulabgänger über die Möglichkeit der vorzeitigen Einberufung zu informieren. Zur Erfüllung dieser Aufgabe ist jedoch die Kenntnis der Daten der Schulabgänger nicht erforderlich. Es genügt, wenn wie in Baden-Württemberg, Hamburg, Hessen und Schleswig-Holstein im Herbst jeden Jahres den Schulbehörden von den Bundeswehrverwaltungsbehörden entsprechende Merkblätter übergeben werden, die an die in Betracht kommenden Schüler verteilt werden. Auf diese Weise kann dem Informationsinteresse der Betroffenen ohne Übermittlung ihrer Daten Rechnung getragen werden.

Zur Vermeidung von Verstößen gegen Vorschriften über den Datenschutz habe ich dem Kultusminister empfohlen, künftig wie in den genannten Ländern zu verfahren.

Eine Eingabe betraf die **Einsichtnahme in Schülerakten.**

Im vorliegenden Fall handelte es sich um eine **Ersatzschule** gemäß § 36 Abs. 3 SchOG. Ersatzschulen erfüllen eine staatliche Aufgabe und fungieren insoweit als beliehene Unternehmen (vgl. Ruckriegel in Ruckriegel/v. d. Groeben/Hunsche, Datenschutz und Datenverarbeitung in Nordrhein-Westfalen, § 1 Anm. 6). Die Aktivität als Schulträger einer staatlich anerkannten Ersatzschule ist als behördliche Tätigkeit anzusehen und als solche zu behandeln (§ 1 Abs. 4 VwVfG). Deshalb finden, obwohl der Träger der Ersatzschule im vorliegenden Fall eine Gesellschaft des privaten Rechts ist, nach meiner Auffassung die Datenschutzvorschriften für öffentliche Schulen Anwendung.

Nach § 16 DSG NW haben öffentliche Stellen einem Betroffenen auf Antrag **Auskunft** über die zu seiner Person gespeicherten personenbezogenen Daten zu erteilen. Dies gilt jedoch nur, soweit die Daten in einer Datei gespeichert sind (§ 1 Abs. 2 Satz 1 DSG NW), nicht aber, wenn sie in Akten festgehalten werden, da Akten keine Datei sind (§ 2 Abs. 3 Nr. 3 DSG NW).

Die Sammlung der Schülerstammblätter stellt allerdings eine Datei dar, da sie eine gleichartig aufgebaute Sammlung von Daten ist, die nach bestimmten Merkmalen erfaßt und geordnet, nach anderen bestimmten Merkmalen umgeordnet und ausgewertet werden kann (§ 2 Abs. 3 Nr. 3 DSG NW). Insoweit besteht also ein Auskunftsrecht des betroffenen Schülers. Ob ein minderjähriger Schüler dieses Recht ohne Einwilligung seines gesetzlichen Vertreters selbst wahrnehmen kann, hängt nach meiner Auffassung davon ab, ob er durch die Auskunfterteilung lediglich einen rechtlichen Vorteil erlangt (§ 12 Abs. 1 Nr. 2 VwVfG NW, § 107 BGB).

Ein allgemeines Akteneinsichtsrecht des Betroffenen ist im Gesetz nicht vorgesehen. Nur im Rahmen eines Verwaltungsverfahrens ist eine Behörde nach § 29 Verwaltungsverfahrensgesetz Nordrhein-Westfalen verpflichtet, den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit die Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist.

Allerdings kann ein allgemeines Akteneinsichtsrecht des Betroffenen aus dem neuen Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung hergeleitet werden. Denn um die hieraus folgenden Ansprüche wirksam geltend machen zu können, muß der Betroffene die über ihn festgehaltenen Daten kennen. Diese Auffassung hat sich jedoch noch nicht allgemein durchgesetzt.

Auf jeden Fall wäre es aus der Sicht des Datenschutzes zu begrüßen, wenn öffentliche Stellen einem Bürger auch ohne gesetzliche Verpflichtung Einsicht in die ihn betreffenden Akten gewähren würden, soweit nicht höherrangige Rechtsgüter Geheimhaltung gebieten.

b) Volkshochschulen

Eine Eingabe betraf die Datenerhebung einer Volkshochschule bei der **Anmeldung der Kursteilnehmer.** Ähnliche Erhebungen finden nach meinen Informationen auch bei anderen Volkshochschulen statt. Erhoben werden Namen, Anschriften, Telefonanschluß, Bankverbindung, Staatsangehörigkeit, Alter, Schulabschluß und soziale Stellung im Beruf. Die Anmeldekarte (Erhebungsbogen) sieht die Erklärung vor, daß sich der Kursteilnehmer mit der Speicherung seiner Angaben zu Beruf und Alter für statistische Zwecke einverstanden erklärt.

Gegen eine solche Erhebung bestehen wegen Fehlens eines Hinweises nach § 10 Abs. 2 Satz 1 DSG NW Bedenken.

Zweck der genannten Vorschrift ist, den Betroffenen über die Rechtslage aufzuklären, damit er selbst prüfen kann, ob und in welchem Umfang er zur Mitwirkung verpflichtet ist. Da-

bei ist zu berücksichtigen, daß auch freiwillige Aussagen und Angaben zur Erlangung einer bestimmten Verwaltungsentscheidung oft auf Grund einer Rechtsvorschrift erhoben werden. In diesen Fällen ist neben der Rechtsvorschrift auch auf die Freiwilligkeit oder die Rechtsfolgen einer unterbliebenen Mitwirkung hinzuweisen.

Zur Vermeidung von Verstößen gegen den Datenschutz habe ich empfohlen, in das Anmeldeformular einen Hinweis aufzunehmen, der etwa folgende Fassung erhalten könnte:

„Die Anmeldung kann nur bearbeitet werden, wenn Familienname, Vorname, Wohnort, Straße und Hausnummer des Kursteilnehmers angegeben werden. Rechtsgrundlage für die Erhebung sind § 37 Abs. 1 des Verwaltungsverfahrensgesetzes Nordrhein-Westfalen und die (im einzelnen jeweils zu benennenden) Vorschriften der Satzung für die Volkshochschule in Verbindung mit der Entgeltordnung für die Volkshochschule.

Die Beantwortung der anderen Fragen ist freiwillig.

Die Angabe der Telefonnummer ist für die Benachrichtigung bei Veranstaltungsänderungen erforderlich.

Die Angabe der Bankverbindung, der Kontonummer und der Bankleitzahl dient der Erstattung der Entgelte, wenn eine Veranstaltung nicht durchgeführt oder abgesagt wird. Rechtsgrundlage ist die (im einzelnen jeweils zu benennende) Vorschrift der Entgeltordnung für die Volkshochschule in Verbindung mit § 13 Abs. 1 der Gemeindekassenverordnung; danach ist der Zahlungsverkehr nach Möglichkeit unbar abzuwickeln.

Die Angaben über Staatsangehörigkeit, Alter, Schulabschluß und soziale Stellung im Beruf dienen statistischen Zwecken; sie werden bei der Volkshochschule in einer Kartei gespeichert und anonymisiert an den Landesverband der Volkshochschulen von Nordrhein-Westfalen e. V. weitergegeben."

Stellt der Betroffene nach diesem Hinweis freiwillig Angaben zu seiner Person zur Verfügung, so willigt er damit, soweit dies nach dem Datenschutzgesetz Nordrhein-Westfalen erforderlich ist, schlüssig in die ihm mitgeteilte Speicherung und Verwendung seiner Daten ein.

Ein weiterer Fall betraf die Frage, ob öffentliche Schulen nach § 11 Abs. 1 Satz 1 DSG NW die **Anschriften von Schulabgängern** auf Anforderung der Volkshochschulen übermitteln dürfen, um den Volkshochschulen die Möglichkeit zu geben, über bestimmte Weiterbildungsangebote zu informieren.

Aus datenschutzrechtlicher Sicht bestehen gegen diese Übermittlung keine Bedenken, wenn die Kenntnis der Anschriften zur Durchführung der den Volkshochschulen obliegenden Aufgaben erforderlich ist.

18. Finanzwesen

a) Steuerverwaltung

In meinem ersten Tätigkeitsbericht (C.15.a) hatte ich darauf hingewiesen, daß die für die Abgabenordnung (AO) zuständigen Referenten der obersten Finanzbehörden und die Datenschutzbeauftragten des Bundes und der Länder über den **Umfang der Kontrollbefugnisse** der Datenschutzbeauftragten unterschiedliche Auffassungen vertreten. Der Finanzminister hat mir nunmehr seine Auffassung mitgeteilt, die mit der der obersten Finanzbehörden des Bundes und der anderen Länder übereinstimmt.

Er vertritt unter Hinweis auf die Stellungnahme der Landesregierung zu meinem ersten Tätigkeitsbericht die Ansicht, der Landesbeauftragte für den Datenschutz könne Kontrollrechte nur ausüben, soweit personenbezogene Daten in einer Datei verarbeitet oder aus einer Datei übermittelt werden. Demgegenüber halte ich, wie oben (A.2.a) ausgeführt, an

meiner Auffassung fest, daß sich die Kontrollbefugnis für die Einhaltung der „anderen Vorschriften über den Datenschutz" nach § 26 Abs.1 Satz 1 DSG NW nicht auf die Datenverarbeitung in Dateien und die Datenübermittlung aus Dateien beschränkt, sondern auch auf den Umgang mit Daten in Akten und anderen Unterlagen erstreckt.

Der Finanzminister ist ferner der Ansicht, daß im Bereich der Datenerhebung — also der Sachverhaltsermittlung durch die Finanzämter — abgesehen von der Beachtung der Hinweispflicht nach § 10 Abs. 2 DSG NW Kontrollbefugnisse durch das Datenschutzgesetz Nordrhein-Westfalen nicht begründet würden. Der Landesbeauftragte sei auch dann nicht berechtigt, die von den Finanzbehörden zur Sachverhaltsaufklärung getroffenen Maßnahmen zu kontrollieren, wenn sich ein Betroffener auf ein Auskunftsverweigerungsrecht berufe.

Dieser Ansicht kann ich ebenfalls nicht folgen. Zu den „anderen Vorschriften über den Datenschutz", deren Einhaltung der Landesbeauftragte zu kontrollieren hat, gehören sowohl das Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung, das für jede Datenerhebung eine gesetzliche Grundlage verlangt, als auch die Vorschriften der Abgabenordnung, die dem Schutz des Betroffenen vor rechtswidrigem Umgang mit seinen Daten dienen. Hierzu ist auch das Auskunftsverweigerungsrecht nach § 102 AO zu rechnen, das als besondere, dem allgemeinen Datenschutzrecht vorgehende Regelung in § 45 Satz 2 Nr. 3 BDSG ausdrücklich genannt wird. Soweit solche „anderen Vorschriften über den Datenschutz" die Datenerhebung regeln, unterliegt deren Einhaltung meiner Kontrolle.

Der Finanzminister vertritt schließlich die Ansicht, daß dem Landesbeauftragten Einsicht in die Datenbestände der Finanzverwaltung nur zu gewähren sei, soweit dadurch keine Rückschlüsse auf bestimmte Personen möglich seien oder von einer Zustimmung des Betroffenen (§ 30 Abs. 4 Nr. 3 AO) ausgegangen werden könne oder in begründeten Einzelfällen ein zwingendes öffentliches Interesse bestehe (§ 30 Abs. 4 Nr. 5 AO). Eine darüber hinausgehende Offenbarungsbefugnis gegenüber dem Landesbeauftragten sei nicht gegeben. Insbesondere könne sie nicht auf § 30 Abs. 4 Nr. 2 AO gestützt werden, da sie durch kein Gesetz ausdrücklich zugelassen werde. Das nordrhein-westfälische Datenschutzrecht könne dem bundesgesetzlich geregelten Steuergeheimnis nicht vorgreifen; die Bundesgesetzgebung enthalte aber keine Bestimmung, die eine Offenbarung gegenüber dem Datenschutzbeauftragten ausdrücklich zulasse.

Dieser Ansicht kann ich aus folgenden Gründen nicht zustimmen.

Nach § 19 Abs. 3 Satz 2 BDSG ist dem Bundesbeauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben uneingeschränkt Einsicht in alle im Zusammenhang mit der Verarbeitung personenbezogener Daten stehenden Unterlagen und Akten, namentlich in die gespeicherten Daten zu gewähren. In § 19 Abs. 3 Satz 3 in Verbindung mit § 12 Abs. 2 Nr.1 BDSG werden die Bundesfinanzbehörden ausdrücklich einbezogen. Damit wird eine Offenbarung gegenüber dem Bundesbeauftragten im Sinne von § 30 Abs. 4 Nr.2 AO ausdrücklich zugelassen.

§ 7 Abs. 2 Satz 1 Nr. 1 BDSG überläßt die Regelung der Datenschutzkontrolle bei der Ausführung von Bundesrecht durch Landesbehörden den Ländern. Berücksichtigt man den Zusammenhang, in dem diese Vorschrift steht, so folgt aus ihr, daß nach dem objektiven Willen des Gesetzgebers die Länder dem § 19 Abs. 3 Satz 2 BDSG entsprechende Regelung für die Datenschutzkontrolle bei den Landesfinanzbehörden treffen dürfen, auch soweit darin eine Offenbarung durch das Steuergeheimnis geschützter Daten gegenüber der Kontrollinstanz vorgesehen wird. Dementsprechend bestimmt § 26 Abs. 3 Nr. 1 DSG NW, ohne hinsichtlich der Landesfinanzbehörden gegen Bundesrecht zu verstoßen, daß der Landesbeauftragte uneingeschränkt Einsicht in die im Zusammenhang mit der Datenverarbeitung stehenden Unterlagen und Akten, namentlich in die gespeicherten Daten verlangen kann, soweit es zur Erfüllung seiner Aufgaben erforderlich ist. § 26 Abs. 3 Nr. 1 DSG NW ist nach meiner Auffassung ebenso wie § 19 Abs. 3 Satz 2 BDSG eine gesetzliche Vorschrift, die eine Offenbarung von Daten im Sinne von § 30 Abs. 4 Nr.2 AO ausdrücklich zuläßt.

Es bleibt abzuwarten, wie sich die Meinungsverschiedenheiten über den Umfang der Kontrollbefugnis auf die Erfüllung meiner Kontrollaufgaben im Bereich der Steuerverwaltung auswirken. Ich werde jedenfalls auch in diesem Bereich Beschwerden nachgehen, die die Verletzung „anderer Vorschriften über den Datenschutz" außerhalb des Anwendungsbereichs der materiellen Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen (§ 1 Abs. 2 DSG NW) rügen.

Einige Bürger haben mich gebeten, ihnen bei der Durchsetzung ihres Rechts auf Auskunft über ihre beim Finanzamt gespeicherten personenbezogenen Daten behilflich zu sein, nachdem das Finanzamt die Auskunft verweigert hatte.

Ich habe die zuständigen Finanzämter auf die bereits in meinem ersten Tätigkeitsbericht (C.15.c) vertretene Auffassung hingewiesen und gebeten, ihre Entscheidung noch einmal zu überprüfen. In allen Fällen haben daraufhin die Finanzämter den Steuerpflichtigen die gewünschte Auskunft erteilt.

Ein gewerbliches Unternehmen, das die Verwaltung von Haus- und Grundbesitz betreibt und dazu eine Vielzahl von personenbezogenen Daten von Mietern sammelt, hat bei mir angefragt, ob das Finanzamt berechtigt sei, Auskunft über diese Daten zu verlangen oder Einsicht in die Unterlagen zu nehmen.

Ich habe darauf hingewiesen, daß ein derartiges Auskunfts- und Einsichtsrecht der Finanzbehörden besteht. Nach § 93 Abs. 1 AO haben außer den am Verfahren Beteiligten (§ 78 AO) auch andere Personen, also auch die Hausverwalter die zur Feststellung eines für die Besteuerung erheblichen Sachverhalts erforderlichen Auskünfte zu erteilen. Andere Personen sollen allerdings erst dann zur Auskunft angehalten werden, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziele führt oder keinen Erfolg verspricht. Gleiches gilt für das Recht der Finanzbehörden, von Dritten die Vorlage von Urkunden zu verlangen (§ 97 AO).

b) Kommunales Finanzwesen

Ein Warenhaus hat mich um Prüfung gebeten, ob es verpflichtet sei, dem Verlangen der Gemeinde nachzukommen, der Hundesteuerstelle Namen und Anschrift eines Kunden mitzuteilen, der in dem Warenhaus einen Hund gekauft hatte.

Meine Prüfung hat ergeben, daß die auf Grund des Kommunalabgabengesetzes erlassene Hundesteuersatzung der Gemeinde dem Hundehalter auferlegt, die Veräußerung seines Hundes sowie Namen und Anschrift des Erwerbers dem Steueramt mitzuteilen. Das Warenhaus ist, soweit es Handel mit Hunden betreibt, Hundehalter im Sinne dieser Satzung. Demnach verstößt das Verlangen der Gemeinde nicht gegen Vorschriften über den Datenschutz.

Mehrere Bürger haben bei mir angefragt, ob es zulässig sei, daß die Gemeinde für die Berechnung der Kanalbenutzungsgebühren Daten der Versorgungsbetriebe über den Frischwasserverbrauch heranzieht. In diesen Fällen erfolgte die Lieferung des Frischwassers durch die Stadtwerke, die in der Rechtsform einer Aktiengesellschaft oder einer Gesellschaft mit beschränkter Haftung geführt werden.

Rechtsgrundlage für die Erhebung von Angaben über den Frischwasserverbrauch als Maßstab für die Entwässerungsgebühren für abgeleitetes Schmutzwasser und damit auch Rechtsgrundlage für das Anfordern dieser Daten bei den Stadtwerken sind die auf Grund der Vorschriften der Gemeindeordnung und des Kommunalabgabengesetzes erlassenen Entwässerungssatzungen der einzelnen Gemeinden. § 11 Abs. 1 DSG NW kommt als Rechtsgrundlage nicht in Betracht, da diese Vorschrift nur die Datenübermittlung zwischen öffentlichen Stellen regelt und die betroffenen Stadtwerke als juristische Personen des privaten Rechts keine öffentlichen Stellen sind. Allerdings dürfen die Gemeinden die genannten Daten nur dann anfordern, wenn die Datenübermittlung auch nach den für die Stadtwerke geltenden Rechtsvorschriften zulässig ist.

Soweit die Stadtwerke juristische Personen des privaten Rechts sind, unterliegen sie den Vorschriften des Bundesdatenschutzgesetzes. Nach § 24 Abs. 1 Satz 1 BDSG ist die Übermittlung personenbezogener Daten zulässig, soweit es zur Wahrung berechtigter Interessen eines Dritten oder der Allgemeinheit erforderlich ist und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Im Hinblick darauf, daß die Gemeinden durch ihre Entwässerungssatzungen den Frischwasserverbrauch als Maßstab für die Entwässerungsgebühren für abgeleitetes Schmutzwasser bestimmt haben und eine andere vertretbare Art der Datenerhebung nicht erkennbar ist, bin ich davon ausgegangen, daß die Datenübermittlung durch die Stadtwerke zur Wahrung der Interessen der Gemeinden wie auch der Allgemeinheit erforderlich ist. Bei der gebotenen Interessenabwägung müssen demgegenüber Interessen des Betroffenen zurücktreten.

Unter den gegebenen Umständen konnte ich einen Verstoß gegen datenschutzrechtliche Vorschriften nicht feststellen.

Ein anderer Bürger hat sich bei mir darüber beschwert, daß das Steueramt einer Gemeinde die Höhe des Wassergeldes und der Kanalbenutzungsgebühren für sein Grundstück einem Mieter bekanntgegeben hat.

Die Vorschrift über das Steuergeheimnis (§ 30 AO) findet auf Wassergeld und Kanalbenutzungsgebühren keine Anwendung. Zwar ist nach § 12 Abs. 1 Nr. 1 Buchst. c des Kommunalabgabengesetzes die genannte Vorschrift über das Steuergeheimnis zu beachten. Dies gilt jedoch nur insoweit, als es sich um kommunale Steuern handelt. Wassergeld und Kanalbenutzungsgebühren sind aber keine Steuern.

Soweit derartige Angaben an Dritte übermittelt werden, findet das Datenschutzgesetz Nordrhein-Westfalen Anwendung. Nach § 13 Abs. 1 Satz 1 DSG NW ist eine Abwägung zwischen den Interessen des Mieters und den Belangen des betroffenen Vermieters geboten. Dabei kommt es auf die Vertragsgestaltung des Mietverhältnisses im einzelnen an. Nur wenn der Mieter die Höhe der Abgaben für seine Rechtsverteidigung kennen muß und darüber hinaus zunächst vergeblich versucht hat, die Belege für das Wassergeld und die Kanalbenutzungsgebühren bei dem Vermieter einzusehen, kann davon ausgegangen werden, daß sein Interesse gegenüber den Belangen des Vermieters überwiegt.

19. Wirtschaft

a) Auskünfte aus dem Gewerberegister

Ein datenschutzrechtlicher Schwerpunkt in der Wirtschaftsverwaltung sind die Auskünfte aus dem Gewerberegister. Die kritische Auseinandersetzung mit dem von den Ländern erarbeiteten Musterentwurf allgemeiner Verwaltungsvorschriften über derartige Auskünfte hat dazu geführt, daß die nordrhein-westfälische Ausführungsanweisung zu den §§ 14, 15 und 55c der Gewerbeordnung (Runderlaß des Ministers für Wirtschaft, Mittelstand und Verkehr vom 24. Juni 1980 — MBl. NW. 1980 S. 1694) zur verbesserten Durchsetzung der Datenschutzvorschriften in wesentlichen Punkten von dem genannten Musterentwurf abweicht.

Dieser Musterentwurf geht davon aus, daß bei Einzelauskünften über Namen, betriebliche Anschrift und angemeldete Tätigkeit eines Gewerbetreibenden (einfache Einzelauskünfte) an Stellen außerhalb des öffentlichen Bereichs in der Regel Beeinträchtigungen schutzwürdiger Belange des Gewerbetreibenden „nicht zu befürchten" seien. Nach der nordrhein-westfälischen Ausführungsanweisung (Nr. 6.2.1) bestehen dagegen bei einfachen Einzelauskünften in der Regel nur dann keine Bedenken, wenn die Auskunft der Verfolgung privatrechtlicher Ansprüche dient und zur Durchsetzung der Ansprüche erforderlich ist. Einzelauskünfte dürfen jedoch „zur Geschäftsanbahnung oder an Auskunfteien oder Detekteien oder ähnliches" nach der genannten Ausführungs-

anweisung nur erteilt werden, wenn der Gewerbetreibende ausdrücklich darin eingewilligt hat.

Auch hinsichtlich der sogenannten Gruppenauskünfte (Auskünfte über mehrere oder eine Vielzahl von Gewerbetreibenden) wird den Belangen des Datenschutzes in der nordrhein-westfälischen Ausführungsanweisung (Nr. 6.2.2) wesentlich besser Rechnung getragen als in dem Musterentwurf. Gruppenauskünfte dürfen nach der Ausführungsanweisung in Nordrhein-Westfalen für Zwecke der Werbung und Meinungsforschung (z. B. an Verbände, Adreßbuchverlage, Versicherungen, Markt- und Meinungsforschungsinstitute) nur bei ausdrücklicher Einwilligung des Gewerbetreibenden erteilt werden. Hiernach bedarf auch die Weitergabe der Anschriften an Berufsverbände zum Zwecke der Mitgliederwerbung der Einwilligung der Betroffenen.

Die Durchsetzung dieser datenschutzfreundlichen Ausführungsanweisung des Ministers für Wirtschaft, Mittelstand und Verkehr des Landes Nordrhein-Westfalen wird von mir nachdrücklich unterstützt.

b) Datenübermittlung an Innungen

Der Minister für Wirtschaft, Mittelstand und Verkehr hatte mich — noch vor Inkrafttreten des Zehnten Buches des Sozialgesetzbuchs — um Stellungnahme gebeten, ob die Übermittlung personenbezogener Daten eines Innungsmitglieds durch die Krankenkasse und das Finanzamt an die Innung zum Zwecke der Beitragsveranlagung mit den Vorschriften über den Datenschutz vereinbar ist.

Die Zulässigkeit der Datenübermittlung von der Innungskrankenkasse an die Innung richtete sich damals nach § 35 Abs. 1 SGB I a. F. Zu den Betriebsgeheimnissen des Innungsmitglieds, die nach dieser Vorschrift geheimzuhalten waren, gehörte die Zahl der Beschäftigten und die Lohn- und die Gehaltssumme.

Die Offenbarung dieser Betriebsgeheimnisse wäre nur dann nicht unbefugt gewesen, wenn der Betroffene zugestimmt oder eine gesetzliche Mitteilungspflicht bestanden hätte.

Eine gesetzliche Mitteilungspflicht hätte eine Rechtsvorschrift erfordert, die ausdrücklich die Weitergabe ansonsten geheimzuhaltender Tatsachen gebietet. Diesen Anforderungen genügte die Innungssatzung nicht, da sie nur die Ermächtigung der Innung, gewisse Daten bei der Krankenkasse zu erfragen, nicht aber eine Verpflichtung der Krankenkasse zur Offenbarung vorsah. Mit einer derartigen Offenbarungsverpflichtung hätte die Innung im übrigen ihre Satzungskompetenz überschritten.

Eine Zustimmung des Betroffenen lag ebenfalls nicht vor. Er hatte sich weder ausdrücklich noch stillschweigend mit der Preisgabe seiner Betriebsgeheimnisse an die Innung einverstanden erklärt. Zwar hatte er mit seinem Antrag auf Aufnahme in die Innung deren Satzung als rechtsverbindlich anerkannt und bislang den Abruf der Lohnsumme unwidersprochen geduldet. Soweit darin eine Zustimmung im Sinne von § 35 Abs. 1 SGB I a. F. hätte liegen können, wäre die Zustimmung jedoch durch spätere Willensäußerungen des Betroffenen als widerrufen anzusehen gewesen. Insbesondere seine Weigerung, die ihm vorgelegte Einverständniserklärung zu unterschreiben, ließ keinen Zweifel daran, daß er mit einer Übermittlung seiner Betriebsgeheimnisse an die Innung nicht einverstanden war.

Nach meiner Auffassung konnte die Innung von den bei der Krankenkasse vorhandenen und für die Beitragsbemessung notwendigen Daten des Betroffenen in datenschutzrechtlich zulässiger Weise nur dadurch Kenntnis erlangen, daß sie ihn in ihrer Satzung zur Vorlage entsprechender Unterlagen verpflichtete.

Entsprechendes gilt im übrigen auch nach Inkrafttreten des Zehnten Buches des Sozialgesetzbuchs. Eine gesetzliche Offenbarungsbefugnis nach den §§ 68 bis 77 SGB X liegt nicht vor, so daß eine Offenbarung ohne Einwilligung des Betroffenen im Einzelfall unzulässig ist (§ 67 Satz 1 SGB X).

Demgegenüber war die Mitteilung des Gewerbesteuermeßbetrages durch das Finanzamt an die Innung zum Zwecke der Beitragsveranlagung datenschutzrechtlich nicht zu beanstanden. Rechtsgrundlage für eine derartige Mitteilung ist § 31 Abs. 1 AO. Danach sind die Finanzbehörden berechtigt, Steuermeßbeträge an Körperschaften des öffentlichen Rechts zur Festsetzung von solchen Abgaben mitzuteilen, die an diese Steuermeßbeträge anknüpfen.

20. Verkehrswesen

a) Fahrerlaubnisse

Anläßlich mehrerer Bürgereingaben habe ich mich mit der Frage befaßt, inwieweit die **Datenerhebung bei Anträgen auf Erteilung einer Fahrerlaubnis** durch die Straßenverkehrsämter mit den Vorschriften über den Datenschutz vereinbar sind. Rechtsgrundlage für die Datenerhebung sind § 2 Abs. 1 Satz 2 des Straßenverkehrsgesetzes (StVG) sowie die §§ 4 ff. und 15c Abs. 1 der Straßenverkehrs-Zulassungs-Ordnung (StVZO).

Auf Grund der genannten Vorschriften bestehen keine datenschutzrechtlichen Bedenken, bei Anträgen auf Erteilung einer Fahrerlaubnis außer den Identifizierungsmerkmalen

- Geburtsname,
- Familienname (bei Abweichung vom Geburtsnamen),
- Vorname,
- letzte bekannte Anschrift,
- Anschrift der gesetzlichen Vertreter (bei Antragstellung durch diese)

folgende personenbezogene Daten zu erheben:

- Geburtsdatum,
- Geburtsort und
- Staatsangehörigkeit.

Vor Erteilung einer Fahrerlaubnis hat die Verwaltungsbehörde beim Kraftfahrt-Bundesamt anzufragen, ob Nachteiliges über den Antragsteller bekannt ist (§ 13c Satz 1 StVZO). Für die Anfragen sind Vordrucke zu verwenden (§ 13d Satz 1 StVZO), über deren Inhalt und Ausgestaltung der Bundesminister für Verkehr mit Zustimmung des Bundesrates für die Verwaltungsbehörden bindende Allgemeine Verwaltungsvorschriften erlassen hat. Danach ist für die Anfrage an das Verkehrszentralregister ein Muster zu verwenden, das die vorgenannten, zur Identifizierung notwendigen Angaben zur Person enthält. Die Bestimmungen dieser Allgemeinen Verwaltungsvorschriften dienen auch dem Interesse des Betroffenen, da sie verhindern sollen, daß wegen nicht hinreichender Identifizierung Auskünfte erteilt werden, die sich nicht auf den Betroffenen beziehen. Bei fehlenden Identifizierungsmerkmalen könnten in Zweifelsfällen erhebliche Nachteile für den Betroffenen entstehen.

Für die Erhebung der vorstehenden Daten besteht zwar eine Rechtsgrundlage; die Antragsvordrucke enthalten jedoch, soweit sie mir bekannt geworden sind, nicht den in § 10 Abs. 2 Satz 1 DSG NW vorgeschriebenen Hinweis auf die Rechtsgrundlage. In den Antragsvordrucken ist künftig auf die Rechtsgrundlage der Datenerhebung hinzuweisen.

Auch die Erhebung des **Geburtsnamens der Mutter** wird von mir datenschutzrechtlich nicht beanstandet.

Nach § 4 Abs. 1 StVG in Verbindung mit § 15b StVZO muß die Verwaltungsbehörde die Fahrerlaubnis entziehen, wenn sich jemand als ungeeignet zum Führen von Kraftfahrzeugen erweist. Ungeeignet ist insbesondere auch, wer gegen Strafgesetze erheblich ver-

stoßen hat (§ 15b Abs. 1 Satz 2 StVZO). Um dies bei gegebenem Anlaß feststellen zu können, ist die Einholung eines Führungszeugnisses beim Bundeszentralregister erforderlich. Nach der für die Verwaltungsbehörden bindenden Zweiten Allgemeinen Verwaltungsvorschrift zur Durchführung des Bundeszentralregistergesetzes, die der Bundesminister der Justiz mit Zustimmung des Bundesrates erlassen hat, ist bei Anträgen einer Behörde auf Erteilung eines Führungszeugnisses auch der Geburtsname der Mutter anzugeben. Die Bestimmung dieser Verwaltungsvorschrift dient auch dem Interesse des Betroffenen, da sie verhindern soll, daß wegen nicht hinreichender Identifizierung Führungszeugnisse erteilt werden, die sich nicht auf den Betroffenen beziehen. Bei fehlenden Identifizierungsmerkmalen könnten auch hier in Zweifelsfällen durch unrichtige Führungszeugnisse erhebliche Nachteile für den Betroffenen eintreten.

Um die Aufgabe nach § 4 Abs. 1 StVG, § 15b StVZO gegebenenfalls unverzüglich erfüllen zu können, ist die Verwaltungsbehörde auf die Kenntnis der für die Einholung eines Führungszeugnisses bestimmten Daten angewiesen. Ihre Erhebung bei der Antragstellung gewährleistet, daß keine Verzögerungen eintreten, die wegen der hohen Gefährdung anderer Verkehrsteilnehmer durch einen zum Führen eines Kraftfahrzeuges ungeeigneten Führerscheininhaber nicht verantwortet werden können.

Die Erhebung des Geburtsnamens der Mutter verstößt auch nicht gegen den verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz. Die mit der Erhebung dieser Angabe verbundene Belastung des Betroffenen, die nicht besonders schwer wiegt, steht in einem angemessenen Verhältnis zu dem damit verfolgten Zweck, Leib und Leben der Bürger durch Entziehung der Fahrerlaubnis ungeeigneter Führerscheininhaber zu schützen.

Das gleiche gilt für die Erhebung über abweichende Personendaten (z. B. Aliasnamen).

Soweit in einzelnen Antragsvordrucken nach der **Berufsbezeichnung** gefragt wird, ist diese Erhebung unzulässig.

Eine Rechtsgrundlage für die Erhebung über den Beruf des Antragstellers ist im Verfahren auf Erteilung einer Fahrerlaubnis nicht gegeben. Es ist auch nicht ersichtlich, für welchen Verwaltungszweck freiwillige Angaben des Antragstellers über seinen Beruf erforderlich sein sollten. Ich vertrete deshalb die Auffassung, daß die Erhebung über den Beruf künftig zu unterbleiben hat.

Hinsichtlich der in den Antragsvordrucken vorgesehenen Erhebung über den **Gesundheitszustand** sowie der in einzelnen Antragsvordrucken zusätzlich vorgesehenen Erhebung über **anhängige Ermittlungs- und Strafverfahren** gilt folgendes.

Nach § 2 Abs. 1 Satz 2 StVG ist die Fahrerlaubnis zu erteilen, wenn unter anderem keine Tatsachen vorliegen, die die Annahme rechtfertigen, daß der Antragsteller zum Führen von Kraftfahrzeugen ungeeignet ist. Die Eignung kann insbesondere wegen schwerer oder wiederholter Verstöße gegen Strafgesetze, Neigung zum Trunk, zur Rauschgiftsucht oder zu Ausschreitungen, insbesondere Roheitsvergehen, sowie durch körperliche oder geistige Mängel beschränkt oder ausgeschlossen sein (§ 9 Satz 1 StVZO).

Danach dürfen Auskünfte sowohl über den Gesundheitszustand des Antragstellers wie über etwa schwebende Ermittlungs- und Strafverfahren eingeholt werden.

Die Ermittlungen der Behörde über den **Gesundheitszustand** des Antragstellers sind nach den genannten Vorschriften erforderlich. Dem steht nicht entgegen, daß in den verschiedenen Antragsvordrucken die Fragen zu einzelnen Krankheiten des Antragstellers unterschiedlich gestellt sind; denn die einzelnen Krankheiten werden zur Erläuterung nur beispielhaft zu der in allen Antragsvordrucken gestellten umfassenden Frage nach dem Gesundheitszustand des Antragstellers aufgezählt.

Bei den über die Eignung des Antragstellers von der Behörde durchzuführenden Ermittlungen sind die Verfahrensgrundsätze der §§ 24 und 26 des Verwaltungsverfahrensgesetzes für das Land Nordrhein-Westfalen (VwVfG NW) zu beachten. Nach § 26 Abs. 1 VwVfG NW können Auskünfte beim Antragsteller eingeholt werden. Gemäß § 10 Abs. 2

Satz 1 DSG NW ist er auf die Rechtsgrundlagen der Erhebung in geeigneter Weise hinzuweisen. Die Auskünfte des Antragstellers sind jedoch nach § 26 Abs. 2 Satz 1 und 2 VwVfG NW freiwillig.

Allerdings wird der Antragsteller bei Nichtbeantwortung der Fragen zum Gesundheitszustand damit rechnen müssen, daß die Behörde von Amts wegen im Rahmen des Untersuchungsgrundsatzes des § 26 Abs. 1 VwVfG NW weitere Ermittlungen durchführen wird. Soweit bei Beantwortung der Fragen oder bei den weiteren Ermittlungen Tatsachen bekannt werden, die Bedenken gegen die Eignung des Antragstellers begründen, kann die Behörde die Beibringung eines amts- oder fachärztlichen Zeugnisses fordern (§ 12 Abs. 1 StVZO).

In die Antragsvordrucke ist ein entsprechender Hinweis nach § 10 Abs. 2 Satz 1 DSG NW aufzunehmen, soweit dies bisher noch nicht geschehen ist.

Sofern in Antragsvordrucken die Erklärung vorgesehen ist, daß der Antragsteller mit einer **Auskunft des Gesundheitsamtes** auf Anfrage der Straßenverkehrsbehörde einverstanden sei und daß er den Amtsarzt von der Schweigepflicht entbinde, ist dies mit § 12 Abs. 1 StVZO nicht vereinbar.

Werden Tatsachen bekannt, die Bedenken gegen die gesundheitliche Eignung des Antragstellers begründen, so kann die Behörde nach dieser Vorschrift nur die Beibringung eins amts- oder fachärztlichen Zeugnisses fordern. Nach dieser Regelung kann der Antragsteller noch nach der ärztlichen Untersuchung entscheiden, ob er das ärztliche Zeugnis der Behörde zuleiten will oder nicht. Bei dieser Rechtslage darf vom Antragsteller nicht gefordert werden, daß er bereits bei Antragstellung einem Amtshilfeersuchen der Straßenverkehrsbehörde an das Gesundheitsamt und damit der unmittelbaren Übersendung des Zeugnisses durch die Untersuchungsstelle an die Straßenverkehrsbehörde zustimmt.

Soweit die Antragsvordrucke mit § 12 Abs. 1 StVZO nicht vereinbar sind, ist eine entsprechende Änderung vorzunehmen.

Soweit in einzelnen Antragsvordrucken nach **anhängigen Ermittlungs- oder Strafverfahren** gefragt wird, ist die Ermittlung der Behörde nach § 2 Abs. 1 Satz 2 StVG in Verbindung mit § 9 Satz 1 StVZO ebenfalls zulässig. Es kann nicht davon ausgegangen werden, daß hier der Grundsatz der Erfoderlichkeit verletzt werde. Die Tatsache, daß nicht in allen Antragsvordrucken nach schwebenden Ermittlungs- und Strafverfahren gefragt wird, spricht nicht gegen die Notwendigkeit dieser Erhebung; denn auch in den Fällen, in denen die Antragsvordrucke diese Frage nicht enthalten, muß nach den genannten Vorschriften eine Ermittlung über die Eignung des Antragstellers im Hinblick auf etwa strafbares Verhalten durchgeführt werden. Die hierzu erforderliche Auskunft darf nach § 26 Abs. 1 VwVfG NW sowohl beim Antragsteller wie auch bei Dritten, insbesondere auch bei anderen Behörden eingeholt werden.

Wird die Auskunft beim Antragsteller selbst eingeholt, ist er wie bei der Erhebung über den Gesundheitszustand auf seine Rechte gemäß § 10 Abs. 2 Satz 1 DSG NW hinzuweisen.

In die Antragsvordrucke ist auch insoweit ein Hinweis nach § 10 Abs. 2 Satz 1 DSG NW aufzunehmen.

Den Minister für Wirtschaft, Mittelstand und Verkehr des Landes Nordrhein-Westfalen habe ich gebeten, darauf hinzuwirken, daß meinen Bedenken künftig hinsichtlich der von den Straßenverkehrsämtern verwendeten Antragsvordrucke Rechnung getragen wird.

Ein Ortsvorsteher hat sich unter datenschutzrechtlichen Gesichtspunkten dagegen gewandt, daß er in einem Verfahren auf Neuerteilung einer Fahrerlaubnis von dem Gemeindedirektor beauftragt worden war, **Ermittlungen über Bedenken gegen die Eignung zum Führen von Kraftfahrzeugen** vorzunehmen.

Nach § 13d Abs. 7 Satz 3 und 4 der Gemeindeordnung Nordrhein-Westfalen (GO NW) kann der Ortsvorsteher mit der Erledigung bestimmter Geschäfte der laufenden Verwal-

tung beauftragt werden, die er in Verantwortung gegenüber dem Gemeindedirektor durchführt. Hierzu gehören auch Ermittlungen über Bedenken gegen die Eignung zum Führen von Kraftfahrzeugen nach § 9 Satz 1 StVZO.

Soweit der Ortsvorsteher Feststellungen über die in § 9 Satz 1 StVZO genannten Mängel zu treffen hat, bestehen keine datenschutzrechtlichen Bedenken. Dies gilt auch für die Fragen nach dem Leumund und den familiären Verhältnissen des Antragstellers, soweit sie sich auf die für die Eignung zum Führen von Kraftfahrzeugen relevanten Sachverhalte beschränken. So kann etwa die Neigung zu Gewalttätigkeiten gegenüber Familienangehörigen durchaus Bedenken gegen die Eignung zum Führen von Kraftfahrzeugen begründen.

Derartige Ermittlungen verstoßen auch nicht gegen den verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz. Die mit ihnen verbundene Belastung steht noch in einem angemessenen Verhältnis zu dem mit ihnen verfolgten Zweck, Leib und Leben der Bürger dadurch zu schützen, daß zum Führen von Kraftfahrzeugen ungeeigneten Personen die Fahrerlaubnis versagt wird.

Bedenklich erscheinen mir jedoch Ermittlungen der örtlichen Behörden über die wirtschaftlichen Verhältnisse des Antragstellers, da für die Eignung wirtschaftliche Gesichtspunkte nicht maßgebend sind (vgl. Entscheidung des Hessischen Verwaltungsgerichtshofs in Verkehrsrechtliche Mitteilungen 1969 S. 48).

Auch bei der Durchführung der Ermittlungen nach § 9 Satz 1 StVZO durch die örtliche Behörde sind die Verfahrensgrundsätze der §§ 24 und 26 VwVfG NW zu beachten. Danach können Auskünfte sowohl beim Antragsteller selbst als auch bei Dritten eingeholt werden.

Soweit die Ermittlungen beim Antragsteller selbst durchgeführt werden, ist er gemäß § 10 Abs. 2 Satz 1 DSG NW auf die Rechtsgrundlagen der Erhebung in geeigneter Weise hinzuweisen. Die Auskünfte des Antragstellers sind jedoch nach § 26 Abs. 2 VwVfG NW freiwillig. Auch hierüber ist er nach § 10 Abs. 2 Satz 1 DSG NW zu belehren.

Auch soweit zur Ermittlung des für die Erteilung der Fahrerlaubnis relevanten Sachverhalts Dritte gehört werden, besteht nach § 26 Abs. 3 VwVfG NW grundsätzlich keine Verpflichtung zur Auskunft. Die Hinweispflicht des § 10 Abs. 2 Satz 1 DSG NW gilt zwar nicht für Datenerhebungen bei einem Dritten. Im Interesse des Datenschutzes wäre es jedoch wünschenswert, auch den Dritten auf die Freiwilligkeit seiner Angaben hinzuweisen.

Die genannten datenschutzrechtlichen Gesichtspunkte sind in dem Runderlaß des Ministers für Wirtschaft und Verkehr des Landes Nordrhein-Westfalen vom 31. Januar 1956 (SMBl. NW. 9210) noch nicht berücksichtigt. Sie sind jedoch bei der Anwendung des genannten Runderlasses seit Inkrafttreten des Datenschutzgesetzes Nordrhein-Westfalen ergänzend zu beachten. Ich habe deshalb dem Minister für Wirtschaft, Mittelstand und Verkehr empfohlen, den Runderlaß entsprechend zu ändern.

Mehrere Eingaben betrafen die **Verwertbarkeit von Straftaten nach Tilgung im Bundeszentralregister.** In diesen Eingaben haben sich Bürger dagegen gewandt, daß frühere unter Alkoholeinwirkung begangene Straßenverkehrsvergehen im Verfahren auf Neuerteilung einer Fahrerlaubnis noch berücksichtigt wurden, obwohl die entsprechenden Eintragungen im Bundeszentralregister bereits getilgt waren. Ich habe die Betroffenen darauf hingewiesen, daß hier eine Ausnahme vom Verwertungsverbot des Bundeszentralregistergesetzes (BZRG) besteht.

Nach § 49 Abs. 1 BZRG darf eine Verurteilung nach Tilgung im Register dem Betroffenen im Rechtsverkehr grundsätzlich nicht mehr vorgehalten und nicht zu seinem Nachteil verwertet werden. Eine Ausnahme von diesem Verwertungsverbot gilt nach § 50 Abs. 2 BZRG für Verfahren, die die Erteilung einer Fahrerlaubnis zum Gegenstand haben, wenn die Verurteilung wegen dieser Tat in das Verkehrszentralregister einzutragen war.

Hiernach ist es grundsätzlich datenschutzrechtlich nicht zu beanstanden, wenn insbesondere alkoholbedingte Straßenverkehrsvergehen im Verfahren auf Neuerteilung der

Fahrerlaubnis nach Löschen im Bundeszentralregister und Verkehrszentralregister noch berücksichtigt werden.

b) Kraftfahrzeugzulassung

In zahlreichen Eingaben haben sich Bürger dagegen gewandt, daß ihre Kraftfahrzeughalterdaten zu Werbezwecken verwendet wurden.

In den meisten Fällen ist auf Grund der durchgeführten Ermittlungen davon auszugehen, daß das Kraftfahrt-Bundesamt die Daten zu Werbezwecken weitergegeben hat. Überwiegend hatten die betroffenen Bürger bei der Zulassung ihres Kraftfahrzeugs darin eingewilligt, daß die Daten zu Werbezwecken verwendet werden dürften.

Für solche Fälle ist darauf hinzuweisen, daß die betroffenen Bürger ihre bei der Kraftfahrzeugzulassung abgegebene Einwilligung in die Datenübermittlung durch das Kraftfahrt-Bundesamt bei den Straßenverkehrsämtern widerrufen können. Die Straßenverkehrsämter werden sodann das Kraftfahrt-Bundesamt entsprechend unterrichten.

In einem Fall hat sich ein Bürger darüber beschwert, daß ein Straßenverkehrsamt Halterdaten an einen Dritten übermittelt hatte. Der Dritte hatte die Übermittlung beantragt, um die Daten seines Unfallgegners zu erhalten. Die Übermittlung der Daten durch das Straßenverkehrsamt ist in einem solchen Fall datenschutzrechtlich nicht zu beanstanden.

Für die Zulässigkeit für die Übermittlung von Halterdaten an Personen oder andere Stellen außerhalb des öffentlichen Bereichs gilt § 26 Abs. 5 der Straßenverkehrs-Zulassungs-Ordnung in Verbindung mit § 13 Abs. 1 Satz 1 DSG NW. Danach ist eine Übermittlung solcher Daten 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.

Der Unfallgeschädigte hat ein berechtigtes Interesse, die Daten des Halters eines am Unfall beteiligten Fahrzeugs zu erfahren. Zur Durchsetzung etwaiger Forderungen aus Verkehrsunfällen ist es erforderlich, daß der Unfallgeschädigte Daten über Halter und Versicherer des an dem Verkehrsunfall beteiligten Fahrzeugs kennt. Bei der Abwägung der Interessen des Unfallgeschädigten mit den Belangen des Unfallbeteiligten an der Geheimhaltung seiner Halterdaten überwiegt das Interesse des Unfallgeschädigten, da sein Interesse nicht nur ein berechtigtes, sondern darüber hinaus auch ein rechtliches Interesse ist.

c) Technische Überwachungsvereine

Die Veröffentlichungspflicht der öffentlichen Stellen über gespeicherte personenbezogene Daten nach § 15 Abs. 1 DSG NW gab Anlaß, die datenschutzrechtliche Einordnung der Technischen Überwachungsvereine e. V. (TÜV) zu prüfen, soweit sie als Technische Prüfstellen für den Kraftfahrzeugverkehr tätig sind.

Bei der datenschutzrechtlichen Einordnung der Technischen Prüfstellen ist davon auszugehen, daß im Bereich des Kraftfahrsachverständigengesetzes (KfSachvG) die anerkannten Sachverständigen und Prüfer des TÜV als „beliehene Unternehmen" hoheitliche Befugnisse ausüben.

Aber auch die Technischen Prüfstellen des TÜV sind im Bereich des Kfz-Sachverständigenwesens öffentliche Stellen der (mittelbaren) Landesverwaltung.

Die Eigenschaft der Technischen Prüfstellen des TÜV als öffentliche Stellen ergibt sich, wie der Verwaltungsgerichtshof München in seinem Urteil vom 11. Februar 1974 (NJW 1975, S. 1796) ausgeführt hat, vor allem aus der engen finanziellen, organisatorischen und fachlichen Verflechtung zwischen Prüfertätigkeit und Prüfstelle, insbesondere aus dem Weisungsrecht, das der Leiter der Prüfstelle gegenüber den Prüfern hat (§ 11 Abs. 3 KfSachvG). Dieses Weisungsrecht des Leiters der Prüfstelle gegenüber den Prüfern ist von der organisatorischen Leitung der Prüfstelle des TÜV im übrigen nicht zu trennen.

Die demgegenüber vertretene Ansicht, der TÜV nehme im Bereich der Prüfstelle keine staatlichen Aufgaben wahr, weil es an der rechtssatzmäßigen Zuweisung fehle, vermag nicht zu überzeugen. Zwar ist in Nordrhein-Westfalen dem TÜV der in § 10 Abs. 1 KfSachvG vorgesehene Auftrag nur durch Briefwechsel erteilt worden. Eine Rechtsverordnungsermächtigung für diesen Auftrag sieht das Kraftfahrsachverständigengesetz aber auch nicht vor. Wollte man gleichwohl für die Aufgabenzuweisung eine Rechtsverordnung fordern, müßte das gleiche auch für die Aufgabenzuweisung an den einzelnen Prüfer gelten. Nach herrschender Meinung wird aber eine besondere rechtssatzmäßige Aufgabenzuweisung für die Prüfer nicht vorausgesetzt.

Soweit die Technischen Prüfstellen öffentliche Stellen sind, finden auf ihre Tätigkeit die Datenschutzgesetze der Länder Anwendung. Auf Grund des § 11 Abs. 2 Satz 2 KfSachvG werden die Prüfbogen bei der Prüfstelle selbst gesammelt. Auswertung und Mitteilung der Auswertungsergebnisse an Aufsichtsbehörde und Kraftfahrt-Bundesamt obliegen der Prüfstelle. Speichernde Stelle sind somit nicht die Prüfer oder der Leiter der Prüfstelle, sondern die Technische Prüfstelle.

Die Konferenz der Datenschutzbeauftragten ist zu dem Ergebnis gelangt, daß die Technischen Prüfstellen für den Kraftfahrzeugverkehr öffentliche Stellen im Sinne der Datenschutzgesetze sind und der Kontrolle der Datenschutzbeauftragten unterliegen.

Für Nordrhein-Westfalen gilt allerdings die Besonderheit, daß die Technischen Prüfstellen, obwohl sie besondere Organisationseinheiten des TÜV darstellen, nicht selbständige Normadressaten des Datenschutzgesetzes sind. Als Normadressat ist vielmehr nach § 1 Abs. 2 Satz 1 DSG NW der jeweilige TÜV als Träger seiner Prüfstellen anzusehen.

21. Eigenbetriebe und öffentliche Unternehmen

a) Verkehrsbetriebe

Auf Grund von Bürgereingaben war zu prüfen, inwieweit die Speicherung personenbezogener Daten in der sogenannten **Schwarzfahrerdatei** eines kommunalen Verkehrsbetriebes zulässig ist.

In dem einen Fall konnte ein 13-jähriger Schüler seine Schülermonatskarte auf der Fahrt zur Schule bei einer Kontrolle nicht vorweisen. Der Verkehrsbetrieb hat daraufhin ein erhöhtes Beförderungsentgelt gefordert. In dem Bescheid darüber wurde mitgeteilt, daß die im Zusammenhang mit der Beanstandung des Fahrausweises aufgenommenen Daten gespeichert würden (§ 22 Abs. 1 DSG NW). Nachdem nachgewiesen werden konnte, daß der Schüler im Zeitpunkt der Beanstandung Inhaber einer gültigen Zeitkarte war, hat der Verkehrsbetrieb den dafür in seinen Beförderungsbedingungen vorgesehenen niedrigeren Betrag als erhöhtes Beförderungsentgelt erhoben. Nach Zahlung dieses Betrages ist der Name des Schülers auf Antrag in der Datei gelöscht worden. In einem anderen Fall bestanden Meinungsverschiedenheiten zwischen einem Fahrgast und dem Verkehrsbetrieb darüber, ob der Fahrschein ordnungsgemäß entwertet worden war.

Nach dem Ergebnis meiner Ermittlungen werden in der Schwarzfahrerdatei außer Namen, Geburtsdatum, Anschrift und Aktenzeichen insbesondere Daten über Art, Höhe der Forderung, über das Verfahren zur Erledigung der Forderung sowie Vermerke über Wiederholungsfälle und Strafanträge gespeichert. Die Speicherung dient dem Verfahren zur Einziehung erhöhter Beförderungsentgelte. Darüber hinaus dient sie der Feststellung eines Wiederholungsfalles im Hinblick auf eine etwaige Strafverfolgung, insbesondere wegen Beförderungserschleichung (§ 265a StGB).

Soweit die Speicherung dem Verfahren zur Einziehung des vom Fahrgast geschuldeten erhöhten Beförderungsentgeltes dient, bestehen gegen ihre Zulässigkeit nach der ersten

Alternative des § 19 Satz 1 DSG NW keine durchgreifenden Bedenken, da die Speicherung zur Geltendmachung eines Zahlungsanspruches im Rahmen der Zweckbestimmung des Vertragsverhältnisses, nämlich des Beförderungsvertrages liegt. Dies kann jedoch dann nicht gelten, wenn die Voraussetzungen für das Erheben eines erhöhten Beförderungsentgeltes auch aus der Sicht des Verkehrsunternehmens so zweifelhaft sind oder ein etwaiges vertragswidriges Verhalten des Fahrgastes so geringfügig ist, daß von der Erhebung des erhöhten Beförderungsentgeltes von vornherein abgesehen wird.

Die Speicherung zum Zwecke einer Strafverfolgung im Wiederholungsfall könnte nur nach der zweiten Alternative des § 19 Satz 1 DSG NW als zulässig angesehen werden. Das setzt voraus, daß die Speicherung zur Wahrung berechtigter Interessen des Verkehrsunternehmens erforderlich ist und kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Zwar haben Verkehrsunternehmen ein berechtigtes Interesse an der strafrechtlichen Verfolgung des Erschleichens einer Beförderungsleistung. Die Speicherung von Daten ist jedoch zur Wahrung dieses Interesses nur dann im Sinne dieser Vorschrift erforderlich, wenn die gespeicherten Daten im Wiederholungsfall bei einem Strafverfahren hinreichend geeignet sind, insbesondere hinsichtlich subjektiver Tatbestandsvoraussetzungen verwertet zu werden.

Ob ein gespeicherter Vorgang als Indiz für ein etwaiges späteres Strafverfahren geeignet ist, kann nur unter Berücksichtigung der jeweiligen Umstände im Einzelfall entschieden werden. Es bestehen jedoch erhebliche Zweifel, ob derartige Daten für ein späteres Strafverfahren verwertbar sind, wenn im Einzelfall eine Fahrt ohne gültigen Fahrausweis als so geringfügig angesehen wird, daß das Verkehrsunternehmen von der Erhebung eines erhöhten Beförderungsentgeltes absieht. Auf jeden Fall kann eine Speicherung dann nicht als erforderlich angesehen werden, wenn sich der Fahrgast unwiderlegt dahin eingelassen hat, daß er seine Zeitkarte vergessen habe oder daß der Fahrscheinautomat defekt gewesen sei oder der Entwerter falsch eingestellt gewesen sein müsse.

Ein ähnliches Problem der Verwertbarkeit für ein etwaiges späteres Strafverfahren stellt sich, wenn ein Strafunmündiger (unter 14 Jahre) ein Verkehrsmittel ohne gültigen Fahrausweis benutzt hat. Noch deutlicher wird die mangelnde Verwertbarkeit gespeicherter Daten für ein etwaiges späteres Strafverfahren, wenn ein Schüler eine gültige Zeitkarte besitzt, sie jedoch bei einer Fahrt nicht vorzeigen kann.

Darüber hinaus setzt eine zulässige Speicherung nach § 19 Satz 1 DSG NW voraus, daß die Erhebung der gespeicherten Daten rechtmäßig war. Hieran bestehen erhebliche Zweifel, wenn der Fahrgast nicht selbst feststellen kann, ob sein Fahrschein wirksam entwertet wurde. Diese Möglichkeit ist nicht gegeben, wenn die Entwerter zwar den Betriebstag, nicht aber den Kalendertag stempeln. Unter diesen Umständen müssen Widersprüche und Unklarheiten bei der Datenerhebung zur Folge haben, daß die Speicherung unterbleibt.

Sind die Voraussetzungen der Speicherung nach der ersten Alternative des § 19 Satz 1 DSG NW wegen Zahlung des erhöhten Beförderungsentgeltes nicht mehr gegeben und sind darüber hinaus im jeweiligen Einzelfall die Voraussetzungen einer Speicherung im Hinblick auf einen etwaigen Wiederholungsfall nach der zweiten Alternative dieser Vorschrift von vornherein nicht erfüllt, so sind die Daten zu sperren (§ 23 Abs. 2 Satz 2 DSG NW) und auf Antrag des Betroffenen zu löschen (§ 23 Abs. 3 Satz 2 DSG NW). Nach § 23 Abs. 3 Satz 1 DSG NW können sie darüber hinaus auch von Amts wegen gelöscht werden. Wenn die Voraussetzungen für die Speicherung nach beiden Alternativen des § 19 Abs. 1 Satz 1 DSG NW von Anfang an nicht gegeben waren, müssen die Daten auch ohne Antrag des Betroffenen gelöscht werden (§ 23 Abs. 3 Satz 2 DSG NW).

Aus diesen Gründen ist es zu begrüßen, daß der Verkehrsbetrieb nach meiner Prüfung generell veranlaßt hat, daß Name und Anschrift

a) von Minderjährigen bei elterlich nicht genehmigter Fahrt,

b) von Strafunmündigen (unter 14 Jahren) auch bei elterlich genehmigter Fahrt, jedoch erst nach Zahlung des erhöhten Beförderungsentgeltes,

c) von Schülern, die ihre Schülerjahresfahrkarte vergessen haben, nach Zahlung des erhöhten Beförderungsentgeltes,

in der Datei gelöscht werden.

Auch in den weiteren oben genannten geringfügigen Fällen, die im Wiederholungsfall als Indiz für eine Strafverfolgung von vornherein nicht geeignet erscheinen, ist nach meiner Auffassung eine Sperrung oder Löschung der noch gespeicherten Daten geboten.

Die Prüfung, welche Löschungsfristen bei einer nach der zweiten Alternative des § 19 Satz 1 DSG NW zulässigen Speicherung dem Erforderlichkeitsgrundsatz entsprechen würde, ist noch nicht abgeschlossen. Nach den Erfahrungen dürfte eine Löschungsfrist von mehr als 1½ Jahren nicht erforderlich sein. Entsprechend werden im vorliegenden Fall bei Zahlung des erhöhten Beförderungsentgeltes die Daten durch den Verkehrsbetrieb bach 1½ Jahren gelöscht, wenn nicht inzwischen ein Wiederholungsfall eingetreten ist.

b) Kreditinstitute

Zahlreiche Bürgereingaben betrafen datenschutzrechtliche Fragen aus dem Bereich der öffentlich-rechtlichen Kreditinstitute.

In einem Fall hat sich ein Bürger darüber beschwert, daß ihm eine **Werbeschrift** eines Kreditinstituts übersandt worden sei, obwohl er sich in die sogenannte Robinson-Liste des Verbandes der Adressenverleger und Direktwerbeunternehmer habe eintragen lassen. Die in die Robinson-Liste eingetragenen Anschriften sollen von den dem Verband angeschlossenen Unternehmen für Werbezwecke nicht mehr verwendet werden.

Meine Ermittlungen haben ergeben, daß das Kreditinstitut ein dem genannten Verband angeschlossenes Werbeunternehmen mit dem Versand der Werbeschriften beauftragt. Das Werbeunternehmen stellt hierfür benötigte Anschriften bereit. Soweit Bürger dem Kreditinstitut mitteilen, daß sie die Zusendung von Werbematerial nicht wünschen, übermittelt das Kreditinstitut dem Werbeunternehmen die Anschriften dieser Bürger mit der Maßgabe, diesen kein Werbematerial mehr zuzusenden.

Der Verband der Adressenverleger und Direktwerbeunternehmer hat mitgeteilt, daß den ihm angeschlossenen Unternehmen der aktuelle Datenbestand der Robinson-Liste zweimal jährlich übermittelt werde, und zwar gegen Ende des ersten Quartals und zu Anfang des vierten Quartals eines Jahres. Es sei deshalb nicht zu verhindern, daß Bürger, die sich **nach** einem Übermittlungszeitpunkt in die Robinson-Liste hätten eintragen lassen, noch bis zum nächsten Übermittlungstermin Werbeschriften erhielten.

Werden solche Daten zu Werbezwecken gespeichert, besteht im Sinne des § 19 Satz 1 DSG NW nur dann kein Grund zur Annahme, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden, wenn eine auf dem neuesten Stand befindliche Robinson-Liste verwendet wird. Ich bin deshalb der Auffassung, daß Reklamesendungen öffentlich-rechtlicher Unternehmen an Bürger zu unterbleiben haben, wenn sich die Robinson-Liste bei dem beauftragten Werbeunternehmen nicht auf dem neuesten Stand befindet.

Ein Bürger hat sich mit der Frage an mich gewandt, ob ein Kreditinstitut Auskünfte über ihn an eine Bausparkasse zum Zweck der nachträglichen Überprüfung eines bereits abgeschlossenen Darlehnsvertrages erteilen dürfe.

Solche **Bankauskünfte** sind nach § 20 Abs. 1 Satz 1 DSG NW nur zulässig im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen oder soweit es zur Wahrung berechtigter Interessen der übermittelnden Stelle oder eines Dritten oder der Allgemeinheit erforderlich ist und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

Soweit die Bankauskunft zum Zweck der Überprüfung eines Darlehensvertrages erforderlich ist, der zwischen dem Betroffenen und dem um die Auskunft ersuchenden Kreditinstitut geschlossen wurde, liegt ein berechtigtes Interesse dieses Kreditinstituts an der Kenntnis der Kundendaten vor. Ob die Übermittlung schutzwürdige Belange des Kunden beeinträchtigt, kann nur unter Berücksichtigung aller Umstände des Falles beurteilt werden. Hierbei ist das Interesse des Kreditinstituts an der Überprüfung des Darlehensvertrages gegen das Interesse des Kunden an der Geheimhaltung seiner Daten abzuwägen.

Sofern Anhaltspunkte dafür bestehen, daß auf Grund der Überprüfung die Durchsetzung oder Sicherung von Rechtsansprüchen des Kreditinstituts gegen den Kunden erforderlich werden könnte, hätte das Kreditinstitut nicht nur ein berechtigtes, sondern auch ein rechtliches Interesse an der Kenntnis der Daten des Kunden. Ein solches Interesse überwiegt in der Regel gegenüber den Belangen des Betroffenen.

Kommen jedoch lediglich Ansprüche des Kreditinstituts etwa gegen einen Kreditvermittler in Betracht, so neige ich zu der Auffassung, daß das Interesse des Kunden an der Geheimhaltung seiner Daten gegenüber den Interessen des Kreditinstituts an der Durchsetzung dieser Ansprüche Vorrang hat. Eine Übermittlung wäre in diesem Fall unzulässig.

Während es sich in dem der Eingabe zugrunde liegenden Fall um eine Bankauskunft handelte, die sich auf die Beantwortung einer gezielten Frage beschränkte, hat ein Kontrollbesuch bei einer Sparkasse ergeben, daß auf Anfrage anderer Kreditinstitute auch allgemeine Bankauskünfte nach Vordruck erteilt werden. Dieser Vordruck wird auch von anderen Sparkassen für Bankauskünfte verwendet. Die Auskünfte erstrecken sich auf die Geschäftsverbindung des Kunden zur Sparkasse und auf seine Kreditwürdigkeit. Zum Teil werden über den Kunden Tatsachen mitgeteilt, wie über gewährte Kredite und über die Inanspruchnahme der Kredite durch den Kunden sowie über Grundbesitz des Kunden. Hinsichtlich der Kreditwürdigkeit sieht der für die Bankauskunft verwendete Vordruck Werturteile vor, wie zum Beispiel:

- Der Angefragte gilt als fleißig und vertrauenswürdig.
- Er erfreut sich eines guten Rufs.
- Der Betrieb wird umsichtig geleitet.
- Die Gesamtverhältnisse des Unternehmens machen einen geordneten Eindruck.
- Für den angefragten Betrag ist die Firma zur Zeit gut.
- Der angefragte Betrag dürfte im Rahmen des Geschäftsumfanges liegen.
- Die finanziellen Verhältnisse erscheinen angespannt. Dies wirkt sich auf die Zahlungsweise aus.
- Wir raten zur Vorsicht.

Die Zulässigkeitsvoraussetzungen nach § 20 Abs. 1 Satz 1 DSG NW für die Erteilung solcher Bankauskünfte durch die Sparkasse liegen im allgemeinen nicht vor.

Die Zweckbestimmung eines Darlehnsvertrages erfordert grundsätzlich nicht, daß die Sparkasse einem anderen Kreditinstitut Auskunft über die wirtschaftlichen Verhältnisse des Kunden erteilt. Diese Auskunft dient vielmehr in aller Regel lediglich einer Vertragsbeziehung, die das andere Kreditinstitut zu dem Kunden anbahnen will.

Auch berechtigte Interessen des anderen Kreditinstituts im Zusammenhang mit der Anbahnung einer Vertragsbeziehung mit dem Kunden rechtfertigen die Übermittlung im Rahmen der Bankauskunft nicht. Das Interesse des betroffenen Kunden an der Geheimhaltung seiner Daten überwiegt. Dies gilt insbesondere für Negativmerkmale. Die Schutzwürdigkeit der Belange des Kunden gegenüber negativen Aussagen ist um so mehr gegeben, als die Werturteile über die Kreditwürdigkeit in tatsächlicher Hinsicht

weitgehend nicht substantiiert sind. Hinzu kommt, daß allein die Nichtbeantwortung der im Vordruck vorgesehenen Fragen zu positiven Merkmalen zu ungewissen negativen Schlußfolgerungen und damit zu Beeinträchtigungen führen können, deren Tragweite der betroffene Kunde kaum zu übersehen vermag. Hieran ändert auch nichts der Hinweis in dem Vordruck, daß die nicht beantworteten Fragen als nicht vorhanden zu betrachten sind. Dieser Vorbehalt weist vielmehr den Empfänger auf die Möglichkeit derartiger Rückschlüsse hin.

Unter den gegebenen Umständen kann keinesfalls davon ausgegangen werden, daß der betroffene Kunde im Rahmen der Allgemeinen Geschäftsbedingungen der Sparkassen zu derartigen Bankauskünften eine wirksame Einwilligung nach § 3 Satz 1 Nr. 2 DSG NW erteilt habe. Für derartige Bankauskünfte bedarf es vielmehr einer eindeutigen Einwilligungserklärung, wie sie für die Datenübermittlung an die Schutzgemeinschaft für allgemeine Kreditsicherung (Schufa) bereits gefordert wird.

Ich habe empfohlen, künftig vor Erteilung solcher allgemeinen Bankauskünfte eine entsprechende Einwilligung des betroffenen Kunden einzuholen.

Die Sparkasse hat im gegebenen Fall zur allgemeinen Frage der Zulässigkeit einer Bankauskunft ausgeführt, daß eine vorsichtig formulierte Bankauskunft über den Betroffenen günstiger sein könne, als über ihn zu schweigen, weil der Dritte aus dem Schweigen noch ungünstigere Schlüsse über die Bonität des Betroffenen ziehen könnte. Dieser Einwand der Sparkasse ist für die Beurteilung, ob schutzwürdige Belange des Betroffenen durch eine Bankauskunft beeinträchtigt werden (§ 20 Abs. 1 Satz 1 zweite Alternative DSG NW), unerheblich. Denn die Wahrung des Geheimhaltungsinteresses kann durchaus auch bereits dann schutzwürdig sein, wenn eine Auskunft über den Betroffenen günstig ausfallen würde. Dies gilt selbst auf die Gefahr hin, daß ein Dritter aus dem Schweigen unrichtige Schlüsse über die Vermögensverhältnisse ziehen sollte. Deshalb muß es grundsätzlich der eigenen freien Entscheidung des betroffenen Bürgers überlassen bleiben, ob eine Bankauskunft über ihn erteilt wird oder nicht. Das Kreditinstitut hat entsprechend die Einwilligung des Bürgers einzuholen.

Hinsichtlich des hier erörterten Vordrucks für eine allgemeine Bankauskunft hat die Sparkasse im gegebenen Fall immerhin eingeräumt, daß die Verwendung des Vordrucks unter dem Gesichtspunkt des Bankgeheimnisses im Einzelfall bedenklich sein könne. Der Vordruck werde deshalb entsprechend einer Verbandsempfehlung im Hinblick auf eine bereits ergangene höchstrichterliche Entscheidung aus der Zeit vor Inkrafttreten der Datenschutzgesetze mit Vorsicht gehandhabt.

Ich bekräftige demgegenüber meine Auffassung, daß datenschutzrechtlich aus den oben dargelegten Gründen derartige allgemeine Bankauskünfte nach Vordruck ohne Einwilligung des Betroffenen grundsätzlich unzulässig sind.

Hinsichtlich der Zusammenarbeit der Sparkassen mit der Schufa hat sich ein Bürger darüber beschwert, daß eine Sparkasse bei Eröffnung eines Girokontos von ihm die Unterzeichnung der sogenannten **Schufa-Klausel** gefordert habe. Diese hat im vorliegenden Fall folgenden Wortlaut:

„Einverständniserklärung des Kontoinhabers nach den Vorschriften des Bundesdatenschutzgesetzes (BDSG) und des Datenschutzgesetzes Nordrhein-Westfalen (DSG NW)

1. Die Sparkasse ist berechtigt, der Schutzgemeinschaft für allgemeine Kreditsicherung (Schufa) Daten des Kontoinhabers über die Errichtung und nicht vertragsgemäße Nutzung dieser Kontoverbindung zur Speicherung zu übermitteln.
2. Die Adresse der zuständigen Schufa lautet:

.....

3. Diese Einverständniserklärung erfolgt im Sinne des § 3 Abs. 1 Nr. 2 BDSG und DSG NW. Eine Durchschrift dieser Einverständniserklärung habe(n) ich/wir erhalten.

.....

Unterschrift"

Der Bürger hält es für nicht gerechtfertigt, daß die Sparkasse die Unterzeichnung der Klausel zur Bedingung für die Kontoeröffnung gemacht habe, da er das Girokonto als Baukonto habe einrichten wollen, um für die Bauabwicklung Gelder einzuzahlen. Überziehungskredite habe er über dieses Konto nicht in Anspruch nehmen wollen.

Die Schufa-Klausel entspricht im vorliegenden Fall in Nr. 1 und 2 dem Vertrag, den Kreditinstitute mit der Schufa geschlossen haben. Nach dem Vertrag sind die angeschlossenen Kreditinstitute verpflichtet, im einzelnen festgelegte Meldepflichten gegenüber der Schufa einzuhalten.

Die Meldepflicht erstreckt sich insbesondere auf Konsumentenkredite bis zur Höhe von 50.000 DM und deren Abwicklungsmerkmale positiver und negativer Art. Meldepflichten bestehen auch hinsichtlich eines Girokontos, wenn die Kontoeröffnung der Schufa durch die Sparkasse angezeigt worden ist. Darüber hinaus sind nach dem Schufa-Vertrag unabhängig von dieser Einmeldung des Girokontos meldepflichtig: Rückscheck, Scheckkartenmißbrauch sowie Einziehung der Scheckvordrucke.

Ob Sparkassen bei Kontoeröffnung ausnahmslos die Unterwerfung unter die Schufa-Klausel verlangen dürfen, richtet sich nach § 9 des Gesetzes zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen (AGB-Gesetz). Danach sind Bestimmungen in Allgemeinen Geschäftsbedingungen unwirksam, wenn sie den Vertragspartner des Verwenders entgegen den Geboten von Treu und Glauben unangemessen benachteiligen (§ 9 Abs. 1 AGB-Gesetz). Die unangemessene Benachteiligung ist im Zweifel insbesondere anzunehmen, wenn eine Bestimmung mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht zu vereinbaren ist (§ 9 Abs. 2 Nr. 1 AGB-Gesetz). Die unangemessene Benachteiligung ist hier nicht schon deshalb zu verneinen, weil das Datenschutzgesetz die Möglichkeit einer Einwilligung vorsieht. Wenn eine Einwilligung in Allgemeinen Geschäftsbedingungen vorgeschrieben wird, kommt es für die Wirksamkeit einer solchen Klausel vielmehr darauf an, ob durch die Allgemeinen Geschäftsbedingungen von dem im Datenschutzgesetz (Zweiter und Dritter Abschnitt) oder anderen Vorschriften enthaltenen Grundgedanken des Datenschutzes wesentlich abgewichen wird. Der Datenschutz wäre wenig glaubwürdig, wenn die Einwilligung des Betroffenen in Allgemeinen Geschäftsbedingungen unterschiedslos als Zulässigkeitsvoraussetzung für die Verarbeitung personenbezogener Daten akzeptiert würde (vgl. Simitis in Simitis/Dammann/Mallmann/Reh, BDSG, 2. Aufl., § 3 Rdnr. 11 ff., 14).

Im Fall der Schufa-Klausel ist allerdings zu berücksichtigen, daß die Einwilligung in die Datenübermittlung und in die weitere Verarbeitung dem Zweck dient, ein Kreditsicherungssystem zu unterhalten und damit im Interesse der Kreditinstitute wie der Kreditnehmer die Kreditvergabe zu erleichtern (vgl. BGH NJW 1978, S. 2151). In Abwägung der beiderseitigen Interessen kann deshalb nicht davon ausgegangen werden, daß hier die Einwilligung in die Übermittlung an die Schufa zum Zweck der Speicherung im Sinne des § 9 Abs. 2 Nr. 1 AGB-Gesetz wesentlich von dem in den Datenschutzgesetzen enthaltenen Grundgedanken abweicht, einer Beeinträchtigung schutzwürdiger Belange des Bürgers entgegenzuwirken (§ 1 Abs. 1 Nr. 1 DSG NW).

Die in der Schufa-Klausel vorgesehene Einwilligung ist insoweit nicht als unwirksam anzusehen. Bedenken habe ich allerdings, soweit im gegebenen Fall das zu eröffnende Girokonto nach der Erklärung des Sparkassenkunden nur auf Guthabenbasis geführt werden soll. In einem solchen Fall müssen die Belange des Betroffenen maßgebend sein. Nach mir vorliegenden Informationen werden auch nicht von allen Sparkassen die Kon-

toeröffnungen ausnahmslos der Schufa gemeldet. Dies spricht dafür, daß die Meldung solcher Kontoeröffnungen für die Aufrechterhaltung des Kreditsicherungssystems nicht erforderlich ist. Unter diesen Umständen ist es nicht gerechtfertigt, wenn Sparkassen auch bei der Eröffnung eines Girokontos auf Guthabenbasis darauf bestehen, daß sich der Kunde der Schufa-Klausel unterwirft.

Bedenken bestehen hinsichtlich der Fassung der Schufa-Klausel insoweit, als der Betroffene nicht genügend über die Bedeutung der Einwilligung aufgeklärt wird (§ 3 Satz 3 DSG NW). Die Wirksamkeit der Einwilligung nach § 3 Satz 1 Nr. 2 DSG NW setzt die Kenntnis der für die Einwilligung erheblichen Umstände beim Betroffenen voraus. Dazu genügt zwar ein allgemeiner Hinweis, der dem Betroffenen gegebenenfalls weitere Fragen nahelegt. Ein solcher eine weitere Nachfrage des Betroffenen begründender Hinweis kann aber nicht bereits darin gesehen werden, daß in der Schufa-Klausel die Schufa als Empfänger der Daten konkret bezeichnet wird. Denn nach dem Wortlaut der Schufa-Klausel muß ein Betroffener, der von dem Kreditsicherungssystem keine nähere Vorstellung hat, annehmen, daß lediglich eine Speicherung bei der Schufa stattfindet. Dieser unvollständige Hinweis kann bei dem Betroffenen zu einem Irrtum führen mit der Folge, daß er sich überhaupt nicht veranlaßt sieht, sich über die weiteren Datenflüsse bei der Schufa zu vergewissern.

Hinsichtlich der Tragweite eines solchen Irrtums ist zu berücksichtigen , daß für den Betroffenen die Speicherung seiner Daten bei der Schufa weniger interessant sein dürfte. Entscheidend für seine Datenschutzposition ist dagegen, daß seine Daten allen Vertragspartnern der Schufa im Rahmen der Anschlußverträge zur Verfügung stehen (vgl. 2.9.2 des Zweiten Tätigkeitsberichts des Bundesbeauftragten für den Datenschutz). Um den hiernach bestehenden Bedenken hinsichtlich der Wirksamkeit der Schufa-Klausel zu begegnen, empfehle ich den Sparkassen, die Schufa-Klausel zur Klarstellung um folgenden Hinweis zu ergänzen:

> „Die Schufa stellt die Daten ihren Vertragspartnern im Rahmen der jeweiligen Anschlußverträge zur Verfügung."

Die Bedenken gegen die Annahme einer wirksamen Einwilligung in die in der Schufa-Klausel genannte Datenverarbeitung verstärken sich, wenn Sparkassen nach Maßgabe des mit der Schufa abgeschlossenen Anschlußvertrages die Schufa-Klausel anders als im vorliegenden Fall auf die Erklärung zu Nr. 1 und 2 der oben wiedergegebenen Klausel beschränken. In diesem Fall findet nach dem Schufa-Vertrag lediglich eine „Benachrichtigung" über die Datenübermittlung an die Schufa und über die Speicherung bei der Schufa statt. Hierbei wird in der Klausel bewußt auf die Worte „Einwilligung" oder „Einverständnis" verzichtet und lediglich festgestellt, daß die Sparkasse zur Datenübermittlung zum Zweck der Speicherung bei der Schufa „berechtigt" sei.

Diese bloße Feststellung der Berechtigung zu der in der Klausel angegebenen Datenverarbeitung entspricht der dem Schufa-Vertrag zugrundeliegenden Rechtsansicht, daß es zu dieser Datenverarbeitung einer Einwilligung des Bürgers nicht bedürfe, daß der Bürger vielmehr lediglich über die erstmalige Datenspeicherung bei der Schufa zu unterrichten sei (§ 34 Abs. 1 Satz 1 BDSG).

Die in dem Schufa-Vertrag vorgesehene Klausel, deren Inhalt gegenüber der im vorliegenden Fall verwendeten Klausel wesentlich eingeschränkt ist, stellt sich somit sowohl nach ihrem Wortlaut als auch nach dem im Schufa-Vertrag angegebenen Zweck nicht als Einwilligung, sondern verbunden mit der Feststellung einer angeblichen Berechtigung lediglich als „Benachrichtigung über die Datenspeicherung" dar.

Zumindest bestehen unter den gegebenen Umständen bei der Auslegung der im Schufa-Vertrag vorgesehenen Schufa-Klausel, wenn sie unter Beschränkung auf diesen Wortlaut von Sparkassen als Allgemeine Geschäftsbedingungen verwendet werden, erhebliche Zweifel, ob es sich bei einer solchen Klausel überhaupt um eine Einwilligung in die beabsichtigte Datenverarbeitung handeln soll. Die Zweifel gehen nach der

Unklarheitenregel des § 5 AGB-Gesetz zu Lasten des Verwenders solcher Allgemeinen Geschäftsbedingungen, da der Verwender sich hätte klarer ausdrücken können und müssen (Palandt zu § 5 AGB-Gesetz Anm. 4). Dies bedeutet, daß Sparkassen, die die Schufa-Klausel auf den im Schufa-Vertrag vorgesehenen Wortlaut beschränken, sich nicht auf eine Einwilligung berufen können.

Da nach meiner Auffassung für die Datenübermittlung der Sparkassen und die weitere Datenverarbeitung der Schufa eine Einwilligung des betroffenen Bürgers erforderlich ist, empfehle ich den Sparkassen, entsprechend dem oben wiedergegebenen Text einer erweiterten Schufa-Klausel in allen Fällen eine ausdrückliche Einwilligungserklärung aufzunehmen.

In einem weiteren Fall einer unzulässigen Datenübermittlung (§ 20 Abs. 1 Satz 1 DSG NW) im Sparkassenbereich hat sich ein Bürger über die **Fehlleitung** einer an ihn gerichteten **Überweisung an einen anderen Kontoinhaber** beschwert, der auch den Überweisungsträger mit sensiblen Daten des Betroffenen erhalten habe.

Bei dem Massengeschäft des Giroverkehrs kommt es immer wieder vor, daß die Kontonummer nicht dem Empfänger entspricht. In einem solchen Fall hat die Empfängerbank sich allein an die Empfängerbezeichnung zu halten (BGH. WM 1978, S. 367). Die Kreditinstitute haben auch im Interesse des Datenschutzes besondere Sorgfalt darauf zu verwenden, daß Überweisungsträger nicht fehlgeleitet werden. Bei einem Kontrollbesuch bei einer Sparkasse habe ich festgestellt, daß dort organisatorische Maßnahmen getroffen worden sind, um solche Fehler zu vermeiden.

Anläßlich einer Bürgereingabe habe ich mich auch mit dem **Einzugsermächtigungsverfahren** befaßt. Auf Grund der zwischen der jeweiligen Sparkasse und einzelnen Zahlungsempfängern getroffenen Vereinbarung über den Einzug von Forderungen mittels Lastschriften darf der Zahlungsempfänger Lastschriften zum Einzug nur einreichen, wenn ihm eine schriftliche Einzugsermächtigung des Zahlungspflichtigen vorliegt. Der Zahlungsempfänger hat zwar auf Verlangen der Sparkasse dieser die Einzugsermächtigung vorzulegen. Die Einzugsermächtigung wird jedoch in dem mir bekanntgewordenen Fall von der Sparkasse im allgemeinen nicht überprüft. Wenn das Konto bei der Sparkasse aufgelöst und ein neues Konto bei einem anderen Kreditinstitut eingerichtet wird, werden bei der Sparkasse noch eintreffende Lastschriften zunächst an das andere Kreditinstitut weitergeleitet. Nach einer gewissen Zeit werden die Lastschriften im vorliegenden Fall aber auch an den Zahlungsempfänger mit einem Vermerk über die neue Bankverbindung des Zahlungspflichtigen zurückgesandt.

Dieses Verfahren stößt auf datenschutzrechtliche Bedenken.

Soweit sich die Sparkasse die Einzugsermächtigung nicht nachweisen läßt, kann nicht hinreichend ausgeschlossen werden, daß mittels Lastschrift ein Konto unbefugt durch einen Zahlungsempfänger belastet wird, wodurch dem Zahlungsempfänger zugleich unbefugt die Angabe übermittelt wird, ob das Konto des angeblich Zahlungsverpflichteten mit einem bestimmten Betrag belastbar ist. Eine solche Datenübermittlung erfüllt nicht die Voraussetzungen des § 20 Abs. 1 Satz 1 DSG NW.

Um dieser auch datenschutzrechtlich relevanten Gefahr eines Mißbrauchs des Lastschriftverfahrens vorzubeugen, wäre es auch aus der Sicht des Datenschutzes zu begrüßen, wenn sich die Sparkasse im Interesse der Konteninhaber bei der ersten Lastschrift die Einzugsermächtigung vorlegen ließe. Seitens der Sparkassen wird allerdings eingewandt, daß ein solches Verfahren unter den gegebenen Umständen nicht praktikabel und die datenschutzrechtlich relevante Mißbrauchsgefahr gering einzuschätzen sei.

Auch die Weiterleitung von Lastschriften bei Auflösung des Sparkassenkontos an ein anderes Kreditinstitut ist nach § 20 Abs. 1 Satz 1 DSG NW nicht gerechtfertigt. Denn die Einzugsermächtigung erstreckt sich nur auf das frühere Konto bei der Sparkasse. Die Erklärung, die der Kunde im Rahmen des sogenannten Sparkassen-Umzugs-Services

abgibt, enthält bisher keine Einwilligung nach § 3 Satz 1 Nr. 2 DSG NW, ein anderes Kreditinstitut über Lastschriften, die das gelöschte Konto betreffen, zu informieren.

Ebensowenig ist es der Sparkasse nach § 20 Abs. 1 Satz 1 DSG NW erlaubt, den Zahlungsempfänger über das neue Konto des Zahlungsverpflichteten im Rahmen des Einzugsermächtigungsverfahrens zu unterrichten. Das berechtigte Interesse des Zahlungsempfängers, die neue Bankverbindung zu erfahren, rechtfertigt die Übermittlung nicht. Denn es kann durchaus den schutzwürdigen Belangen des Zahlungsverpflichteten entsprechen, daß der Zahlungsempfänger im Lastschriftverfahren nicht über das neue Konto unterrichtet wird. Hier überwiegt das Interesse des betroffenen Kunden an der Geheimhaltung seiner Daten.

Wenn die Sparkasse im Einzugsermächtigungsverfahren einem anderen Kreditinstitut und gegebenenfalls dem Zahlungsempfänger Daten übermitteln will, empfehle ich, die Einwilligung des Kunden gemäß § 3 Satz 1 Nr. 2 DSG NW im Rahmen des sogenannten Sparkassen-Umzugs-Services durch Ergänzung des entsprechenden Vordrucks einzuholen.

Bei einem Kontrollbesuch bei einer Sparkasse habe ich festgestellt, daß zur Erstellung der **Pensionsrückstellungsbilanz** zahlreiche Daten des versorgungsberechtigten Personals einem externen Versicherungsmathematiker übermittelt werden.

Es ist nicht ersichtlich, daß zum Zweck dieser Berechnungen die Übermittlung des Namens und Vornamens der Versorgungsberechtigten und ihrer Ehefrauen erforderlich ist. Die Verwendung einer Kennziffer für den Versorgungsberechtigten dürfte ausreichen.

Ich habe gebeten zu prüfen, ob künftig so verfahren werden kann. Der gegen meinen Vorschlag erhobene Einwand, daß bei Verwendung einer Kennziffer eine Verwechslungsgefahr bestehe, vermag nicht zu überzeugen.

Mehrere Eingaben betrafen die **Datensicherung** bei Sparkassen. In einem Fall war zu prüfen, ob eine Sparkasse für den Datenträgeraustausch Magnetbänder verwendet, auf denen sich nicht nur die jeweils für den Datenträgeraustausch benötigten Daten befinden, sondern auch Daten, die aus der früheren Verwendung der Magnetbänder stammen. Die Verwendung von Magnetbändern im Datenträgeraustausch, auf denen die Daten aus der früheren Verwendung der Bänder nur insoweit gelöscht sind, als das Band für den erneuten Datenträgeraustausch beansprucht wird, verstößt gegen die Datenschutzgrundsätze der §§ 5 Abs. 1, 6 Abs. 1, 3 Satz 1 in Verbindung mit § 20 DSG NW, weil damit mehr Daten als erforderlich weitergegeben werden. Ich habe festgestellt, daß die Sparkasse ein Löschgerät einsetzte, um die Daten aus der früheren Verwendung der für den Datenträgeraustausch bestimmten Bänder zu löschen.

In einer weiteren Eingabe wurde Beschwerde darüber geführt, daß die Konten der Angestellten einer Sparkasse nicht genügend vor der Einsichtnahme durch andere Mitarbeiter geschützt seien.

Welche technischen und organisatorischen Maßnahmen zur Datensicherung der Mitarbeiterkonten erforderlich sind, kann nur in genauer Kenntnis der Verhältnisse bei der jeweiligen Sparkasse beurteilt werden. Sofern die technischen und organisatorischen Voraussetzungen dafür vorliegen, kommt folgendes Verfahren in Betracht: Die Daten der Mitarbeiterkonten sind dem Kontenführer nur in der Weise zugänglich, daß ein bestimmter Mitarbeiter hinzugezogen werden muß, der erst durch Betätigung eines Kontrollschlüssels den Zugriff dieser Daten zuläßt (Vier-Augen-Prinzip). Über die Vorgänge wird ein maschinenbezogenes Journal erstellt. Die Maßnahmen zur Sicherung der Mitarbeiterkonten werden durch die Innenrevision geprüft.

Um die Zugriffskontrolle bei den Mitarbeiterkonten wie auch bei den Konten der übrigen Bankkunden zu gewährleisten, sollten die hierzu verwendeten geheimen Kenn-Nummern der Zugriffsberechtigten möglichst vielstellig sein. Sie sollten in unregelmäßigen und nicht zu großen Zeitabständen geändert werden. Die Kenn-Nummern

sollten anderen Mitarbeitern nur zugänglich sein, soweit es für den störungsfreien Ablauf des Geschäftsbetriebes unumgänglich notwendig ist. Auf diese Weise kann einer mißbräuchlichen Verwendung der geheimen Kenn-Nummern entgegengewirkt werden.

22. Neue Medien

a) Grundsätze

Die Vielfalt der Kommunikationsmöglichkeiten im Bereich der Neuen Medien (Bildschirmtext, Videotext, Kabelfernsehen, Teletext, Satellitenfernsehen) und die damit oft notwendigerweise verbundene Preisgabe personenbezogener Daten durch den einzelnen Teilnehmer ließen es den Datenschutzbeauftragten des Bundes und der Länder geboten erscheinen, bereits im Vorfeld einer möglichen Einführung einzelner Dienste gewisse Mindestforderungen zum Datenschutz zu erheben. Die von ihnen beschlossenen „Grundsätze für den Datenschutz bei den Neuen Medien (insbesondere bei Bildschirmtext und Kabelfernsehen)" sind in der Anlage zu diesem Bericht abgedruckt. Darin finden sich Aussagen zu der Informationssammlung über Teilnehmer, der Bedeutung der „Einwilligung" bei der Speicherung von Teilnehmerdaten sowie der Datenschutzkontrolle und der Datensicherung.

Ziel der Grundsätze ist ein umfassender Schutz des Teilnehmers und seiner personenbezogenen Daten. Sie sollen für den Datenschutz bei den Neuen Medien sicherstellen, daß die anlaufenden Erprobungen und die ihnen zugrundeliegenden Vorschriften den Datenschutz von vornherein berücksichtigen und dieser dem Einsatz neuer Technologien nicht nachfolgt. Die jeweils die Pilotprojekte planenden öffentlichen Stellen sowie die Parlamente sind aufgerufen, den mit diesen Forderungen angesprochenen Freiraum des Bürgers zu respektieren und durch entsprechende Datenschutzregelungen seine Privatsphäre zu schützen.

Für die Mitte des Jahres 1981 hat die Landesregierung Nordrhein-Westfalen einen Gesetzentwurf zum Kabelpilotprojekt Dortmund angekündigt. Ich gehe davon aus, daß die von den Datenschutzbeauftragten aufgestellten Grundsätze bei dem Gesetzesvorhaben Berücksichtigung finden.

b) Bildschirmtext

Der Beginn des Feldversuchs mit Bildschirmtext wurde durch Verordnung der Landesregierung auf den 1. Juni 1980 festgesetzt. Entsprechend meinen Ausführungen im ersten Tätigkeitsbericht (C. 19.) habe ich die Durchführung des Bildschirmtextversuchs beobachtet.

Für den Bereich der Bildschirmtextzentrale hatte sich der Gesetzgeber damit begnügt, daß meinen Forderungen ohne gesetzliche Verpflichtung durch einen rechtsverbindlichen Schriftwechsel zwischen der Deutschen Bundespost und dem Land Nordrhein-Westfalen Rechnung getragen wird. Nach meinen bisherigen Feststellungen steht das derzeitige Verfahren aber noch keineswegs im Einklang mit der Zusage des Bundesministers für das Post- und Fernmeldewesen, meinem sachlichen Anliegen in vollem Umfange Rechnung zu tragen.

So wird gegenwärtig für die automatisierte Auswertung des Versuchs nicht, wie zugesagt, nur jeder 50. Suchvorgang verfolgt und mit einer individuellen Kennung des Teilnehmers aufgezeichnet, sondern bereits jeder 10. Suchvorgang. Ich habe begründete Zweifel, ob die Ausdehnung auf jeden 10. Suchvorgang zu einer ebenso sicheren Anonymisierung führt, wie die von mir zunächst geforderte Regelung, nach der die durch Kombinieren verschiedener Kenngrößen gebildeten Gruppen mindestens 30 Teilnehmer umfassen müssen.

Darüber hinaus habe ich feststellen müssen, daß sämtliche Aufzeichnungen, die hiernach erfaßt werden, zur Zeit noch personenbezogen gespeichert sind. Die zugesagte und auch vorgesehene Anonymisierung unterbleibt offenbar nur deshalb, weil Angaben der die Begleituntersuchung durchführenden Wissenschaftler über die Definition von Benutzergruppen noch nicht vorliegen und deshalb die einzelnen Teilnehmer den Benutzergruppen noch nicht zugeordnet werden konnten.

Der Chef der Staatskanzlei hat daraufhin die beteiligten Wissenschaftler um möglichst umgehende Vornahme der erforderlichen Festlegungen gebeten und an den Bundesminister für das Post- und Fernmeldewesen die Bitte gerichtet, die notwendigen technischen Maßnahmen zur Anonymisierung unverzüglich einzuleiten.

Es bleibt festzuhalten, daß somit in wesentlichen Punkten, auf die ich im Hauptausschuß des Landtags besonders hingewiesen hatte (vgl. Vorlage 8/2299), meinen Forderungen bis jetzt noch nicht Rechnung getragen wurde.

Nach Mitteilung des Chefs der Staatskanzlei ist die Bildschirmtextzentrale im übrigen technisch nicht in der Lage, Name und Anschrift des Teilnehmers nur dann in die für den Anbieter bestimmte Antwortseite des Teilnehmers einzusetzen, wenn es sich um Dienste im Rahmen von Vertragsverhältnissen oder vertragsähnlichen Vertrauensverhältnissen handelt.

Auf einen möglichen Verstoß von Anbietern gegen § 4 Abs. 3 a) und b) des Bildschirmtextversuchsgesetzes NW habe ich den insoweit zuständigen Regierungspräsidenten Düsseldorf hingewiesen. Es ging um die Frage, ob Teilnehmer veranlaßt worden sind, auch gegen ihren Willen Namen und Anschrift an verschiedene Anbieter zu übermitteln. Das abschließende Ergebnis der vom Regierungspräsidenten in Düsseldorf zugesagten Überprüfung liegt noch nicht vor.

D. Organisatorische und technische Maßnahmen

Vor allem aus Kontrollbesuchen ergaben sich zahlreiche Empfehlungen, die organisatorische und technische Maßnahmen zur Verbesserung des Datenschutzes betrafen. In ihrer Bedeutung sind diese Empfehlungen nur selten auf die kontrollierten Stellen beschränkt. Sie sind vielmehr im allgemeinen übertragbar.

Die übertragbaren Empfehlungen werden in diesem Abschnitt zusammengestellt. Selbstverständlich ist dies keine vollständige Liste aller erforderlichen organisatorischen und technischen Maßnahmen. Die folgende Zusammenstellung enthält lediglich solche Empfehlungen, die auf Grund von tatsächlich festgestellten Mängeln oder Schwachstellen gegeben wurden.

Den meiner Kontrolle unterliegenden Behörden und sonstigen öffentlichen Stellen wird nahegelegt, auf dieser Grundlage ihre eigenen Maßnahmen zur Datensicherung zu überprüfen.

1. Bestellung eines internen Datenschutzbeauftragten

a) Allgemeine Empfehlung

Im Datenschutzgesetz Nordrhein-Westfalen ist die Bestellung eines internen Datenschutzbeauftragten nicht ausdrücklich vorgesehen. Allerdings besteht nach den §§ 6 und 8 DSG NW die Verpflichtung der Verwaltung zur datenschutzrechtlichen Selbstkontrolle. Dazu gehört insbesondere, die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen sowie die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen. Daher empfiehlt es sich, verbindlich festzulegen, wem die hiermit verbundene Verantwortung übertragen ist. Organisatorisch angemessen ist es im allgemeinen, die mit dem Datenschutz verbundenen zentralen Zuständigkeiten zusammenzufassen und dafür einen internen Datenschutzbeauftragten zu bestellen.

Dem internen Datenschutzbeauftragten sollten insbesondere folgende Aufgaben übertragen werden:

- Mitwirken bei der Schaffung von Dienstanweisungen für den Datenschutz
- Regelmäßige und unvermutete Kontrollen der Durchführung dieser Dienstanweisungen
- Verstärkte Kontrolltätigkeit in besonders sensiblen Bereichen
- Unterweisen der Mitarbeiter über den Datenschutz
- Führen der Übersicht nach § 8 DSG NW und deren laufende Überprüfung auf Vollständigkeit und Richtigkeit
- Unterweisen der Mitarbeiter über das korrekte Ausfüllen der dieser Übersicht dienenden Vordrucke.

Im Hinblick auf die große Bedeutung der übertragenen Schutzaufgabe sollte der interne Datenschutzbeauftragte in dieser Funktion direkt an die oberste Führungsebene berichten. Organisatorisch sollte er so zugeordnet sein, daß dadurch keine Interessenkonflikte vorprogrammiert sind. Er sollte daher nicht dem ADV-Bereich und möglichst auch keinem der Fachbereiche angehören.

Der interne Datenschutzbeauftragte hat in seiner Tätigkeit auf ihm nicht unterstellte Bereiche einzuwirken und diese zu kontrollieren. Wichtig ist es daher auch, seine Aufgabe schriftlich und im Detail festzulegen und alle betroffenen Stellen über diese Funktionsbeschreibung zu informieren.

b) Datenschutzbeauftragter bei einem Leistungsträger im Sinne von § 35 Abs. 1 SGB I

Für die dem Datenschutzgesetz Nordrhein-Westfalen unterworfenen Behörden und sonstigen öffentlichen Stellen besteht, soweit sie Leistungsträger im Sinne von § 35 Abs. 1 SGB I sind, seit 1. Januar 1981 eine neue Rechtslage. Nach § 79 Abs. 1 letzter Halbsatz SGB X sind die §§ 28 und 29 des Bundesdatenschutzgesetzes (Bestellung und Aufgaben eines Beauftragten für den Datenschutz) auf die in § 35 SGB I genannten Stellen entsprechend anzuwenden.

Daraus ergibt sich, daß Behörden und sonstige öffentliche Stellen, soweit sie Leistungsträger im Sinne des § 35 Abs. 1 SGB I sind, einen Beauftragten für den Datenschutz zu bestellen haben.

2. Maßnahmen der Strukturorganisation

Die Datensicherung hat bereits bei der Strukturorganisation zu beginnen. Ziel der hier zu treffenden Maßnahmen ist im allgemeinen eine Funktionstrennung; sie sollen die Zuordnung bestimmter Funktionen zu unterschiedlichen Organisationseinheiten bewirken.

a) Entwicklung von ADV-Programmen

– Programmfreigabe durch den Fachbereich

In mehreren Fällen wurde festgestellt, daß bei der Freigabe von ADV-Programmen die Verantwortung des Auftraggebers (Fachbereiches, Anwenders) keine angemessene Berücksichtigung fand. Der ADV-Bereich gab in diesen Fällen die Programme selbst frei. In einem Fall war er sogar von seinen Auftraggebern ausdrücklich zur endgültigen Freigabe ermächtigt. Eine solche Situation ist unbefriedigend, da sie nicht der Verantwortung des Auftraggebers für den fachlichen Programminhalt Rechnung trägt.

Nach Fertigstellung eines Programms sollte ein Testat der für die Programmierung verantwortlichen Stelle nicht ausreichend für die Freigabe zum Produktionslauf sein. In jedem Falle ist eine abschließende Überprüfung durch den Anwender (Anwendertest) erforderlich. Nur der Anwender sollte ein neues Programm freigeben können.

Eine solche Freigabe durch den Anwender sollte nicht nur bei neuentwickelten Programmen, sondern auch dann immer erfolgen, wenn von einer Programmänderung der fachliche Programminhalt betroffen ist. Eine Ausnahme bilden lediglich systembedingte Programmänderungen, die ohne Einfluß auf den fachlichen Programminhalt sind. Hier kann der ADV-Bereich selbst über die Freigabe entscheiden.

Im Rahmen der Programmfreigabe sollte an geeigneter Stelle auch zum Ausdruck kommen, daß mit dem Programm den Anforderungen des Datenschutzes Rechnung getragen wird. Die Frage einer zusätzlichen Freigabe durch den internen Datenschutzbeauftragten (oben D. 1. a) bleibt hiervon unberührt.

– Programmfreigabe durch die ADV-Revision

Falls eine getrennte Organisationseinheit mit der Aufgabe der ADV-Revision besteht, liegt es zunächst nahe, diese mit der alleinigen Anwenderfreigabe zu beauftragen. Jedenfalls wird damit dem Grundsatz Rechnung getragen, daß die Freigabe nicht allein durch die ADV-Abteilung erfolgen darf.

Bedenklich ist bei einer derartigen Regelung allerdings, daß die Freigabe nicht durch diejenige Stelle erfolgt, welche die fachliche Verantwortung für die mit dem Programm durchgeführten Arbeiten trägt. Bei diesem Vorgehen übernimmt vielmehr die ADV-Revision in vollem Umfang die Rolle des Anwenders. Bei der späteren Revisionstätigkeit kann dann die Situation entstehen, daß die ADV-Revision ihre eigenen Entscheidungen zu kontrollieren hat.

- **Vorläufige Programmfreigabe**

  Es kann Situationen geben, in denen aus Termingründen von dem normalerweise zu praktizierenden Freigabeverfahren abgewichen werden muß. Für diese Fälle sollte schriftlich eine Regelung festgelegt sein, nach der eine vorläufige Freigabe erfolgen kann. Zum Beispiel könnte für derartige Ausnahmesituationen der Projektleiter zur vorläufigen Freigabe ermächtigt werden.

  Selbstverständlich bleibt die Notwendigkeit unberührt, unverzüglich nachträglich eine endgültige Freigabe herbeizuführen.

- **Programmaufträge vom Fachbereich**

  Die Entwicklung neuer Programme und die Durchführung von Programmänderungen sollten, soweit diese nicht rein systembedingt sind, ausschließlich nach vorheriger schriftlicher Auftragserteilung erfolgen. Dabei sollte der Auftrag durch den Auftraggeber so weit spezifiziert werden, daß die fachliche Seite des Programms dadurch eindeutig festgelegt ist.

  Ausnahmen von dieser Regelung sollten ausdrücklich auf Programmänderungen beschränkt werden, von denen der fachliche Programminhalt nicht betroffen ist. In allen anderen Fällen sollte ausnahmslos ein schriftlicher Auftrag des Fachbereichs Voraussetzung der Organisations- und Programmierarbeiten sein.

- **Entwicklung von Programmen in einer Programmiergemeinschaft**

  Unter dem Gesichtspunkt der Datensicherheit ist die Entwicklung von Programmen in einer Programmiergemeinschaft ausdrücklich zu begrüßen. Die aus Sicherheitsgründen zu fordernde Trennung zwischen Programmierung und späterer Abwicklung ist hier in besonderem Umfang verwirklicht. Ein Mißbrauch wird daurch wesentlich erschwert.

  Die gewonnene Sicherheit kann allerdings dadurch aufgehoben werden, daß an den zentral entwickelten Programmen vor ihrem späteren Einsatz noch dezentrale Anpassungen vorgenommen werden. Auf diese Weise kann sogar der ursprüngliche Gewinn an Sicherheit in sein Gegenteil verkehrt werden, falls diese Anpassungsarbeiten nicht hinreichenden Kontrollen unterworfen sind.

  Der abschließende Freigabetest von Programmen, die in einer Programmiergemeinschaft entwickelt wurden, muß selbstverständlich bei den späteren Anwendern (Auftraggebern) der Programme liegen.

- **Maßnahmen bei dezentraler Abwicklung der ADV-Arbeiten**

  Werden bei ADV-Arbeiten durch dezentral eingesetzte Kleincomputer abgewickelt, so ist es vom Standpunkt der Datensicherheit sehr zu begrüßen, wenn die Entwicklung der dort zum Ablauf kommenden Programme zentral erfolgt. Fachaufsicht und Kontrolle sind bei dezentraler Programmentwicklung im allgemeinen nicht hinreichend gesichert. Die zentral entwickelten Programme sollten allerdings ohne jede Änderung dezentral eingesetzt werden.

  Die Zuständigkeit einer dezentralen Stelle erstreckt sich dann ausschließlich auf die Anwendung fertig vorgegebener Systeme. Die zentrale Programmierung und der Verzicht auf jegliche Änderung von Programmen durch Mitarbeiter der dezentralen Stelle sind für die Datensicherheit von großer Bedeutung.

Aus Gründen der Datensicherheit ist es außerdem unbedingt notwendig, die dezentralisierte Abwicklung der ADV-Arbeiten durch ergänzende organisatorische und technische Maßnahmen abzusichern. Der geringere Wert der eingesetzten ADV-Geräte darf keinesfalls dazu verleiten, die zur Datensicherung notwendigen technischen Maßnahmen oder die Maßnahmen der Struktur- und Ablauforganisation zu vernachlässigen.

b) Abwicklung von ADV-Programmen

— Funktionstrennung Programmierung/Maschinenbedienung

Die Funktionstrennung zwischen Programmierung und Maschinenbedienung ist Bestandteil des Sicherheitssystems und sollte ohne Einschränkung gelten. Maßnahmen, die diese Funktionstrennung im Einzelfall aufheben, müssen als sehr bedenklich bezeichnet werden. Sie sollten daher nicht zugelassen werden.

Auch bei Testarbeiten sollte die Aufgabe der Maschinenbedienung nicht auf Programmierer übertragen werden. Die Frage, ob es notwendig ist, daß neben den Maschinenbedienern auch Programmierer im Rechenzentrum anwesend sind, kann im Einzelfall unter Anlegung strenger Maßstäbe entschieden werden. Dazu sollte auch festgelegt werden, wer für eine derartige Entscheidung zuständig ist.

— Funktionstrennung Maschinenbedienung/Archivverwaltung

Eine Funktionstrennung zwischen Maschinenbedienung und Archivverwaltung ist aus Gründen der Sicherheit sehr zu empfehlen. Das Datenarchiv sollte den Maschinenbedienern keinesfalls direkt zugänglich sein. Die Maschinenbediener sollten vielmehr von einem Archivverwalter alle für die laufende Arbeit erforderlichen Bänder erhalten und diese nach Durchführung der Arbeit auch an den Archivverwalter zurückgeben.

— Verantwortlichkeit der Arbeitsvorbereitung

In einem Rechenzentrum wurden nach der Freigabe die Programme vom Programmierer aus der Testbibliothek in die Produktionsbibliothek überstellt. Die neuen Programme bzw. die geänderten Fassungen alter Programme standen damit direkt für Produktionsläufe zur Verfügung.

Die Arbeitsvorbereitung war in diesen Prozeß nicht eingeschaltet, obgleich bei ihr die letzte Verantwortung für die Ordnungsmäßigkeit des Einsatzes der Programme liegt. Entsprechend der Verantwortungsabgrenzung soll es aber gerade die Arbeitsvorbereitung sein, die nach Einsicht in die Freigabeunterlagen ein Programm in die Produktionsbibliothek übernimmt. Erst dadurch wird die Verantwortlichkeit der Arbeitsvorbereitung voll gesichert.

— Auswertung der Aufzeichnungen aus dem Rechenzentrum

Ein Protokoll der Meldungen des Bedienungsblattschreibers wird im allgemeinen erstellt, und die Maschinenbediener führen auch Protokoll über eventuelle besondere Ereignisse. Beide Protokolle werden regelmäßig aufbewahrt.

Wichtig ist es, darüber hinaus die Zuständigkeit für eine nachträgliche unabhängige Kontrolle und Auswertung dieser Aufzeichnungen festzulegen. Eine derartige Kontrolle, die sich auf stichprobenartig ausgewählte Zeiträume oder Sachverhalte beschränken könnte, ist unter dem Gesichtspunkt der Datensicherheit sehr zu empfehlen. Zuständig für Veranlassung und Durchführung der Kontrolle könnte der interne Datenschutzbeauftragte sein (oben D.1.a). Jedenfalls sollten diesem die Ergebnisse jeder Kontrolle zugeleitet werden.

3. Maßnahmen der Ablauforganisation

Eine besonders große Zahl einzelner Maßnahmen ist im Bereich der Ablauforganisation zu treffen. Als Grundlage gehört dazu die organisatorische Gestaltung der Arbeitsverfahren. Zu den Maßnahmen der Ablauforganisation zählen aber auch die Anweisungen, die organisatorische Entscheidungen für zukünftige Einzelfälle enthalten.

a) Schriftform

– Schriftliche Dienstanweisung

Zur Regelung des Ablaufs im ADV-Bereich und in den Fachabteilungen dient im allgemeinen eine Vielzahl von Anweisungen. Es ist für die Sicherheit aller Arbeiten von großer Bedeutung, daß jedem Mitarbeiter der Inhalt aller ihn betreffenden und jeweils gültigen Anweisungen ohne Zweifel bekannt ist. Erst dadurch erhalten die Anweisungen die erforderliche Verbindlichkeit.

In der Praxis konnten gerade hier deutliche Gefährdungen der Ablaufsicherheit festgestellt werden. Häufig wurden wichtige Anweisungen nur mündlich erteilt. In einem Fall wurden mehrere einander überschneidende Anweisungen zu unterschiedlichen Zeitpunkten herausgegeben, und den Mitarbeitern war anschließend nicht bekannt, welche Regelung für einen bestimmten Sachverhalt jeweils verbindlich war.

Es ist daher dringend zu empfehlen, alle wichtigen Vorschriften zu einer schriftlichen Dienstanweisung zusammenzufassen. Diese Dienstanweisung muß fortgeschrieben werden und jedem Mitarbeiter, soweit sein Arbeitsgebiet von ihr betroffen ist, bekannt sein.

– Schriftliche Aufträge der Arbeitsvorbereitung

Bestandteil des Sicherheitssystems bei der Verarbeitung personenbezogener Daten sollte es sein, daß die Maschinenbedienung bezüglich der durchzuführenden Arbeiten keine Freiheiten hat. Falls eine Arbeitsvorbereitung als eigene Organisationseinheit existiert, ist es dieser in jedem Falle möglich, die erforderlichen Aufträge schriftlich an die Maschinenbedienung zu geben. Gerade in eiligen Fällen empfiehlt sich sogar die schriftliche Auftragserteilung ganz besonders, um auf Irrtümer zurückzuführende Fehlarbeiten auszuschließen.

Es sollte daher ohne Ausnahme festgelegt werden, daß maschinelle Arbeiten mit personenbezogenen Daten nur auf Grund eines schriftlichen Auftrages durchgeführt werden dürfen.

– Programmdokumentation

Im Rahmen eines umfassenden Systems der Datensicherheit spielt die Programmdokumentation zweifellos eine nicht zu unterschätzende Rolle. Eine vollständige und aussagekräftige Programmdokumentation sollte wenigstens folgende Bestandteile enthalten:

- Programminhalt und Programmgliederung
- Anwendungsbereich
- Datenflußplan
- Programmablaufplan
- Schlüsselverzeichnis
- Datei- und Satzaufbau
- Ein- und Ausgabe
- Formulare, Listenbilder
- Programmliste
- Bedienungsanleitung
- Anweisung für Arbeitsvorbereitung und Nachbereitung
- Protokolle des abschließenden Anwendertests und der Freigabe

- Testdaten
- Name des verantwortlichen Programmierers

Nur bei logisch einfachen Programmen besonders geringen Umfanges sollte es zulässig sein, auf einzelne Bestandteile der vollständigen Programmdokumentation zu verzichten. Ein derartiger Verzicht setzt allerdings in jedem Falle voraus, daß dadurch Aussagekraft und Verständlichkeit der Programmdokumentation nicht eingeschränkt werden.

— Mitnahme von Taschen und Mänteln in den Maschinenraum

Ein Verbot von der Mitnahme von Taschen und Mänteln in den Maschinenraum existierte teilweise nicht, oder es war nur mündlich ausgesprochen worden.

Im Hinblick auf die Erfordernisse der Datensicherheit sollte dieses Verbot schriftlich festgelegt und in die Dienstanweisung aufgenommen werden.

— Überprüfung von Diensträumen, die geräumt und Dritten überlassen werden

Eine Stadtverwaltung hatte Diensträume, die aufgegeben und Dritten überlassen wurden, nicht hinreichend überprüft. Dies hatte zur Folge, daß in den Räumen Akten mit personenbezogenen Daten verblieben, die beim Abriß Dritten zugänglich wurden.

Der Vorgang gab Veranlassung, allgemein zu empfehlen, daß durch Dienstanweisung sichergestellt wird, daß sich in Dienstgebäuden oder einzelnen Diensträumen, die geräumt und Dritten überlassen werden, spätestens im Zeitpunkt der Übernahme keine Unterlagen mit personenbezogenen Daten mehr befinden. Die Dienstanweisung soll insbesondere folgende Verpflichtungen enthalten:

- Alle Räumlichkeiten sind vor der Überlassung eingehend zu besichtigen.
- Über den Verlauf und das Ergebnis der Besichtigung ist eine Niederschrift zu fertigen.
- Bis zur Feststellung der vollständigen Räumung sind alle beteiligten Stellen über jede Änderung des Verfahrensstandes zu unterrichten.

b) Sicherungsmaßnahmen für die Arbeit von Rechenzentren

— Vier-Augen-Prinzip im Maschinenraum

Aus Gründen der Datensicherheit sollten Rechenzentren hinreichender Größe personenbezogene Daten nur in Anwesenheit von wenigstens zwei Mitarbeitern verarbeiten dürfen (Vier-Augen-Prinzip). Personalengpässe während Krankheits- und Urlaubszeiten führen allerdings in Einzelfällen dazu, daß das Vier-Augen-Prinzip nicht vollständig eingehalten wird.

Im Hinblick auf die große Bedeutung für die Datensicherheit habe ich in allen geeigneten Fällen empfohlen, daß ein Betrieb des Maschinenraums mit nur einem Maschinenbediener ohne jede Ausnahme vermieden wird.

— closed-shop-Betrieb

Rechenzentren arbeiten im allgemeinen im closed-shop-Betrieb. Das bedeutet, daß nur solche Mitarbeiter Zutritt erhalten, deren Anwesenheit aus arbeitstechnischen Gründen erforderlich ist.

Wichtig ist, auch die zugelassenen Ausnahmefälle eindeutig zu regeln. Hier sollten sehr strenge Regeln gelten:

- Eine Ausnahme ist nur zulässig, wenn sie sich bei Anlegung strengster Maßstäbe als notwendig erweist.
- Es sollte schriftlich festgelegt werden, wer befugt ist zu entscheiden, daß ein derartiger Ausnahmefall vorliegt.

— Zutritt von Programmierern zum Maschinenraum

Programmierer und Systemprogrammierer sollten in der Regel nur eine beschränkte Zutrittsberechtigung zum Maschinenraum haben. Arbeitstechnisch gibt es keinen Grund, diesen Mitarbeitern einen unbeschränkten Zutritt zu gestatten. Es ist im Gegenteil sogar zu fordern, daß der Zutritt zum Maschinenraum auf wenige Sonderfälle eingeschränkt wird.

— Abwicklung von Arbeiten bei Anwesenheit von Besuchern im Maschinenraum

Falls Besucher mit Sondergenehmigung den Maschinenraum betreten, muß ohne jede Einschränkung sichergestellt sein, daß diese nicht unbefugt Kenntnis von personenbezogenen Daten erhalten können. Dies kann im Einzelfall dadurch geschehen, daß Zugang zu druckenden oder anzeigenden Geräten verhindert wird.

Falls eine derartige technische Maßnahme nicht möglich ist, sollte die Dienstanweisung bestimmen, daß Listen mit personenbezogenen Daten nicht gedruckt werden dürfen, während sich Besucher im Maschinenraum aufhalten.

c) Abwicklung von Test- und Echtläufen

— Verwendung anonymisierter Testdaten

Bei einigen datenverarbeitenden Stellen werden Programmtests in Einzelfällen mit echten Daten ohne deren Anonymisierung durchgeführt. Der Programmierer bedient sich dabei teilweise sogar der echten Daten der Produktionsdateien.

Ein derartiges Testverfahren bedeutet eine unnötige Gefährdung der Produktionsdateien, und der Programmierer erhält ohne Notwendigkeit Einblick in nicht anonymisierte Daten. Aus Sicherheitsgründen sollte ein anderes Testverfahren gewählt werden.

Keine Bedenken bestehen, aus den Produktionsdateien nach dem letzten oder nach einem früheren Änderungsstand durch Anonymisierung der Daten Testdateien abzuleiten. Diese Testdateien aus anonymisierten Daten können dem Programmierer ohne Einschränkung für Programmtests zur Verfügung stehen. Einwände aus der Sicht des Datenschutzes bestehen dann nicht mehr, und auch eine Gefährdung der Produktionsdateien durch Programmtests ist damit ausgeschlossen.

— Direktänderung von Programmen im Arbeitsspeicher

Bei Kontrollbesuchen stellte ich in zwei Fällen fest, daß Direktänderungen von Programmen im Arbeitsspeicher zugelassen wurden. Das bedeutet, daß freigegebene und im echten Betrieb eingesetzte Programme während ihres Ablaufs durch den zuständigen Programmierer im Arbeitsspeicher geändert werden durften.

Eine Änderung von freigegebenen Programmen, die im Echtbetrieb eingesetzt sind, durch Schreiben in den Arbeitsspeicher muß als außerordentlich bedenklich angesehen werden. Die Sicherheit der Verarbeitung wird damit aufgehoben. Es muß außerdem befürchtet werden, daß die zum Ablauf kommende Programmversion nicht dokumentiert wird.

Daher sollten Direktänderungen freigegebener Programme im Arbeitsspeicher ohne jede Ausnahme untersagt werden.

— Kennzeichnung von Arbeiten mit personenbezogenen Daten

In einem Hochschulrechenzentrum wird nach meinen Feststellungen mit der Möglichkeit gerechnet, daß ADV-Programme aus Forschung und Lehre mit personenbezogenen Daten arbeiten, ohne daß diese Bearbeitung personenbezogener Daten für das Hochschulrechenzentrum erkennbar ist. Die Programme laufen dann auch nicht unter dem erforderlichen organisatorischen Schutz.

Dem Hochschulrechenzentrum habe ich empfohlen, alle Benutzer zu verpflichten, Arbeiten mit personenbezogenen Daten deutlich zu kennzeichnen. Jeder Auftraggeber muß wissen, daß Arbeiten ohne diese Kennzeichnung bei ihrem Ablauf nicht hinreichend geschützt sind und daß der Auftraggeber bei nicht gekennzeichneten Arbeiten mit personenbezogenen Daten die volle Verantwortung für die Beeinträchtigung des Datenschutzes trägt.

d) Handhabung von Magnetbändern

— Räumliche Bereiche für Magnetbänder

Bei einigen datenverarbeitenden Stellen gibt es keine Festlegung, in welchen räumlichen Bereichen sich Magnetbänder befinden dürfen. Nach meinen Feststellungen befanden sich dann Magnetbänder nicht nur in den Bereichen Maschinenraum und Archiv. Magnetbänder mit personenbezogenen Daten lagen vielmehr auch in der Arbeitsvorbereitung und teilweise sogar in den Arbeitsräumen der Programmierer.

Aus Gründen der Datensicherung sollten die Bereiche, in denen sich Magnetbänder befinden dürfen, erheblich eingeschränkt werden.

Fachliche Gesichtspunkte stehen einer derartigen Beschränkung nicht entgegen. Sie würde die Möglichkeit der Abgangskontrolle und damit die Datensicherheit erhöhen.

— Buchführung über das Datenträgerarchiv

Eine aussagefähige Buchführung über das Datenträgerarchiv und die Bewegung der Magnetbänder ist wesentlicher Bestandteil der Datensicherung. Die Buchführung muß unter anderem die internen Bewegungen von Magnetbändern erkennen lassen und registrieren, welche Magnetbänder im Rahmen eines Datenträgeraustauschs die datenverarbeitende Stelle verlassen und wieder dorthin zurückkommen.

Bei Kontrollbesuchen habe ich im allgemeinen eine ausreichende Buchführung über das Datenträgerarchiv vorgefunden, so daß nur ergänzende Hinweise erforderlich waren. In einem Falle fand zwar eine regelmäßige Buchführung statt, aber es wurde nicht kontrolliert, ob die in den Archiven vorhandenen Magnetbänder mit den Angaben der Buchführung übereinstimmten.

Es ist selbstverständlich, daß die Übereinstimmung von Archivbestand und Buchführung durch einen entsprechenden Soll-Ist-Vergleich zu kontrollieren ist.

— Löschen von Magnetbändern

Auf die Notwendigkeit, Magnetbänder vor der Rücksendung im Rahmen eines Datenträgeraustauschs zu löschen, hatte ich bereits in meinem ersten Tätigkeitsbericht (D.2.d) hingewiesen. Inzwischen hatte ich in einer Reihe von Fällen Veranlassung, diesen Hinweis aufzugreifen und zu ergänzen.

Häufig wird die Datensicherheit dadurch gefährdet, daß zum Versand bestimmte Magnetbänder vor dem Beschreiben nicht gelöscht werden. Damit besteht die Gefahr, daß Reste einer aus der früheren Verwendung des Magnetbandes stammenden Datei, die durch die für den Versand vorgesehene Datei nicht überschrieben wurden, dem Empfänger zusätzlich bekanntgegeben werden.

Einzelne datenverarbeitende Stellen glauben, dieser Gefahr dadurch begegnen zu können, daß sie ihre Magnetbänder den einzelnen Programmen fest zuordnen, wodurch nur solche Daten zusätzlich bekanntgegeben werden können, die bereits zu einem früheren Zeitpunkt demselben Empfänger als Datei bekanntgegeben wurden.

Sehr fraglich erscheint es allerdings, ob die getroffene Regelung lückenlos eingehalten werden kann. Außerdem wird bei diesem Verfahren jedenfalls für die wegen unterlassener Löschung zusätzlich auf dem Magnetband aufgezeichneten Daten ein unnötiges Transportrisiko übernommen.

Um alle angesprochenen Risiken zu beseitigen, habe ich folgende Maßnahmen empfohlen:

- Magnetbänder, auf denen Daten bekanntgegeben werden, sollten so gelöscht werden, daß sie außer den zur Bekanntgabe vorgesehenen Daten keine weiteren personenbezogenen Daten enthalten.
- Magnetbänder, die eine datenverarbeitende Stelle im Rahmen des Datenträgeraustauschs erhalten hat und die sie nach Auswertung der Daten zurückgibt, sollten vor der Rücksendung gelöscht werden.
- Die datenverarbeitenden Stellen sollten auf ihre Partner einwirken, damit auch diese entsprechend verfahren.

— Postversand von Magnetbändern mit Wertangabe

Jeder Transport von Magnetbändern mit personenbezogenen Daten ist mit einem Risiko verbunden. Dieses Risiko sollte nach Möglichkeit ausgeschlossen werden.

Falls eine Versendung über die Deutsche Bundespost erfolgt, kann durch Wertangabe eine besondere Sicherung erreicht werden. Sendungen mit Wertangabe werden gesichert aufbewahrt, und ihre interne Weitergabe erfolgt in kontrollierter Form. Falls maschinenlesbare Datenträger mit personenbezogenen Daten auf dem Postweg transportiert werden, sollte deren Einlieferung daher als Wertbrief oder Wertpaket erfolgen.

e) Vernichtung von Unterlagen

— Vernichtung von Datenträgern

Anfragen von Behörden und eigene Feststellungen gaben im Berichtszeitraum mehrfach Veranlassung, zur Frage der Vernichtung von Datenträgern Stellung zu nehmen.

- Datenschutzrechtliche Bedenken gegen eine Vernichtung von Altpapier mit personenbezogenen Daten im Fremdauftrag entfallen nicht schon dann, wenn die Firmen sich bereiterklären, die Bestimmungen des Datenschutzgesetzes Nordrhein-Westfalen zu beachten.

  Werden Datenträger aus Dateien (§ 1 Abs. 2 Satz 1 DSG NW) vernichtet, handelt es sich datenschutzrechtlich um Löschung von Daten und damit um eine Phase der Datenverarbeitung (§ 2 Abs. 2 Nr. 4, § 1 Abs. 1 Nr. 1 DSG NW). Die Vernichtung entsprechenden Altpapiers durch Privatunternehmen ist damit Auftragsdatenverarbeitung, bei der der Auftraggeber den Vorschriften des Datenschutzgesetzes voll unterworfen bleibt (§ 7 Abs. 1 Satz 1 DSG NW). Auch ist dieser verpflichtet sicherzustellen, daß der Auftragnehmer die Bestimmungen des Datenschutzgesetzes Nordrhein-Westfalen beachtet und sich der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft (§ 7 Abs. 1 Satz 2 DSG NW).

  Wie die Beachtung der Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen sichergestellt werden kann, muß im Hinblick auf die besonderen Verhältnisse des Einzelfalles entschieden werden. In jedem Falle ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technisch-organisatorischen Sicherungsmaßnahmen (§ 6 DSG NW und die Anlage zu dieser Vorschrift) sorgfältig auszuwählen. Seine Pflichten — insbesondere Art und Weise der Vernichtung und technisch-organisatorische Sicherungsmaßnahmen sowie die Unterwerfungserklärung nach § 7 Abs. 1 Satz 2 DSG NW — müssen vertraglich klar und eindeutig festgelegt werden. So ist eine Vernichtung erst dann gewährleistet, wenn es auf keine Weise mehr möglich ist, den Inhalt aus dem vernichteten Schriftgut zu rekonstruieren. In dem Vertrag muß ein Weisungs- und Kontrollrecht des Auftraggebers vereinbart werden. Außerdem ist vorzusehen, daß die bei dem Auftragnehmer bei der Datenverarbeitung beschäftigten Personen auf das Datengeheimnis nach § 5 Abs. 2 Satz 1 DSG NW zu verpflichten sind.

- Auch soweit es sich lediglich um Akten oder sonstige Unterlagen mit personenbezogenen Daten handelt, auf die die materiellen Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen keine Anwendung finden, trifft die speichernde Stelle eine ähnliche besondere Sorgfaltspflicht.

  Nach Artikel 4 Abs. 2 der Landesverfassung hat jeder Anspruch auf Schutz seiner personenbezogenen Daten. Öffentliche Stellen haben es nicht nur zu unterlassen, solche Daten ohne gesetzliche Grundlage oder Einwilligung des Betroffenen weiterzugeben; sie müssen auch die technischen und organisatorischen Maßnahmen treffen, die zum Schutz der Daten gegen unbefugten Zugriff Dritter erforderlich sind.

  Auch insoweit sollten mit Auftragnehmern ausreichende Sicherungsmaßnahmen vertraglich vereinbart und ihre Einhaltung fortlaufend kontrolliert werden.

- Nicht mehr benötigte Unterlagen mit sensiblen Daten sollten grundsätzlich nicht durch private Unternehmen, sondern durch eine öffentliche Stelle vernichtet werden. Sofern aus besonderen Gründen eine Vernichtung durch eine nichtöffentliche Stelle für erforderlich gehalten wird, ist die Vernichtung durch Mitarbeiter der speichernden Stelle ständig zu überwachen. Stichprobenartige Kontrollen genügen nicht.

— Rückgabe von Unterlagen

Eine Behörde hatte an die Herstellerfirma ihrer Datenverarbeitungsanlage zur Fehlerermittlung und -analyse Arbeitsspeicherauszüge abgegeben. Es ist im allgemeinen davon auszugehen, daß diese Arbeitsspeicherauszüge auch personenbezogene Daten enthalten können. Selbstverständlich ist daher, daß eine Weitergabe von Arbeitsspeicherauszügen nur als letztes Mittel zur Unterstützung der Fehlersuche zulässig ist.

Ich bin um Stellungnahme gebeten worden, wie die abschließende Vernichtung der Unterlagen sichergestellt werden sollte. Von der Herstellerfirma war zunächst lediglich zugesagt worden, sämtliche Unterlagen nach Abschluß der Fehlerermittlung selbst zu vernichten.

Diese Regelung bedeutet aber ein Sicherheitsrisiko und ist unbefriedigend. Ich habe daher empfohlen zu vereinbaren, daß die Herstellerfirma verpflichtet wird, sämtliche ihr überlassenen Arbeitsspeicherauszüge nach Abschluß der Fehlerermittlung an die speichernde Stelle zur Vernichtung zurückzugeben.

f) Fernmündliche Auskunftsersuchen

Nach § 36 Abs. 2 Satz 1 DSG NW dürfen Meldebehörden Namen, akademische Grade und Anschriften eines oder mehrerer vom Empfänger bezeichneter Betroffener an Personen oder andere nicht-öffentliche Stellen übermitteln. Da diese Vorschrift die Auskunftserteilung von keinen weiteren Voraussetzungen abhängig macht und es abweichend von § 13 Abs. 1 Satz 1 DSG NW weder auf ein berechtigtes Interesse des Empfängers noch auf schutzwürdige Belange des Betroffenen ankommt, ist in diesen Fällen eine Feststellung der Identität des Empfängers nicht erforderlich. Nach dem derzeitigen Erkenntnisstand habe ich deshalb gegen eine fernmündliche oder mündliche Auskunftserteilung nach § 36 Abs. 2 Satz 1 DSG NW ohne Feststellung der Identität des Auskunftsuchenden keine Bedenken.

Dagegen müssen bei der Übermittlung von Namen, akademischen Graden und Anschriften einer Vielzahl Betroffener nach § 36 Abs. 2 Satz 2 DSG NW die in meinem ersten Tätigkeitsbericht (D.2.e) dargelegten Grundsätze beachtet werden. Das gleiche gilt für die Übermittlung anderer personenbezogener Daten an nicht-öffentliche Stellen nach § 13 Abs. 1 Satz 1 DSG NW wie auch an öffentliche Stellen nach § 11 Abs. 1 Satz 1 DSG NW.

4. Technische Maßnahmen

Die Notwendigkeit technischer Maßnahmen ist für den Außenstehenden am leichtesten erkennbar. Dies hat zur Folge, daß deren Verwirklichung oft auch im Zentrum der Diskussion über die Datensicherheit steht. Technik allein schafft aber keine Sicherheit. Technische Maßnahmen können daher immer nur Hilfsmittel darstellen. Die Datensicherheit hängt entscheidend von deren Einbettung in einen organisatorischen Rahmen ab.

a) Gestaltung von Sicherheitsbereichen

— Aufteilung des Sicherheitsbereichs

Das Beratungsersuchen einer kommunalen Datenverarbeitungszentrale gab Veranlassung, zur Aufteilung des Sicherheitsbereichs Stellung zu nehmen. Bei einem Rechenzentrum hinreichender Größe sollte der Sicherheitsbereich nach Möglichkeit in drei Zonen unterteilt sein, die sich nach den Zutrittsberechtigungen unterscheiden lassen:

a) Berechtigung zum Betreten des Sicherheitsbereichs
b) Berechtigung zum Betreten des Maschinenraums (innerhalb des Sicherheitsbereichs)
c) Zusätzliche Berechtigung zum Betreten des Datenträgerarchivs

Hierbei bedeutet a) die geringste und c) die umfassendste Berechtigung.

Zur Diskussion stand außerdem die Frage der Zuordnung des Papierlagers. Falls es sich dabei nicht um ein Lager für den täglichen Bedarf, sondern um ein solches für den Gesamtbedarf handelt, sollte dieses nicht zum Sicherheitsbereich gehören, und es sollte auch keine Verbindungstür besitzen, die unmittelbar in den Maschinenraum führt.

— Arbeitsplatz für Techniker der Herstellerfirma

Bei dem Kontrollbesuch in einem größeren Rechenzentrum wurde festgestellt, daß die Techniker der Herstellerfirma ihren Arbeitsplatz im Maschinenraum hatten. Dort befanden sich auch Schreibtische und Schränke, die den Technikern fest zugeordnet waren.

Es wurde empfohlen, für die Techniker einen vom Maschinenraum abgetrennten Raum vorzusehen und in diesem auch die Schreibtische und Schränke der Techniker aufzustellen. Die kontrollierte Stelle bestätigte, daß eine derartige Regelung bereits geplant sei.

— Isolierte Aufstellung einer Datenverarbeitungsanlage für die Verarbeitung personenbezogener Daten

In einem Hochschulrechenzentrum war vorgesehen, für die Bearbeitung der Verwaltungsaufgaben eine zusätzliche Datenverarbeitungsanlage (Verwaltungsrechner) zu installieren. Auf dem neuen Verwaltungsrechner sollten möglichst alle Programme mit personenbezogenen Daten ablaufen.

Es wurde empfohlen, diesen Verwaltungsrechner so zu installieren, daß ein Zugang für Unbefugte unmöglich ist. Besonders günstig wäre zweifellos die Installation in einem getrennten Raum. Falls dies nicht realisierbar ist, sollte der Standort der neuen Anlage jedenfalls deutlich von der übrigen Rechenzentrumsfläche abgesetzt sein, und es sollte eine eindeutige Markierung geben (z.B. gespannte Kordel), die erkennen läßt, daß ein Betreten der unmittelbaren Umgebung des Verwaltungsrechners für Unbefugte nicht zulässig ist.

— Lagerung von Magnetbändern im Maschinenraum

Bei einer datenverarbeitenden Stelle war es wegen der räumlichen Enge nicht möglich, Magnetbänder ausschließlich im Archiv zu lagern. Der Maschinenraum wurde

daher als ebenfalls gesicherter Bereich zusätzlich für die Lagerung von Magnetbändern benutzt. Gelagert wurden dort nicht nur Bänder, die voraussichtlich im Laufe des Tages zur Verarbeitung kommen sollten, sondern auch reine Archivbänder. Sämtliche im Maschinenraum lagernden Magnetbänder waren dort frei zugänglich.

Grundsätzlich sollte ein räumlich getrenntes Magnetbandarchiv angestrebt werden. Solange dies wegen Platzmangels nicht verwirklicht werden kann, sollten die im Rechenzentrum lagernden Archivbänder in verschließbaren Schränken aufbewahrt werden. Zugang zu diesen Schränken sollten die Archivverwalter und nicht die Maschinenbediener haben.

Als vorläufige Lösung sollte daher das Rechenzentrum mit verschließbaren Schränken für Magnetbänder ausgestattet werden, deren Schlüssel bei den Archivverwaltern liegen.

— **Regale im Auslagerungsarchiv**

Als zusätzlichen Schutz gegen die Vernichtung archivierter Daten hatte eine von mir kontrollierte Stelle ein Auslagerungsarchiv in einem gesicherten Raum eines anderen Gebäudes eingerichtet. Bei diesem Raum handelte es sich um den Tresorraum einer anderen Organisationseinheit, die auch dessen Schlüssel hatte.

Die ausgelagerten Magnetbänder lagen in dem Tresorraum ohne jeden zusätzlichen Schutz offen auf Regalen.

Ich habe dringend empfohlen, dies zu ändern und in dem Tresorraum einen verschließbaren Stahlschrank aufzustellen, dessen Schlüssel bei der datenverarbeitenden Stelle liegt. Die ausgelagerten Bänder sind dann ausschließlich in diesem Schrank aufzubewahren.

b) Technische Einrichtungen

— **Zugangskontrollsystem**

Die Installation eines maschinellen Zugangskontrollsystems ist heute bei größeren Rechenzentren üblich oder wird jedenfalls von diesen angestrebt. Ein derartiges Zugangskontrollsystem sollte den Zugang zu den einzelnen Zonen des Sicherheitsbereichs kontrollieren. Es ist damit ohne Schwierigkeiten möglich, den Zugang entsprechend unterschiedlichen Zugangsberechtigungen für die einzelnen Zonen des Sicherheitsbereichs zu gewähren.

— **Einbruchmeldeanlage**

Außerhalb der Dienstzeit sollten der Maschinenraum und diejenigen Räume, in denen Datenträger mit personenbezogenen Daten lagern, zusätzlich gesichert werden. In die Sicherung sollte neben dem eigentlichen Datenarchiv auch ein eventuelles Auslagerungsarchiv einbezogen werden.

Um unbefugten Zugang zu personenbezogenen Daten zu verhindern, empfiehlt es sich, den Maschinenraum, das Datenarchiv und das Auslagerungsarchiv durch Einbruchmeldeanlagen zu sichern, falls diese Räume nicht bereits durch geeignete Maßnahmen gesichert sind.

— **Türsicherung**

Je nach räumlicher Anordnung gibt es Türen, die zwar ständig geschlossen gehalten werden sollen, deren Überwachung aber besonders notwendig erscheint. Insbesondere handelt es sich dabei um die Türen zum Maschinenraum und zum Datenträgerarchiv.

In einigen Fällen habe ich empfohlen, Anzeigen vorzusehen, die bei geöffneter Tür ansprechen.

– Fenstersicherung

Fenster zum Maschinenraum sollen grundsätzlich geschlossen bleiben. Aus Sicherheitsgründen werden sie heute bei größeren Rechenzentren in Panzerglas ausgeführt. In zwei Fällen gaben Kontrollbesuche Veranlassung , auch auf die Frage der Fenstersicherung einzugehen.

Bei einer datenverarbeitenden Stelle war es noch möglich, die Fenster des Maschinenraums zu öffnen. Diese Tatsache wurde bei Schwierigkeiten mit der Klimaanlage als angenehm empfunden. Das damit verbundene Sicherheitsrisiko sollte allerdings nicht in Kauf genommen werden. Ich habe daher empfohlen, durch entsprechende Maßnahmen sicherzustellen, daß die Fenster generell geschlossen bleiben.

Bei einer anderen datenverarbeitenden Stelle waren die Fenster in Dreifachverglasung angefertigt. Ein Öffnen war technisch ausgeschlossen. Die Fenster waren daher auch im Notfall als Fluchtwege nicht benutzbar. Um einen zusätzlichen Fluchtweg zu schaffen, war ein Fenster des Maschinenraums mit einer Vorrichtung zum Öffnen versehen worden. Ich habe empfohlen sicherzustellen, daß dieses Fenster jedenfalls nicht unbemerkt geöffnet werden oder versehentlich offenbleiben kann. Zu diesem Zweck sollte eine Anzeige eingebaut werden, die bei geöffnetem Fenster anspricht.

– Schlüsselnummern auf Archivschränken

Es ist heute üblich, in die Schlösser von Schreibtischen und Schränken die zugehörigen Schlüsselnummern äußerlich sichtbar einzuprägen. Bei Verlust eines Schlüssels wird dadurch die Ersatzbeschaffung wesentlich erleichtert. Mißbrauch soll ausgeschlossen werden, indem derartige Schlüssel nicht auf jede einfache Anfrage von der Lieferfirma der Büromöbel herausgegeben werden.

Die Sicherheit eines Schrankes, in dessen Schloß die Schlüsselnummer eingeprägt ist, muß dennoch als eingeschränkt angesehen werden. Falls in einem solchen Schrank maschinenlesbare Datenträger mit personenbezogenen Daten lagern, sind daher zusätzliche Sicherungsmaßnahmen geboten. Eine mögliche Maßnahme könnte darin bestehen, daß der Schrank in einem Raum steht, der normalerweise abgeschlossen und nur wenigen Mitarbeitern zugänglich ist.

Falls keine ausreichenden zusätzlichen Sicherungen möglich sind, sollten in derartigen Fällen die in die Schlösser eingeprägten Nummern unlesbar gemacht werden.

5. Organisatorisch-technische Maßnahmen

Zu den organisatorisch-technischen Maßnahmen sollen Maßnahmen gerechnet werden, die zwar organisatorischer Natur sind, die aber mit Hilfe der Technik verwirklicht werden. Verschiedene Maßnahmen, deren Bedeutung für die Datensicherung ganz erheblich ist, sind hier einzuordnen.

a) Sicherung von Datenstationen

– Paßwortschutz

Der Schutz von Datenstationen durch die Vergabe von Paßworten ist eine allgemein übliche Sicherungsmaßnahme. Dadurch können insbesondere die Anforderungen der Nr. 4 (Benutzerkontrolle), 5 (Zugriffskontrolle) und 7 (Eingabekontrolle) der Anlage zu § 6 Abs. 1 Satz 1 DSG NW ganz oder teilweise erfüllt werden.

Feststellungen bei verschiedenen datenverarbeitenden Stellen gaben Veranlassung, auf folgendes hinzuweisen:

- Das vom Benutzer eingetastete Paßwort sollte auf dem Bildschirm nicht erscheinen, damit es nicht von einem unbefugten Dritten zur Kenntnis genommen werden kann. Die Anzeige auf dem Bildschirm sollte unterdrückt werden.
- Die Sicherheit wächst mit der Länge des verwendeten Paßwortes. Paßworte unter 6 Stellen sollten möglichst nicht verwandt werden. Aus Gründen der Datensicherheit wäre es zu begrüßen, wenn wenigstens achtstellige Paßworte zum Einsatz kämen.
- Häufige Änderung der Paßworte erhöht die Sicherheit beträchtlich. Es ist nicht ververtretbar, Paßworte über Jahre nicht zu ändern. Die Gültigkeitsdauer eines Paßwortes sollte im Normalfall einige Monate nicht überschreiten. In besonderen Fällen kann ein wesentlich schnellerer Wechsel von Paßworten angemessen sein.

— Sicherung gespeicherter Paßworte

Zur Logik eines einfachen Paßwortverfahrens gehört es, daß die den Benutzern zugeteilten Paßworte zusätzlich in der Datenverarbeitungsanlage gespeichert und damit für die Identifikation der Benutzer verfügbar sind. Es ist dann erforderlich, die in der Anlage gespeicherten Paßworte vor unberechtigter Kenntnisnahme absolut zu schützen, um deren mißbräuchliche Benutzung zu verhindern. Der Schutz sollte so umfassend sein, daß er auch gegenüber Mitarbeitern mit ADV-Kenntnissen und Zugang zur Datenverarbeitungsanlage wirksam ist.

Ein einfaches und außerordentlich wirksames Mittel zum Schutz von Paßworten liegt in der Einwegverschlüsselung (vgl. Datenschutz-Berater Nr. 6 vom 15. 6. 1980 S. 1 — 4). Bei diesem Verfahren wird nicht das Paßwort selbst, sondern ein verschlüsseltes Paßwort gespeichert. Die Identifikation des Benutzers erfolgt, indem dessen Paßwort bei jeder Verwendung erneut in der Datenverarbeitungsanlage verschlüsselt und mit dem gespeicherten verschlüsselten Paßwort verglichen wird. Bei der Einwegverschlüsselung muß allerdings ein solches Verschlüsselungsverfahren gewählt werden, mit dem es bei Kenntnis des Verschlüsselungsalgorithmus und des (in der Datenverarbeitungsanlage gespeicherten) verschlüsselten Paßwortes nicht auf einfache Weise möglich ist, auf das Paßwort rückzuschließen.

Die Einwegverschlüsselung bietet ein einfach anwendbares Verfahren zur Absicherung vergebener Paßworte gegen deren mißbräuchliche Benutzung. Ich habe daher empfohlen, dieses Verfahren anzuwenden, sobald ein Paßwortschutz verwirklicht wird.

— Zuordnung einzelner Datenstationen zu bestimmten Funktionen

Die Zugriffskontrolle nach Nr. 5 der Anlage zu § 6 Abs. 1 Satz 1 DSG NW sollte nicht nur über einen Paßwortschutz verwirklicht werden. Es sollte vielmehr auch von der Möglichkeit Gebrauch gemacht werden, einzelne Datenstationen nur für gewisse Funktionen zuzulassen. Zugriffsbeschränkungen wären dann zusätzlich an die Geräte und nicht nur an die Personen gebunden.

Ich habe empfohlen, von der Möglichkeit Gebrauch zu machen, die Funktionen einzelner Datenstationen oder wenigstens die Funktionen von Gruppen von Datenstationen so zu beschränken, daß die noch verbleibende Zugriffsmöglichkeit den dienstlichen Erfordernissen entspricht.

— Berechtigung von Datenstationen in der Arbeitsvorbereitung

Es ist heute üblich, die Arbeitsvorbereitung eines Rechenzentrums durch Einsatz von Datenstationen zu unterstützen. Diese Datenstationen sollten allerdings in ihrer Nutzungsmöglichkeit den Aufgaben der Arbeitsvorbereitung angepaßt und in ihrer Funktion entsprechend eingeschränkt sein.

Bei einem Kontrollbesuch wurde festgestellt, daß in der Arbeitsvorbereitung installierte Datenstationen in ihrer Nutzungsmöglichkeit nicht eingeschränkt waren. Sie be-

saßen unter anderem die Berechtigung zur interaktiven Programmentwicklung. Aufgabengebiet und Zuständigkeit der Arbeitsvorbereitung machen aber eine derartige Berechtigung nicht erforderlich. Wegen der aus Sicherheitsgründen anzustrebenden Funktionstrennung ist es sogar sehr bedenklich, wenn Datenstationen der Arbeitsvorbereitung auch Möglichkeiten zum Erstellen und Ändern von Programmen bieten.

Es wurde daher empfohlen, die Datenstationen der Arbeitsvorbereitung möglichst umgehend in ihrer Berechtigung auf die zu erledigenden Arbeiten einzuschränken. Auf keinen Fall sollte von dort eine Möglichkeit zur interaktiven Programmentwicklung bestehen.

b) Sicherung von Dateien

— Verwendung privilegierter Transaktionen

Bei einem überprüften Informationssystem waren die Anforderungen der Zugriffskontrolle entsprechend Nr. 5 der Anlage zu § 6 Abs. 1 Satz 1 DSG NW durch einen Transaktionsschutz realisiert. Transaktionen, die außerhalb des ADV-Bereichs verfügbar waren, wurden ausschließlich entsprechend der Berechtigung der Benutzer zugelassen.

Allerdings gab es darüber hinaus Transaktionen, mit denen beliebige Dateien gelesen und sogar verändert werden konnten. Derartige privilegierte Transaktionen standen nur dem ADV-Bereich zur Verfügung und wurden aus technischen Gründen für erforderlich gehalten, um in Notfällen Dateifehler beseitigen zu können.

Zur Erhöhung der Sicherheit wurde empfohlen, verbindlich festzulegen, daß die Verwendung der privilegierten Transaktionen in jedem Einzelfall ausdrücklich vom Leiter des ADV-Bereichs oder von dessen Vertreter im Amt genehmigt werden muß.

— Interaktiver Programmtest

In einem Hochschulrechenzentrum ist die Datenverarbeitungsanlage über eine große Anzahl festgeschalteter Leitungen mit Datenstationen oder Steckdosen für den Anschluß von Datenstationen innerhalb des Hochschulbereichs verbunden. Darüber hinaus kann die Anlage über 5 Wählleitungen aus dem Fernsprechnetz der Deutschen Bundespost angesprochen werden. Von sämtlichen Anschlüssen besteht jederzeit die Möglichkeit, Programmtests interaktiv durchzuführen.

Auf derselben Datenverarbeitungsanlage werden auch Arbeiten mit personenbezogenen Daten abgewickelt. Es handelt sich dabei um Arbeiten aus den Bereichen Verwaltung und Bibliothek. Außerdem liegen auf der Datenverarbeitungsanlage sämtliche personenbezogenen Arbeiten aus den Bereichen Forschung und Lehre.

Da die Abwicklung interaktiver Programmtests nicht auf bestimmte Tageszeiten beschränkt ist, können gleichzeitig mit diesen auf derselben Anlage Programme mit personenbezogenen Daten zum Ablauf kommen.

Wegen der weitgehenden Eingriffsmöglichkeiten, die eine interaktiv arbeitende Datenstation besitzt, und wegen der Unmöglichkeit einer Kontrolle der Benutzer habe ich Bedenken gegen diese Form der Arbeitsabwicklung geäußert. Im wesentlichen sah ich zwei Wege, um meine Bedenken auszuräumen:

— In erster Linie ist anzustreben, daß interaktive Programmtests nicht auf derselben Anlage durchgeführt werden, auf der auch personenbezogene Daten verarbeitet werden. Ich wurde darüber informiert, daß beabsichtigt sei, baldmöglichst eine zusätzliche Datenverarbeitungsanlage für Verwaltungsaufgaben (Verwaltungsrechner) anzuschaffen. Daraufhin habe ich empfohlen, diesen neuen Verwaltungsrechner so zu dimensionieren, daß seine Kapazität für sämtliche Arbeiten aus den Bereichen Verwaltung und Bibliothek ausreichend ist und daß er auch die Arbeiten der Forschung und Lehre, soweit sie personenbezogene Daten benutzen, übernehmen kann.

– Soweit und solange die Durchführung der Arbeiten auf verschiedenen Datenverarbeitungsanlagen nicht möglich ist, habe ich eine zeitliche Trennung empfohlen. Dazu müßten allerdings zu gewissen Zeiten die interaktiven Programmtests völlig unterbunden werden.

– Verwendung von Dateietiketten

Bei Kontrollbesuchen konnte festgestellt werden, daß Dateietiketten grundsätzlich verwendet und ausgewertet werden. Lediglich in Sonderfällen wird auf deren Verwendung oder Auswertung verzichtet.

Ein Verzicht auf Dateietiketten oder deren Auswertung beeinträchtigt die Verarbeitungssicherheit. Es sollte daher ohne Einschränkung sichergestellt werden, daß sämtliche Magnetbänder mit Dateietiketten versehen und diese auch ohne Ausnahme ausgewertet werden.

c) Sicherung der Verarbeitung

– Logband bei Direktänderungen

Mehrfach wurde die Ansicht vertreten, eine Eingabekontrolle (Nr. 7 der Anlage zu § 6 Abs. 1 Satz 1 DSG NW) sei besonders schwer zu verwirklichen. Zweifellos ist es zutreffend, daß bei arbeitenden ADV-Verfahren und abgeschlossener Programmentwicklung eine Erweiterung von Programmen und Dateien im Hinblick auf die Forderungen der Eingabekontrolle nur mit Schwierigkeiten zu verwirklichen ist. Zur kurzfristigen Lösung bieten sich hier vor allem organisatorische Maßnahmen an.

Langfristig ist damit zu rechnen, daß in zunehmendem Umfang Transaktionen zugelassen werden, die unmittelbare Änderungen von Bestandsdateien zur Folge haben. Fragen der Datensicherung gewinnen dann erhöhte Bedeutung. Diese Tatsache sollte bei der Planung und Neukonzeption ganzer Verfahren von Anfang an Berücksichtigung finden.

Unter diesem Gesichtspunkt wurde von mir auf die Möglichkeit hingewiesen, sämtliche Dateiänderungen mit Verursacher und Zeitpunkt auf einem Logband zu archivieren. Die Logbänder der einzelnen Arbeitstage könnten nach Dateien und nach Sortierkriterien der Datensätze innerhalb der Dateien sortiert und anschließend gemischt werden. Auf diese Weise entstünde eine Historie aller Datensätze, die jede Änderung eines Datensatzes mit Verursacher und Zeitpunkt der Änderung enthält.

Bei Neuentwicklungen könnte dieses Konzept eine leicht realisierbare Verbesserung der Datensicherheit ermöglichen (vgl. Pütter in ÖVD 1973, S. 454 – 471 und 1976, S. 76 – 80).

– Sperren und Löschen von Datenfeldern

In § 17 DSG NW ist geregelt, unter welchen Umständen Daten zu sperren oder zu löschen sind. Es ist nicht auszuschließen, daß in einem konkreten Fall lediglich einzelne Datenfelder eines Datensatzes betroffen sind. Von einer datenverarbeitenden Stelle wurde ich darauf hingewiesen, daß man dort unter diesen Umständen Schwierigkeiten sieht, der Forderung des Gesetzes nachzukommen.

Auf die Durchführung einer vom Gesetz geforderten Maßnahme kann aber nicht mit der Begründung verzichtet werden, die Programme sähen eine solche Möglichkeit nicht vor. Die datenverarbeitende Stelle muß daher sicherstellen, daß Forderungen nach Sperrung oder Löschung von Daten erforderlichenfalls auch realisiert werden können. Das Fehlen der entsprechenden Programmeigenschaften darf keinen Hinderungsgrund darstellen.

– Übermittlung von Daten durch Datenfernverarbeitung

Ein Beratungsersuchen gab mir Veranlassung, darauf hinzuweisen, daß zur Verringerung des Transportrisikos und damit zur Verbesserung des Datenschutzes bei der Übermittlung von Daten die Datenfernverarbeitung dem Datenträgeraustausch vorzuziehen ist.

E. Sonstige allgemeine Fragen des Datenschutzes

1. Datenerhebung

Zahlreiche Eingaben befassen sich mit der Datenerhebung. Die Erkenntnisse im Berichtszeitraum insbesondere in den Bereichen des Schulwesens, des Verkehrswesens, des Sozialwesens und des Personenstandswesens zeigen, daß nach wie vor zu viele Daten erhoben werden. Der Appell der Datenschutzbeauftragten des Bundes und der Länder, die Datenerhebung auf das unerläßliche Maß zu beschränken (D.1.d meines ersten Tätigkeitsberichts), hat deshalb auch heute noch aktuelle Bedeutung. Die Behörden bleiben aufgefordert, alle Fragebögen, Antragsvordrucke und sonstige Unterlagen für die Datenerhebung daraufhin zu überprüfen, ob auch tatsächlich alle verlangten Daten für die Aufgabe der Behörde konkret erforderlich sind.

Sofern nicht die Erhebung bestimmter Daten in einer Rechtsvorschrift ausdrücklich vorgesehen ist, dürfen nur solche Angaben verlangt werden, deren Kenntnis zur Aufgabenerfüllung unbedingt notwendig ist. Eine Erhebung auf der Grundlage der Freiwilligkeit ist nur dann gerechtfertigt, wenn die Kenntnis der Daten für die Aufgabenerfüllung zumindest dienlich ist.

Sofern die Daten bei dem Betroffenen erhoben werden, ist er nach § 10 Abs. 2 DSG NW auf die der Datenerhebung zugrunde liegende Rechtsvorschrift oder auf die Freiwilligkeit hinzuweisen. Gegen diese Hinweispflicht wird noch in zahlreichen Fällen verstoßen. Oft fehlt ein solcher Hinweis überhaupt; in manchen Fällen ist er unrichtig.

Zweck der Vorschrift ist, den Betroffenen über die Rechtslage aufzuklären, damit er selbst prüfen kann, ob und in welchem Umfang er zur Mitwirkung verpflichtet ist. Dabei ist zu berücksichtigen, daß auch freiwillige Aussagen und Angaben zur Erlangung einer bestimmten Verwaltungsentscheidung oft auf Grund einer Rechtsvorschrift erhoben werden. In diesen Fällen ist neben der Rechtsvorschrift auch auf die Freiwilligkeit oder die Rechtsfolgen einer unterbliebenen Mitwirkung hinzuweisen. Dabei sollte dem Betroffenen zugleich die vorgesehene Nutzung erläutert werden. Nur auf Grund einer solchen umfassenden Unterrichtung vor der Erhebung ist der Betroffene in der Lage, sich frei zu entscheiden, ob er die von ihm erfragten Angaben machen will.

Im übrigen halte ich an meiner Auffassung fest, daß die Hinweispflicht nach § 10 Abs. 2 DSG NW auch dann besteht, wenn die zu erhebenden Daten nicht in einer Datei gespeichert werden sollen. Der in der Stellungnahme der Landesregierung zu meinem ersten Tätigkeitsbericht (S. 15) vertretenen Auffassung, daß diese Vorschrift nur in dem durch § 1 Abs. 2 und 3 DSG NW festgelegten Rahmen herangezogen werden könne, vermag ich mich nicht anzuschließen. § 10 Abs. 2 DSG NW reicht, wie auch die Entstehungsgeschichte der entsprechenden Vorschrift des § 9 Abs. 2 BDSG bestätigt, über den Anwendungsbereich der anderen materiellen Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen hinaus.

2. Datengeheimnis

Zahlreiche Anfragen öffentlicher Stellen betrafen die Abgrenzung des Personenkreises, der nach § 5 Abs. 1 DSG NW das Datengeheimnis zu beachten hat und deshalb nach § 5 Abs. 2 Satz 1 DSG NW zu verpflichten ist.

Der Kreis der Personen, die „bei der Datenverarbeitung beschäftigt" sind, ist nach dem Wortlaut des § 5 Abs. 1 DSG NW nicht eindeutig zu bestimmen. Deshalb muß zur Auslegung der Zweck der Vorschrift herangezogen werden. Das Datengeheimnis soll den Betroffenen vor unbefugter Nutzung und Weitergabe seiner in einer Datei gespeicherten 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 Zugang zu in einer Datei gespeicherten Daten haben.

Hierbei kann es entgegen der Auffassung des Innenministers nicht darauf ankommen, ob diese Personen im Zusammenhang mit dem Verarbeitungsprozeß mit geschützten Daten in Berührung kommen. Werden 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 oder aus einer inhaltlich mit ihr übereinstimmenden Unterlage übermittelt werden. Das gleiche muß für das Verbot der unbefugten Weitergabe und sonstigen Nutzung nach § 5 Abs. 1 DSG NW gelten.

Soweit Ratsmitglieder Zugang zu personenbezogenen Daten haben, die in einer Datei gespeichert sind, gilt somit auch für sie die Vorschrift über das Datengeheimnis mit der Folge, daß sie nach § 5 Abs. 2 Satz 1 DSG NW zu verpflichten sind. Entsprechendes muß für sachkundige Bürger im Sinne des § 42 Abs. 1 und 3 der Gemeindeordnung, für die nicht dem Rat und der Verwaltung angehörenden stimmberechtigten und beratenden Mitglieder des Jugendwohlfahrtsausschusses, für Vertreter der Kirchen und der Lehrerschaft im Schulausschuß nach § 12 Abs. 2 des Schulverwaltungsgesetzes sowie für Mitglieder der Bezirksvertretungen und Ortsvorsteher gelten.

Zwar sind Ratsmitglieder nach § 30 Abs. 2 in Verbindung mit § 22 Abs. 1 der Gemeindeordnung verpflichtet, über die ihnen in ihrer Tätigkeit bekanntgewordenen Angelegenheiten, deren Geheimhaltung besonders vorgeschrieben ist, Verschwiegenheit zu bewahren. Diese Verschwiegenheitspflicht der Ratsmitglieder — wie auch die Pflicht der Beamten zur Amtsverschwiegenheit nach § 64 Abs. 1 Satz 1 des Landesbeamtengesetzes — schließt eine Verpflichtung zur Wahrung des Datengeheimnisses aber weder aus, noch macht sie sie entbehrlich.

Die Vorschrift über das Datengeheimnis kann auch eine Verpflichtung von Personen gebieten, die nicht der eigenen Verwaltung angehören. So habe ich die Ansicht vertreten, daß zu diesem Kreis auch Techniker von Herstellerfirmen gehören, die die zur Verfügung gestellte Hardware zu warten oder instandzusetzen haben und dabei personenbezogene Daten einsehen können.

Keinesfalls kann damit — wie in einem Falle vorgetragen — eine Abwertung des Datengeheimnisses verbunden sein. Die Verpflichtung nach § 5 Abs. 2 DSG NW hat keine konstitutive Wirkung. Sie soll auf gesetzliche Pflichten hinweisen und einen Verbotsirrtum ausschließen. Sie will das Risiko eines unzulässigen Umgangs mit personenbezogenen Daten zu Lasten betroffener Bürger vermindern und der Gefahr einer mißbräuchlichen Nutzung vorbeugen. Um dies zu erreichen, muß im Interesse des Bürgers überall dort auf das Datengeheimnis hingewiesen werden, wo die Möglichkeit seiner Verletzung besteht. Je stärker die Beachtung des Datengeheimnisses in das Bewußtsein all derer rückt, die mit personenbezogenen Daten anderer in Berührung kommen, desto geringer wird die Zahl der Verstöße sein, und dies insbesondere im Bereich des sogenannten menschlichen Versagens.

Soweit private Dienstleistungsunternehmen für öffentliche Stellen Datenverarbeitung im Auftrag betreiben, stellte sich die Frage, ob eine bereits vorgenommene Verpflichtung ihrer Bediensteten nach dem Bundesdatenschutzgesetz eine weitere Verpflichtung nach dem Datenschutzgesetz Nordrhein-Westfalen entbehrlich mache.

Unabhängig von einer bereits vorgenommenen Verpflichtung auf das Datengeheimnis nach § 5 Abs. 2 Satz 1 BDSG ist eine Verpflichtung dieser Personen nach § 5 Abs. 2 Satz 1 DSG NW zwingend erforderlich, da für den Datenschutz bei den öffentlichen Stellen des Landesbereichs, soweit sie nicht als Sozialleistungsträger tätig werden, nicht das Bundesdatenschutzgesetz, sondern das Datenschutzgesetz Nordrhein-Westfalen gilt. Dem steht nicht entgegen, daß die Vorschriften über das Datengeheimnis in den beiden Gesetzen fast wörtlich übereinstimmen.

3. Auftragsdatenverarbeitung

Öffentliche Stellen des Landesbereichs, die Daten in ihrem Auftrag durch andere verarbeiten lassen, haben häufig noch Schwierigkeiten, die ihnen durch § 7 Abs. 1 DSG NW auferlegten Pflichten voll zu erfüllen.

Das gilt insbesondere hinsichtlich der gesetzlichen Verpflichtung **sicherzustellen**, daß der Auftragnehmer die Bestimmungen des Datenschutzgesetzes Nordrhein-Westfalen beachtet (§ 7 Abs. 1 Satz 2 DSG NW). Naturgemäß kann nicht abstrakt beurteilt werden, wie die Beachtung der Vorschriften des Datenschutzgesetzes sichergestellt werden kann. Dies muß unter Berücksichtigung der besonderen Verhältnisse des Einzelfalls entschieden werden. Ich habe hierzu in mehreren Fällen Hinweise gegeben (vgl. oben D.3.e).

In Stellungnahmen zu vertraglichen Vereinbarungen über eine beabsichtigte Datenverarbeitung im Auftrag bin ich wiederholt auch auf die Verpflichtung eingegangen sicherzustellen, daß sich das Dienstleistungsunternehmen als Auftragnehmer meiner Kontrolle unterwirft (§ 7 Abs. 1 Satz 2 DSG NW). Soweit Aufträge an bundesländerübergreifende Unternehmen erteilt werden, habe ich empfohlen, in dem Vertrag die Unterwerfung unter die Kontrolle des Landesbeauftragten für den Datenschutz mit dem Zusatz zu vereinbaren, daß dieser auch einen anderen Landesbeauftragten oder den Bundesbeauftragten mit der Wahrnehmung der Kontrolle beauftragen kann.

Ein überregionales Unternehmen, das auch Daten im Auftrag öffentlicher Stellen des Landesbereichs verarbeitet, hat die Ansicht vertreten, daß bei zunehmender Nutzung der Möglichkeiten des Rechnerverbundes die Durchführung der in § 7 Abs. 1 Satz 2 DSG NW vorgesehenen Kontrolle durch den Landesbeauftragten für den Datenschutz praktisch nicht durchführbar sei. Die Abgabe einer Unterwerfungserklärung entsprechend der gesetzlichen Bestimmung des Datenschutzgesetzes Nordrhein-Westfalen stieße deshalb ins Leere und erübrige sich damit. Man werde deshalb die in Nordrhein-Westfalen betroffenen Auftraggeber bitten, von der Forderung auf Unterwerfung unter die Kontrolle des Landesbeauftragten bis zur Klärung der vom Bundesverband der Deutschen Industrie an die Aufsichtsbehörde des Landes Nordrhein-Westfalen herangetragenen Frage abzusehen.

Ich bin dem mit Nachdruck entgegengetreten. Die Absicht des Unternehmens läuft darauf hinaus, die Auftraggeber zu einem Verstoß gegen geltendes Datenschutzrecht aufzufordern. Weigern sich Auftragnehmer, die nach § 7 Abs. 1 Satz 2 DSG NW erforderliche Unterwerfungserklärung abzugeben, so ist Datenverarbeitung im Auftrag öffentlicher Stellen des Landesbereichs bei ihnen nicht zulässig.

Die Regierungspräsidenten Arnsberg und Köln als Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bei der Prüfung von Dienstleistungsunternehmen der Datenverarbeitung gemäß §§ 30/40 BDSG wiederholt feststellen müssen, daß Auftraggeber aus dem öffentlichen Bereich ihren Verpflichtungen nach § 7 Abs. 1 DSG NW nicht in dem erforderlichen Umfange nachgekommen sind. Der Innenminister hat dies zum Anlaß genommen, im Erlaßwege darauf hinzuwirken, daß bei festgestellten Verstößen die jeweils zuständige Aufsichtsbehörde (Dienst-, Fach-, Kommunal- oder Rechtsaufsichtsbehörde) eingeschaltet wird.

4. Veröffentlichung nach § 15 DSG NW und Auskunft nach § 16 DSG NW

Die datenverarbeitenden Stellen haben nach § 15 Abs. 1 Satz 1 DSG NW in Verbindung mit der Verordnung über die **Veröffentlichung** der Angaben über gespeicherte personenbezogene Daten (Datenschutzveröffentlichungsverordnung Nordrhein-Westfalen — DSVeröffVO NW —) die erforderlichen Angaben unverzüglich nach der ersten Einspeicherung zum nächsten Veröffentlichungstermin — März, Juni, September oder Dezember — bekanntzugeben. Die Veröffentlichung im März ist mit einem Sachregister zu versehen.

Aus der Kommunalverwaltung ist die Frage aufgeworfen worden, ob bei den Folgeveröffentlichungen neben den eingetretenen Veränderungen stets auch die unverändert gebliebenen Angaben über die Dateien bekanntzugeben sind. Ich habe dies verneint. 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. Zu diesem Zweck genügt es, nach der ersten Veröffentlichung über gespeicherte personenbezogene Daten nur die Veränderungen bekanntzugeben. Es ist nicht erforderlich, bei Veränderungen jeweils die fortgeschriebene Übersicht der Angaben über die Dateien vollständig zu veröffentlichen. Aus dem gleichen Grunde ist auch nicht erforderlich bekanntzugeben, daß keine Veränderungen eingetreten sind. Durch die regelmäßigen Veröffentlichungen und die Bekanntgabe eines Sachregisters ist gewährleistet, daß sich der Betroffene Einblick in die Veröffentlichungen des aktuellen Standes der Dateien verschaffen kann, zumal ihm auf Antrag die bisherigen Bekanntmachungen zugänglich zu machen sind (§ 15 Abs. 1 Satz 2 DSG NW).

In einem anderen Fall habe ich darauf hingewiesen, daß jährlich im März ein Sachregister auch dann zu veröffentlichen ist, wenn zu diesem Termin selbst keine Veränderungen der Angaben über die Dateien bekanntzugeben sind. Zwar geht § 3 Abs. 2 DSVeröffVO NW nach seinem Wortlaut davon aus, daß das Sachregister im März jeweils einer Veröffentlichung nach § 15 Abs. 1 DSG NW beigefügt wird. Der Absicht, dem Bürger dadurch den Zugang zu den Veröffentlichungen des aktuellen Standes der Dateien zu ermöglichen, würde es jedoch widersprechen, ein Sachregister nur im Falle veränderter Angaben über die Dateien zu veröffentlichen.

Die Anfrage eines Oberkreisdirektors betraf die Abgrenzung zwischen § 15 Abs. 2 Nr. 1 (Ausnahme von der Veröffentlichungspflicht für bestimmte Behörden) und § 16 Abs. 3 Nr. 4 DSG NW (Verbot bestimmter Auskünfte). § 16 Abs. 3 Nr. 4 DSG NW verbietet es der speichernden Stelle, dem Betroffenen **Auskunft** über die Übermittlung personenbezogener Daten an die in § 15 Abs. 2 Nr. 1 DSG NW und in § 12 Abs. 2 Nr. 1 BDSG genannten Behörden aus dem Bereich der staatlichen Sicherheit, der Strafverfolgung und der Finanzverwaltung zu erteilen. Damit ist sichergestellt, daß die Zielsetzung des § 16 Abs. 2 DSG NW nicht umgangen werden kann, nach der diese Behörden von einer Auskunftsverpflichtung ausgenommen sind.

Gegenstand des § 16 DSG NW sind zur Person des einzelnen Betroffenen gespeicherte (Individual-) Daten. Demgegenüber beziehen sich die Vorschriften über die Veröffentlichung in § 15 Abs. 1 Nr. 4 und 5 DSG NW lediglich auf die **Art** der **regelmäßig** zu übermittelnden Daten. Die Pflicht, die Art der regelmäßig zu übermittelnden Daten bekanntzugeben, wird durch das in § 16 Abs. 3 Nr. 4 DSG NW ausgesprochene Verbot nicht berührt.

Es ist zwar nicht zu verkennen, daß der Bürger durch die Veröffentlichung nach § 15 Abs. 1 DSG NW allgemein von einem Datenfluß an Behörden aus dem Bereich der staatlichen Sicherheit, der Strafverfolgung und der Finanzverwaltung erfährt. Kenntnis davon, ob und welche Daten konkret zu seiner Person bei den in § 15 Abs. 2 Nr. 1 DSG NW genannten Behörden gespeichert sind, erhält er damit aber nicht.

Die Veröffentlichung nach § 15 Abs. 1 DSG NW umfaßt daher auch die Art der regelmäßig an die in § 15 Abs. 2 Nr. 1 DSG NW genannten Behörden zu übermittelnden Daten. Auskunftsersuchen Betroffener, die sich auf die Übermittlung personenbezogener Daten an die in § 15 Abs. 2 Nr. 1 DSG NW und in § 12 Abs. 2 Nr. 1 BDSG genannten Behörden beziehen, sind dagegen nach § 16 Abs. 3 Nr. 4 DSG NW abzulehnen.

Ein Bürger hat in einer Eingabe die Auffassung vertreten, daß er berechtigt sei, von einer bestimmten der Aufsicht des Landes Nordrhein-Westfalen unterstehenden juristischen Person des öffentlichen Rechts, die am Wettbewerb teilnimmt (§ 18 Nr. 2 DSG NW), Auskunft über sämtliche ihn betreffende Einzelangaben (auch interner Art) in verständlicher Form zu verlangen.

Der Auskunftsanspruch (§ 22 Abs. 2 DSG NW) beschränkt sich auf Angaben über persönliche oder sachliche Verhältnisse des Betroffenen (§ 2 Abs. 1 DSG NW). Hierzu gehören auch Angaben über die Herkunft der Daten, soweit sie als Teil des Datensatzes des Betroffenen mitgespeichert sind. Betriebsinterne Daten wie Bearbeitungshinweise und Personalnummer des zuständigen Sachbearbeiters sind keine solche Angaben, da sie über den Betroffenen nichts aussagen. Ein Anspruch auf Auskunft über diese Daten besteht somit nicht.

Nach § 22 Abs. 2 Satz 4 DSG NW ist die Auskunft grundsätzlich schriftlich zu erteilen. Auf welche Weise die schriftliche Auskunft erteilt wird, ist ohne Bedeutung. Sie kann auch aus einem Computer-Auszug bestehen. Allerdings muß der Auszug so abgefaßt sein, daß der Betroffene den Inhalt ohne Vorkenntnisse versteht. Er darf keine Angaben enthalten, die für den Betroffenen unverständlich sind. Dies gilt auch dann, wenn diese Angaben keine personenbezogene Daten sind. Soweit nicht auf eine verschlüsselte Angabe der Daten verzichtet wird, sind diese ausreichend zu erläutern. Ich habe die speichernde Stelle gebeten, diese Rechtslage im Interesse des auskunftsuchenden Bürgers künftig bei der Auskunfterteilung zu berücksichtigen.

Auf Grund einer weiteren Bürgereingabe habe ich zur Frage der Auskunft in solchen Fällen Stellung genommen, bei denen die gespeicherten Daten Einzelangaben über die Verhältnisse mehrerer Betroffener enthalten. Ich habe nochmals klargestellt, daß bei Daten mit Doppelbezug das Auskunftsrechts nach § 16 DSG NW grundsätzlich von jedem der Betroffenen geltend gemacht werden kann (vgl. oben C.6.).

5. Grenzüberschreitender Datenverkehr

Mit der Verabschiedung der **Europarat-Konvention** und der **OECD-Leitlinien** sind die Bemühungen um die Harmonisierung des europäischen Datenschutzrechts im Berichtszeitraum ein Stück weitergekommen.

Am 17. September 1980 hat der Ministerrat des Europarats das „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten" beschlossen. Es ist das Ergebnis mehrjähriger Erörterungen in einem Expertenausschuß des Europarats unter intensiver Beteiligung der Regierungen der einzelnen europäischen Länder. Das Übereinkommen ist am 28. Januar 1981 durch Vertreter der Bundesregierung unterzeichnet worden. Zur Vorbereitung des Ratifizierungsverfahrens hat der Bundesminister des Innern die Unterlagen den Regierungen der Bundesländer zugeleitet.

Am 23. September 1980 hat der Rat der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD)„Leitlinien für den Schutz der Privatsphäre und den grenzüberschreitenden Verkehr personenbezogener Daten" verabschiedet. Diesen Leitlinien dürfte vor allem auch Bedeutung für die Datenschutzpraxis multinationaler Unternehmen zukommen.

Für die Auswirkungen der beiden Übereinkommen wird es wesentlich darauf ankommen, mit welcher Intensität die Mitgliedsländer bestrebt sein werden, ihre nationale Gesetzgebung nunmehr den auf europäischer Ebene festgelegten Anforderungen anzupassen.

Die Frage, welche Stelle für die Bundesrepublik Deutschland als hilfeleistende Behörde im Sinne der Europarat-Konvention benannt werden soll (D.5. meines ersten Tätigkeitsberichts), ist nach wie vor offen. Die Datenschutzbeauftragten der Länder und des Bundes haben übereinstimmend empfohlen, alle Datenschutz-Kontrollinstanzen für den öffentlichen und den privaten Bereich und darüber hinaus zusätzlich — aus Gründen der Vereinfachung für ausländische Stellen — eine weitere Stelle als „Briefkasten" zu benennen. Nach den Vorstellungen der Datenschutzbeauftragten könnte diese Funktion der Bundesbeauftragte für den Datenschutz wahrnehmen.

Angesichts einer rasanten technischen Entwicklung auf dem Gebiet der Mikroelektronik und der Nachrichtenübermittlung sollte der Beitrag, den Europarat-Konvention und OECD-Leitlinien auf dem Wege zu mehr Datenschutz bei Informationsflüssen im staatenübergreifenden Bereich leisten können, nicht unterschätzt werden. Gleichwohl bleibt aufmerksam zu beobachten und abzuwarten, ob die bisherigen Initiativen genügen. Dies gilt insbesondere im Hinblick auf Tendenzen, Datenverarbeitung — etwa zur gleichmäßigen Auslastung von Rechenzentren — vermehrt ins Ausland zu verlagern.

F. Stand und weiterer Ausbau des Datenschutzes

Eine systematische Überprüfung der gesamten Verwaltung auf Mängel bei dem Umgang mit personenbezogenen Daten ist nur langfristig möglich. Bei der Größe der nordrhein-westfälischen Verwaltung und der im Verhältnis hierzu geringen Zahl der Mitarbeiter des Landesbeauftragten für den Datenschutz wird sie niemals flächendeckend sein können. Umso mehr kommt es darauf an, daß von den im Einzelfall durchgeführten Kontrollen eine Signalwirkung ausgeht. Inwieweit diese zu Verbesserungen des Datenschutzes bei anderen Stellen führt, läßt sich allerdings nur schwer abschätzen. Ein Urteil darüber, in welchem Umfang die Anforderungen des Datenschutzes in der Verwaltung bereits verwirklicht sind, ist noch nicht möglich.

In meinem ersten Tätigkeitsbericht hatte ich auf Grund bisheriger Erkenntnisse mehrere Änderungen des Datenschutzgesetzes Nordrhein-Westfalen vorgeschlagen. Die Erfahrungen im Berichtszeitraum haben die Notwendigkeit dieser Änderungen bestätigt. Ich halte deshalb an den Vorschlägen fest und werde meine Überlegungen auch in die Diskussion über die Novellierung des Bundesdatenschutzgesetzes einbringen.

Düsseldorf, den 31. März 1981

Dr. Weyer

Anlage
(zu C.22.a)

Grundsätze für den Datenschutz bei den Neuen Medien (insbesondere bei Bildschirmtext und Kabelfernsehen)

Beschluß der 7. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Berlin am 11. Dezember 1980

Übersicht

Vorbemerkung

Die nachstehenden Grundsätze für den Datenschutz bei den Neuen Medien sollen sicherstellen, daß die anlaufenden Erprobungen und die ihnen zugrundeliegenden Vorschriften den Datenschutz von vornherein berücksichtigen und dieser dem Einsatz neuer Technologien nicht nachfolgt.

Die Grundsätze können dem Stand der Vorhaben und der technischen Entwicklung entsprechend nicht abschließend sein.

1 Informationssammlung über Teilnehmer

1.1 Bei der Einführung Neuer Medien ist der Datenschutz sicherzustellen. Dies gilt auch für die Versuchsphase. Bereits hierfür sollten gesetzliche Regelungen getroffen werden.

1.2 Personenbezogene Benutzerdaten dürfen nur erhoben, gespeichert oder übermittelt werden, soweit ihre Verarbeitung für den Betrieb unumgänglich ist und ohne sie eine der gesetzlich zugelassenen Kommunikationsformen der Neuen Medien nicht durchgeführt werden kann.

1.3 Der Schutz der in den Neuen Medien anfallenden personenbezogenen Teilnehmerdaten kann nicht auf deren Verarbeitung in Dateien beschränkt werden.

1.4 Sofern bei bestimmten Diensten eine unmittelbare Teilnehmer-Anbieter-Kommunikation vorgesehen ist, dürfen Daten nur in dem Umfang festgehalten und übermittelt werden, wie dies zur Durchführung des jeweiligen Dienstes erforderlich und aufgrund der einschlägigen gesetzlichen Regelung zulässig ist.

1.5 Gebühren und Entgelte sind in anonymer Form zu berechnen und abzurechnen, soweit eine individualisierbare Registrierung von einzelnen Kommunikationsvorgängen zur Abwicklung von Vertragsverhältnissen nicht erforderlich ist. Sollte eine zusätzliche Kontrolle erforderlich werden, so könnte beim Benutzer eine Zähleinrichtung installiert werden.

2 Bedeutung des Versuchsstadiums (Pilotprojekte)

2.1 Bereits in der Versuchsphase ist ein möglichst wirksamer Datenschutz sicherzustellen, da diese Phase die spätere Nutzung der Neuen Medien prägt.

2.2 In der Versuchsphase ist zu prüfen, ob weitere Datenschutzregelungen auf dem Gebiet der Neuen Medien nötig sind oder ob vorhandene Vorschriften modifiziert werden müssen.

2.3 Im Rahmen wissenschaftlicher Begleituntersuchungen ist dafür zu sorgen, daß auch die Datenschutzfragen besonders geprüft werden.

2.4 Im Rahmen einer wissenschaftlichen Begleituntersuchung ist der Zugriff auf gespeicherte Datenbestände nur gestattet, sofern diese Daten anonymisiert worden sind. Darüber hinausgehende Daten dürfen nur von den Teilnehmern direkt erfragt werden.

Die Datenverarbeitung sollte in allen Phasen nur mit Einwilligung des Teilnehmers erfolgen (vgl. dazu Ziff. 3).

3 Die Bedeutung der „Einwilligung" bei der Speicherung von Teilnehmerdaten

3.1 Die Speicherung von Teilnehmerdaten in einer Form, die die Erstellung individueller Persönlichkeitsprofile gestattet, ist zu verbieten. Darüber hinaus kann in einzelnen Diensten die Speicherung besonders sensibler Daten aus dem „unantastbaren Bereich privater Lebensgestaltung" (vgl. BVerfGE 27, 1, 7; s. a. § 27 Abs. 3 Satz 3 BDSG) grundsätzlich verboten werden. Eine Einwilligung des Teilnehmers hebt das Verbot nicht auf.

3.2 Im übrigen ist eine Speicherung von Teilnehmerdaten erlaubt,

a) wenn eine gesetzliche Regelung dies zuläßt;

b) wenn der Teilnehmer seine Einwilligung gibt.

Diese Einwilligung ist nur wirksam, wenn der Teilnehmer zuvor sorgfältig über ihre Konsequenzen aufgeklärt worden ist (informed consent). Dies gilt auch für den Abschluß von Verträgen.

4 Rückkanal und sonstige technische Vorkehrungen, über die Äußerungen der Teilnehmer dem System gegenüber kundgegeben werden können

4.1 Nutzungsmöglichkeiten des Rückkanals und aller sonstigen technischen

Vorkehrungen, über die Äußerungen der Teilnehmer dem System gegenüber kundgetan werden können, sollen nach Möglichkeit gesetzlich geregelt werden. Soweit Teilnehmerdaten gespeichert werden können, dürfen sie nur zu dem Zweck verwertet werden, zu dem sie offenbart wurden.

4.2 Persönlichkeitsprofile der Teilnehmer dürfen anhand der in der Betriebszentrale anlaufenden Kommunikationsdaten nicht erstellt werden. Dies gilt für jede Betriebszentrale, unabhängig von der angewendeten Technologie.

4.3 Abstimmungen und Wahlen über den Rückkanal dürfen nicht durchgeführt werden.

5 Medienprivileg

5.1 Das Verhältnis des Medienprivilegs zu den Neuen Medien bedarf insgesamt einer eingehenden Untersuchung.

5.2 Dabei muß insbesondere geprüft werden,

- ob die einzelnen Neuen Medien als Presse bzw. Rundfunk anzusehen sind oder ob es sich um Medien sui generis handelt,
- in welchen Fällen nach geltendem Recht personenbezogene Daten ausschließlich zu publizistischen Zwecken verarbeitet werden,
- ob der Geltungsbereich des Medienprivilegs im Hinblick auf die für die Benutzer bestehenden Gefahren sachgerecht geregelt ist,
- falls dies bejaht wird:

  ob der Geltungsbereich zur Klarstellung gesetzlich geregelt werden soll,
- falls dies verneint wird:

  inwieweit der Geltungsbereich neu geregelt werden sollte.

Schließlich bedarf besonderer Erörterung die Gefahr, daß in Medienarchiven gespeicherte, personenbezogene Daten in die Speicherzentralen eingegeben werden und unter Berufung auf das Medienprivileg (§ 1 Abs. 3 BDSG und entsprechende Regelungen in den Ländergesetzen) frei zugänglich gemacht werden. Unter diesem Gesichtspunkt verdienen auch die im Urteil des Bundesverfassungsgerichts vom 5. Juni 1973 — 1 BvR 536/72 — (BVerfGE 35, S. 202 ff. (219 ff.) „Lebach") aufgestellten Grundsätze zum Schutze der Persönlichkeit vor dem Zugriff der Öffentlichkeit besondere Berücksichtigung.

6 Fernmeldegeheimnis und Neue Medien

6.1 Im gesamten Netzbereich werden die zentralen Einrichtungen der Neuen Medien ebenso wie die Übertragungswege vom Fernmeldegeheimnis im Sinne von Art. 10 GG umfaßt, sofern es sich dabei um juristische Personen des öffentlichen Rechts handelt.

6.2 Folgt man der Auffassung, daß die zentralen Einrichtungen der Neuen Medien keine Fernmeldeanlagen sind, ist ein dem Fernmeldegeheimnis vergleichbares Amtsgeheimnis für den Nutzungsbereich — unter Umständen in Verfassungsrang — zu schaffen.

6.3 Die Einblicknahme in und die Übermittlung von personenbezogenen Daten aus Speichereinrichtungen einer Bildschirmtext- bzw. Kabelfernsehzentrale sind nur aufgrund gesetzlicher Regelungen unter engen, genau bestimmten Voraussetzungen zulässig. Unter Datenschutzgesichtspunkten ist es bedenklich, die Regelungen des Gesetzes zu Art. 10 GG uneingeschränkt anzuwenden.

6.4 Für die in den zentralen Einrichtungen der Neuen Medien beschäftigten Bediensteten ist ein Zeugnisverweigerungsrecht und für alle dort gespeicherten Daten ein Beschlagnahmeverbot (vgl. § 97 StPO) zu verlangen.

7 Datenschutzkontrolle und Datensicherung

7.1 Die Kontrolle des Datenschutzes bei Neuen Medien sollte Aufgabe der Datenschutzbeauftragten des Bundes und der Länder sein.

7.2 Beim Anschluß von EDV-Einrichtungen durch Teilnehmer sind hinreichende technische und organisatorische Maßnahmen zu fordern, sowohl hardware- als auch softwaremäßig, z. B. Schlüsselschalter, Paßwortroutinen usw.